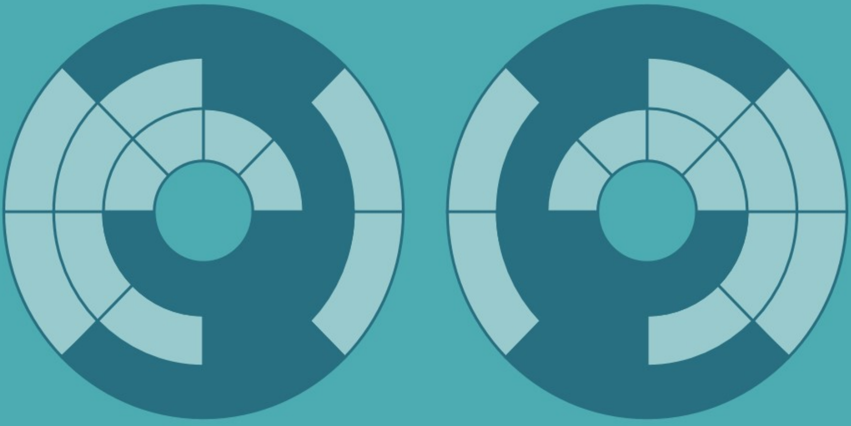
Applied and Numerical Harmonic Analysis

Stochastic Models, Information Theory, and Lie Groups

Volume 2

Analytic Methods and Modern Applications



Gregory S. Chirikjian

Birkhäuser

Birkhäuser

Applied and Numerical Harmonic Analysis

Gregory S. Chirikjian

Stochastic Models, Information Theory, and Lie Groups, Volume 2

Analytic Methods and Modern Applications

Birkhäuser

Gregory S. Chirikjian
Department of Mechanical Engineering
The Johns Hopkins University
Baltimore, MD 21218-2682
USA
gregc@jhu.edu

ISBN 978-0-8176-4943-2 e-ISBN 978-0-8176-4944-9
DOI 10.1007/978-0-8176-4944-9
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2011941792

Mathematics Subject Classification (2010): 22E60, 53Bxx, 53C65, 58A15, 58J65, 60D05, 60H10, 70G45, 82C31, 94A15, 94A17

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.birkhauser-science.com)

To my family

ANHA Series Preface

The *Applied and Numerical Harmonic Analysis (ANHA)* book series aims to provide the engineering, mathematical, and scientific communities with significant developments in harmonic analysis, ranging from abstract harmonic analysis to basic applications. The title of the series reflects the importance of applications and numerical implementation, but richness and relevance of applications and implementation depend fundamentally on the structure and depth of theoretical underpinnings. Thus, from our point of view, the interleaving of theory and applications and their creative symbiotic evolution is axiomatic.

Harmonic analysis is a wellspring of ideas and applicability that has flourished, developed, and deepened over time within many disciplines and by means of creative cross-fertilization with diverse areas. The intricate and fundamental relationship between harmonic analysis and fields such as signal processing, partial differential equations (PDEs), and image processing is reflected in our state-of-the-art *ANHA* series.

Our vision of modern harmonic analysis includes mathematical areas such as wavelet theory, Banach algebras, classical Fourier analysis, time-frequency analysis, and fractal geometry, as well as the diverse topics that impinge on them.

For example, wavelet theory can be considered an appropriate tool to deal with some basic problems in digital signal processing, speech and image processing, geophysics, pattern recognition, biomedical engineering, and turbulence. These areas implement the latest technology from sampling methods on surfaces to fast algorithms and computer vision methods. The underlying mathematics of wavelet theory depends not only on classical Fourier analysis, but also on ideas from abstract harmonic analysis, including von Neumann algebras and the affine group. This leads to a study of the Heisenberg group and its relationship to Gabor systems, and of the metaplectic group for a meaningful interaction of signal decomposition methods. The unifying influence of wavelet theory in the aforementioned topics illustrates the justification for providing a means for centralizing and disseminating information from the broader, but still focused, area of harmonic analysis. This will be a key role of *ANHA*. We intend to publish with the scope and interaction that such a host of issues demands.

Along with our commitment to publish mathematically significant works at the frontiers of harmonic analysis, we have a comparably strong commitment to publish major advances in the following applicable topics in which harmonic analysis plays a substantial role:

Antenna theory
Biomedical signal processing
Digital signal processing
Fast algorithms
Gabor theory and applications
Image processing
Numerical partial differential equations
Prediction theory
Radar applications
Sampling theory
Spectral estimation
Speech processing
Time-frequency and time-scale analysis
Wavelet theory

The above point of view for the *ANHA* book series is inspired by the history of Fourier analysis itself, whose tentacles reach into so many fields.

In the last two centuries Fourier analysis has had a major impact on the development of mathematics, on the understanding of many engineering and scientific phenomena, and on the solution of some of the most important problems in mathematics and the sciences. Historically, Fourier series were developed in the analysis of some of the classical PDEs of mathematical physics; these series were used to solve such equations. In order to understand Fourier series and the kinds of solutions they could represent, some of the most basic notions of analysis were defined, e.g., the concept of "function." Since the coefficients of Fourier series are integrals, it is no surprise that Riemann integrals were conceived to deal with uniqueness properties of trigonometric series. Cantor's set theory was also developed because of such uniqueness questions.

A basic problem in Fourier analysis is to show how complicated phenomena, such as sound waves, can be described in terms of elementary harmonics. There are two aspects of this problem: first, to find, or even define properly, the harmonics or spectrum of a given phenomenon, e.g., the spectroscopy problem in optics; second, to determine which phenomena can be constructed from given classes of harmonics, as done, for example, by the mechanical synthesizers in tidal analysis.

Fourier analysis is also the natural setting for many other problems in engineering, mathematics, and the sciences. For example, Wiener's Tauberian theorem in Fourier analysis not only characterizes the behavior of the prime numbers, but also provides the proper notion of spectrum for phenomena such as white light; this latter process leads to the Fourier analysis associated with correlation functions in filtering and prediction problems, and these problems, in turn, deal naturally with Hardy spaces in the theory of complex variables.

Nowadays, some of the theory of PDEs has given way to the study of Fourier integral operators. Problems in antenna theory are studied in terms of unimodular trigonometric polynomials. Applications of Fourier analysis abound in signal processing, whether with the fast Fourier transform (FFT), or filter design, or the adaptive modeling inherent in time-frequency-scale methods such as wavelet theory. The coherent states of mathematical physics are translated and modulated Fourier transforms, and these are used, in conjunction with the uncertainty principle, for dealing with signal reconstruction in communications theory. We are back to the raison d'être of the *ANHA* series!

John J. Benedetto
Series Editor
University of Maryland
College Park

Preface

Preface to Volume 1

As an undergraduate student at a good engineering school, I had never heard of stochastic processes or Lie groups (even though I double majored in Mathematics). As a faculty member in engineering I encountered many problems where the recurring themes were "noise" and "geometry." When I went to read up on both topics I found fairly little at this intersection. Now, to be certain, there are many wonderful texts on one of these subjects or the other. And to be fair, there are several advanced treatments on their intersection. However, for the engineer or scientists who has the modest goal of modeling a stochastic (i.e., time-evolving and random) mechanical system with equations with an eye towards numerically simulating the system's behavior rather than proving theorems, very few books are out there. This is because mechanical systems (such as robots, biological macromolecules, spinning tops, satellites, automobiles, etc.) move in multiple spatial dimensions, and the configuration space that describes allowable motions of objects made up of rigid components does not fit into the usual framework of linear systems theory. Rather, the configuration space manifold is usually either a Lie group or a homogeneous space.[1]

My mission then became clear: write a book on stochastic modeling of (possibly complicated) mechanical systems that a well-motivated first-year graduate student or undergraduate at the senior level in engineering or the physical sciences could pick up and read cover-to-cover without having to carry around twenty other books. The key point that I tried to keep in mind when writing this book was that the art of mathematical modeling is very different than the art of proving theorems. The emphasis here is on "how to calculate" quantities (mostly analytically by hand and occasionally numerically by computer) rather than "how to prove." Therefore, some topics that are treated at great detail in mathematics books are covered at a superficial level here, and some concrete analytical calculations that are glossed over in mathematics books are explained in detail here. In other words the goal here is not to expand the frontiers of mathematics, but rather to translate known results to a broader audience.

The following quotes from Felix Klein[2] in regard to the modern mathematics of his day came to mind often during the writing process:

[1] The reader is not expected to know what these concepts mean at this point.

[2] F. Klein, *Development of Mathematics in the* 19*th Century*, translated by M. Ackerman as part of *Lie Groups: History, Frontiers and Applications*, Vol. IX, Math Sci Press, 1979.

> The exposition, intended for a few specialized colleagues, refrains from indicating any connection with more general questions. Hence it is barely accessible to colleagues in neighboring fields and totally inaccessible to a larger circle...
> In fact, the physicist can use little, and the engineer none at all, of these theories in his tasks.

The later of these was also referenced in Arnol'd's classic book[3] as an example of how work that is initially viewed as esoteric can become central to applied fields.

In order to emphasize the point that this book is for practitioners, as I present results they generally are not in "definition-proof-theorem" format. Rather, results and derivations are presented in a flowing style. Section headings punctuate results so that the presentation (hopefully) does not ramble on too much.

Another difference between this book and one on pure mathematics is that while pathological examples can be viewed as the fundamental motivation for many mathematical concepts (e.g, the behavior of $\sin \frac{1}{x}$ as $x \to 0$), in most applications most functions and the domains on which they are defined do not exhibit pathologies. And so practitioners can afford to be less precise than pure mathematicians.

A final major difference between this presentation and those written by mathematicians is that rather than the usual "top-down" approach in which examples follow definitions and theorems, the approach here is "bottom-up" in the sense that examples are used to motivate concepts throughout this book and the companion volume. Then after the reader gains familiarity with the concepts, definitions are provided to capture the essence of the examples.

To help with the issue of motivation and to illustrate the art of mathematical modeling, case studies from a variety of different engineering and scientific fields are presented. In fact, so much material is covered that this book has been split into two volumes. Volume 1 (which is what you are reading now) focuses on basic stochastic theory and geometric methods. The usefulness of some of these methods may not be clear until the second volume. For example, some results pertaining to differential forms and differential geometry that are presented in Volume 1 are not applied to stochastic models until they find applications in Volume 2 in the form of Integral Geometry (also called Geometric Probability) and in Multivariate Statistical Analysis. Volume 2 serves as an in-depth (but accessible) treatment of Lie groups, and the extension of statistical and information-theoretic techniques to that domain.

I have organized Volume 1 into the following 9 chapters and an appendix: Chapter 1 provides an introduction and overview of the kinds of the problems that can be addressed using the mathematical modeling methods of this book. Chapter 2 reviews every aspect of the Gaussian distribution, and uses this as the quintessential example of a probability density function. Chapter 3 discusses probability and information theory and introduces notation that will be used throughout these volumes. Chapter 4 is an overview of white noise, stochastic differential equations (SDEs), and Fokker–Planck equations on the real line and in Euclidean space. The relationship between Itô and Stratonovich SDEs is explained and examples illustrate the conversions between these forms on multi-dimensional examples in Cartesian and curvilinear coordinate systems. Chapter 5 provides an introduction to Geometry including elementary projective, algebraic, and differential geometry of curves and surfaces. That chapter begins with some concrete examples that are described in detail. Chapter 6 introduces differential forms and the generalized Stokes theorem. Chapter 7 generalizes the treatment of surfaces and

[3] See Arnol'd, VI, *Mathematical Methods of Classical Mechanics*, Springer-Verlag, Berlin, 1978.

polyhedra to manifolds and polytopes. Geometry is first described using a coordinate-dependent presentation that some differential geometers may find old fashioned, but it is nonetheless fully rigorous and general, and far more accessible to the engineer and scientist than the elegant and powerful (but cryptic) coordinate-free descriptions. Chapter 8 discusses stochastic processes in manifolds and related probability flows. Chapter 9 summarizes the current volume and introduces Volume 2. The appendix provides a comprehensive review of concepts from linear algebra, multivariate calculus, and systems of first-order ordinary differential equations. To the engineering or physical science student at the senior level or higher, some of this material will be known already. But for those who have not seen it before, it is presented in a self-contained manner. In addition, exercises at the end of each chapter in Volume 1 reinforce the main points. There are more than 150 exercises in Volume 1. Volume 2 also has many exercises. Over time I plan to build up a full solution set that will be uploaded to the publisher's webpage, and will be accessible to instructors. This will provide many more worked examples than space limits allow within the volumes.

Volume 1 can be used as a textbook in several ways. Chapters 2–4 together with the appendix can serve as a one-semester course on continuous-time stochastic processes. Chapters 5–8 can serve as a one-semester course on elementary differential geometry. Or, if chapters are read sequentially, the whole book can be used for self-study. Each chapter is meant to be relatively self contained, with its own references to the literature. Altogether there are approximately 250 references that can be used to facilitate further study.

The stochastic models addressed here are equations of motion for physical systems that are forced by noise. The time-evolving statistical properties of these models are studied extensively. Information theory is concerned with communicating and extracting content in the presence of noise. Lie groups either can be thought of as continuous sets of symmetry operations, or as smooth high-dimensional surfaces which have an associated operator. That is, the same mathematical object can be viewed from either a more algebraic or more geometric perspective.

Whereas the emphasis of Volume 1 is on basic theory of continuous-time stochastic processes and differential geometric methods, Volume 2 provides an in-depth introduction to matrix Lie groups, stochastic processes that evolve on Lie groups, and information-theoretic inequalities involving groups. Volume 1 only has a smattering of information theory and Lie groups. Volume 2 emphasizes information theory and Lie groups to a much larger degree.

Information theory consists of several branches. The branch originating from Shannon's mathematical theory of communication is covered in numerous engineering textbooks with minor variants on the titles "Information Theory" or "Communications Theory." A second branch of information theory, due to Wiener, is concerned with filtering of noisy data and extracting a signal (such as in radar detection of flying objects). The third branch originated from the field of mathematical statistics in which people like Fisher, de Bruijn, Cramér, and Rao developed concepts in statistical estimation. It is primarily this third branch that is addressed in Volume 1, and so very little of the classical engineering information theory is found here. However, Shannon's theory is reviewed in detail in Volume 2, where connections between many aspects of information and group theory are explored. And Wiener's filtering ideas (which have a strong connection with Fourier analysis) find natural applications in the context of deconvolving functions on Lie groups (an advanced topic that is also deferred to Volume 2).

Volume 2 is a more formal and more advanced presentation that builds on the basics covered in Volume 1. It is composed of three parts. Part 1 begins with a detailed treatment of Lie groups including elementary algebraic, differential geometric, and functional analytic properties. Classical variational calculus techniques are reviewed, and the coordinate-free extension of these concepts to Lie groups (in the form of the Euler–Poincaré equation) are derived and used in examples. In addition, the basic concepts of group representation theory are reviewed along with the concepts of convolution of functions and Fourier expansions on Lie groups. Connections with multivariate statistical analysis and integral geometry are also explored. Part 2 of Volume 2 is concerned with the connections between information theory and group theory. An extension of the de Bruijn inequality to the context of Lie groups is examined. Classical communication-theory problems are reviewed, and information inequalities that have parallels in group theory are explained. Geometric and algebraic problems in coding theory are also examined. A number of connections to problems in engineering and biology are provided. For example, it is shown how a spherical optical encoder developed by the author and coworkers[4] can be viewed as a decoding problem on the rotation group, $SO(3)$. Also, the problem of noise in coherent optical communication systems is formulated and the resulting Fokker–Planck equation is shown to be quite similar to that of the stochastic Kinematic cart that is described in the introductory chapter of Volume 1. This leads to Part 3 of Volume 2, which brings the discussion back to issues close to those in Volume 1. Namely, stochastic differential equations and Fokker–Planck equations are revisited. In Volume 2 all of these equations evolve on Lie groups (particularly the rotation and rigid-body-motion groups). The differential geometric techniques that are presented in Volume 1 are applied heavily in this setting. Several closely related (though not identical) concepts of "mean" and "covariance" of probability densities on Lie groups are reviewed, and their propagation under iterated convolutions is studied. As far as the descriptions of probability densities on Lie groups are concerned, closed-form Gaussian-like approximations are possible in some contexts, and Fourier-based solutions are more convenient in others. The coordinate-based tools needed for realizing these expressions as concrete quantities (which can in principle be implemented numerically) are provided in Volume 2.

During a lecture I attended while writing this book, an executive from a famous computer manufacturer said that traditionally technical people have been trained to be "I-shaped," meaning an education that is very deep in one area, but not broad. The executive went on to say that he now hires people who are "T-shaped," meaning that they have a broad but generally shallow background that allows them to communicate with others, but in addition have depth in one area. From this viewpoint, the present book and its companion volume are "Π-shaped," with a broad discussion of geometry that is used to investigate three areas of knowledge relatively deeply: stochastic models, information theory, and Lie groups.

It has been a joy to write these books. It has clarified many issues in my own mind. And I hope that you find them both interesting and useful. And while I have worked hard to eliminate errors, there will no doubt be some that escaped my attention. Therefore I welcome any comments/corrections and plan to keep an updated online erratum page which can be found by searching for my name on the web.

There are so many people without whom this book would not have been completed. First, I must thank John J. Benedetto for inviting me to contribute to this series that he is editing, and Tom Grasso at Birkhäuser for making the process flow smoothly.

[4] Stein, D., Scheinerman, E.R., Chirikjian, G.S., "Mathematical models of binary spherical-motion encoders," *IEEE-ASME Trans. Mechatron.*, 8(2), 234-244, 2003.

A debt of gratitude is owed to a number of people who have worked (and maybe suffered) through early drafts of this book. These include my students Kevin Wolfe, Michael Kutzer, and Matt Moses who received very rough drafts, and whose comments and questions were very useful in improving the presentation and content. I would also like to thank all of my current and former students and colleagues for providing a stimulating environment in which to work.

Mathematicians Ernie Kalnins, Peter T. Kim, Willard Miller, Jr., and Julie Mitchell provided comments that helped significantly in identifying mathematical errors, fine-tuning definitions, and organizing topics. I am thankful to Tamás Kalmár-Nagy, Jennifer Losaw, Tilak Ratnanather, and Jon Selig for finding several important typographical errors. John Oprea went way above and beyond the call of duty to read and provide detailed comments on two drafts that led to a significant reorganization of the material. Andrew D. Lewis provided some very useful comments and the picture of a torus that appears in Chapter 5. Andrew Douglas, Tak Igusa, and Frank C. Park each provided some useful and/or encouraging comments. Wooram Park helped with some of the figures.

I would like to thank William N. Sharpe, Jr. for hiring me many years ago straight out of graduate school (even after knowing me as an undergraduate), and Nick Jones, the Benjamin T. Rome Dean of the JHU Whiting School of Engineering, for allowing me to have the sabbatical during the 2008 calendar year that was used to write this book after my service as department chair finished.

I would also like to thank the faculty and staff of the Institute for Mathematics and Its Applications (IMA) at the University of Minnesota for the three week-long workshops that I attended there during part of the time while I was writing this book. Some of the topics discussed here percolated through my mind during that time.

Last but not least, I would like to thank my family. Writing a single-author book can be a solitary experience. And so it is important to have surroundings that are "fuuuun."

Baltimore, Maryland *Gregory Chirikjian*
May 2009

Preface to Volume 2

This book, Volume 2, builds on the fundamental results and differential-geometric terminology established in Volume 1. The goal of Volume 2 is to bring together three fields of study that are usually treated as disjoint subjects: stochastic models, information theory, and Lie groups.[5]

Stochastic phenomena appear frequently in engineering and physics. From one perspective, stochasticity (i.e., randomness) can be viewed as an inherent characteristic of the physical world, and developing mathematical models that describe this inherent stochasticity allows us to understand truly random phenomena. Alternatively, stochastic modeling can be thought of as a way to sweep the true complexity of the physical world under the rug by calling a phenomenon random when it is too complicated to model deterministically. The benefit of a stochastic model in that case is that the computational effort can be far less than that required to describe a complex deterministic system. Stochastic models can be used to generate estimates of the average behavior of very complicated deterministic systems together with the variance of these estimates. For example, a rigid model of a macromolecule being subjected to impacts by the surrounding solvent molecules could be modeled using a molecular dynamics simulation involving millions of molecules. However, the details of the interactions can be quite computationally intensive. In contrast, viewing the macromolecule as being forced by Gaussian white noise (i.e., increments of a Wiener process) allows for the relatively simple description of the behavior as a stochastic differential equation (SDE) or the corresponding Fokker–Planck equation (FPE). The relationship between SDEs and FPEs was explored in detail in Volume 1, which can be viewed as the "prequel" to the current volume.

In Volume 1 the probabilistic foundations of information theory (e.g., the definitions of and properties of entropy, mutual information, entropy-power inequality, etc.) were reviewed, but almost none of Shannon's mathematical theory of communication (which is the information theory known to engineers) was described. Shannon's information theory is concerned with the passage of data through noisy environments (called channels) as efficiently as possible. Such channels might be copper wires, fiber optic cables, the atmosphere (for radio, laser, and microwave transmission), the ocean (for acoustic/ sonar signals), and so forth. This means that the data should be coded in some way so as not to be corrupted by random noise in the environment. The simplest robust scheme would be to repeat the message many times, but this would not be efficient. If the noise characteristics of the channel are known, then the data can be coded (or packaged) before it is sent so as to reach the receiver with high probability and at a high rate. Of course, there is a trade-off between the speed of transmission and the probability that the original message is actually received. One model for the way data is corrupted during transmission is by Gaussian noise. The communication channels that subject data to this kind of noise are called Gaussian channels. From this description it should be clear that stochastic models of information channels go hand-in-hand with the design of codes for transmission of data through known channels. And when the physical nature of the channel (or the action of intelligent agents that transmit, receive, and process information in the physical world) is of interest, Lie groups enter in several ways.

[5] This material is based upon work supported by the National Science Foundation under Grant No. IIS-0915542.
Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

Lie groups have been studied intensively over the past century. These are continuous sets of operations that can be composed and inverted and for which an identity element exists and the associative law holds. The Lie groups of most interest in engineering applications are the rotation and rigid-body-motion groups in two- and three-dimensional space. In physics, other Lie groups such as the special unitary groups and the Galilean group describe invariants/symmetries of systems of interest. For example, all of the equations of classical mechanics are invariant under Galilean transformations, and unitary groups describe symmetries in quantum mechanics and particle physics. Strong connections have existed between Lie groups and stochastic processes for many decades. For example, in the 1930s, Perrin studied the rotational Brownian motion of rigid molecules; that is, the orientation of a molecule follows a stochastic path induced by its environment. In the estimation of the position and orientation of a robot, satellite, or submarine from noisy and/or incomplete data, measurements corrupted by noise are used to determine a best guess of the kinematic state of the system. Such topics have been investigated since the early 1970s and are still being studied today.

Although strong historical connections exist between information theory and stochastic models and between stochastic models and Lie groups, direct connections between information theory and Lie groups are far less explored. In coding theory, finite groups arise in several contexts (e.g., as groups of symmetry operations acting on sphere packings, Abelian groups over finite fields, coset codes, etc.). Although these concepts are reviewed in this book, they are not the focus. Lie groups (as opposed to finite groups) are connected to information theory in several ways that have not been explored much in the literature. Indeed, one of the main contributions of this book is the exploration of the connection between Lie groups and information theory. In some cases, these connections are through a stochastic model. In other cases, the connections are direct. For example, Lie groups have associated with them certain algebraic structures such as subgroups and coset spaces. Probability density functions (pdfs) over a Lie group can be marginalized over a subgroup or coset space and concepts of conditional and marginal entropy and mutual information can be defined. Additionally, the group operation can be used to define a convolution operation. It is shown in this book that the entropy of the convolution of two pdfs on a Lie group is no less than the entropy of the individual pdfs and that a version of the famous data processing inequality holds for Lie groups.

These rather abstract connections between information-theoretic concepts and Lie groups are supported by certain applications. For example, consider a mobile robot, bacterium, or animal that wonders around foraging for resources uses sensory information to update its position and orientation in space. This “infotaxis” (information-driven motion) is defined by the processing of sensory information resulting in action in the physical world and, specifically, the action that results is a trajectory in the Lie group of rigid-body motions. As a second example, when information is transmitted as pulses through a fiber optic cable using a certain transmission and reception strategy, the rate of information transmission is limited by the fact that lasers are imperfect physical devices and the pulses are not perfectly sharp. This is due to spontaneous (and uncontrolled) emission of photons in the laser cavity. The resulting “phase noise” leads to a blurring of the pulses and a reduction in the rate of reliable information transmission. As it turns out, the stochastic model that describes this noise leads to SDEs and FPEs that evolve on the Euclidean group of the plane. Additionally, characteristics of these pdfs indicate the rate at which information can be reliably transmitted. Other examples of the connection between Lie groups and information theory arise in biomolecular applications. DNA is known to carry the genetic information in all known living organisms. This information is described by the classical discrete information theory, and many books on bioinformatics address this. However, there is also information (of the continuous kind) that describes fluctuations in the shape of biomolecules. For example, the spatial packing density for genetic information is a function of how DNA molecules are packaged in chromosomes. It is possible to ask questions about how the sequential content of DNA impacts its flexibility and how the resulting ensemble of Brownian-motion-generated conformations differ from each other. This type of question is at the interface of information theory and statistical mechanics, where concepts of entropy and the Lie groups describing the motion of molecules come together.

This book is structured as follows:

In Chapter 10 the concept of Lie groups and their relationship to Lie algebras are defined rigorously and many examples are provided in the concrete setting of matrices.

Chapter 11 discusses functions on Lie groups and how concepts such as the derivative of functions and Taylor series extend from $\mathbb{R}^n$ to this setting.

Chapter 12 discusses integration on Lie groups and Fourier expansions.

Chapter 13 reviews classical variational calculus and its extensions to the case when the functionals of interest have arguments in a Lie group and Lie algebra.

Chapters 14 is an introduction to statistical mechanics via stochastic differential equations. The specific emphasis is on physical systems that can be modeled as multiple rigid bodies and hence have a configuration space that is a Lie group. Also in this chapter, concepts from ergodic theory are discussed.

In Chapter 15 the concept of entropy from statistical mechanics is modified for the context of robotic parts handling, and the relationship to the principal kinematic formula from the field of Integral Geometry is rederived, used, and modified. In particular, that chapter discusses the problem of automated assembly and how Sanderson's concept of parts entropy (which is the Shannon entropy of a random variable on a Euclidean group) provides a connection between Lie groups and information theory. Since parts occlude each other, knowing how much volume is available for a part to move in the group of rigid-body motions without bumping into another part is important in the computation of parts entropy. That is where the principal kinematic formula comes in.

Chapter 16 examines the relationship among matrix Lie groups, multivariate analysis, and random matrix theory. As it turns out, the covariance matrix for a multi-variate Gaussian distribution, which is a symmetric positive-definite matrix, can be thought of as a point in a quotient space of two groups of the form $GL^+(n,\mathbb{R})/SO(n,\mathbb{R})$.[6] As a result, if we know how to integrate over the group $GL^+(n,\mathbb{R})$ (which consists of all $n \times n$ matrices with real entries and positive determinant) and the rotation group in n-dimensional space, $SO(n,\mathbb{R})$, then from this knowledge we will know how to integrate over the space of all covariance matrices. This is important because the sample covariance obtained from any experiment is never exactly the same as the ideal covariance of the pdf describing the physical phenomenon being investigated. The field of multi-variate statistical analysis studies the distribution of possible covariance matrices; that is, whereas $\rho(\mathbf{x};\mathbf{0},\mathit{\Sigma})$ describes a Gaussian distribution on $\mathbb{R}^n$ with zero mean and covariance $\mathit{\Sigma}$, in multivariate analysis the distribution of covariances, $f(\mathit{\Sigma})$, is a pdf on the space $GL^+(n,\mathbb{R})/SO(n,\mathbb{R})$, called the Wishart distribution. Lie-theoretic terminology and results are useful in that context. This provides one link between Lie groups and classical probability and statistics, which are, in turn, linked to information theory. Connections between multi-variate analysis and the theory of random matrices are natural, and in recent years, random matrix theory has become a popular tool to model communication networks. This brings us back to information theory.

[6] The reader is not expected to know what this means yet.

Chapter 17 reviews classical information theory (the theory of communication) including Shannon's source-coding and channel-coding theorems. Several classical information-theory results such as the data processing inequality and the Shannon–Hartley theorem for the capacity of a continuous channel with Gaussian noise are reviewed. This chapter also shows how Lie groups enter into communication problems both as symmetries of equations describing physical channels (e.g., the (linear) telegraph equation, and (nonlinear) soliton-based communication strategies) as well as serving as the domain in which signals evolve (laser phase noise).

Chapter 18 discusses algebraic and geometric aspects of coding/decoding problems. For example, Hamming codes and the relationship to packing of spheres in high-dimensional Euclidean spaces is reviewed. It is also shown how one can design codes on Lie groups. For example, in a usual motor, a rotary encoder is used to measure the angle through which the motor turns. This can be viewed as a coding/decoding problem on the group $SO(2)$. For a spherical motor, such as the one co-invented by the author, an encoding strategy is needed in order to control it. This problem can be thought of as coding theory on the Lie group $SO(3)$. Similar problems exist in the design and use of fiducial patterns for use in medical imaging.

Chapter 19 introduces the author's observations about how classical information theory extends to the case when the random variables under investigation live in a Lie group rather than in Euclidean space. It discusses how inequalities of classical information theory (the de Bruijn inequality, the data processing inequality, and the Cramér–Rao bound) extend to the setting of Lie groups.

Chapter 20 is a return to the sorts of stochastic processes discussed in Volume 1, but with a focus on Lie groups. Properties of Fokker–Planck equations on Lie groups are discussed, and the properties and mathematical machinery developed in Chapters 10–12 are used to analyze the properties of solutions of these Fokker–Planck equations. This includes several concrete physical problems (rotational Brownian motion, conformational fluctuations of DNA, bacterial chemotaxis).

Chapter 21 applies the properties of the stochastic models from Chapter 20 by introducing the concept of a Gaussian channel on a Lie group and the concept of injecting noise through fiber bundles (which are a differential geometric structure that was briefly discussed in Chapter 7 and the description of which is expanded here). The nonholonomic kinematic cart is again used as the prototypical example of a system to which this methodology can be applied.

Chapter 22 provides a summary of this book and discusses other application areas that are ripe for future work. These include so-called "infotaxis" (or information-driven motion), connections between statistical mechanics and conformational aspects of biomolecular information theory, and medical imaging problems.

According to folklore, when Claude Shannon (the engineer) was pondering what name to give to the quantity that he was studying, John von Neumann (the mathematician) advocated the use of the word "entropy" and is purported to have said to him:

> No one really knows what entropy is, so in a debate you will always have the advantage.

Regardless of whether or not I understand entropy, I'd like to think that both of these men (as well as Wiener, Itô, and Stratonovich) would be happy to see the confluence of information-theoretic, geometric, stochastic, and Lie-algebraic ideas that are summarized here for a wide audience.

Perhaps the most important issue that needs to be addressed in this preface is a question that has been asked by some students, which is "Dr. C, why did you make this two volumes? Now I have two books to buy!" There are several answers to this question:

- Contrary to intuition, the cost of a single large book can be quite prohibitive relative to the cost of each of these volumes. By cutting the book into two volumes, readers who are only interested in topics in one of the volumes do not need to pay the extra price that would have accompanied a single large volume. Students may be more interested in Volume 1, whereas researchers who already know the definitions and basic principles in Volume 1 may be more interested Volume 2.
- Each volume is just the right size that it can be slipped into a backpack and read (or at least skimmed) on an intercontinental airplane trip. For the busy researcher, there is little time in daily life to sit down and actually read, whereas the quiet undisturbed time of a trip is ideal for reading. A larger book would not travel as well.
- When reading a large book contained within two hard covers, it can be quite annoying when reading p. 826 to be required to access necessary definitions on p. 17. The process of flipping back and forth a massive number of pages to connect the necessary concepts can impede the learning process and add wear and tear to the book. In contrast, if p. 17 is in Volume 1 and the page that would have been p. 826 is actually p. 399 in Volume 2, then both pages can be viewed *simultaneously* without flipping.

Finally, I have many people to thank. The students who took my class for credit during the Spring 2010 semester worked hard to find errors: Martin Kendal Ackerman, Graham Beck, Mike Kutzer, Mike Mashner, Matt Moses, Valentina Staneva, Roberto Tron, Kevin Wolfe, and Yan Yan. Comments by Garrett Jenkinson, Manu Madhav, Shahin Sefati, John Swensen, and Tom Wedlick were also helpful in modifying the presentation. Useful comments by Andrea Censi, Ming Liao, and Rolf Schneider have also improved the presentation and helped to eliminate errors. Any errors that are found after publication will be posted as a list of errata on my lab's webpage, together with an addendum including additional exercises and pointers to the ever-growing literature, as was done for Volume 1. Last but not least, I have my whole family to thank for their love and support.

Baltimore, Maryland *Gregory Chirikjian*
June 2011

Contents

10

Lie Groups I: Introduction and Examples

The concept of a *group* was described briefly in Chapter 1. This chapter serves as an introduction to a special class of groups, the *Lie groups*, which are named after Norwegian mathematician Sophus Lie.[1] Furthermore, when referring to Lie groups, what will be meant in the context of this book is *matrix Lie groups*, where each element of the group is a square invertible matrix. Other books focusing specifically on matrix groups include [3, 9, 19].

In a sense, matrix Lie groups are "the most like $\mathbb{R}^n$" of any mathematical structure other than vector spaces. Indeed, $\mathbb{R}^n$ together with the operation of addition is an example of a Lie group. More generally, each point in a Lie group, G, is locally indistinguishable from a point in $\mathbb{R}^n$ (i.e., G is a manifold), and, globally, G is orientable. Furthermore, G has an operator, $\circ$, that takes two elements to produce another (i.e., $g_1, g_2 \in G$ means that $g_1 \circ g_2 \in G$), much like the way that the operation of addition takes two vectors and produces another. However, Lie groups are generally not commutative (i.e., $g_1 \circ g_2 \neq g_2 \circ g_1$), and, generally, it is not possible to multiply a group element by a scalar to produce another element in the same group.

This chapter begins with a more detailed introduction to group theory than that which was provided in Chapter 1. This is followed by the definition and properties of matrix Lie groups and their associated Lie algebras. The matrix exponential map is shown to convert elements of a Lie algebra into elements of a matrix Lie group, and the matrix logarithm plays the inverse role. A fundamental tool for performing computations that are described in a local parametrization is the Jacobian matrix for a matrix Lie group. Examples of matrix Lie groups are provided together with explicit computations of the exponential map and Jacobian matrices.

The main things to take away from this chapter are as follows:

- Knowledge of the basic definitions of Lie group theory;
- The ability to identify which sets of matrices form Lie groups and which do not;
- Facility with computing the exponential and logarithm maps and Jacobian matrices for Lie groups.

This chapter is structured as follows. Section 10.1 is a general introduction to group theory. Section 10.2 focuses on the main kind of group use throughout this book—the matrix Lie groups—and discusses their relationship to Lie algebras. Section 10.3 describes how structure constants of a matrix Lie algebra change with a change of basis. Section 10.4 introduces the concept of a Jacobian matrix for a Lie group, which is a

[1] "Lie" is pronounced as *Lee*, not *lye*.

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_1,

central tool in describing how to differentiate and integrate functions on Lie groups that are expressed in coordinates. Section 10.5 introduces the concepts of the adjoint matrices *Ad* and *ad* and the Killing form. Section 10.6 provides numerous examples of concrete computations associated with Lie groups using coordinates. When one is learning a new subject and presented with many examples, the tendency is to extrapolate too much and imagine that *everything* fits within the newly learned framework. Therefore, Section 10.7 presents examples of mathematical objects of interest that fail in one or more ways to be a Lie group. That discussion is followed by the chapter summary.

10.1 Introduction to Group Theory

The concept of a group was defined in Chapter 1, but it is worthwhile to define it again here. First, the concept of a binary operation needs to be defined.

10.1.1 Binary Operations

Given a set G, a *(closed) binary operation* is a composition law that takes any two elements of G and returns an element of G (i.e., $g_1 \circ g_2 \in G$ whenever $g_1, g_2 \in G$). This can be viewed alternatively as a mapping $b : G \times G \to G$ with $b(g_1, g_2) \doteq g_1 \circ g_2$. In some books, $b(\cdot, \cdot)$ is referred to as the binary operation, and in others, $\circ$ is. For the most part, the notation here will use $\circ$ as the binary operation, although to connect with the literature it is useful to understand both notations.

As an example let $G = \mathbb{R}^{N \times N}$ and as a binary operation, consider the multiplication of square matrices $A, B \in \mathbb{R}^{N \times N}$. Then $\circ =$ matrix multiplication, and $b(A, B) = AB$. Now, consider the same set of matrices with $\circ = +$, in which case $b(A, B) = A + B$. With either of these operations, the result is a square matrix of the same dimension. As another example, consider the vector cross product, in which $\mathbf{a}, \mathbf{c} \in \mathbb{R}^3$ are used together with the cross product operation to form another vector $\mathbf{a} \times \mathbf{c} \in \mathbb{R}^3$. Therefore, $b(\mathbf{a}, \mathbf{c}) = \mathbf{a} \times \mathbf{c}$ is a binary operation. As a final example, consider two permutations $\pi_1, \pi_2 \in \Pi_n$, and the operation of composition as defined in Section 6.2. Since $\pi_1 \circ \pi_2 \in \Pi_n$, it follows that $\circ$ is a binary operation.

Not every operator that acts on two elements of a set is a binary operation. For example, given two vectors $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, the dot product $\mathbf{v} \cdot \mathbf{w}$ and the wedge product $\mathbf{v} \wedge \mathbf{w}$ are *not* binary operations. Although they take in two vectors of the same kind, their output is a different kind of object. Likewise, the multiplication of matrices $A \in \mathbb{R}^{m \times n}$ and $B \in \mathbb{R}^{n \times p}$ for $m \neq n \neq p$ would not be a binary operation for two reasons: (a) the inputs are not objects of the same kind and (b) the output $AB \in \mathbb{R}^{m \times p}$ is of a different kind than both of the inputs.

10.1.2 Groups, Groupoids, and Semi-groups

The pair $(G, \circ)$ consisting of the set G and binary operation $\circ$ form a mathematical structure that is called a *groupoid* or a *magma*. (The word groupoid can also mean something different in other areas of mathematics, but since there will be no ambiguity in the context of this text, this is the word that will be used here.)

A *group* is a special kind of groupoid such that for any elements $g, g_1, g_2, g_3 \in G$, the following properties hold:

1. $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$.

2. There exists an element $e \in G$ such that $e \circ g = g$.
3. For every element $g \in G$, there is an element $g^{-1} \in G$ such that $g^{-1} \circ g = e$.

The first of the above properties is called *associativity*; the element e is called the *identity* of G; and g^{-1} is called the *inverse* of $g \in G$. In order to distinguish between the group and the set, the former is denoted $(G, \circ)$, unless the operation is understood from the context, in which case G refers to both the set and the group. In the special case when for every two elements $g_1, g_2 \in G$, it is true that $g_1 \circ g_2 = g_2 \circ g_1$, the group is called *commutative* (or *Abelian*).

A Concrete Example: Symmetry Operations on the Equilateral Triangle

Groups often arise in describing operations that preserve shape. Consider the set of symmetry operations acting on the equilateral triangle shown in Figure 10.1. Imagine a triangle made of some solid material. When viewed from above along the normal to the plane of the triangle, label its vertices clockwise as 1, 2, 3. Additionally, assume that there is a triangular "slot" in a table into which this triangle can fit. The slot also has vertices labeled 1, 2, 3 that appear clockwise when viewed from above. Assume that initially the triangle sits in the slot with 1 matched to 1, 2 matched to 2, and 3 matched to 3.

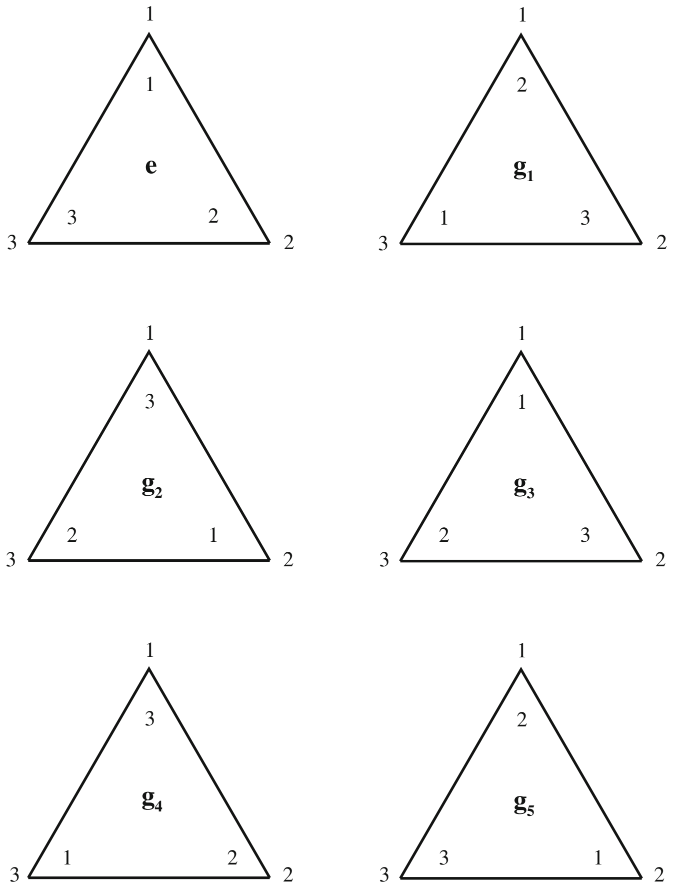


Fig. 10.1. Symmetry Operations for the Equilateral Triangle

There are six symmetry elements (ways to rotate or flip the triangle and fit it back in the slot):

$g_0 = e$, which is to to do nothing (and hence it is the identity);
g_1, rotate counterclockwise by $2\pi/3$ radians;
g_2, rotate counterclockwise by $4\pi/3$ radians;
g_3, rotate the triangle by π radians around the axis defined by its center and vertex 1 fixed within it;
g_4, rotate the triangle by π radians around the axis defined by its center and vertex 2 fixed within it;
g_5, rotate the triangle by π radians around the axis defined by its center and vertex 3 fixed within it.

The set of these operations of the triangle will be denoted here as

$$G_T \doteq \{e, g_1, g_2, g_3, g_4, g_5\}.$$

Now, if we *define* the composition of two such operations g_i followed by g_j to be $g_i \circ g_j$, then the following table results, where g_i is taken from the column on the left and g_j is taken from the row on top.

$$\begin{array}{c|cccccc}
\circ & e & g_1 & g_2 & g_3 & g_4 & g_5 \\
\hline
e & e & g_1 & g_2 & g_3 & g_4 & g_5 \\
g_1 & g_1 & g_2 & e & g_4 & g_5 & g_3 \\
g_2 & g_2 & e & g_1 & g_5 & g_3 & g_4 \\
g_3 & g_3 & g_5 & g_4 & e & g_2 & g_1 \\
g_4 & g_4 & g_3 & g_5 & g_1 & e & g_2 \\
g_5 & g_5 & g_4 & g_3 & g_2 & g_1 & e
\end{array} . \tag{10.1}$$

Working with this this table, it can be verified that all of the properties are satisfied in order for $(G_T, \circ)$ to be a group. Indeed, this group can be identified with the permutations Π_3 discussed in Section 6.2 of Volume 1. One way to identify each symmetry operator with a permutation is to assign each vertex number in the mobile triangle to the vertex number in the fixed triangular slot to which it moves. For example, g_1 can be viewed as a permutation that moves vertex 1 to location 3, vertex 2 to location 1, and vertex 3 to location 2. Then the statement $g_1 \circ g_3 = g_4$ is equivalent to the product of permutations

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

using the convention for multiplying permutations used in Section 6.2.

Abstract Group Theory

In abstract group theory, a number of statements about groups can be proven immediately from the defining properties 1–3 listed at the beginning of Section 10.1.2—namely (a) the identity element is unique; (b) the identity also satisfies $g \circ e = g$; (c) the inverse of any element is unique; (d) the left inverse is equal to the right inverse (i.e., $g \circ g^{-1} = e$). Sometimes these immediate consequences are included in the definition of a group. They follow from the cancellation rule $a \circ x = b \Longrightarrow x = a^{-1} \circ b$, which is proved below.

From the definition, any equation on a group of the form $a \circ x = b$ can be solved by applying a^{-1} on the left and using the associative law:

$$a \circ x = b \Longrightarrow a^{-1} \circ (a \circ x) = (a^{-1} \circ a) \circ x = a^{-1} \circ b \Longrightarrow e \circ x = a^{-1} \circ b \Longrightarrow x = a^{-1} \circ b.$$

A variation on this theme is that

$$c \circ x = c \circ d \Longrightarrow x = d \tag{10.2}$$

because c^{-1} can be multiplied on the left.

Consider the series of equalities [5]

$$(a^{-1} \circ a) \circ e = e \circ e = e = a^{-1} \circ a.$$

Applying the associative law and the cancellation rule in (10.2) to this gives

$$a^{-1} \circ (a \circ e) = a^{-1} \circ a \Longrightarrow a \circ e = a. \tag{10.3}$$

This proves that the left identity is the right identity. Now, using the cancellation rule in (10.2) together with the fact that e is both the left and right identity can be used to prove that the left inverse a^{-1} is also a right inverse [5]:

$$a^{-1} \circ (a \circ a^{-1}) = (a^{-1} \circ a) \circ a^{-1} = e \circ a^{-1} = a^{-1} = a^{-1} \circ e \Longrightarrow a \circ a^{-1} = e. \tag{10.4}$$

Other statements about abstract groups are left as exercises.

Of the examples listed in Section 10.1.1, only the permutation example and the matrix addition examples are groups. The vector cross product is not associative, there is no identity element, and there is no inverse. So it is “far from” being a group. The matrix multiplication example is “almost” a group. The problem is that, in general, matrices are not invertible under the operation of multiplication. In general, a groupoid that satisfies Properties 1 and 2 but not Property 3 is called a *semi-group*. In stochastic processes semi-groups play an important role. For example, if $f(x, t_1)$ and $f(x, t_2)$ are any solutions to the heat equation on the line, subject to the initial conditions $f(x, 0) = \delta(x)$, then the convolution operation makes $f(x, t_1) * f(x, t_2) = f(x, t_1 + t_2)$ a member of this set also. The Dirac delta serves as the identity, and convolution is the associative operation for the semi-group consisting of the set $\{f(x, t) \mid t \in \mathbb{R}_{>0}\}$. However, since convolution tends to smear (and increase entropy), there is no solution to the heat equation that can serve as an inverse.

If a set of $N \times N$ matrices with real entries is restricted to only those that can be inverted, then the result is

$$GL(N, \mathbb{R}) \doteq \{A \in \mathbb{R}^{N \times N} \mid \det A \neq 0\}. \tag{10.5}$$

This set together with the operation of matrix multiplication forms a group—the *general linear group* “over the real numbers.” More generally, $\mathbb{R}$ can be replaced with any field, $\mathbb{F}$, such as the complex numbers $\mathbb{C}$.[2] Then $GL(N, \mathbb{F})$ is called the general linear group over the field $\mathbb{F}$. The identity element for this group is $\mathbb{I}_N$, the $N \times N$ identity matrix.[3]

If the stronger condition that the determinant be a positive real number is imposed, then the resulting set

$$GL^{+}(N, \mathbb{R}) \doteq \{A \in GL(N, \mathbb{R}) \mid \det A > 0\} \tag{10.6}$$

is also a group under the operation of matrix multiplication.

[2] Properties of fields in general were discussed in Section A.1.1 of Volume 1, and they will be revisited in Section 18.2.1 in the context of coding theory.

[3] When the dimension is clear from the context, this will be written as $\mathbb{I}$.

10.1.3 Subgroups

A *subgroup* is a subset of a group ($H \subseteq G$) which is itself a group that is closed under the group operation of G. This means that $h^{-1} \in H$ whenever $h \in H$. The notation for this is $H \leq G$. If $H \leq G$ and $H \neq G$, then H is called a *proper subgroup* of G, which is denoted as $H < G$. This notation parallels that of a proper subset. Each group has at least two improper subgroups: $\{e\}$ and itself.

For example, within the permutation group Π_n, consider only those permutations that leave the last $n-k$ entries in their original locations. This will be a subgroup of Π_n that is much like Π_k. A different subgroup of Π_n is the one consisting of cyclic permutations.

Additionally, since every real number is a special case of a complex number, it follows that $GL(N,\mathbb{R}) < GL(N,\mathbb{C})$. Furthermore, since $\det(AB) = \det(A)\,\det(B)$,

$$SL(N,\mathbb{F}) \doteq \{A \in \mathbb{F}^{N\times N} \mid \det(A) = +1\} \subset GL(N,\mathbb{F}) \tag{10.7}$$

forms a subgroup, and so we can write $SL(N,\mathbb{F}) < GL(N,\mathbb{F})$.

As another example, the subset of $GL(N,\mathbb{C})$ consisting of unitary matrices forms a proper subgroup:

$$U(N) \doteq \{A \in \mathbb{C}^{N\times N} \mid AA^* = \mathbb{I}\} < GL(N,\mathbb{C}). \tag{10.8}$$

This is called the *unitary group*.

A number of the classically studied groups are obtained as intersections of the groups listed above. For example, we have the following:

The intersection of the unitary and special linear groups yields the *special unitary group*

$$SU(N) \doteq U(N) \cap SL(N,\mathbb{C}) < GL(N,\mathbb{C}). \tag{10.9}$$

The intersection of the unitary and real general linear groups yields the *orthogonal group*[4]

$$O(N,\mathbb{R}) \doteq \{A \in GL(N,\mathbb{R}) \mid AA^T = \mathbb{I}\} = U(N) \cap GL(N,\mathbb{R}). \tag{10.10}$$

The real special orthogonal group is

$$SO(N) \doteq \{A \in GL(N,\mathbb{R}) \mid AA^T = \mathbb{I}; \det A = +1\} = U(N) \cap SL(N,\mathbb{R}). \tag{10.11}$$

A broad class of subgroups that appears frequently in group theory, called a *conjugate subgroup*, is generated by conjugating all of the elements of an arbitrary subgroup with a fixed element g of the group. This is denoted as

$$gHg^{-1} \doteq \{g \circ h \circ g^{-1} \mid h \in H\} \tag{10.12}$$

for a single (fixed) $g \in G$ with $g \notin H < G$. For example, if $G = SO(3)$ and $H \cong SO(2)$ consists of matrices of the form

$$R_3(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

[4] Usually when there is no ambiguity, the shorthand $O(N)$ is used for $O(N,\mathbb{R})$.

then if $g_{\mathbf{n}} = [\mathbf{a}, \mathbf{b}, \mathbf{n}] \in SO(3)$, the subgroup $K_{\mathbf{n}} \doteq g_{\mathbf{n}} H g_{\mathbf{n}}^{-1} < SO(3)$ has the property that each element of $K_{\mathbf{n}}$, when premultiplying $\mathbf{n} \in \mathbb{R}^3$, will leave $\mathbf{n}$ fixed.

In general, if $H_1, H_2 \leq G$ and $g\, H_1\, g^{-1} = H_2$ for a $g \in G$, then H_1 and H_2 are said to be conjugate to each other. A subgroup $N \leq G$ which is conjugate to itself so that $gNg^{-1} = N$ for *all* $g \in G$ is called a *normal* subgroup of G. In this case, the notation $N \trianglelefteq G$ is used, which reflects the possibility that N could equal G. However, if N is both a normal and a proper subgroup of G, then the notation $N \triangleleft G$ is used.

For example, consider again the group $(G_T, \circ)$ of symmetry operations of the triangle. The proper subgroups can be observed from the table (10.1). They are $\{e\}$, $H_1 = \{e, g_1, g_2\}$, $H_2 = \{e, g_3\}$, $H_3 = \{e, g_4\}$, and $H_4 = \{e, g_5\}$.

The subgroups H_2, H_3, and H_4 are conjugate to each other, e.g.,

$$g_1 H_2 g_1^{-1} = H_4; \quad g_1 H_3 g_1^{-1} = H_2; \quad g_1 H_4 g_1^{-1} = H_3;$$

H_1 is conjugate to itself:

$$gH_1g^{-1} = H_1$$

for all $g \in G$. Hence, H_1 is a normal subgroup.

In general, given two subgroups of a group, $H \leq G$ and $K \leq G$, then the product

$$HK \doteq \{h \circ k | h \in H, k \in K\}$$

will be a subset (but not necessarily a subgroup) of G (i.e., $HK \subseteq G$). For example, in the case of the group $(G_T, \circ)$, $H_1 H_i = H_i H_1 = G$ for $i = 2, 3, 4$, $H_2 H_3 = \{e, g_2, g_3, g_4\} \subset G$, $H_3 H_2 = \{e, g_1, g_3, g_4\} \subset G$, etc. More generally, if $N \trianglelefteq G$ and $H \leq G$, then $NH = HN$, but this equality would not hold if one of the subgroups were not normal.

10.1.4 Group Actions and Transformation Groups

A *transformation group* $(G, \circ)$ is a group that acts on a set S in such a way that $g \cdot x \in S$ is defined for all $x \in S$ and $g \in G$ and has the properties

$$e \cdot x = x \quad \text{and} \quad (g_1 \circ g_2) \cdot x = g_1 \cdot (g_2 \cdot x) \in S \tag{10.13}$$

for all $x \in S$ and $e, g_1, g_2 \in G$. The operation $\cdot$ defines the *action* of G on S.

If any two elements of $x_1, x_2 \in S$ can be related as $x_2 = g \cdot x_1$ for some $g \in G$, then G is said to act *transitively* on S. An action is called *free* if whenever $g \cdot x = x$ for at least one $x \in X$, this means that g must be e.

For example, the permutation group Π_n acts transitively and freely on the set of numbers $\{1, 2, \ldots, n\}$, the group of rigid-body motions in n-dimensional Euclidean space acts transitively on $\mathbb{R}^n$. Additionally, the group of symmetry operations of the triangle acts transitively on the set of all orderings of the vertices of the triangle. In contrast, the action of the rotation group on $\mathbb{R}^n$ is neither transitive nor free since a point at radius r from the origin cannot be moved to a different radius by rotating about the origin, and it is possible to rotate a unit vector without changing its direction.[5]

If S is a set and G is a group that acts on it, the notation S/G (or $G \backslash S$) is used to denote the set of equivalence classes of S under the action of G. In other words, if G does not act transitively on S, then it divides it into disjoint equivalence classes

[5] In almost all instances of group actions in this book, the group acts from the left as $g \cdot x$. It is also possible to define right actions, $x \cdot g$, that have analogous properties. But these are only used in Chapter 21 in the context of fiber bundles.

called *orbits*. The quintessential example of this is $\mathbb{R}^n/SO(n)$ (or $SO(n)\backslash\mathbb{R}^n$) in which rotations divide $\mathbb{R}^n$ into an infinite number of concentric spheres. Although many books use the notation S/G, the notation $G\backslash S$ is, in a sense, more natural when G acts from the left as in (10.13).

10.1.5 Cosets

Given a subgroup $H \leq G$ and any fixed $g \in G$, the *left coset* gH is defined as

$$gH \doteq \{g \circ h | h \in H\}.$$

Similarly, the *right coset* Hg is defined as

$$Hg \doteq \{h \circ g | h \in H\}.$$

In the special case when $g \in H$, the corresponding left and right cosets are equal to H. More generally, for all $g \in G$, $g \in gH$ and $g_1 H = g_2 H$ if and only if $g_2^{-1} \circ g_1 \in H$. Likewise for right cosets, $Hg_1 = Hg_2$ if and only if $g_1 \circ g_2^{-1} \in H$.

Any group is divided into disjoint left (right) cosets, and the statement "g_1 and g_2 are in the same left (right) coset" is an equivalence relation on the group G. This can be written explicitly for the case of right cosets as

$$g_1 \sim g_2 \quad \Longleftrightarrow \quad g_1 \circ g_2^{-1} \in H. \tag{10.14}$$

Since H is a subgroup (and hence is itself a group), it is easy to verify that

$$g \circ g^{-1} = e \in H, \tag{10.15}$$

$$g_1 \circ g_2^{-1} \in H \quad \Longrightarrow \quad (g_1 \circ g_2^{-1})^{-1} \in H, \tag{10.16}$$

and

$$g_1 \circ g_2^{-1} \in H, \quad g_2 \circ g_3^{-1} \in H \quad \Longrightarrow \quad (g_1 \circ g_2^{-1}) \circ (g_2 \circ g_3^{-1}) = g_1 \circ g_3^{-1} \in H. \tag{10.17}$$

Hence, $\sim$ satisfies the properties of an equivalence relation as defined in Section 1.4.3 since $g \sim g$ follows from (10.15), $g_1 \sim g_2 \Rightarrow g_2 \sim g_1$ follows from (10.16), and $g_1 \sim g_2$ and $g_2 \sim g_3$ implies $g_1 \sim g_3$ from (10.17). An analogous argument holds for left cosets with the equivalence relation defined as

$$g_1 \sim g_2 \Longleftrightarrow g_1^{-1} \circ g_2 \in H$$

instead of (10.14). Sometimes instead of the general $\sim$, the more specialized notation

$$g_1 \equiv g_2 \bmod H$$

is used to denote either of the equivalence relations above when "left" or "right" has been specified in advance.

Returning to the example of the group of symmetry operations of the equilateral triangle, the left cosets are

$$\begin{gathered}
H_1 = eH_1 = g_1 H_1 = g_2 H_1; \quad \{g_3, g_4, g_5\} = g_3 H_1 = g_4 H_1 = g_5 H_1. \\
H_2 = eH_2 = g_3 H_2; \quad \{g_1, g_4\} = g_1 H_2 = g_4 H_2; \quad \{g_2, g_5\} = g_2 H_2 = g_5 H_2. \\
H_3 = eH_3 = g_4 H_3; \quad \{g_2, g_3\} = g_2 H_3 = g_3 H_3; \quad \{g_1, g_5\} = g_1 H_3 = g_5 H_3. \\
H_4 = eH_4 = g_5 H_4; \quad \{g_1, g_3\} = g_1 H_4 = g_3 H_4; \quad \{g_2, g_4\} = g_2 H_4 = g_4 H_4.
\end{gathered}$$

The right cosets are

$$
\begin{aligned}
H_1 = H_1 e = H_1 g_1 = H_1 g_2; \quad \{g_3, g_4, g_5\} = H_1 g_3 = H_1 g_4 = H_1 g_5. \\
H_2 = H_2 e = H_2 g_3; \quad \{g_1, g_5\} = H_2 g_1 = H_2 g_5; \quad \{g_2, g_4\} = H_2 g_2 = H_2 g_4. \\
H_3 = H_3 e = H_3 g_4; \quad \{g_1, g_3\} = H_3 g_1 = H_3 g_3; \quad \{g_2, g_5\} = H_3 g_2 = H_3 g_5. \\
H_4 = H_4 e = H_4 g_5; \quad \{g_1, g_4\} = H_4 g_1 = H_4 g_4; \quad \{g_2, g_3\} = H_4 g_2 = H_4 g_3.
\end{aligned}
$$

10.1.6 Coset Spaces and Quotient Groups

For the moment, consider a finite group G with subgroup H. An important property of gH and Hg is that they have the same number of elements as H. Since the group is divided into disjoint cosets, each with the same number of elements, it follows that the number of cosets must divide without remainder the number of elements in the group. The set of all left (or right) cosets is called the left (or right) *coset space* and is denoted as G/H (or $H\backslash G$). The number of cosets is related to the number of elements in the group and subgroup by the equality

$$
|G/H| = |H\backslash G| = |G|/|H|. \tag{10.18}
$$

This result is called *Lagrange's theorem* [5].[6]

Returning to the example of the symmetry operations of the equilateral triangle, we have the set of left cosets (or left-coset space)

$$
\begin{aligned}
G_T/H_1 &= \{\{e, g_1, g_2\}, \{g_3, g_4, g_5\}\}, \\
G_T/H_2 &= \{\{e, g_3\}, \{g_1, g_4\}, \{g_2, g_5\}\}, \\
G_T/H_3 &= \{\{e, g_4\}, \{g_2, g_3\}, \{g_1, g_5\}\}, \\
G_T/H_4 &= \{\{e, g_5\}, \{g_1, g_3\}, \{g_2, g_4\}\}.
\end{aligned}
$$

The corresponding right-coset spaces $H\backslash G$ are

$$
\begin{aligned}
H_1\backslash G_T &= \{\{e, g_1, g_2\}, \{g_3, g_4, g_5\}\}, \\
H_2\backslash G_T &= \{\{e, g_3\}, \{g_1, g_5\}, \{g_2, g_4\}\}, \\
H_3\backslash G_T &= \{\{e, g_4\}, \{g_1, g_3\}, \{g_2, g_5\}\}, \\
H_4\backslash G_T &= \{\{e, g_5\}, \{g_1, g_4\}, \{g_2, g_3\}\}.
\end{aligned}
$$

From this example it is clear that $|H_i\backslash G_T| = |G_T/H_i| = |G_T|/|H_i|$. Note also that $G_T/H_1 = H_1\backslash G_T$, which follows from H_1 being a normal subgroup.

Other examples of coset spaces include $SO(3)/K_{\mathbf{n}} \cong SO(3)/SO(2) \cong S^2$. Additionally, the polar decomposition from the Appendix of Volume 1, $A = SQ$, which is equivalent to $AQ^{-1} = S$, can be viewed as defining a coset space $GL^+(N, \mathbb{R})/SO(N)$.

In general, it is possible to define an action of a group G on a left-coset space such that for any $g_1 \in G$ and $g_2H \in G/H$, $g_1 \cdot (g_2H) = (g_1 \circ g_2)H$. In the case when G acts transitively on G/H, then G/H is called a *homogeneous space*; that is, a homogeneous space is a special kind of coset space. A homogeneous space where $H \leq G$, both being connected Lie groups, is a Riemannian manifold.

[6] Although Lagrange's theorem is for finite groups in which it makes sense to count the number of group elements, the concept of a coset space holds more generally, and for Lie groups, Lagrange's theorem holds with $|\cdot|$ being interpreted as volume.

A special kind of homogeneous space $M = G/H$ for which a set of operations called *involutions* (or *involutive isometries*) exist is called a *globally symmetric space* if certain conditions are met. In particular, given points $x, p \in M$, an involution $in_p : M \to M$ is defined by the properties $in_p(p) = p$ and $in_p(in_p(x)) = x$, which, in addition, preserves the metric. Here, by definition, in_p is not allowed to be the identity map. If for each in_p it is the case that p is its only fixed point, then M is a globally symmetric space. In contrast, a locally symmetric space is one for which each mapping in_p need not be globally defined, but rather is defined on an open ball around p, such that $in_p : B_p \to B_p$. Either way, geodesics that pass through p are mapped into themselves with a reversal of direction, with preservation of sectional curvature on the domain where in_p is defined. A globally symmetric space is also a locally symmetric space. Examples of globally symmetric spaces include compact connected Lie groups and spheres in any dimension. Additionally, it can be shown that any Riemannian manifold that has constant sectional curvature is automatically a locally symmetric space.

When N is a normal subgroup, then the left- and right-coset spaces are the same: $G/N = N\backslash G$. Furthermore, it is possible to endow this coset space with a group operation as described in the theorem below:

Theorem 10.1 *(The Quotient Group).* *If $N \trianglelefteq G$, then the coset space G/N together with the binary operation $(g_1N)(g_2N) = (g_1 \circ g_2)N$ is a group (called the quotient group).*

See [8] or [12] for a proof.

The quotient G/N of two finite groups $N \triangleleft G$ will always will be smaller than G in the sense that $|G/N| = |G|/|N|$ from Lagrange's theorem, and for Lie groups, the dimension of G/N will be smaller than the dimension of G if $\dim(N) > 0$.

Again returning to the example of the symmetry operations of the equilateral triangle, the coset space G_T/H_1 (or $H_1\backslash G_T$) is therefore a group. The Cayley table for G_T/H_1 is

$\circ$	H_1	gH_1
H_1	H_1	gH_1
gH_1	gH_1	H_1

10.1.7 Double-Coset Decompositions

Let $H < G$ and $K < G$. Then for any $g \in G$, the set

$$HgK \doteq \{h \circ g \circ k | h \in H, k \in K\} \tag{10.19}$$

is called the *double coset* of H and K, and any $g' \in HgK$ (including $g' = g$) is called a *representative* of the double coset. Although a double-coset representative often can be described with two or more different pairs (h_1, k_1) and (h_2, k_2) so that $g' = h_1 \circ g \circ k_1 = h_2 \circ g \circ k_2$, g' is counted only once in HgK. Hence, $|HgK| \leq |G|$, and, in general, $|HgK| \neq |H| \cdot |K|$. In general, the set of all double cosets of H and K is denoted $H\backslash G/K$. Hence, we have the hierarchy $g \in HgK \in H\backslash G/K$. It can be shown that membership in a double coset is an equivalence relation; that is, G is partitioned into disjoint double cosets, and for $H < G$ and $K < G$, either $Hg_1K \cap Hg_2K = \emptyset$ or $Hg_1K = Hg_2K$.

10.1.8 Mappings Between Groups

Special kinds of mappings that transform elements of one group into elements in another play important roles in group theory. These are explained in the following subsections.

Homomorphisms

A *homomorphism* is a mapping from one group to a subset of another, $\phi : (G, \circ) \rightarrow (H, \hat{\circ})$, such that

$$\phi(g_1 \circ g_2) = \phi(g_1) \,\hat{\circ}\, \phi(g_2).$$

The values $\phi(g)$ for *all* $g \in G$ must be contained in a subset of H, but it is possible that elements of H exist for which there are no counterparts in G.

It follows immediately from this definition that $\phi(g) = \phi(g \circ e) = \phi(g) \,\hat{\circ}\, \phi(e)$, and so $\phi(e)$ must be the identity in H. Likewise, $\phi(e) = \phi(g \circ g^{-1}) = \phi(g) \,\hat{\circ}\, \phi(g^{-1})$, and so $(\phi(g))^{-1} = \phi(g^{-1})$. Thus, a homomorphism $\phi : G \rightarrow H$ maps inverses of elements in G to the inverses of their counterparts in H, and the identity of G is mapped to the identity in H.

For example, for any $A \in G < GL(n, \mathbb{R})$, the function $\phi(A) = |\det(A)|$ defines homomorphism $\phi : G \rightarrow (\mathbb{R}_{>0}, \cdot)$.

In general, a homomorphism will map more elements of G to the identity of H than just the identity. The set of all $g \in G$ for which $\phi(g) = \phi(e)$ is called the *kernel* of the homomorphism and is denoted as $Ker(\phi)$:

$$Ker(\phi) \doteq \{g \in G \mid \phi(g) = \phi(e)\}.$$

It is easy to see from the definition of homomorphism that if $g_1, g_2 \in Ker(\phi)$, then so are their inverses and products. Thus, $Ker(\phi)$ is a subgroup of G, and, moreover, it is a normal subgroup because given any $g \in Ker(\phi)$ and $g_1 \in G$,

$$\phi(g_1^{-1} \circ g \circ g_1) = (\phi(g_1))^{-1} \,\hat{\circ}\, \phi(g) \,\hat{\circ}\, \phi(g_1) = (\phi(g_1))^{-1} \,\hat{\circ}\, \phi(g_1) = \phi(e);$$

that is, conjugation of $g \in Ker(\phi)$ by any $g_1 \in G$ results in another element in $Ker(\phi)$, and so $Ker(\phi)$ is a normal subgroup of G, which is written as $Ker(\phi) \trianglelefteq G$.

In general, a homomorphism $\phi : G \rightarrow H$ will map all the elements of G to some subset of H. This subset is called the *image* of the homomorphism, which is written as $Im(\phi) \subseteq H$. More specifically, since a homomorphism maps the identity of G to the identity of H, and inverses in G map to inverses in H, and for any $g_1, g_2 \in G$, it follows that $\phi(g_1) \,\hat{\circ}\, \phi(g_2) = \phi(g_1 \circ g_2) \in Im(\phi)$, therefore $Im(\phi)$ must be a subgroup of H. This is written as $Im(\phi) \leq H$. (Note also that if $K \leq G$, then the image of K in H under the homomorphism $\phi : G \rightarrow H$, restricted to elements of K, is also a subgroup of H.)

For example, if $G = GL^{+}(N, \mathbb{R})$ and $\phi(A) = |\det(A)|$ then $Im(\phi) = \mathbb{R}_{>0}$, and if $G = SO(N)$, then $Im(\phi) = \{1\}$ and both $(\mathbb{R}_{>0}, \cdot)$ and $(\{1\}, \cdot)$ are groups, where here $\cdot$ denotes scalar multiplication.[7]

Isomorphisms

A bijective homomorphism from G to H is called an *isomorphism.* When such an isomorphism exists between groups, the groups are called *isomorphic* to each other. If H and G are isomorphic, the notation $H \cong G$ is used. For example, the group of symmetry operations of the triangle, G_T, is isomorphic to the permutation group Π_3.

An isomorphism is a kind of equivalence relation. The following three theorems (written below as one theorem with three parts) are fundamental in group theory.

[7] The shorthand $|A|$ will be used frequently for $|\det(A)|$ when there is no confusion with the same notation used to denote the the number of elements in a set.

Theorem 10.2 *(The Isomorphism Theorems)***.** *Let G and H be groups with $S \leq G$, $N \trianglelefteq G$, $K \trianglelefteq G$, $K \leq N$, and $\phi : G \to H$ be a homomorphism. Then*

1. *$G/Ker(\phi) \cong Im(\phi) \leq H$;*
2. *$SN \leq G$, $S \cap N \trianglelefteq S$, and $(SN)/N \cong S/(S \cap N)$;*
3. *$N/K \trianglelefteq G/K$ and $(G/K)/(N/K) \cong G/N$.*

See [8] or [12] for a proof.

As an example of part 1, consider the group $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ consisting of the set of integers $\{0, 1, \ldots, n-1\}$ and operation of addition modulo n. Let $G = \mathbb{Z}_3$ and $H = G_T$ (the symmetry operations of the triangle). Then a homomorphism $\phi : \mathbb{Z}_3 \to G_T$ can be defined as $\phi(0) = e$, $\phi(1) = g_1$, and $\phi(2) = g_2$. In this case, $Ker(\phi) = \{0\}$, $G/Ker(\phi) = \mathbb{Z}_3/\{0\} = \mathbb{Z}_3 = G$, $Im(\phi) = H_1$. G and H_1 are isomorphic, and the mapping ϕ is the isomorphism between $\mathbb{Z}_3$ and H_1 (i.e., $\phi(\mathbb{Z}_3) = H_1$ and $\mathbb{Z}_3 = \phi^{-1}(H_1)$).

As another example of part 1, let $G = \mathbb{Z}_4$, $H = \mathbb{Z}_2$, and the homomorphism be defined as $\phi(g) = g \pmod 2$. Then $\phi(0) = 0 \pmod 2$, $\phi(1) = 1 \pmod 2$, and $\phi(2) = 2 = 0 \pmod 2$, and $\phi(3) = 3 = 1 \pmod 2$. Then $Ker(\phi) = \{0, 2\}$ and $Im(\phi) = \mathbb{Z}_2 = H$. The coset space $G/Ker(\phi) = \{\{0, 2\}, \{1, 3\}\}$ can be made into a group with operation defined by the rule $\{0, 2\} \circ \{0, 2\} = \{0, 2\}$, $\{0, 2\} \circ \{1, 3\} = \{1, 3\} \circ \{0, 2\} = \{1, 3\}$, and $\{1, 3\} \circ \{1, 3\} = \{0, 2\}$ and is isomorphic to $H = \mathbb{Z}_2$ under the correspondence $\{0, 2\} \leftrightarrow 0$ and $\{1, 3\} \leftrightarrow 1$.

As a demonstration of the second part, let $G = \mathbb{Z}_8$, $N = \{0, 2, 4, 6\} \triangleleft G$, $K = \{0, 4\} < N$. Then $N \cap K = K$ and $NK = N$ and $(NK)/N = N/N \cong \mathbb{Z}_1$. On the other hand, $K/(N \cap K) = K/K \cong \mathbb{Z}_1$, and so the second isomorphism theorem holds for this example.

To demonstrate the third part, using this same example, observe that $K = \{0, 4\} \triangleleft \mathbb{Z}_8 = G$, $N/K \cong \mathbb{Z}_2$, $G/K \cong \mathbb{Z}_4$, and $(G/K)/(N/K) \cong \mathbb{Z}_2$. Since $G/N \cong \mathbb{Z}_2$, the third isomorphism theorem is demonstrated

A common kind of isomorphism that is encountered in applications is from a group onto itself, $c_h : G \to G$, where c_h denotes conjugation:

$$c_h(g) \doteq h \circ g \circ h^{-1} \tag{10.20}$$

for some fixed $h \in G$. This is an isomorphism because it is a homomorphism (i.e., $c_h(g_1 \circ g_2) = c_h(g_1) \circ c_h(g_2)$) and it is invertible (i.e., $g = h^{-1} \circ c_h(g) \circ h$). There is one such conjugation mapping for each $h \in G$. Furthermore, it is possible to compose two conjugation mappings as

$$c_{h_1}(c_{h_2}(g)) = h_1 \circ (h_2 \circ g \circ h_2^{-1}) \circ h_1^{-1} = (h_1 \circ h_2) \circ g \circ (h_1 \circ h_2)^{-1} = c_{h_1 \circ h_2}(g).$$

Therefore, the set of conjugation mappings $C \doteq \{c_h \mid h \in G\}$ (with operation of composition) is isomorphic to $(G, \circ)$, which is written as $C \cong G$.

In contrast, the bijective maps $r_h : G \to G$ and $l_h : G \to G$ defined by

$$r_h(g) \doteq g \circ h^{-1} \quad \text{and} \quad l_h(g) \doteq h \circ g, \tag{10.21}$$

respectively, are *not* isomorphisms from G to G for each fixed h. This is because, in general, $r_h(g_1) \circ r_h(g_2) \neq r_h(g_1 \circ g_2)$, and similarly for l_h.

However, the set of all mappings of the form $R \doteq \{r_h \mid h \in G\}$ (with operation of composition) is isomorphic to G because

$$r_{h_1}(r_{h_2}(g)) = (g \circ h_2^{-1}) \circ h_1^{-1} = g \circ (h_2^{-1} \circ h_1^{-1}) = g \circ (h_1 \circ h_2)^{-1} = r_{h_1 \circ h_2}(g)$$

defines a homomorphism, $G \to R$, and the mapping $r_h : G \to G$ is bijective since g can be uniquely recovered from $r_h(g)$ by performing the computation $g = r_h(g) \circ h$, and so $r_h^{-1} = r_{h^{-1}}$ exists for each $h \in G$. Therefore, $R \cong G$. A similar calculation holds for l_h, and so $L \doteq \{l_h \mid h \in G\} \cong G$ also.

Automorphisms

An isomorphism of a group G onto itself is called an *automorphism*. Conjugation of all elements in a group by one fixed element is an example of an automorphism. The set of all automorphisms of G onto itself is denoted as $Aut(G)$. The group operation for $Aut(G)$ is the composition of any two individual automorphisms.

If $(H, \circ)$ and $(G, \hat{\circ})$ are two arbitrary groups and if there exists a homomorphism $\phi : H \to Aut(G)$, and each $\phi(h)$ for $h \in H$ is a mapping from G to G, which can be denoted as φ_h.

$$\varphi_{h_1}(\varphi_{h_2}(g)) \;=\; \varphi_{h_1 \circ h_2}(g) \;=\; \varphi_{h_1}(g) \,\hat{\circ}\, \varphi_{h_2}(g) \;\in\; G. \tag{10.22}$$

The identity element $\varphi_e \in Aut(G)$ has the property $\varphi_e(g) = g$ for every $g \in G$.

Generating New Mappings from Old Ones

Given two finite ordered sets X and Y, which contain $|X|$ and $|Y|$ elements, respectively, each $\pi \in \Pi_{|X|}$ and $\sigma \in \Pi_{|Y|}$ define natural maps $\pi : X \to X$ and $\sigma : Y \to Y$, respectively, according to the rule

$$\pi(x_i) = x_{\pi^{-1}(i)} \qquad \text{and} \qquad \pi(y_j) = y_{\sigma^{-1}(j)},$$

where $X = \{x_1, x_2, \ldots, x_{|X|}\}$ and $Y = \{y_1, y_2, \ldots, y_{|Y|}\}$. Given a mapping $m : X \to Y$, it is possible to compose this with the permutations to produce four new mappings:

$$\begin{tikzcd} X \arrow[r, "m"] \arrow[dr, "\sigma\circ m"'] & Y \arrow[d, "\sigma"] \\ & Y \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "\pi"] \arrow[dr, "m\circ\pi"'] & X \arrow[d, "m"] \\ & Y \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "\pi"] \arrow[dr, "\sigma\circ m\circ\pi"'] & X \arrow[d, "\sigma\circ m"] \\ & Y \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "m\circ\pi"] \arrow[dr, "\sigma\circ m\circ\pi"'] & Y \arrow[d, "\sigma"] \\ & Y \end{tikzcd} \tag{10.23}$$

These four planar triangular commutative diagrams can be assembled into a single spatial (tetrahedral) commutative diagram by matching together the edges and vertices in a consistent way. A projection of this diagram into the plane is

$$\begin{tikzcd} X \arrow[r, "m\circ\pi"] \arrow[d, "\pi"'] \arrow[dr] & Y \arrow[d, "\sigma"] \\ X \arrow[r, "\sigma\circ m"'] \arrow[ur, "m"] & Y \end{tikzcd}$$

where the unlabeled arrow corresponds to the function $(\sigma \circ m \circ \pi)(x) \doteq \sigma(m(\pi(x)))$.

If $(H, \circ)$ and $(K, \bullet)$ are groups and $\phi : H \to K$ is a homomorphism, then the above construction can be used to create new groups and homomorphisms because for any $h \in H$, $\sigma \in \Pi_{|K|}$, $\pi \in \Pi_{|H|}$, $\sigma(\phi(\pi(h))) \in K$, and for any $h_1, h_2 \in H$ and $\phi(h_1), \phi(h_2) \in K$, operations $\hat{\circ}$ and $\hat{\bullet}$ can be defined such that

$$\begin{aligned}\sigma(\phi(\pi(h_1)))\hat{\bullet}\sigma(\phi(\pi(h_2))) &= \sigma(\phi(\pi(h_1)) \bullet \phi(\pi(h_2))) \\ &= \sigma(\phi(\pi(h_1)\hat{\circ}\pi(h_2))) = \sigma(\phi(\pi(h_1 \circ h_2))).\end{aligned}$$

This is described by the commutative diagram

$$\begin{tikzcd}
(H, \hat{\circ}) \arrow[r, leftrightarrow] \arrow[d] \arrow[dr] & (H, \circ) \arrow[d, "\phi"] \arrow[dl, crossing over] \\
(K, \hat{\bullet}) \arrow[r, leftrightarrow] & (K, \bullet)
\end{tikzcd}$$

where unlabeled arrows denote new homomorphisms.

Functions

A function on a group is a mapping from the group into a field $\mathbb{F}$ (which can be thought of in the present context as being either $\mathbb{R}$ or $\mathbb{C}$). A field is, by definition, necessarily a group under the operation of addition: $(\mathbb{F}, +)$. Additionally, if the number 0 is removed, $(\mathbb{F} - \{0\}, \cdot)$ is a group where $\cdot$ denotes scalar multiplication. A function is denoted as $f : G \to \mathbb{F}$. In special cases, a function can also be a homomorphism between groups. However, generally this will not be how functions are viewed.

Given a function $f : G \to \mathbb{F}$, new functions can be defined either by using permutations in a manner similar to the above or by "shifting" the functions by a particular group element $h \in G$ as

$$(L_h f)(g) \doteq f(h^{-1} \circ g) \quad \text{and} \quad (R_h f)(g) \doteq f(g \circ h). \tag{10.24}$$

These new functions, which have interesting and useful properties, are not to be confused with the mappings in (10.21).

10.1.9 Products of Groups

Three different kinds of products of groups are defined in this subsection.

Direct Products

The *direct product* of two groups $(K, \circ)$ and $(H, \hat{\circ})$ is the group $(G, \odot) \doteq (K, \circ) \times (H, \hat{\circ})$ such that $G = K \times H$ (where here $\times$ denotes the Cartesian product), and for any two elements $g_1 = (k_1, h_1)$, $g_2 = (k_2, h_2) \in G$ the group operation is defined as $g_1 \odot g_2 \doteq (k_1 \circ k_2, h_1 \,\hat{\circ}\, h_2)$.

This is not the only kind of product that can be formed between two groups. Two more examples of products between groups are presented below.

Semi-direct Products

Let the group $(H, \circ)$ be a transformation group that acts on the set N where $(N, +)$ is itself an Abelian group. Then the *semi-direct product* of $(H, \circ)$ and $(N, +)$ is the new group formed by letting[8]

$$(N \times H, \hat{\circ}) \doteq (N, +) \rtimes (H, \circ) \doteq (H, \circ) \ltimes (N, +)$$

such that for any two elements $g_1 = (n_1, h_1)$, $g_2 = (n_2, h_2) \in N \times H$, the group operation is defined as $g_1 \hat{\circ} g_2 = (h_1 \cdot n_1 + n_2, h_1 \circ h_2) \in N \times H$, where $\cdot$ denotes the action of H on N. A shorthand for this in which the group operations are suppressed is $N \rtimes H$.

It can be shown that N always will be a normal subgroup of $N \rtimes H$:

$$N \lhd N \rtimes H.$$

In applications, one of the most important examples of this is the Euclidean motion group (also called the special Euclidean group):

$$SE(n) \doteq (\mathbb{R}^n, +) \rtimes SO(n).$$

Much more will be said about this later.

The concept of a semi-direct product can be made even more general. If $(H, \circ)$ and $(N, \bullet)$ are two arbitrary groups and if a homomorphism $\varphi : H \rightarrow Aut(N)$ exists, then a more general kind of semi-direct product can be defined using (10.22) as

$$(N \times H,\, \hat{\circ}) \doteq (N, \bullet) \rtimes_{\varphi} (H, \circ), \qquad \text{where} \qquad (n_1, h_1)\hat{\circ}(n_2, h_2) \doteq (n_1 \bullet \varphi_{h_1}(n_2), h_1 \circ h_2). \tag{10.25}$$

A specific example of this would be be when H and N are matrix groups of the same dimension, and so both $\bullet$ and $\circ$ reduce to the same operation of matrix multiplication. In this context, if $\varphi_h(n) \doteq hnh^{-1} \in N$, it can be used to define a semi-direct product. Examples of this are the special Euclidean and Galilean groups, as illustrated in the exercises.

Wreath Products

As another kind of product, consider the following. Given a finite group $(G, \circ)$, the Cartesian product of the set G with itself n times is denoted as

$$G^n = \underbrace{G \times \cdots \times G}_{n\ times}.$$

The *wreath product* of G and Π_n is the group $G \wr \Pi_n \doteq (G^n \times \Pi_n, \diamond)$, where the product of two elements in $G^n \times \Pi_n$ is defined as

$$(h_1, \ldots, h_n; \sigma) \diamond (g_1, \ldots, g_n; \pi) \doteq (h_1 \circ g_{\sigma^{-1}(1)}, \ldots, h_n \circ g_{\sigma^{-1}(n)}; \sigma\pi). \tag{10.26}$$

In summary, the concepts of cosets and quotients, homomorphisms and isomorphisms, and products of groups play central roles in group theory. Two general observations related to these concepts are as follows: (1) It can be shown that all Abelian (commutative) groups are isomorphic to those that are formed by direct products of the following Abelian groups: cyclic permutations, $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, and the group of planar rotations that acts transitively on the unit circle; (2) every finite group is isomorphic to a subgroup of a sufficiently large permutation group. A book devoted to the theory of

[8] Some books use $N \ltimes H$ instead of $N \rtimes H$ to denote the semi-direct product.

finite groups would be concerned with the careful proof of such statements. However, the purpose of this section in the current context is as "cultural background." In fact, very little will be done with finite groups in this book. Lie groups are of interest inasmuch as they are a continuous domain (i.e., locally like $\mathbb{R}^n$) on which stochastic flows can evolve. The remaining sections of this chapter as well as the following two chapters are concerned with the analytic and geometric properties of Lie groups.

10.2 Matrix Lie Groups and Lie Algebras

In this section a very important kind of group is examined. These are the matrix Lie groups. A *matrix Lie group* $(G, \circ)$ is a group for which the set G is an analytic manifold[9] for which each $g \in G$ is an $N \times N$ matrix, the group operation $\circ$ is matrix multiplication, and the mappings $a(g_1, g_2) = g_1 \circ g_2$ and $b(g) = g^{-1}$ are both *analytic.*[10] The dimension of a Lie group is the dimension of the associated manifold G, which is different than the dimension of the matrices $g \in G \subset \mathbb{R}^{N \times N}$. Every matrix Lie group considered in this book is a subgroup of $GL(N, \mathbb{R})$ or $GL(N, \mathbb{C})$ for some $N \in \{2, 3, \ldots\}$. When referring to Lie groups throughout this book, what will be meant is matrix Lie groups. Even more specifically, connected matrix Lie groups will be the ones of most relevance to applications. For the most part, the scope will be limited to subgroups of the group $GL^+(N, \mathbb{R})$.

Since the condition that distinguishes $GL^+(N, \mathbb{R})$ is the positivity of the determinant of its elements, the determinant-trace formula (A.77) of Volume 1 gives a hint that the matrix exponential of other $N \times N$ matrices, which need not be invertible, will be a way to produce elements of $GL^+(N, \mathbb{R})$.

Given a matrix Lie group, elements sufficiently close to the identity are written as $g(t) = e^{tX}$ for some $X \in \mathcal{G}$ (the set $\mathcal{G}$ is called the *(matrix) Lie algebra* of G) and t near 0. Elements of $\mathcal{G}$ can be obtained by taking the matrix logarithm of elements of G. For matrix Lie groups, the corresponding Lie algebra is denoted with lowercase letters. For example, the Lie algebras of the groups $GL(N, \mathbb{R})$, $SO(N)$, and $SE(N)$ are respectively denoted as $gl(N, \mathbb{R})$, $so(N)$, and $se(N)$.

10.2.1 A Usable Definition of Matrix Lie Groups

It was stated earlier that a Lie group $(G, \circ)$ is a special kind of group in which the set G is a manifold and the operations of composition, $(g_1, g_2) \to g_1 \circ g_2$ and inversion $g \to g^{-1}$ are analytic.[11] This somewhat abstract definition can be made very concrete in the context of the special kind of Lie groups discussed in this book (i.e., matrix Lie groups). Let $g = g(\mathbf{q}) = [g_{ij}(\mathbf{q})]$ be a parameterization of the matrix Lie group G, where $\mathbf{q} \in D \subset \mathbb{R}^n$. Each matrix entry $g_{ij}(\mathbf{q})$ for $i, j = 1, \ldots, N$ is an analytic real-valued

[9] The concept of an analytic manifold was defined in Chapter 7.

[10] This means that viewing g, g_1, g_2 as $N \times N$ matrices, a convergent Taylor series can also be defined for the functions $a : \mathbb{R}^{N \times N} \times \mathbb{R}^{N \times N} \to \mathbb{R}^{N \times N}$ and $b : \mathbb{R}^{N \times N} \to \mathbb{R}^{N \times N}$.

[11] Recall that an analytic function is one which can, at any point in its domain, be expanded in a convergent Taylor series. Hence, all of its derivatives exist and an analytic function is therefore smooth, but the converse is not always true. This highly technical distinction is often blurred, and the substitution of "smooth" for "analytic" has few, if any, consequences in applications.

function.[12] The smoothness of the group operation means that given any two elements $g_1 = g(\mathbf{q})$ and $g_2 = g(\mathbf{q}')$, then $g_1 \circ g_2 = g(\mathbf{p}(\mathbf{q}, \mathbf{q}'))$ with the vector-valued function $\mathbf{p}(\mathbf{q}, \mathbf{q}')$ being smooth (infinitely differentiable) in both $\mathbf{q}$ and $\mathbf{q}'$. Similarly, the smoothness of the inversion operation means that when writing $[g(\mathbf{q})]^{-1} = g(\mathbf{v}(\mathbf{q}))$ the vector-valued function $\mathbf{v}(\mathbf{q})$ is smooth.

Example 1: $\boldsymbol{GL(2, \mathbb{R})}$
If $G = GL(2, \mathbb{R})$, group elements and their inverses are of the form

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{and} \quad A^{-1} = \frac{1}{a_{11}a_{22} - a_{12}a_{21}} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

In this case, the parameter vector is $\mathbf{q} = [a_{11}, a_{12}, a_{21}, a_{22}]^T$ and $D \subset \mathbb{R}^4$ is defined by the condition that $a_{11}a_{22} - a_{12}a_{21} \neq 0$. The product of two group elements is simply matrix multiplication, and so

$$\mathbf{p}(\mathbf{q}, \mathbf{q}') = \begin{pmatrix} a_{11}a'_{11} + a_{12}a'_{21} \\ a_{11}a'_{12} + a_{12}a'_{22} \\ a_{21}a'_{11} + a_{22}a'_{21} \\ a_{21}a'_{12} + a_{22}a'_{22} \end{pmatrix}.$$

Clearly, this is infinitely differentiable with respect to any a_{ij} and any a'_{ij}. Similarly, using the classical quotient rule for the derivative, the expression for each entry in A^{-1},

$$\mathbf{v}(\mathbf{q}) = \frac{1}{a_{11}a_{22} - a_{12}a_{21}} \begin{pmatrix} a_{22} \\ -a_{12} \\ -a_{21} \\ a_{11} \end{pmatrix},$$

is infinitely differentiable as long as $|A| \neq 0$.

Example 2: $\boldsymbol{SE(2)}$
As a second example, the group $SE(2)$ with elements of the form

$$g(x, y, \theta) = \begin{pmatrix} \cos\theta & -\sin\theta & x \\ \sin\theta & \cos\theta & y \\ 0 & 0 & 1 \end{pmatrix}$$

and operation of matrix multiplication of two such group elements $g(x, y, \theta)$ and $g(x', y', \theta')$ is a Lie group because the parameter vector $\mathbf{q} = [x, y, \theta]^T$ gives

$$\mathbf{p}(\mathbf{q}, \mathbf{q}') = \begin{pmatrix} x'\cos\theta - y'\sin\theta + x \\ x'\sin\theta + y'\cos\theta + y \\ \theta + \theta' \end{pmatrix}$$

and inversion gives

$$\mathbf{v}(\mathbf{q}) = \begin{pmatrix} -x\cos\theta - y\sin\theta \\ x\sin\theta - y\cos\theta \\ -\theta \end{pmatrix}.$$

Both of these are infinitely differentiable vector-valued functions with respect to their arguments.

[12] The extension to the case of complex-valued matrices can be made easily, but the discussion here is restricted to the real case. This can be done without loss of generality for reasons discussed in Appendix A.8 in Volume 1.

10.2.2 Broad Classes of Matrix Lie Groups

A number of (matrix) Lie groups have already been discussed, including $GL(N,\mathbb{F})$, $GL^+(N,\mathbb{R})$, $SL(N,\mathbb{F})$, $U(N)$, and $SO(N)$.

Additional examples of Lie groups which act on $\mathbb{R}^N$ are as follows:

1. The group $SO(p,q)$ consists of all $N \times N$ real matrices ($N = p+q$) with unit determinant that preserve the matrix
$$I(p,q) = \begin{pmatrix} \mathbb{I}_p & \mathbb{O}_{p\times q} \\ \mathbb{O}_{q\times p} & -\mathbb{I}_q \end{pmatrix}, \tag{10.27}$$
where $\mathbb{I}_p$ is the $p \times p$ identity matrix and $\mathbb{O}_{p\times q}$ is the $p \times q$ zero matrix—that is, $Q \in SO(p,q)$ satisfies
$$Q^T I(p,q) Q = I(p,q).$$
$SO(p,q)$ is an $N(N-1)/2$-dimensional Lie group. The corresponding Lie algebra is denoted $so(p,q)$.
2. The scale-Euclidean (or similitude) group, $SIM(N)$, which consists of all pairs $(e^a R, \mathbf{b})$, where $a \in \mathbb{R}$, $R \in SO(N)$, and $\mathbf{b} \in \mathbb{R}^N$, has the group operation $g_1 \circ g_2 = (e^{a_1+a_2} R_1 R_2, R_1\mathbf{b}_2 + \mathbf{b}_1)$ and acts on $\mathbb{R}^N$ by translation, rotation, and dilation as $\mathbf{x}' = e^a R\mathbf{x} + \mathbf{b}$. It is a $(1 + N(N+1)/2)$-dimensional Lie group, with corresponding Lie algebra $sim(N)$.
3. The group $\mathbb{R}^N \rtimes GL^+(N,\mathbb{R})$, which is the set of all pairs $g = (e^a L, \mathbf{b})$ for $\mathbf{b} \in \mathbb{R}^N$, $a \in \mathbb{R}$, and $L \in SL(N,\mathbb{R})$, acts on objects in $\mathbb{R}^N$ by translation, rotation, shear, stretch, and dilation. In short, this is the most general type of deformation of Euclidean space which transforms all parallel lines into parallel lines and preserves orientation. This group is $N(N+1)$-dimensional.

Other examples will be presented in later sections in detail. However, first, the general important properties shared by all Lie groups are reviewed.

10.2.3 The Exponential and Logarithm Maps

Given a general matrix Lie group, elements sufficiently close to the identity are written as $g = \exp(X)$ for some $X \in \mathcal{G}$ (the Lie algebra of G) with $\|X\| \ll 1$. The general concept of a Lie algebra was defined in the appendix of Volume 1. Here, the matrix Lie algebra $\mathcal{G}$ can be thought of as the set of all matrices $\{X\}$ (not only ones for which $\|X\| \ll 1$) such that the exponential of each X results in an element of G. As mentioned earlier, in the case in which G is a specific matrix Lie group such as $GL(N,\mathbb{R})$, $SO(N)$, or $SE(N)$, then the corresponding Lie algebra would be denoted as $gl(N,\mathbb{R})$, $so(N)$, or $se(N)$, respectively.

Explicitly, in the context of matrix Lie groups (which are the only Lie groups considered here), the exponential map is simply the matrix exponential[13]
$$\exp(X) = \sum_{k=0}^{\infty} \frac{X^k}{k!}. \tag{10.28}$$

[13] The symbols X, Y, Z, and $X_1, X_2, \ldots, X_n$ will be used to denote generic elements of the Lie algebra $\mathcal{G}$, which is a vector space. The notation $\{E_i\}$ is used to denote a "natural" basis for this vector space that is "most analogous" to the natural basis $\{\mathbf{e}_i\}$ in $\mathbb{R}^n$.

The matrix logarithm is defined by the Taylor series about the identity matrix:

$$\log(g) = \log(\mathbb{I} + (g - \mathbb{I})) = \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(g - \mathbb{I})^k}{k}. \tag{10.29}$$

For matrix Lie groups, operations such as $g - \mathbb{I}$ and division of g by a scalar are well defined.

The exponential map takes an element of the Lie algebra and produces an element of the Lie group. This is written as

$$\exp : \mathcal{G} \to G.$$

The logarithm does just the opposite:

$$\log : G \to \mathcal{G}.$$

In other words, $\log(\exp X) = X$ and $\exp(\log(g)) = g$. Additionally, although it is possible to exponentiate any element of a Lie algebra, the logarithm is only defined in a ball around the identity element of G. In some cases, this ball extends over the whole of G, or up to G minus a set of measure zero, but, in general, caution must be exercised in the application of the logarithm.

If $g, h \in G$, then $g \circ h \in G$, and if $X, Y \in \mathcal{G}$, then $X + Y \in \mathcal{G}$. Since g, h, X, and Y are all matrices of the same dimension, they can be multiplied in any way. For example, gX, XY, and XhY are all valid. However, the result usually will not be in G or in $\mathcal{G}$. However, as it turns out, matrix products such as gXg^{-1}, $h^{-1}Xh$, and gYg^{-1} are in $\mathcal{G}$. In order to be consistent with notation, when multiplying two elements of G, the $\circ$ will be kept (even though it is just matrix multiplication). However, $\circ$ will not be used for matrix products between Lie algebra basis elements or between group elements and Lie algebra basis elements.

Every element in the neighborhood of the identity of a connected matrix Lie group G can be described with the exponential parameterization

$$g = g(x_1, x_2, \ldots, x_n) = \exp\left(\sum_{i=1}^{n} x_i E_i\right) \tag{10.30}$$

where n is the dimension of the group and $\{E_i\}$ is a basis for $\mathcal{G}$ which is orthonormal with respect to a given inner product. For some Lie groups, the exponential parameterization extends over the whole group.

For example, consider the so-called "$ax + b$ group," or affine group of the line, which can be viewed as the set of all matrices of the form

$$g(a, b) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, \quad \text{where } (a, b) \in \mathbb{R}_{>0} \times \mathbb{R}.$$

This group acts on the real line as

$$\begin{pmatrix} x' \\ 1 \end{pmatrix} = g(a, b) \begin{pmatrix} x \\ 1 \end{pmatrix};$$

that is, $x' = ax + b$ (hence the name).

A basis for the Lie algebra of this group is

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \qquad E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

An inner product can be defined in which this basis is orthonormal. The exponential map for this group is

$$\exp\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} e^x & \left(\frac{e^x - 1}{x}\right) y \\ 0 & 1 \end{pmatrix}.$$

10.2.4 The $\vee$ Operator

For any Lie algebra, the "vee" operator, $\vee$, is defined such that

$$\left(\sum_{i=1}^{n} x_i E_i\right)^{\vee} \doteq \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix}. \tag{10.31}$$

It is defined so that the following diagram commutes:

$$\begin{tikzcd} X, Y \in \mathcal{G} \arrow[r, "\vee"] \arrow[dr, "(X,Y)"'] & \mathbf{x}, \mathbf{y} \in \mathbb{R}^n \arrow[d, "\mathbf{x}\cdot\mathbf{y}"] \\ & \mathbb{R} \end{tikzcd} \tag{10.32}$$

where (X, Y) is an inner product for $\mathcal{G}$.

This notation is a generalization of that used in [16] in the context of the group of rigid-body motions, which has been studied extensively in kinematics and robotics [1, 6, 14, 18]. In the case of the $ax + b$ group, $(xE_1 + yE_2)^\vee = [x, y]^T$.

The vector $\mathbf{x} \in \mathbb{R}^n$ in (10.31) can be obtained from $g \in G$ from the formula

$$\mathbf{x} = (\log g)^\vee. \tag{10.33}$$

In the case of the $ax + b$ group, this means solving the equations $a = e^x$ and $b = (e^x - 1)y/x$ for x and y in terms of a and b.

In general, given any smooth curve $g(t) \in G$, it can be shown that

$$\boxed{g^{-1}\frac{dg}{dt} \in \mathcal{G} \quad \text{and} \quad \frac{dg}{dt}g^{-1} \in \mathcal{G}.} \tag{10.34}$$

Therefore,

$$\left(g^{-1}\frac{dg}{dt}\right)^\vee \quad \text{and} \quad \left(\frac{dg}{dt}g^{-1}\right)^\vee \in \mathbb{R}^n.$$

This fact will be quite important in all that follows.

10.2.5 The Adjoint Operator $Ad(g)$

The *adjoint* operator is defined as

$$\boxed{Ad(g_1)X \doteq \frac{d}{dt}\left(g_1 \circ e^{tX} \circ g_1^{-1}\right)\Big|_{t=0} = \frac{d}{dt}\exp(t g_1 X g_1^{-1})\Big|_{t=0} = g_1 X g_1^{-1}.} \tag{10.35}$$

This gives a homomorphism $Ad : G \to GL(\mathcal{G})$ from the group into the set of all invertible linear transformations of $\mathcal{G}$ onto itself. It is a homomorphism because

$$Ad(g_1)Ad(g_2)X = g_1(g_2 X g_2^{-1})g_1^{-1} = (g_1 \circ g_2)X(g_1 \circ g_2)^{-1} = Ad(g_1 \circ g_2)X.$$

It is linear because

$$\begin{aligned} Ad(g)(c_1X_1 + c_2X_2) &= g(c_1X_1 + c_2X_2)g^{-1} = c_1gX_1g^{-1} + c_2gX_2g^{-1} \\ &= c_1Ad(g)X_1 + c_2Ad(g)X_2. \end{aligned}$$

For example, in the case of the $ax + b$ group,

$$Ad(g)E_1 = gE_1g^{-1} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -b \\ 0 & 0 \end{pmatrix} = E_1 - bE_2$$

and

$$Ad(g)E_2 = gE_2g^{-1} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/a & -b/a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} = aE_2.$$

10.2.6 The Lie Bracket and $ad(X)$

In the special case of a 1-parameter subgroup when $g = g(t)$ is an element close to the identity,[14] we can approximate $g(t) \approx I + tX$ for small t. Then we get $Ad(I + tX)Y = Y + t(XY - YX)$. The following definitions of $ad(X)$ and $[X, Y]$ are useful:

$$ad(X)Y \doteq \frac{d}{dt}\left(Ad(e^{tX})Y\right)\Big|_{t=0} \tag{10.36}$$

and

$$[X, Y] \doteq ad(X)Y = XY - YX. \tag{10.37}$$

The term $[X, Y]$ is called the *Lie bracket* of the elements $X, Y \in \mathcal{G}$. The $ad(X)$ in (10.36) is also called the adjoint. From this definition, it follows that the two adjoints $ad(X)$ and $Ad(g)$ are related as

$$\boxed{Ad(\exp tX) = \exp(t \cdot ad(X)).} \tag{10.38}$$

When $t = 1$, the equality in (10.38) is visualized graphically with the commutative diagram

$$\begin{tikzcd} \mathcal{G} \arrow[r, "\exp"] \arrow[d, "ad"'] & G \arrow[d, "Ad"] \\ ad(\mathcal{G}) \arrow[r, "\exp"'] & Ad(G) \end{tikzcd}$$

It is clear from the definition in (10.37) that the Lie bracket is linear in each entry:

$$[c_1X_1 + c_2X_2, Y] = c_1[X_1, Y] + c_2[X_2, Y]$$

[14] In the context of matrix Lie groups, one natural way to measure distance is as a matrix norm of the difference of two group elements.

and

$$[X, c_1Y_1 + c_2Y_2] = c_1[X, Y_1] + c_2[X, Y_2].$$

Furthermore, the Lie bracket is antisymmetric:

$$[X, Y] = -[Y, X], \tag{10.39}$$

and hence $[X, X] = 0$. Given a basis $\{E_1, \ldots, E_n\}$ for the matrix Lie algebra $\mathcal{G}$, any arbitrary element can be written as

$$X = \sum_{i=1}^{n} x_i E_i.$$

The Lie bracket of any two elements will result in a linear combination of all basis elements. This is written as

$$\boxed{[E_i, E_j] = \sum_{k=1}^{n} C_{ij}^k E_k.} \tag{10.40}$$

The constants C_{ij}^k are called the *structure constants* of the Lie algebra $\mathcal{G}$. Note that the structure constants are anti-symmetric: $C_{ij}^k = -C_{ji}^k$. Their particular values depend both on the choice of basis used and the ordering of the basis elements, and so it would make sense to write $C_{ij}^k = C_{ij}^k(E_1, \ldots, E_n)$, although this dependence is usually suppressed once the choice of a basis and the ordering of its elements are fixed.

It can be checked that for any three elements of the Lie algebra, the *Jacobi identity* is satisfied:

$$[X_1, [X_2, X_3]] + [X_2, [X_3, X_1]] + [X_3, [X_1, X_2]] = 0. \tag{10.41}$$

As a result of the Jacobi identity, $ad(X)$ satisfies

$$ad([X, Y]) = ad(X)\ ad(Y) - ad(Y)\ ad(X).$$

10.2.7 The Baker–Campbell–Hausdorff Formula

Given any two elements of a matrix Lie algebra, X and Y, the Lie bracket was defined earlier as $[X, Y] = XY - YX$. An important relationship called the *Baker–Campbell–Hausdorff formula* exists between the Lie bracket and matrix exponential (see [4, 7, 11])—namely the logarithm of the product of two Lie group elements written as exponentials of Lie algebra elements can be expressed as

$$Z(X, Y) \doteq \log(e^X e^Y).$$

By introducing the function

$$F(x) \doteq \frac{\log x}{x - 1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k + 1}(x - 1)^k$$

and evaluating it with exponentiated adjoint operators (which are defined by Taylor series in analogy with the definition of the matrix exponential), it can be shown that [13]

$$Z(X, Y) = Y + \int_0^1 F(\exp(t\, ad(X)) \exp(ad(Y)))X dt.$$

Substituting into the Taylor series for $F(x)$ and integrating term by term then gives

$$\begin{aligned} Z(X,Y) = & X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}([X,[X,Y]] + [Y,[Y,X]]) \\ & + \frac{1}{48}([Y,[X,[Y,X]]] + [X,[Y,[Y,X]]]) + \cdots . \end{aligned} \tag{10.42}$$

This expression is verified by expanding e^X and e^Y in the Taylor series of the form in (10.28) and then substituting the result into (10.29) with $g = e^X e^Y$ to obtain $Z(X,Y)$.

10.3 Change of Basis in a Matrix Lie Algebra

A Lie algebra is a vector space, and as with any vector space, the basis is not unique. This section addresses how quantities such as Lie brackets and structure constants change with a change in the choice of basis for the case of a matrix Lie algebra.

10.3.1 General Change of Basis

As is true with any vector space, the choice of basis is not unique. Given a basis for a matrix Lie algebra, $X_1, \ldots, X_n \in \mathcal{G}$, it is always possible to define new basis elements $Y_i = \sum_{j=1}^{n} a_{ij} X_j$, where $A = [a_{ij}] \in GL(n, \mathbb{R})$. The question then becomes how the structure constants and various functions of the structure constants are changed under this change of basis.

Using the notation $A^{-1} = [a_{ij}^{-1}]$, it follows that $X_i = \sum_{j=1}^{n} a_{ij}^{-1} Y_j$. Letting the structure constants in the basis $Y_1, \ldots, Y_n$ be denoted $C_{ij}^k(A)$ with $C_{ij}^k(\mathbb{I}) = C_{ij}^k$ being those defined with respect to the natural orthonormal basis $X_1, \ldots, X_n$, it becomes immediately clear that, on the one hand,

$$[Y_i, Y_j] = \sum_{k=1}^{n} C_{ij}^k(A) Y_k = \sum_{k=1}^{n} C_{ij}^k(A) \sum_{j=1}^{n} a_{ij} X_j$$

and, on the other hand,

$$\begin{aligned} [Y_i, Y_j] &= \left[\sum_{k=1}^{n} a_{ik} X_k, \sum_{l=1}^{n} a_{jl} X_l \right] \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ik} a_{jl} [X_k, X_l] \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ik} a_{jl} \sum_{m=1}^{n} C_{kl}^m X_m \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} \sum_{m=1}^{n} a_{ik} a_{jl} C_{kl}^m \sum_{p=1}^{n} a_{mp}^{-1} Y_p \\ &= \sum_{p=1}^{n} \left(\sum_{k=1}^{n} \sum_{l=1}^{n} \sum_{m=1}^{n} a_{ik} a_{jl} C_{kl}^m a_{mp}^{-1} \right) Y_p . \end{aligned}$$

Thus,

$$C_{ij}^p(A) = \sum_{k=1}^{n} \sum_{l=1}^{n} \sum_{m=1}^{n} a_{ik} a_{jl} C_{kl}^m a_{mp}^{-1} . \tag{10.43}$$

This relationship is invertible because interchanging the roles of $C_{ij}^{k}(A)$ and $C_{ij}^{k}(\mathbb{I})$ and using A^{-1} as the transformation matrix from basis $\{Y_i\}$ to basis $\{X_i\}$ gives

$$C_{ij}^{p} = \sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n} a_{ik}^{-1} a_{jl}^{-1} C_{kl}^{m}(A) a_{mp}. \tag{10.44}$$

The veracity of this expression can be observed by direct substitution of (10.44) into (10.43), and vice versa.

It follows from (10.43) that

$$\begin{aligned} C_{ji}^{p}(A) &= \sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n} a_{jk} a_{il} C_{kl}^{m} a_{mp}^{-1} \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n} a_{jl} a_{ik} C_{lk}^{m} a_{mp}^{-1} \\ &= -\sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n} a_{jl} a_{ik} C_{kl}^{m} a_{mp}^{-1} \\ &= -\sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n} a_{ik} a_{jl} C_{kl}^{m} a_{mp}^{-1} \\ &= -C_{ij}^{p}(A). \end{aligned}$$

The only thing that was used above was a change in the name of dummy variables of summation and the skew symmetry of the structure constants in the original basis. It also follows from the invertibility of (10.44) and (10.43) that if $C_{ij}^{k} = 0$ for all i, j, and k, then $C_{ij}^{k}(A) = 0$ for all i, j, and k, and vice versa. This makes perfect sense, because this is the necessary and sufficient condition for the Lie group to be Abelian, which is a property that should not depend on the choice of basis. In fact, other critical functions of the structure constants will also be invariant under a change of basis. This is explored more below.

10.3.2 Invariance of Functions of Structure Constants

Now, consider the following vector-valued function of the structure constants:

$$\mathbf{f}(C) = \sum_{i=1}^{n}\left(\sum_{j=1}^{n} C_{ij}^{j}\right)\mathbf{e}_i,$$

where $\{\mathbf{e}_i\}$ is the natural basis for $\mathbb{R}^n$. The vector $\mathbf{f}(C) \in \mathbb{R}^n$ has two interesting properties. First,

$$\|\mathbf{f}(C)\| = 0 \iff \|\mathbf{f}(C(A))\| = 0 \tag{10.45}$$

for any $A \in GL(n, \mathbb{R})$. Second, if $R \in SO(n)$, then

$$\|\mathbf{f}(C(R))\| = \|\mathbf{f}(C)\|. \tag{10.46}$$

These are both verified by evaluating $\sum_{j=1}^{n} C_{ij}^{j}(A)$ using (10.43):

$$\begin{aligned}\sum_{j=1}^{n} C_{ij}^{j}(A) &= \sum_{j=1}^{n}\sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n} a_{ik}a_{jl}C_{kl}^{m}a_{mj}^{-1} \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n} a_{ik}\left(\sum_{j=1}^{n} a_{mj}^{-1}a_{jl}\right)C_{kl}^{m} \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n}\sum_{m=1}^{n} a_{ik}\delta_{ml}C_{kl}^{m} \\ &= \sum_{k=1}^{n}\sum_{l=1}^{n} a_{ik}C_{kl}^{l} \\ &= \sum_{k=1}^{n} a_{ik}\left(\sum_{l=1}^{n} C_{kl}^{l}\right).\end{aligned}$$

Since the scalar quantities $\sum_{l=1}^{n} C_{kl}^{l}$ for $k = 1, \ldots, n$ are the entries of the vector $\mathbf{f}(C)$, expressions (10.45) and (10.46) follow from

$$\mathbf{f}(C(A)) = A\mathbf{f}(C). \tag{10.47}$$

In terms of components, (10.45) can be written as

$$\sum_{l=1}^{n} C_{kl}^{l} = 0 \Longleftrightarrow \sum_{l=1}^{n} C_{kl}^{l}(A) = 0 \tag{10.48}$$

10.3.3 Changes of Basis Due to Adjoint Action

The change of basis described in the previous subsection is completely general, with no relationship between the matrix A and the Lie group G resulting from exponentiating weighted sums of basis elements $X_i \in \mathcal{G}$. Furthermore, the fact that each X_i is a matrix was not used at all. In contrast, for any $g \in G$, the change of basis $X_i \to gX_i\,g^{-1}$ can be made. In this subsection, the special properties of this change of basis are examined.

Let $Y_i = gX_i\,g^{-1}$ for some fixed $g \in G$. The matrix $A = [a_{ij}]$ relating $\{X_i\}$ and $\{Y_i\}$ is then a function of g (i.e., $A = A(g)$ and $C_{ij}^{k}(A) = C_{ij}^{k}(A(g))$). The elements of the matrix $A(g)$ are computed explicitly as $a_{ij}(g) = (X_i,\, gX_j\,g^{-1})$.

Then, on the one hand,

$$[Y_i, Y_j] = \sum_{k=1}^{n} C_{ij}^{k}(A(g))Y_k = \sum_{k=1}^{n} C_{ij}^{k}(A(g))\,gX_k\,g^{-1} = g\left[\sum_{k=1}^{n} C_{ij}^{k}(A(g))X_k\right]g^{-1}$$

and, on the otherhand,

$$[Y_i, Y_j] = [gX_i\,g^{-1},\, gX_j\,g^{-1}] = g\,[X_i, X_j]\,g^{-1} = g\left[\sum_{k=1}^{n} C_{ij}^{k}X_k\right]g^{-1}.$$

This implies that

$$C_{ij}^{k}(A(g)) = C_{ij}^{k}(A(e)) = C_{ij}^{k}(\mathbb{I}) = C_{ij}^{k}.$$

Thus, the change of basis due to adjoint action is very special in that it preserves the value of each individual structure constant.

10.4 Inner Products on Matrix Lie Algebras

By equipping a matrix Lie algebra with an appropriate inner product, it becomes possible to compute many quantities of interest, including Jacobian matrices and components of vector fields.

10.4.1 Calculating Jacobians

Given a finite-dimensional matrix Lie group, an orthogonal basis for the corresponding (matrix) Lie algebra can always be found when an appropriate inner product is defined. Such a basis can be constructed by the Gram–Schmidt orthogonalization procedure starting with any Lie algebra basis (see Appendix A.1.4 of Volume 1).

An inner product between arbitrary elements of the Lie algebra, $Y = \sum_i y_i E_i$ and $Z = \sum_j z_j E_j$, can be defined such that

$$(Y, Z) \doteq \sum_{i=1}^{n} y_i z_i, \qquad \text{where} \qquad (E_i, E_j) = \delta_{ij}. \tag{10.49}$$

The basis $\{E_i\}$ is then orthonormal with respect to this inner product. *The definition of the inner product together with the constraint of orthonormality in (10.49) defines a metric tensor for the Lie group according to the procedure described below.* If $Y, Z \in \mathbb{R}^{N\times N}$ and if $(Y, Z)_W \doteq \text{tr}(YWZ^T)$ for some positive definite $W = W^T \in \mathbb{R}^{N\times N}$ then this defines an inner product. If W is fixed, it is always possible to find an orthonormal basis $\{E_i\}$. Alternatively, given any basis $\{X_i\}$, the orthogonality condition $(X_i, X_j)_{W'} = \delta_{ij}$ (which amounts to $N(N+1)/2$ constraints) can be satisfied by choosing the $N(N+1)/2$ free parameters that define W'.

Let $\mathbf{q} = [q_1, \ldots, q_n]^T$ be a column vector of local coordinates. Then $g(t) = \tilde{g}(\mathbf{q}(t))$ is a curve in G, where $\tilde{g} : \mathbb{R}^n \to G$ is the local parameterization of the Lie group G. Henceforth, the tilde will be dropped since it will be clear from the argument whether the function $g(t)$ or $g(\mathbf{q})$ is being referred to. The right-Jacobian matrix for an n-dimensional Lie group parameterized with local coordinates $q_1, \ldots, q_n$ is the matrix $J_r(\mathbf{q})$ that relates rates of change $\dot{\mathbf{q}}$ to $g^{-1}\dot{g}$ and likewise for $J_l(\mathbf{q})$ and $\dot{g}g^{-1}$, where a dot denotes d/dt. Specifically,

$$\dot{g}g^{-1} = \sum_j \omega_j^l E_j \qquad \text{and} \qquad \boldsymbol{\omega}^l = J_l(\mathbf{q})\dot{\mathbf{q}}$$

and

$$g^{-1}\dot{g} = \sum_j \omega_j^r E_j \qquad \text{and} \qquad \boldsymbol{\omega}^r = J_r(\mathbf{q})\dot{\mathbf{q}}.$$

In other words,

$$(\dot{g}g^{-1}, E_k) = \left(\sum_j \omega_j^l E_j, E_k\right) = \sum_j \omega_j^l \,(E_j, E_k) = \sum_j \omega_j^l \delta_{jk} = \omega_k^l.$$

The scalars ω_k^l can be stacked in an array to form the column vector $\boldsymbol{\omega}^l = [\omega_1^l, \omega_2^l, \ldots, \omega_n^l]^T$. Analogous calculations follow for the “r” case. This whole process is abbreviated with the “$\vee$” operation as

$$\boxed{\left(\dot{g}g^{-1}\right)^{\vee} = \boldsymbol{\omega}^l \qquad \text{and} \qquad \left(g^{-1}\dot{g}\right)^{\vee} = \boldsymbol{\omega}^r.} \tag{10.50}$$

Given an orthogonal basis $E_1, \ldots, E_n$ for the Lie algebra, projecting the left and right tangent operators onto this basis yields elements of the right- and left-Jacobian matrices[15]:

$$(J_r)_{ij} = \left(g^{-1}\frac{\partial g}{\partial q_j}, E_i\right) \quad \text{and} \quad (J_l)_{ij} = \left(\frac{\partial g}{\partial q_j}g^{-1}, E_i\right). \tag{10.51}$$

In terms of the $\vee$ operation this is written as

$$\left(g^{-1}\frac{\partial g}{\partial q_j}\right)^{\vee} = J_r(\mathbf{q})\,\mathbf{e}_j \quad \text{and} \quad \left(\frac{\partial g}{\partial q_j}g^{-1}\right)^{\vee} = J_l(\mathbf{q})\,\mathbf{e}_j.$$

As another abuse of notation, the distinction between $J(\mathbf{q})$ and $J(g(\mathbf{q}))$ can be blurred in both the left and right cases. Again, it is clear which is being referred to from the argument of these matrix-valued functions.

Note that $J_r(h \circ g) = J_r(g)$ and $J_l(g \circ h) = J_l(g)$. For the groups considered below, the parameterizations used extend over the whole group with singularities of measure zero.

Left- and right-invariant versions of the metric tensor are expressed as matrices using the Jacobians in (10.51) as

$$G_r(\mathbf{q}) = J_r^T(\mathbf{q})\,J_r(\mathbf{q}) \quad \text{and} \quad G_l(\mathbf{q}) = J_l^T(\mathbf{q})\,J_l(\mathbf{q}). \tag{10.52}$$

These depend on the basis $\{E_i\}$ used. Stated in a different way, they depend on the weighting matrix used to define the inner product on the Lie algebra.

Returning again to the example of the $ax + b$ group, a straightforward calculation shows that

$$J_r = \begin{pmatrix} 1/a & 0 \\ 0 & 1/a \end{pmatrix} \quad \text{and} \quad J_l = \begin{pmatrix} 1/a & 0 \\ -b/a & 1 \end{pmatrix}.$$

Note that

$$\det(J_r) = \frac{1}{a^2} \neq \det(J_l) = \frac{1}{a}.$$

10.4.2 Invariant Vector Fields

For an N-dimensional matrix Lie group, we denote two special kinds of vector fields as

$$V_l(g) = \sum_{i=1}^{n} v_i E_i g \quad \text{and} \quad V_r(g) = \sum_{i=1}^{n} v_i g E_i.$$

The subscripts of V denote on which side the Lie algebra basis element E_i appears. Here, $E_i g$ and $g E_i$ are simply matrix products and $\{v_i\}$ are real numbers.[16] For a vector field $V(g)$ on a matrix Lie group (which need not be left or right invariant), the left- and right-shift operations are defined as

$$L(h)V(g) = h\,V(g) \quad \text{and} \quad R(h)V(g) = V(g)\,h,$$

[15] The "l" and "r" convention used here for Jacobians and for vector fields is opposite that used in the mathematics literature. The reason for the choice made here is to emphasize the location of the "the most informative part" of the expression. In Jacobians, this is the location of the partial derivatives. In vector fields, this is where the components defining the field appear.

[16] We restrict the discussion to real vector fields.

where $h \in G$. Then it is clear that V_r is *left invariant* and V_l is *right invariant* in the sense that

$$L(h)V_r(g) = V_r(h \circ g) \quad \text{and} \quad R(h)V_l(g) = V_l(g \circ h).$$

This means that there are left- and right-invariant ways to extend the inner product $(\cdot, \cdot)$ on the Lie algebra over the whole group—namely for all $Y, Z \in \mathcal{G}$, we can define right and left inner products respectively as

$$(gY, gZ)_g^r \doteq (Y, Z) \quad \text{and} \quad (Yg, Zg)_g^l \doteq (Y, Z)$$

for any $g \in G$. In this way, the inner product of two invariant vector fields $Y_r(g)$ and $Z_r(g)$ (or $Y_l(g)$ and $Z_l(g)$) yields

$$((Y_r(g), Z_r(g))_g^r = ((Y_l(g), Z_l(g))_g^l = (Y, Z).$$

10.5 Adjoint Matrices and the Killing Form

This section introduces the concept of the Killing form and its relationship to adjoint matrices, thereby providing a linear-algebraic way to compute quantities used in the classification of Lie groups.

10.5.1 The Killing Form

A *bilinear form* $B(X, Y)$ for $X, Y \in \mathcal{G}$ is said to be *Ad*-invariant if

$$B(X, Y) = B(Ad(g)X, Ad(g)Y)$$

for any $g \in G$. In the case of real matrix Lie groups (and the corresponding Lie algebras), which are the ones of most interest in engineering applications, a symmetric ($B(X, Y) = B(Y, X)$) and invariant bilinear form, called the *Killing form* (named after Wilhelm Karl Joseph Killing), is defined as

$$\boxed{B(X, Y) \doteq \text{trace}(ad(X)\, ad(Y)).} \tag{10.53}$$

The Killing form is important in the context of harmonic analysis because the Fourier transform and inversion formula can be defined for large classes of groups that are defined by the behavior of their Killing form. The classification of Lie groups according to the properties of the Killing form is based on *Cartan's Criteria* (named after Elie Cartan, who also developed the theory of differential forms) [20]. For example, a Lie group is called *nilpotent* if $B(X, Y) = 0$ for all $X, Y \in \mathcal{G}$. A Lie group is called *solvable* if and only if for all $X, Y, Z \in \mathcal{G}$, the equality $B(X, [Y, Z]) = 0$ holds. *Semi-simple* Lie groups are those for which $B(X, Y)$ is nondegenerate (i.e., the determinant of the $n \times n$ matrix with elements $B(E_i, E_j)$ is nonzero, where $\{E_1, \ldots, E_n\}$ ($n \geq 2$) is a basis for $\mathcal{G}$). For example, the Heisenberg groups are nilpotent, the rotation groups are semi-simple, and the group of rigid-body motions of the plane is solvable (although for higher dimensions, it is not).

10.5.2 The Matrices of $Ad(g)$, $Ad^*(g)$, $ad(X)$, and $B(X,Y)$

The formal coordinate-independent definitions of the adjoints $Ad(g)$ and $ad(X)$ and the Killing form $B(X,Y)$ are central to the theory of Lie groups. Although such definitions are sufficient for mathematicians to prove many fundamental properties, it is useful for computation to have such concepts illustrated with matrices.

As with all linear operators, $Ad(g)$ and $ad(X)$ are expressed as matrices using an appropriate inner product and concrete basis for the Lie algebra. In particular, with the inner product defined earlier for Lie algebras, we have

$$[Ad(g)]_{ij} \doteq (E_i, Ad(g)E_j) = (E_i, gE_jg^{-1}) \tag{10.54}$$

and

$$[ad(X)]_{ij} \doteq (E_i, ad(X)E_j) = (E_i, [X, E_j]). \tag{10.55}$$

Another way to view these is by using the $\vee$ operator defined previously that converts Lie algebra basis elements E_i to elements of the natural basis element $\mathbf{e}_i \in \mathbb{R}^n$,

$$(E_i)^\vee = \mathbf{e}_i.$$

Then the matrix with elements given in (10.54) will be

$$[Ad(g)] = [(gE_1g^{-1})^\vee, \ldots, (gE_ng^{-1})^\vee].$$

As with the adjoint operator itself, this matrix representation satisfies

$$\boxed{[Ad(g_1)][Ad(g_2)] = [Ad(g_1 \circ g_2)].} \tag{10.56}$$

It is this matrix that relates left and right Jacobians. Using the $\vee$ notation, we may write

$$J_l = \left[\left(\frac{\partial g}{\partial x_1}g^{-1}\right)^\vee, \ldots, \left(\frac{\partial g}{\partial x_n}g^{-1}\right)^\vee\right]$$

and

$$J_r = \left[\left(g^{-1}\frac{\partial g}{\partial x_1}\right)^\vee, \ldots, \left(g^{-1}\frac{\partial g}{\partial x_n}\right)^\vee\right].$$

Since

$$\left(g\left(g^{-1}\frac{\partial g}{\partial x_1}\right)g^{-1}\right)^\vee = \left(\frac{\partial g}{\partial x_1}g^{-1}\right)^\vee,$$

it follows that

$$J_l = [Ad(g)]J_r.$$

Hence, if the Jacobians are known, we can write[17]

$$[Ad(g)] = J_l J_r^{-1}. \tag{10.57}$$

[17] When the context is clear, the distinction between $Ad(g)$ and $[Ad(g)]$ can be blurred. However, here, where the concepts are being explained for the first time, it is important to understand the difference.

Another related definition is[18]

$$[Ad^*(g_1)] \doteq [Ad(g_1)]^{-T}. \tag{10.58}$$

This so-called *co-adjoint* operator matrix has the property

$$\boxed{[Ad^*(g_1)][Ad^*(g_2)] = [Ad^*(g_1 \circ g_2)]}\,, \tag{10.59}$$

which looks similar to (10.56). In a sense, the reason for this is that the reversal of orders induced by the matrix inverse and the transpose cancel each other.

The matrix with elements given in (10.55) will be

$$[ad(X)] = [([X, E_1])^\vee, \ldots, ([X, E_n])^\vee].$$

This then gives a concrete tool with which to calculate the $n \times n$ matrix with entries

$$[B]_{ij} = B(E_i, E_j) = \mathrm{tr}([ad(E_i)][ad(E_j)]). \tag{10.60}$$

B is then degenerate if and only if

$$\det([B]) = 0.$$

If $\det([B]) \neq 0$, the Lie algebra is called *semi-simple*. If $[B]_{ij} = 0$ for all i and j, the Lie algebra is called *nilpotent*.

Returning again to the $ax + b$ group as an example, in this case

$$[Ad(g)] = \begin{pmatrix} 1 & 0 \\ -b & a \end{pmatrix}.$$

Similarly, the calculations

$$[X, E_1] = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -b \\ 0 & 0 \end{pmatrix}$$

and

$$[X, E_2] = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$$

are used together with the orthonormality of the basis to give

$$[ad(X)] = \begin{pmatrix} 0 & 0 \\ -b & a \end{pmatrix} \quad \text{and} \quad [B] = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

where the latter is computed from the former using (10.60).

Clearly, this is degenerate, and the $ax + b$ group is not semi-simple.

10.5.3 Relationship Between $ad(X)$ and $B(X, Y)$, and the Structure Constants

Recall that the structure constants of a real Lie algebra are defined by

$$[E_i, E_j] = \sum_{k=1}^{N} C_{ij}^k E_k.$$

[18] Given an invertible matrix A, the shorthand A^{-T} denotes $(A^{-1})^T = (A^T)^{-1}$.

From the anti-symmetry of the Lie bracket (10.39) and the Jacobi identity (10.41), respectively, we see that

$$C_{ij}^{k} = -C_{ji}^{k} \tag{10.61}$$

and

$$\sum_{j=1}^{N}(C_{ij}^{l}C_{km}^{j} + C_{mj}^{l}C_{ik}^{j} + C_{kj}^{l}C_{mi}^{j}) = 0. \tag{10.62}$$

The matrix entries of $[ad(E_k)]_{ij}$ are related to the structure constants as

$$[ad(E_k)]_{ij} = (E_i, [E_k, E_j]) = \left(E_i, \sum_{m=1}^{N} C_{kj}^{m} E_m\right).$$

For a real Lie algebra, the inner product

$$(X, Y) = \text{trace}(XWY^T)$$

is linear in Y, and so

$$[ad(E_k)]_{ij} = \sum_{m=1}^{N}(E_i, E_m)C_{kj}^{m} = C_{kj}^{i}.$$

Then

$$\begin{aligned} B(E_i, E_j) &= \text{trace}(ad(E_i)\, ad(E_j)) \\ &= \sum_{m=1}^{N}\sum_{n=1}^{N}[ad(E_i)]_{mn}[ad(E_j)]_{nm} \\ &= \sum_{m=1}^{N}\sum_{n=1}^{N} C_{in}^{m}C_{jm}^{n}. \end{aligned}$$

10.5.4 Conditions for Unimodularity

A Lie group for which $\det[Ad(g)] = 1$ for all $g \in G$ is called *unimodular.* Most of the groups that will arise in applications in this book are unimodular. In Chapter 12, the condition of unimodularity will be quite convenient when it comes to integration on certain Lie groups. In this subsection, several equivalent conditions for unimodularity are reviewed. These conditions can be stated in terms of the left and right Jacobians, which can be computed in any parameterization that covers the whole group manifold, or in terms of parameter-free descriptions based on properties of the Lie algebras corresponding to the groups.

Each of the following are necessary and sufficient conditions for a Lie group to be unimodular:[19]

$$\det J_r = \det J_l, \tag{10.63}$$

[19] Here, the determinant of an operator is defined as the determinant of the matrix of the operator. Henceforth, when it is clear from the context that the adjoint matrix is being discussed, the notation Ad (and ad) will be used in place of $[Ad]$ (and $[ad]$).

$$\det[Ad(g)] = 1, \tag{10.64}$$

$$\operatorname{tr}[ad(X)] = 0, \tag{10.65}$$

$$\sum_{k=1}^{n} C_{jk}^{k} = 0 \quad \text{for } j = 1, \ldots, n. \tag{10.66}$$

Conditions (10.63) and (10.64) are equivalent because $J_l = [Ad(g)]J_r$, and so $\det[Ad(g)] = 1$ iff $\det J_l = \det J_r$. Conditions (10.64) and (10.65) are equivalent due to the relationship $\exp[ad(X)] = [Ad(\exp X)]$ and the trace-determinant formula (A.77) of Volume 1.

Condition (10.66) is the same as (10.48) and results from an argument related to the invariance of the volume element to an orthogomal change of basis in the Lie algebra. Indeed, conditions (10.63)–(10.65) are invariant under such a change of basis.

10.6 Examples

When learning an abstract concept, it is important to explore examples to gain a full understanding. This section presents 10 examples of Lie groups, some described in multiple different parameterizations, to illustrate the general concepts and definitions presented so far.

10.6.1 The Heisenberg Nilpotent Group

The Heisenberg group is a famous group in physics. However, the reason for presenting it first is not because of its importance but rather because of its simplicity.

Definition and Parameterization

The Heisenberg group, $H(3)$, is defined by elements of the form

$$g(\alpha, \beta, \gamma) = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{where } \alpha, \beta, \gamma \in \mathbb{R} \tag{10.67}$$

and the operation of matrix multiplication. Therefore, the group law can be viewed in terms of parameters as[20]

$$g(\alpha_1, \beta_1, \gamma_1) \circ g(\alpha_2, \beta_2, \gamma_2) = g(\alpha_1 + \alpha_2, \beta_1 + \beta_2 + \alpha_1\gamma_2, \gamma_1 + \gamma_2).$$

The identity element is the identity matrix $g(0, 0, 0)$, and the inverse of an arbitrary element $g(\alpha, \beta, \gamma)$ is

$$g^{-1}(\alpha, \beta, \gamma) = g(-\alpha, \alpha\gamma - \beta, -\gamma).$$

[20] Here the operation $\circ$ is written explicitly, but it is common to suppress this for matrix groups and to denote the product simply by juxtaposing two group elements.

Lie Algebra and Exponential Map

Basis elements for the Lie algebra are

$$E_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \quad E_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \quad E_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}. \tag{10.68}$$

The Lie bracket, $[E_i, E_j] = E_i E_j - E_j E_i$, for these basis elements gives

$$[E_1, E_2] = [E_2, E_3] = 0 \quad \text{and} \quad [E_1, E_3] = E_2.$$

If the inner product for the Lie algebra spanned by these basis elements is defined as $(X, Y) = \mathrm{tr}(XY^T)$, then this basis is orthonormal: $(E_i, E_j) = \delta_{ij}$.

The group $H(3)$ is nilpotent because $(x_1E_1 + x_2E_2 + x_3E_3)^n = 0$ for all $n \geq 3$. As a result, the matrix exponential is a polynomial in the coordinates $\{x_i\}$:

$$\exp \begin{pmatrix} 0 & x_1 & x_2 \\ 0 & 0 & x_3 \\ 0 & 0 & 0 \end{pmatrix} = g(x_1, x_2 + \tfrac{1}{2}x_1x_3, x_3). \tag{10.69}$$

The parameterization in (10.67) can be viewed as the following product of exponentials:

$$g(\alpha, \beta, \gamma) = g(0, \beta, 0)g(0, 0, \gamma)g(\alpha, 0, 0) = \exp(\beta E_2)\exp(\gamma E_3)\exp(\alpha E_1).$$

The logarithm is obtained by solving for each x_i as a function of α, β, and γ. By inspection, this is $x_1 = \alpha$, $x_3 = \gamma$, and $x_2 = \beta - \alpha\gamma/2$. Therefore,

$$\log g(\alpha, \beta, \gamma) = \begin{pmatrix} 0 & \alpha & \beta - \alpha\gamma/2 \\ 0 & 0 & \gamma \\ 0 & 0 & 0 \end{pmatrix}.$$

Jacobians and Adjoints

The Jacobian matrices for this group can be computed in either parameterization. In terms of α, β, and γ,

$$\frac{\partial g}{\partial \alpha} = E_1; \quad \frac{\partial g}{\partial \beta} = E_2; \quad \frac{\partial g}{\partial \gamma} = E_3.$$

A straightforward calculation then gives

$$g^{-1}\frac{\partial g}{\partial \alpha} = E_1; \quad g^{-1}\frac{\partial g}{\partial \beta} = E_2; \quad g^{-1}\frac{\partial g}{\partial \gamma} = E_3 - \alpha E_2.$$

Therefore,

$$J_r(\alpha, \beta, \gamma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -\alpha \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad J_r^{-1}(\alpha, \beta, \gamma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}. \tag{10.70}$$

A similar calculation shows that

$$J_l(\alpha,\beta,\gamma) = \begin{pmatrix} 1 & 0 & 0 \\ -\gamma & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad J_l^{-1}(\alpha,\beta,\gamma) = \begin{pmatrix} 1 & 0 & 0 \\ \gamma & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{10.71}$$

The adjoint matrix, defined by $[Ad(g)]\mathbf{x} = (gXg^{-1})^\vee$, is computed by evaluating

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & x_1 & x_2 \\ 0 & 0 & x_3 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\alpha & \alpha\gamma - \beta \\ 0 & 1 & -\gamma \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & x_1 & -\gamma x_1 + x_2 + \alpha x_3 \\ 0 & 0 & x_3 \\ 0 & 0 & 0 \end{pmatrix}.$$

Therefore,

$$(gXg^{-1})^\vee = \begin{pmatrix} x_1 \\ -\gamma x_1 + x_2 + \alpha x_3 \\ x_3 \end{pmatrix} \quad \text{and} \quad [Ad(g(\alpha,\beta,\gamma))] = \begin{pmatrix} 1 & 0 & 0 \\ -\gamma & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}.$$

The fact that $\det[Ad(g)] = 1$ for all $g \in G$ indicates that this group is unimodular. This fact is independent of the parameterization. For example,

$$J_r(\mathbf{x}) = \begin{pmatrix} 1 & 0 & 0 \\ x_3/2 & 1 & -x_1/2 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad J_l(\mathbf{x}) = \begin{pmatrix} 1 & 0 & 0 \\ -x_3/2 & 1 & x_1/2 \\ 0 & 0 & 1 \end{pmatrix}. \tag{10.72}$$

Some properties of the matrix exponential parameterization for $H(3)$ are

$$J_r(\mathbf{x}) = J_r^{-1}(-\mathbf{x}) = J_l^{-1}(\mathbf{x}) = J_l(-\mathbf{x}) \quad \text{and} \quad J_r(\mathbf{x})\mathbf{x} = J_l(\mathbf{x})\mathbf{x} = \mathbf{x}. \tag{10.73}$$

It can be shown that

$$Ad(g(\mathbf{x})) = J_l(\mathbf{x})J_r^{-1}(\mathbf{x}) = [J_l(\mathbf{x})]^2 = J_l(2\mathbf{x}) = \begin{pmatrix} 1 & 0 & 0 \\ -x_3 & 1 & x_1 \\ 0 & 0 & 1 \end{pmatrix}. \tag{10.74}$$

10.6.2 The Group of Rigid-Body Motions of the Euclidean Plane, *SE*(2)

In the applications that follow in other chapters, the groups of rigid-body motions will play an important role. Here, the motion group of the plane is studied in detail.

Elements, Operation, and Action

The special Euclidean group $SE(2)$, that acts on the plane, $\mathbb{R}^2$, can be viewed as the set of matrices

$$g(x_1, x_2, \theta) = \begin{pmatrix} \cos\theta & -\sin\theta & x_1 \\ \sin\theta & \cos\theta & x_2 \\ 0 & 0 & 1 \end{pmatrix} \tag{10.75}$$

with group operation of matrix multiplication. The action of this group on the plane is defined as

$$g \cdot \mathbf{r} \doteq \begin{pmatrix} r_1\cos\theta - r_2\sin\theta + x_1 \\ r_1\sin\theta + r_2\cos\theta + x_2 \end{pmatrix}$$

for any $\mathbf{r} = [r_1, r_2]^T \in \mathbb{R}^2$. The action defined in this way is not simply matrix multiplication of g and $\mathbf{r}$ (which dimensionally would not make sense).

Parameterization and Jacobians in T-R Coordinates

Note that any planar rigid-body motion can be decomposed into the translation–rotation (T-R) product

$$g(x_1, x_2, \theta) = \exp(x_1 E_1 + x_2 E_2)\exp(\theta E_3),$$

where

$$E_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \quad E_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}; \quad E_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Using the weighting matrix

$$W = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix},$$

the inner product $(X, Y) = \frac{1}{2}\mathrm{tr}(XWY^T)$, the basis $\{E_i\}$ for the Lie algebra $se(2)$ is orthogonal: $(E_i, E_j) = \delta_{ij}$. The Lie algebra $se(2)$ corresponds to rigid-body velocities in the plane.

The Jacobians for this parameterization, basis, and weighting matrix are then of the form

$$J_r = \left[\left(\frac{\partial g}{\partial x_1} g^{-1}\right)^\vee, \ \left(\frac{\partial g}{\partial x_2} g^{-1}\right)^\vee, \ \left(\frac{\partial g}{\partial \theta} g^{-1}\right)^\vee\right] = \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$J_l = \left[\left(g^{-1}\frac{\partial g}{\partial x_1}\right)^\vee, \ \left(g^{-1}\frac{\partial g}{\partial x_2}\right)^\vee, \ \left(g^{-1}\frac{\partial g}{\partial \theta}\right)^\vee\right] = \begin{pmatrix} 1 & 0 & x_2 \\ 0 & 1 & -x_1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Substitution into the definitions yields

$$[Ad(g)] = \begin{pmatrix} \cos\theta & -\sin\theta & x_2 \\ \sin\theta & \cos\theta & -x_1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Note that

$$\det(J_l) = \det(J_r) = \det[Ad(g)] = 1.$$

This parameterization is not unique, although it is probably the most well-known one.

Parameterization and Jacobians in Exponential Coordinates

As an alternative, consider the exponential parameterization

$$g(v_1, v_2, \alpha) = \exp(v_1 E_1 + v_2 E_2 + \alpha E_3) = \exp\begin{pmatrix} 0 & -\alpha & v_1 \\ \alpha & 0 & v_2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} \cos\alpha & -\sin\alpha & [v_2(-1+\cos\alpha) + v_1 \sin\alpha]/\alpha \\ \sin\alpha & \cos\alpha & [v_1(1-\cos\alpha) + v_2\sin\alpha]/\alpha \\ 0 & 0 & 1 \end{pmatrix}. \tag{10.76}$$

Comparing this with (10.75), it is clear that $\alpha = \theta$, but $x_i \neq v_i$.

The corresponding Jacobians in this exponential parametrization are

$$J_r = \begin{pmatrix} (\sin\alpha)/\alpha & (1-\cos\alpha)/\alpha & (\alpha v_1 - v_2 + v_2\cos\alpha - v_1\sin\alpha)/\alpha^2 \\ (\cos\alpha - 1)/\alpha & (\sin\alpha)/\alpha & (v_1 + \alpha v_2 - v_1\cos\alpha - v_2\sin\alpha)/\alpha^2 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$J_l = \begin{pmatrix} (\sin\alpha)/\alpha & (\cos\alpha - 1)/\alpha & (\alpha v_1 + v_2 - v_2\cos\alpha - v_1\sin\alpha)/\alpha^2 \\ (1-\cos\alpha)/\alpha & (\sin\alpha)/\alpha & (-v_1 + \alpha v_2 + v_1\cos\alpha - v_2\sin\alpha)/\alpha^2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Therefore,

$$\det(J_l) = \det(J_r) = \frac{2(1-\cos\alpha)}{\alpha^2}.$$

Additionally, when

$$X = \begin{pmatrix} 0 & -\alpha & v_1 \\ \alpha & 0 & v_2 \\ 0 & 0 & 0 \end{pmatrix},$$

it follows that

$$[ad(X)] = \begin{pmatrix} 0 & -\alpha & v_2 \\ \alpha & 0 & -v_1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad [B] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

This $[B]$ is clearly degenerate, and $SE(2)$ is therefore not semi-simple (neither is $SE(3)$).

10.6.3 The Group $SL(2,\mathbb{R})$

The group $SL(2,\mathbb{R})$ consists of all 2×2 matrices with real entries with determinant equal to unity. In other words, for $a, b, c, d \in \mathbb{R}$, elements of $SL(2,\mathbb{R})$ are of the form

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{where } ad - bc = 1.$$

A basis for the Lie algebra $sl(2,\mathbb{R})$ is

$$X_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \quad X_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \quad X_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

An alternative basis for the Lie algebra $sl(2,\mathbb{R})$ is

$$E_1 = X_1; \quad E_2 = X_2; \quad E_3 = \frac{1}{2}(X_3 - X_1).$$

The Iwasawa Decomposition

The *Iwasawa decomposition* allows one to write an arbitrary $g \in SL(2,\mathbb{R})$ in the form

$$g = u_1(\theta)u_2(t)u_3(\xi),$$

where

$$u_1(\theta) = \exp(\theta E_1) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$
$$u_2(t) = \exp(tE_2) = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix},$$
$$u_3(\xi) = \exp(\xi E_3) = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}.$$

The subgroups defined by the above u_i are not the only subgroups of $SL(2,\mathbb{R})$. For example, exponentiating matrices of the form ζX_3 results in a subgroup of matrices of the form

$$\exp(\zeta X_3) = \begin{pmatrix} \cosh\zeta & \sinh\zeta \\ \sinh\zeta & \cosh\zeta \end{pmatrix}.$$

Jacobians

Using the Iwasawa decomposition (which is defined using the basis $\{E_i\}$) to parameterize $SL(2,\mathbb{R})$ and computing Jacobians in the Lie algebra $sl(2,\mathbb{R})$ using the basis $\{E_i\}$ gives

$$J_r(\theta,t,\xi) = \frac{1}{2}\begin{pmatrix} e^{-2t} + e^{2t}(1+\xi^2) & -2e^{2t}\xi & e^{2t} - e^{-2t}(1+e^{4t}\xi^2) \\ -2\xi & 2 & 2\xi \\ -1 & 0 & 1 \end{pmatrix}$$

and

$$J_l(\theta,t,\xi) = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2\cos 2\theta & 2\sin 2\theta \\ -e^{2t} & -e^{2t}\sin 2\theta & e^{2t}\cos 2\theta \end{pmatrix}.$$

More generally, it is possible to compute an exponential parameterization using one basis for the Lie algebra and then to evaluate the Jacobian using either the same or a different basis.

It is easy to verify that

$$\det(J_r(\theta,t,\xi)) = \det(J_l(\theta,t,\xi)) = \frac{1}{2}e^{2t}.$$

Hence, $SL(2,\mathbb{R})$ is *unimodular* (which means the determinants of the left and right Jacobians are the same).

10.6.4 The Motion Group of the Lobachevsky Plane, $L(2)$

Consider the set of matrices of the form

$$g(t,u,v) = \begin{pmatrix} \cosh(t) & \sinh(t) & u \\ \sinh(t) & \cosh(t) & v \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} M(t) & \mathbf{x}(u,v) \\ \mathbf{0}^T & 1 \end{pmatrix}, \quad \text{where } t,u,v \in \mathbb{R}. \qquad (10.77)$$

This is a three-dimensional Lie group under the operation of matrix multiplication. It is called the Lobachevsky motion group and is denoted as $L(2)$. The space on which this group acts is called the Lobachevsky (or hyperbolic) plane.

The inverse of $g(t,u,v)$ is of the form

$$g^{-1}(t,u,v) = \begin{pmatrix} M(-t) & -M(-t)\mathbf{x}(u,v) \\ \mathbf{0}^T & 1 \end{pmatrix}.$$

Basis elements for the Lie algebra are

$$E_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \quad E_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}; \quad E_3 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{10.78}$$

The commutation relations are

$$[E_1, E_2] = 0; \quad [E_1, E_3] = -E_2; \quad [E_2, E_3] = -E_1.$$

An inner product for this Lie algebra can be defined as

$$(X,Y) = \frac{1}{2}\,\mathrm{tr}(XWY^T), \quad \text{where } W = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

With this inner product, $(E_i, E_j) = \delta_{ij}$. Direct calculation verifies that

$$g^{-1}\frac{\partial g}{\partial u} = \cosh(t)E_1 - \sinh(t)E_2; \quad g^{-1}\frac{\partial g}{\partial v} = -\sinh(t)E_1 + \cosh(t)E_2; \quad g^{-1}\frac{\partial g}{\partial t} = E_3;$$

and so

$$J_r(t,u,v) = \begin{pmatrix} \cosh(t) & -\sinh(t) & 0 \\ -\sinh(t) & \cosh(t) & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

$$\frac{\partial g}{\partial u}g^{-1} = E_1; \quad \frac{\partial g}{\partial v}g^{-1} = E_2; \quad \frac{\partial g}{\partial t}g^{-1} = E_3 - vE_1 - uE_2;$$

and so

$$J_l(t,u,v) = \begin{pmatrix} 1 & 0 & -v \\ 0 & 1 & -u \\ 0 & 0 & 1 \end{pmatrix}.$$

Clearly, $\det J_r = \det J_l = 1$, and so this group is unimodular. The adjoint matrix can be calculated as

$$[Ad(g)] = J_l\, J_r^{-1} = \begin{pmatrix} M(t) & -\mathbf{x}(u,v) \\ \mathbf{0}^T & 1 \end{pmatrix}.$$

10.6.5 The Lorentz Group, $SO(2,1)$

This group consists of elements g such that[21]

$$g^T I(2,1) g = I(2,1), \qquad \text{where } I(2,1) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

[21] The higher-dimensional group $SO(3,1)$ is actually the Lorentz group, which preserves the space–time quadratic form $\mathbf{x}^T I(3,1)\mathbf{x}$, with the fourth dimension representing time, which is normalized by the speed of light, taken here as $c = 1$.

Basis elements for the Lie algebra are

$$E_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}; \quad E_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}; \quad E_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}. \tag{10.79}$$

The commutation relations are

$$[E_1, E_2] = -E_3; \quad [E_2, E_3] = E_1; \quad [E_1, E_3] = -E_2.$$

The basis $\{E_i\}$ is orthonormal with respect to the inner product

$$(X, Y) = \frac{1}{2}\,\mathrm{tr}(XY^T).$$

The matrix exponential gives

$$\exp(tE_1) = \begin{pmatrix} \cosh(t) & 0 & \sinh(t) \\ 0 & 1 & 0 \\ \sinh(t) & 0 & \cosh(t) \end{pmatrix}, \tag{10.80}$$

$$\exp(uE_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cosh(u) & \sinh(u) \\ 0 & \sinh(u) & \cosh(u) \end{pmatrix}, \tag{10.81}$$

$$\exp(vE_3) = \begin{pmatrix} \cos(v) & -\sin(v) & 0 \\ \sin(v) & \cos(v) & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{10.82}$$

The computation of Jacobians and adjoint are left as an exercise.

10.6.6 The Rotation Group, *SO*(3)

In this subsection, the Jacobian matrices for $SO(3)$ are computed in two different coordinate systems: exponential coordinates and Euler angles.

Parameterization Using Exponential Coordinates

The Lie algebra $so(3)$ consists of skew-symmetric matrices of the form

$$X = \begin{pmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{pmatrix} = \sum_{i=1}^{3} x_i E_i. \tag{10.83}$$

The skew-symmetric matrices $\{E_i\}$ form a basis for the set of all such 3×3 skew-symmetric matrices, and the coefficients $\{x_i\}$ are all real. The $\vee$ operation extracts these coefficients from a skew-symmetric matrix, X, to form a column vector $[x_1, x_2, x_3]^T \in \mathbb{R}^3$. Then $X\mathbf{y} = \mathbf{x} \times \mathbf{y}$ for any $\mathbf{y} \in \mathbb{R}^3$, where $\times$ is the usual vector cross product.

In this case, the adjoint matrices are

$$[Ad(R)] = R \quad \text{and} \quad [ad(X)] = X.$$

Furthermore,

$$[X, Y]^{\vee} = \mathbf{x} \times \mathbf{y}.$$

It is well known (see [8] for derivation and references) that

$$R(\mathbf{x}) = e^X = \mathbb{I} + \frac{\sin \|\mathbf{x}\|}{\|\mathbf{x}\|} X + \frac{(1 - \cos \|\mathbf{x}\|)}{\|\mathbf{x}\|^2} X^2, \tag{10.84}$$

where $\|\mathbf{x}\| = (x_1^2 + x_2^2 + x_3^2)^{\frac{1}{2}}$, and it can be shown that $R(\mathbf{x})\mathbf{x} = \mathbf{x}$.

An interesting and useful fact is that except for a set of measure zero, all elements of $SO(3)$ can be captured with the parameters within the open ball defined by $\|\mathbf{x}\| < \pi$, and the matrix logarithm of any group element parameterized in this range is also well defined. It is convenient to know that the angle of the rotation, $\theta(R)$, is related to the exponential parameters as $|\theta(R)| = \|\mathbf{x}\|$. Furthermore,

$$\log(R) = \frac{1}{2} \frac{\theta(R)}{\sin \theta(R)} (R - R^T),$$

where

$$\theta(R) = \cos^{-1}\left(\frac{\text{trace}(R) - 1}{2}\right).$$

Invariant definitions of directional (Lie) derivatives and integration measure for $SO(3)$ can be defined. When computing these invariant quantities in coordinates (including exponential coordinates), a Jacobian matrix comes into play. It can be shown that the left- and right-Jacobian matrices for $SO(3)$ are related as

$$J_l = R\, J_r. \tag{10.85}$$

Jacobians for Exponential Coordinates

Relatively simple analytical expressions have been derived by Park [17] for the Jacobian J_l and its inverse when rotations are parameterized as in (10.84). These expressions are

$$J_l(\mathbf{x}) = \mathbb{I} + \frac{1 - \cos \|\mathbf{x}\|}{\|\mathbf{x}\|^2} X + \frac{\|\mathbf{x}\| - \sin \|\mathbf{x}\|}{\|\mathbf{x}\|^3} X^2 \tag{10.86}$$

and

$$J_l^{-1}(\mathbf{x}) = \mathbb{I} - \frac{1}{2} X + \left(\frac{1}{\|\mathbf{x}\|^2} - \frac{1 + \cos \|\mathbf{x}\|}{2\|\mathbf{x}\| \sin \|\mathbf{x}\|}\right) X^2.$$

The corresponding Jacobian J_r and its inverse are then calculated using (10.85) as [8]

$$J_r(\mathbf{x}) = \mathbb{I} - \frac{1 - \cos \|\mathbf{x}\|}{\|\mathbf{x}\|^2} X + \frac{\|\mathbf{x}\| - \sin \|\mathbf{x}\|}{\|\mathbf{x}\|^3} X^2$$

and

$$J_r^{-1}(\mathbf{x}) = \mathbb{I} + \frac{1}{2} X + \left(\frac{1}{\|\mathbf{x}\|^2} - \frac{1 + \cos \|\mathbf{x}\|}{2\|\mathbf{x}\| \sin \|\mathbf{x}\|}\right) X^2.$$

Note that

$$J_l = J_r^T.$$

The determinants are

$$|\det(J_l)| = |\det(J_r)| = \frac{2(1-\cos\|\mathbf{x}\|)}{\|\mathbf{x}\|^2}.$$

Despite the $\|\mathbf{x}\|^2$ in the denominator, these determinants are well behaved at the identity, which follows from expanding $\cos\|\mathbf{x}\|$ in a Taylor series.

Euler Angles and Associated Jacobians

Exponential coordinates are not the only way to describe rotations. In fact, they are not even the most well-known parameterization. The "ZXZ" *Euler angles* are defined as

$$R_{ZXZ}(\alpha,\beta,\gamma) \doteq R_3(\alpha)R_1(\beta)R_3(\gamma), \tag{10.87}$$

where the fundamental rotations $R_i(\phi)$ were defined in (A.42)–(A.44) of Volume 1.

The Jacobian matrices associated with this parametrization are

$$J_l(\alpha,\beta,\gamma) = [\mathbf{e}_3, R_3(\alpha)\mathbf{e}_1, R_3(\alpha)R_1(\beta)\mathbf{e}_3] = \begin{pmatrix} 0 & \cos\alpha & \sin\alpha\sin\beta \\ 0 & \sin\alpha & -\cos\alpha\sin\beta \\ 1 & 0 & \cos\beta \end{pmatrix} \tag{10.88}$$

and

$$J_r = R^T J_l = [R_3(-\gamma)R_1(-\beta)\mathbf{e}_3, R_3(-\gamma)\mathbf{e}_1, \mathbf{e}_3] = \begin{pmatrix} \sin\beta\sin\gamma & \cos\gamma & 0 \\ \sin\beta\cos\gamma & -\sin\gamma & 0 \\ \cos\beta & 0 & 1 \end{pmatrix}. \tag{10.89}$$

It is easy to see that

$$J_l^{-1} = \begin{pmatrix} -\cot\beta\sin\alpha & \cos\alpha\cot\beta & 1 \\ \cos\alpha & \sin\alpha & 0 \\ \csc\beta\sin\alpha & -\cos\alpha\csc\beta & 0 \end{pmatrix} \text{ and } J_r^{-1} = \begin{pmatrix} \csc\beta\sin\gamma & \cos\gamma\csc\beta & 0 \\ \cos\gamma & -\sin\gamma & 0 \\ -\cot\beta\sin\gamma & -\cos\gamma\cot\beta & 1 \end{pmatrix}. \tag{10.90}$$

Note that

$$|J_l| = |J_r| = \sin\beta.$$

The Adjoint and Killing Form for $SO(3)$

When the inner product is normalized so that $(E_i, E_j) = \delta_{ij}$,

$$[Ad(R)] = J_l\, J_r^{-1} = R,$$

where J_r and J_l are given above in two different parameterizations.

A straightforward calculation shows

$$[ad(X)] = X \quad \text{and} \quad [B] = -2\mathbb{I}_3.$$

Hence, $SO(3)$ is semi-simple.

10.6.7 The Group $GL(2,\mathbb{R})$

Elements of $GL(2,\mathbb{R})$ are invertible 2×2 real matrices:

$$g(x_1,x_2,x_3,x_4) = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}.$$

A basis for the Lie algebra $gl(2,\mathbb{R})$ is

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}; \quad E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; \quad E_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}; \quad E_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

An inner product can be defined in which this basis is orthonormal.

The Jacobians in this parameterization, basis, and inner product are

$$J_r = \frac{1}{\det g}\begin{pmatrix} x_4 & 0 & -x_2 & 0 \\ 0 & x_4 & 0 & -x_2 \\ -x_3 & 0 & x_1 & 0 \\ 0 & -x_3 & 0 & x_1 \end{pmatrix} \quad \text{and} \quad J_l = \frac{1}{\det g}\begin{pmatrix} x_4 & -x_3 & 0 & 0 \\ -x_2 & x_1 & 0 & 0 \\ 0 & 0 & x_4 & -x_3 \\ 0 & 0 & -x_2 & x_1 \end{pmatrix}.$$

The determinants are

$$\det(J_l) = \det(J_r) = \frac{1}{|\det g|^2}.$$

10.6.8 The Scale-Euclidean Group of the Plane

A basis for the Lie algebra of the scale-Euclidean group $SIM(2)$ is

$$E_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \; E_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}; \; E_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \; E_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

This basis is orthonormal with respect to an appropriate inner product.

The parameterization

$$g(x_1,x_2,\theta,a) = \exp(x_1E_1 + x_2E_2)\exp(\theta E_3 + aE_4)$$

$$= \begin{pmatrix} e^a\cos\theta & -e^a\sin\theta & x_1 \\ e^a\sin\theta & e^a\cos\theta & x_2 \\ 0 & 0 & 1 \end{pmatrix}$$

extends over the whole group.

The Jacobians are

$$J_r = \begin{pmatrix} e^{-a}\cos\theta & e^{-a}\sin\theta & 0 & 0 \\ -e^{-a}\sin\theta & e^{-a}\cos\theta & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad J_l = \begin{pmatrix} 1 & 0 & x_2 & -x_1 \\ 0 & 1 & -x_1 & -x_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Note that

$$\det(J_r) = e^{-2a} \neq \det(J_l) = 1.$$

As a general rule, subgroups of the affine group with elements of the form

$$g = \begin{pmatrix} A & \mathbf{b} \\ \mathbf{0}^T & 1 \end{pmatrix}$$

will have left and right Jacobians whose determinants are different unless $\det(A) = 1$.

10.6.9 $SE(3)$, The Group of Rigid-Body Motions

In this subsection, Jacobians for $SE(3)$ are computed in two different coordinate systems.

Exponential Coordinates

The Euclidean motion group, $SE(3)$, is the semi-direct product of $\mathbb{R}^3$ with the special orthogonal group, $SO(3)$. We represent elements of $SE(3)$ using 4×4 homogeneous transformation matrices

$$g = \begin{pmatrix} R & \mathbf{t} \\ \mathbf{0}^T & 1 \end{pmatrix}$$

and identify the group law with matrix multiplication. The inverse of any group element is written as

$$g^{-1} = \begin{pmatrix} R^T & -R^T\mathbf{t} \\ \mathbf{0}^T & 1 \end{pmatrix}.$$

The Lie algebra $se(3)$ consists of "screw" matrices of the form

$$X = \begin{pmatrix} 0 & -x_3 & x_2 & x_4 \\ x_3 & 0 & -x_1 & x_5 \\ -x_2 & x_1 & 0 & x_6 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \sum_{i=1}^{6} x_i E_i. \tag{10.91}$$

For small translational (rotational) displacements from the identity along (about) the ith coordinate axis, the homogeneous transforms representing infinitesimal motions look like

$$g_i(\epsilon) \doteq \exp(\epsilon E_i) \approx I_4 + \epsilon E_i,$$

where I_4 is the 4×4 identity matrix and

$$E_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \quad E_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \quad E_3 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix};$$

$$E_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \quad E_5 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}; \quad E_6 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

These are related to the basis elements for $so(3)$ (which are for the moment denoted as $\{\hat{E}_i\}$ to distinguish them from $\{E_i\}$) as

$$E_i = \begin{pmatrix} \hat{E}_i & \mathbf{0} \\ \mathbf{0}^T & 0 \end{pmatrix} \tag{10.92}$$

when $i = 1, 2, 3$.

The matrices $\{E_i\}$ form a basis for the set of all such 4×4 screw matrices, and the coefficients $\{x_i\}$ are all real. The $\vee$ operation is defined to extract these coefficients from a screw matrix to form a column vector $X^\vee = [x_1, x_2, x_3, x_4, x_5, x_6]^T \in \mathbb{R}^6$. The double use of $\vee$ in the $so(3)$ and $se(3)$ cases will not cause confusion, since the object to which it is applied defines the sense in which it is used.

It will be convenient to define $\boldsymbol{\omega} = [x_1, x_2, x_3]^T$ and $\mathbf{v} = [x_4, x_5, x_6]^T$ so that

$$X^\vee = \mathbf{x} = \begin{pmatrix} \boldsymbol{\omega} \\ \mathbf{v} \end{pmatrix}.$$

Large motions are also obtained by exponentiating these matrices; for example,

$$\exp(tE_3) = \begin{pmatrix} \cos t & -\sin t & 0 & 0 \\ \sin t & \cos t & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \exp(tE_6) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

More generally, it can be shown that

$$g(X^\vee) = \exp X = \begin{pmatrix} R(\boldsymbol{\omega}) & \hat{J}_l(\boldsymbol{\omega})\mathbf{v} \\ \mathbf{0}^T & 1 \end{pmatrix}. \tag{10.93}$$

where $\hat{J}_l(\boldsymbol{\omega})$ is the $SO(3)$ Jacobian in (10.86) evaluated at $\boldsymbol{\omega}$. The form of (10.93) follows from the expression for the matrix exponential given in [8]. From the form of (10.93), it is clear that if g has rotational part R and translational part $\mathbf{t}$, then the matrix logarithm can be written in closed form as

$$X = \log(g) = \begin{pmatrix} \log R & \hat{J}_l^{-1}((\log R)^\vee)\mathbf{t} \\ \mathbf{0}^T & 0 \end{pmatrix} \quad \text{and} \quad X^\vee = \begin{pmatrix} (\log R)^\vee \\ \hat{J}_l^{-1}((\log R)^\vee)\mathbf{t} \end{pmatrix}. \tag{10.94}$$

The adjoint matrices for $SE(3)$ are

$$[Ad(g)] = \begin{pmatrix} R & \mathbb{O}_3 \\ TR & R \end{pmatrix} \in \mathbb{R}^{6\times 6} \quad \text{and} \quad [ad(X)] = \begin{pmatrix} \Omega & \mathbb{O}_3 \\ V & \Omega \end{pmatrix} \in \mathbb{R}^{6\times 6},$$

where $V^\vee = \mathbf{v}$, $\Omega^\vee = \boldsymbol{\omega}$, and $T^\vee = \mathbf{t}$.

Jacobians in Exponential Coordinates

The Jacobians for $SE(3)$ using exponential parameters are then

$$J_l(\mathbf{x}) = \left[\left(\frac{\partial g}{\partial x_1} g^{-1} \right)^\vee, \left(\frac{\partial g}{\partial x_2} g^{-1} \right)^\vee, \dots, \left(\frac{\partial g}{\partial x_6} g^{-1} \right)^\vee \right]$$

and

$$J_r(\mathbf{x}) = \left[\left(g^{-1} \frac{\partial g}{\partial x_1} \right)^\vee, \left(g^{-1} \frac{\partial g}{\partial x_2} \right)^\vee, \dots, \left(g^{-1} \frac{\partial g}{\partial x_6} \right)^\vee \right].$$

The right Jacobian for $SE(3)$ in exponential coordinates can be computed from (10.93) as

$$J_r(\mathbf{x}) = \begin{pmatrix} \hat{J}_r(\boldsymbol{\omega}) & \mathbb{O}_3 \\ e^{-X} \frac{\partial}{\partial \boldsymbol{\omega}^T} \left(\hat{J}_l(\boldsymbol{\omega})\mathbf{v} \right) & \hat{J}_r(\boldsymbol{\omega}) \end{pmatrix}, \tag{10.95}$$

where $\mathbb{O}_3$ is the 3×3 zero matrix. It becomes immediately clear that the determinants of these $SE(3)$ and $SO(3)$ Jacobians are related as

$$|J_r(\mathbf{x})| = |\hat{J}_r(\boldsymbol{\omega})|^2. \tag{10.96}$$

Jacobians in Translation–Rotation Coordinates

When the rotations are parameterized as $R = R(q_1, q_2, q_3)$ and the translations are parameterized using Cartesian coordinates $\mathbf{t}(q_4, q_5, q_6) = [q_4, q_5, q_6]^T$,

$$J_r(\mathbf{q}) = \begin{pmatrix} \hat{J}_r & \mathbb{O}_3 \\ \mathbb{O}_3 & R^T \end{pmatrix} \quad \text{and} \quad J_l(\mathbf{q}) = \begin{pmatrix} \hat{J}_l & \mathbb{O}_3 \\ T\hat{J}_l & \mathbb{I}_3 \end{pmatrix}, \tag{10.97}$$

where $\mathbb{O}_3$ is the 3×3 zero matrix, $\hat{J}_l$ and $\hat{J}_r$ are the left and right Jacobians for $SO(3)$ in the parameterization (q_1, q_2, q_3), and T is the 3×3 skew-symmetric matrix such that $T\mathbf{x} = \mathbf{t} \times \mathbf{x}$. For example, this could be either of the parameterizations used in Section 10.6.6. Many other specialized parameterizations of $SO(3)$ and $SE(3)$ exist and will be discussed in the companion volume to this book.

10.6.10 The Weyl–Heisenberg Group and Its Semidirect Product with $SL(2, \mathbb{R})$

In this section the six-dimensional group of symmetries of the heat equation on the real line first discussed in Chapter 2 is examined.

The Weyl–Heisenberg Group, $W(1)$

Recall from Chapter 2 of Volume 1 that matrices of the form

$$B = B(u, v, w) = \begin{pmatrix} 1 & v & 2w + uv/2 \\ 0 & 1 & u \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{where } u, v, w \in \mathbb{R}, \tag{10.98}$$

are closed under matrix multiplication

$$B(u, v, w)\, B(u', v', w') = B(u + u', v + v', w + w' + (vu' - uv')/4). \tag{10.99}$$

From this it is clear that

$$[B(u, v, w)]^{-1} = B(-u, -v, -w).$$

This group of matrices is called the *Weyl–Heisenberg group*, which will be denoted here as $W(1)$.

The basis elements for the Lie algebra of $W(1)$ can be taken as

$$E_1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}; \quad E_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}; \quad E_3 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

The commutation relations are

$$[E_1, E_2] = E_3; \quad [E_1, E_3] = [E_2, E_3] = 0.$$

It follows that

$$B^{-1}\frac{\partial B}{\partial u} = \begin{pmatrix} 0 & 0 & -v/2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = E_2 - (v/2)E_3,$$

$$B^{-1}\frac{\partial B}{\partial v} = \begin{pmatrix} 0 & 1 & u/2-v \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = E_1 + (u/2-v)E_3,$$

$$B^{-1}\frac{\partial B}{\partial w} = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 2E_3.$$

With this choice of basis and the inner product,

$$(E_i, E_j) = \mathrm{tr}(E_i E_j^T) = \delta_{ij}.$$

Similarly,

$$\frac{\partial B}{\partial u}B^{-1} = \begin{pmatrix} 0 & 0 & v/2 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = E_2 + (v/2)E_3,$$

$$\frac{\partial B}{\partial v}B^{-1} = \begin{pmatrix} 0 & 1 & -u/2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = E_1 - (u/2)E_3,$$

$$\frac{\partial B}{\partial w}B^{-1} = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 2E_3.$$

Then the coefficients in each of the matrices above can be "plucked off" and used to form the columns of the Jacobians

$$J_r = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ -v/2 & (u/2-v) & 2 \end{pmatrix} \quad \text{and} \quad J_l = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ v/2 & -u/4 & 2 \end{pmatrix}.$$

The Semi-direct Product of $W(1)$ and $SL(2,\mathbb{R})$

Recall from Volume 1 that the equations (2.79)–(2.81) defined operators $(T_1(B)f)(x,t)$ and $(T_2(A)f)(x,t)$ that convert solutions of the heat equation into other solutions where $B \in W(1)$ and $A \in SL(2,\mathbb{R})$. Then the fact that $(T_2(A)(T_1(B)f))(x,t)$ and $(T_1(B)(T_2(A)f))(x,t)$ preserve solutions of the heat equation means that there must be a way to combine $W(1)$ and $SL(2,\mathbb{R})$ to form a larger group of transformations.

The key to obtaining this larger group is the observation that the composite adjoint operator, when applied to any function, has the property

$$T_2(A^{-1})T_1(B)T_2(A) = T_1(B'), \tag{10.100}$$

where $B = B(u,v,w)$, $A = A(\alpha,\beta,\gamma,\delta)$, and $B' = B(u\delta - v\beta, v\alpha - u\gamma, w)$.

Define for the set of pairs $g = (A, B) \in SL(2, \mathbb{R}) \times W(1)$:

$$T(g) = T_2(A)T_1(B).$$

Using this construction, the following group operation can be defined:

$$\begin{aligned} T(g_1)T(g_2) &= [T_2(A_1)T_1(B_1)][T_2(A_2)T_1(B_2)] \\ &= T_2(A_1)[T_2(A_2)T_2(A_2^{-1})]T_1(B_1)T_2(A_2)T_1(B_2) \\ &= [T_2(A_1)T_2(A_2)][T_2(A_2^{-1})T_1(B_1)T_2(A_2)]T_1(B_2) \\ &= T_2(A_1A_2)\{[T_2(A_2^{-1})T_1(B_1)T_2(A_2)]T_1(B_2)\} \\ &= T(g_1 \circ g_2). \end{aligned} \tag{10.101}$$

This is discussed in the references provided in Chapter 2.

In terms of parameters, if $g = g(\alpha, \beta, \gamma, \delta; u, v, w)$ with the constraint that $\alpha\delta - \beta\gamma = 1$, then the parameters of $g_1 \circ g_2 = g'$ would be given by the array

$$\begin{pmatrix} \alpha' \\ \beta' \\ \gamma' \\ \delta' \\ u' \\ v' \\ w' \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 + \beta_1\gamma_2 \\ \alpha_1\beta_2 + \beta_1\delta_2 \\ \gamma_1\alpha_2 + \delta_1\gamma_2 \\ \gamma_1\beta_2 + \delta_1\delta_2 \\ u_1\delta_2 - v_1\beta_2 + u_2 \\ v_1\alpha_2 - u_1\gamma_2 + v_2 \\ w_1 + w_2 + (v_1\alpha_2 - u_1\gamma_2)u_2/4 - (u_1\delta_2 - v_1\beta_2)v_2/4 \end{pmatrix}. \tag{10.102}$$

The first four rows in the above equation are the same as that for the group product $A_1A_2 = A'$ for $SL(2, \mathbb{R})$. Of course, only three of these rows are independent due to the constraint that $\det A = 1$. The last three rows illustrate the adjoint action of $SL(2, \mathbb{R})$ on $W(1)$. All together, (10.102) can be thought of as the definition of a six-dimensional group.

10.7 Objects That Are Not Quite Groups

When presented with a new definition and numerous examples illustrating the definition, there is a tendency to believe "well then, doesn't everything satisfy this definition?" Therefore, a number of examples of mathematical objects that satisfy some (but not all) of the group axioms are reviewed. These are therefore *not* groups.

10.7.1 Case Study 1: Closure Can Fail

First, consider the set of 3×3 matrices of the form

$$A(a, b, c, d, e) = \begin{pmatrix} 1 & a & b \\ 0 & c & d \\ e & 0 & 1 \end{pmatrix}, \quad \text{where } a, b, c, d, e \in \mathbb{R}.$$

This is a parameterized set of matrices that defines a five-dimensional manifold embedded in $\mathbb{R}^{3\times 3} \cong \mathbb{R}^9$, but it is not a Lie group because closure fails:

$$\begin{pmatrix} 1 & a_1 & b_1 \\ 0 & c_1 & d_1 \\ e_1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & c_2 & d_2 \\ e_2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 + b_1 e_2 & a_2 + a_1 c_2 & b_1 + b_2 + a_1 d_2 \\ d_1 e_2 & c_1 c_2 & d_1 + c_1 d_2 \\ e_1 + e_2 & e_1 a_2 & 1 + e_1 b_2 \end{pmatrix}.$$

From this it is clear that the structure of the 1s and 0s in the matrix are not preserved under matrix multiplication, and the fundamental property of closure is not satisfied. Note, however, that if we restrict the form of the matrices such that $e_i = 0$ and define $g(a,b,c,d) = A(a,b,c,d,0)$, then closure is satisfied and the product law

$$g(a_1,b_1,c_1,d_1)g(a_2,b_2,c_2,d_2) = g(a_2 + a_1c_2, b_1 + b_2 + a_1d_2, c_1c_2, d_1 + c_1d_2)$$

results. In fact, by restricting $c_i > 0$, an inverse of each element can be defined and this forms a group called the *Mautner group* with identity element $g(0,0,1,0)$.

10.7.2 Case Study 2: Even If Closure Holds, Associativity Can Fail

Consider the abstract set $\{e, a, b, c, d\}$ and operation defined by the table

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	a	d	e
c	c	d	e	a	b
d	d	b	c	e	a

Clearly, closure is satisfied because the table is populated only with the elements of the set. However, using the table, we see that $(a \circ b) \circ c = d \circ c = e$. On the other hand, $a \circ (b \circ c) = a \circ d = c$. Therefore, $(a \circ b) \circ c \neq a \circ (b \circ c)$.

10.7.3 Case Study 3: Another Example of When Associativity Can Fail

As another example of an object that is not a group, consider continuous rigid-body motion within an environment with crystallographic symmetry.[22] Let rigid-body motions in $\mathbb{R}^n$ be denoted as $g = (R, \mathbf{t}) \in SE(n)$. Consider a crystal lattice in $\mathbb{R}^n$ with unit cell $\Gamma\backslash\mathbb{R}^n$ defined by some proper crystallographic space group $\Gamma < SE(n)$. The coset space $\Gamma\backslash SE(n)$ is then a set of motions equivalent under Γ such that all $\sigma \in \Gamma\backslash SE(n)$ act on all $\mathbf{x} \in \Gamma\backslash\mathbb{R}^n$ to produce the equivalent $\sigma \cdot \mathbf{x}$.

This can be thought of in intuitive terms. As the origin of a reference frame attached to a rigid body moves from the "primary" crystallographic unit to any other, the reference frame can be "brought back" to the primary cell by removing (via modular arithmetic) the translations that take the frame outside of the primary cell. Let this be denoted as $[g] = ([R], [\mathbf{t}])$, where $[g] \in \Gamma\backslash SE(n)$. Then for any $\mathbf{x} \in \Gamma\backslash\mathbb{R}^n$ (the unit cell), $[g] \cdot \mathbf{x} \in \Gamma\backslash\mathbb{R}^n$ also. Furthermore, for any $g_1, g_2 \in SE(n)$, $[g_1] \cdot ([g_2] \cdot \mathbf{x}) \in \Gamma\backslash\mathbb{R}^n$. It is also the case that $[g_1 \circ g_2] \cdot \mathbf{x} \in \Gamma\backslash\mathbb{R}^n$. However,

$$[g_1 \circ g_2] \cdot \mathbf{x} \neq [g_1] \cdot ([g_2] \cdot \mathbf{x}) \quad \text{and} \quad [g_1 \circ g_2] \circ [g_3] \neq [g_1] \circ [g_2 \circ g_3].$$

[22] For more details, see Chirikjian, G.S., "Mathematical Aspects of Molecular Replacement: I. Algebraic Properties of Motion Spaces," *Acta. Cryst. A* A67, pp. 435–446, 2011.

For example, consider the lattice constructed from translating rectangular tiles in the plane of dimensions $w \times h$ with the primary/reference cell occupying $(x, y) \in [0, w] \times [0, h]$. In this case, $[R] = R$ (since $\mathbb{I} \backslash SO(2) \cong SO(2)$) and $[\mathbf{t}] = [t_1 \bmod w, t_2 \bmod h]^T$.

10.7.4 Case Study 4: Even If Associativity Holds Closure Doesn't Have to

Given a set of square matrices, $\{A, B, C, \ldots\}$, the Kronecker product is associative,

$$A \,\widehat{\otimes}\, (B \,\widehat{\otimes}\, C) = (A \,\widehat{\otimes}\, B) \,\widehat{\otimes}\, C,$$

but it does not produce matrices of the same dimensions as the original matrices and therefore violates closure.

10.7.5 Case Study 5: An Identity and Inverse Need Not Exist Even When Associativity and Closure Hold

As a first example of this phenomenon, consider usual matrix multiplication and the set consisting of all real square matrices of dimension N, $\mathbb{R}^{N \times N}$. The identity matrix $\mathbb{I}_N$ is in this set and associativity of matrix multiplication holds, but not every square matrix is invertible.

As a second example, consider the set of functions on any discrete group Γ, $f : \Gamma \to \mathbb{C}$, such that

$$\sum_{\gamma \in \Gamma} |f(\gamma)|^2 < \infty.$$

The set of all such functions is denoted as $L^2(\Gamma)$. Then it is possible to define a convolution operation for any two such functions, $f_1, f_2 \in L^2(\Gamma)$, as

$$(f_1 \star f_2)(\gamma') = \sum_{\gamma \in \Gamma} f_1(\gamma) f_2(\gamma^{-1} \circ \gamma').$$

It can be shown that $\star$ is associative $(f_1 \star f_2) \star f_3 = f_1 \star (f_2 \star f_3)$, but for general functions $f_i \in L^2(\Gamma)$, the convolution operation will not be commutative: $f_1 \star f_2 \neq f_2 \star f_1$.

A Kronecker delta function, $\delta(\gamma)$, can be defined that is equal to unity when $\gamma = e$ and zero otherwise. This then has the property that $\delta \star f = f \star \delta$. Therefore, $(L^2(\Gamma), \star)$ is a set with associative (but noncommutative) operation and an identity element, δ. However, in general, it is not possible to define $f^{-1} \in L^2(\Gamma)$ such that $f^{-1} \star f = \delta$. Thus, this does not form a group.

10.8 Chapter Summary

This chapter presented the basics of the theory of matrix Lie groups. This included a brief review of general group theory, the definition of a matrix Lie group, the exponential and logarithm maps, adjoint transformations, and Jacobian matrices. These tools will be used in the following two chapters to define derivatives and integrals of functions on Lie groups. These, in turn, will be invaluable in defining properties of stochastic processes on Lie groups. For other introductions to group theory that emphasize different topics, see [2, 10, 15].

In the next chapter there will be some discussion of differential forms. It turns out that the behavior of differential forms on a manifold, in general (and a Lie group in particular), is related to its topological properties. This is a subfield of modern mathematics referred to as de Rham cohomology theory. We will touch on this in a very elementary way as a small detour from the main themes of this book.

10.9 Exercises

10.1. Prove that there is one and only one identity element for any group.

10.2. Prove that for any group $(G, \circ)$, for each $g \in G$ there is exactly one inverse: $g^{-1} \in G$.

10.3. Prove that for any group $(G, \circ)$ and for any $a, b \in G$ that $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

10.4. Prove that for any group $(G, \circ)$ with identity element e and arbitrary $g \in G$ that $e^{-1} = e$ and $(g^{-1})^{-1} = g$.

10.5. Prove that the definition of the semi-direct product in (10.25) satisfies the definition of a group. Hint: Show that the identity is (e_N, e_H), where e_N is the identity for N and e_H is the identity for H and $(n, h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1})$.

10.6. Prove that the definition of the wreath product in (10.26) satisfies the definition of a group. Hint: Show that the identity is $(e, e, \ldots, e; \pi_0)$, where π_0 is the identity permutation, and for any $g_1, \ldots, g_n \in G$ and $\pi \in \Pi_n$, the inverse of $(g_1, \ldots, g_n; \pi) \in G^n \wr \Pi_n$ is $(g_1, \ldots, g_n; \pi)^{-1} = (g_{\pi(1)}^{-1}, \ldots, g_{\pi(n)}^{-1}; \pi^{-1})$.

10.7. Show that the set of real $N \times N$ rotation matrices $SO(N, \mathbb{R})$ (which is usually written simply as $SO(N)$) forms a group under the operation of matrix multiplication. Additionally, show that $SO(N) = SU(N) \cap GL(N, \mathbb{R})$.

10.8. Show that the subgroup of Π_n in which there is no change to the last $n-k$ entries is isomorphic to Π_k.

10.9. Let G be a group and $\mathbb{F}$ be a field. For any given function $f : G \to \mathbb{F}$, show that $(L_h f)(g)$ and $(R_h f)(g)$ in (10.24) have the properties

$$(L_{h_1}(L_{h_2} f))(g) = (L(h_1 \circ h_2) f)(g),$$
$$(R_{h_1}(R_{h_2} f))(g) = (R(h_1 \circ h_2) f)(g),$$

and

$$(R_{h_1}(L_{h_2} f))(g) = (L_{h_2}(R_{h_1} f))(g).$$

10.10. Let $SE(n)$ denote the group of "special Euclidean" transformations (rigid-body motions) in n-dimensional Euclidean space.

(a) Show that pure translations and pure rotations each form subgroups.
(b) Show that the translation subgroup is normal; that is, let H denote the set of pure rotations and N denote the set of pure translations. Show that pure translations and rotations described respectively with matrices of the form

$$(n, e_H) \doteq \begin{pmatrix} \mathbb{I} & \mathbf{r} \\ \mathbf{0}^T & 1 \end{pmatrix} \in SE(n); \quad (e_N, h) \doteq \begin{pmatrix} A & \mathbf{0} \\ \mathbf{0}^T & 1 \end{pmatrix} \in SE(n)$$

each can be used to define groups under the operation of matrix multiplication, and an arbitrary element of $SE(n)$ can be written as $(n, h) = (n, e_H)(e_N, h)$.

(c) Show that

$$(n_1, h_1)(n_2, h_2) = (n_1, e_H)[(e_N, h_1)(n_2, e_H)(e_N, h_1)^{-1}](e_N, h_1)(e_N, h_2).$$

10.11. Elements of the Galilean group can be thought of as matrices of the form

$$M(R, \mathbf{v}, \mathbf{b}, a) \doteq \begin{pmatrix} R & \mathbf{v} & \mathbf{b} \\ \mathbf{0}^T & 1 & a \\ \mathbf{0}^T & 0 & 1 \end{pmatrix}, \quad \text{where } R \in SO(3),\ \mathbf{v}, \mathbf{b} \in \mathbb{R}^3,\ a \in \mathbb{R}.$$

Verify that this is a group under matrix multiplication. What is its identity and what is the form of its inverse? Show that this can be written as a double semi-direct product. What is the dimension of this Lie group?

10.12. For the group $SO(p, q)$ defined in Example 1 in Section 10.2.2, compute (a) Lie algebra basis elements, (b) the structure constants, and (c) the matrix exponential function.

10.13. For the group $SIM(N)$ defined in Example 2 in Section 10.2.2, compute (a) Lie algebra basis elements, (b) the structure constants, and (c) the matrix exponential function.

10.14. For the group $\mathbb{R}^N \rtimes GL^+(N, \mathbb{R})$ defined in Example 3 in Section 10.2.2, compute (a) Lie algebra basis elements, (b) the structure constants, and (c) the matrix exponential function.

10.15. Verify that $SO(3)$ and $SE(3)$ are unimodular.

10.16. Prove that in every parameterization of a Lie group, $g = g(\mathbf{q}) \in G$, that

$$J_l(\mathbf{q}) = [Ad(g(\mathbf{q}))]\, J_r(\mathbf{q}). \tag{10.103}$$

10.17. Verify (10.71).

10.18. Verify the left and right Jacobians for $H(3)$ given in (10.72).

10.19. Verify (10.72) and $[Ad(g)]$ for $H(3)$ given in (10.74) in the exponential parameterization in (10.69).

10.20. Verify that the one-parameter subgroups stated in (10.80)–(10.82) are in fact contained in $SO(2, 1)$, and rederive them using the definition of the matrix exponential.

10.21. Using the product-of-exponential parameterization

$$g(t, u, v) = \exp(tE_1) \exp(uE_2) \exp(vE_3),$$

compute the Jacobians $J_r(t, u, v)$ and $J_l(t, u, v)$ and adjoint matrix $Ad(g(t, u, v))$ for the group $SO(2, 1)$. Is it unimodular?

10.22. Consider 2×2 matrices of the form

$$g = \begin{pmatrix} e^{\lambda} & x \\ 0 & e^{-\lambda} \end{pmatrix}, \quad \lambda, x \in \mathbb{R}.$$

Verify that this is a Lie group under the operation of matrix multiplication. Construct an inner product and orthonormal basis elements for the Lie algebra. What are the commutation relations? Compute the Jacobians and adjoint matrix. Is this a unimodular Lie group?

10.23. Consider 2×2 matrices of the form

$$g = \begin{pmatrix} e^{\lambda} & x \\ 0 & e^{\mu} \end{pmatrix}, \qquad \lambda, \mu, x \in \mathbb{R}.$$

Verify that this is a Lie group under the operation of matrix multiplication. Construct an inner product and orthonormal basis elements for the Lie algebra. What are the commutation relations? Compute the Jacobians and adjoint matrix. Is this a unimodular Lie group?

10.24. Verify that the group $GL(2, \mathbb{R})$ consisting of real 2×2 invertible matrices is unimodular. Hint: Use the parameterization

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{with } ad - bc \neq 0.$$

As a basis for the Lie algebra, use

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad E_4 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

What are the commutation relations? Based on what you observe for this case, is it possible to infer that $GL(n, \mathbb{R})$ is unimodular? Explain.

10.25. Verify that the the affine group of the line, or "$ax + b$" group, with elements of the form

$$g(a, b) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

and Lie algebra basis elements

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

is *not* unimodular.

10.26. (a) Show that the Euler-angle-like product-of-exponential decomposition holds for $W(1)$:

$$B(u, v, w) = \exp[(2w + uv/2)E_3] \exp[uE_2] \exp[vE_1].$$

(b) Compute the matrix exponential parameterization $B = \exp[aE_1 + bE_2 + cE_3]$ and compare.

10.27. Compute the matrix exponential parametrization for $SL(2, \mathbb{R})$.

10.28. Using the definitions in (2.79)–(2.81), show that (10.100) holds.

10.29. The group law for the six-dimensional "heat group" can be thought of abstractly in terms of (10.101) and concretely in terms of (10.102). It is usually convenient to think of group elements as matrices. Is it possible in this case to construct matrices, $M(g)$, with the property that $M(g_1 \circ g_2) = M(g_1)M(g_2)$?

10.30. Verify the group law in (10.99). Hint: Given B, $u = b_{23}$, $v = b_{12}$, and $w = \frac{1}{2}b_{13} - \frac{1}{4}b_{12}b_{23}$.

10.31. Prove (10.93). Hint: See the way that the matrix exponential for $SE(3)$ is calculated in [8].

10.32. Prove that $GL(2,\mathbb{R})$ and $SL(2,\mathbb{R})$ are semi-simple.

10.33. Show that real 3×3 matrices of the form

$$g(x,y,z,t) = \begin{pmatrix} 1 & x & z \\ 0 & t & y \\ 0 & 0 & 1 \end{pmatrix}$$

form a Lie group under multiplication for $x, y, x \in \mathbb{R}$ and $t \in \mathbb{R} - \{0\}$. This is called the *Mautner group*. Calculate the left- and right-Jacobian matrices and their determinants. Is this a unimodular group?

10.34. Show that since (10.62) holds, so too does

$$\sum_{j=1}^{N} \left(C_{ij}^{l}(A) C_{km}^{j}(A) + C_{mj}^{l}(A) C_{ik}^{j}(A) + C_{kj}^{l}(A) C_{mi}^{j}(A) \right) = 0.$$

10.35. In analogy with the "ZXZ" Euler angles in (10.87), the "ZYZ" Euler angles for $SO(3)$ are defined by

$$R_{ZYZ}(\alpha,\beta,\gamma) \doteq R_3(\alpha) R_2(\beta) R_3(\gamma). \tag{10.104}$$

Show that these two sets of angles are related by the equality

$$R_{ZYZ}(\alpha,\beta,\gamma) = R_{ZXZ}(\alpha + \pi/2, \beta, \gamma - \pi/2)$$

and compute J_l and J_r for the ZYZ case.

References

1. Angeles, J., *Rational Kinematics*, Springer, New York, 1989.
2. Artin, M., *Algebra*, Prentice Hall, Upper Saddle River, NJ, 1991.
3. Baker, A., *Matrix Groups: An Introduction to Lie Group Theory*, Springer, New York, 2002.
4. Baker, H.F., "Alternants and continuous groups," *Proc. London Math. Soc.* (Second Series), 3, pp. 24–47, 1904.
5. Birkhoff, G., MacLane, S., *A Survey of Modern Algebra*, 4th ed., Macmillan Publishing Co., New York, 1977.
6. Bottema, O., Roth, B., *Theoretical Kinematics*, Dover, New York, 1990.
7. Campbell, J.E., "On a law of combination of operators," *Proc. London Math. Soc.*, 29, pp. 14–32, 1897.
8. Chirikjian, G.S., Kyatkin, A.B., *Engineering Applications of Noncommutative Harmonic Analysis*, CRC Press, Boca Raton, FL, 2001.
9. Curtis, M.L., *Matrix Groups*, 2nd ed., Springer, New York, 1984.
10. Gilmore, R., *Lie Groups, Lie Algebras, and Some of Their Applications*, Dover, New York, 2006.
11. Hausdorff, F., "Die symbolische Exponentialformel in der Gruppentheorie," *Berich. der Sachsichen Akad. Wissensch.*, 58, pp. 19–48, 1906.
12. Inui, T., Tanabe, Y., Onodera, Y., *Group Theory and Its Applications in Physics*, 2nd ed., Springer-Verlag, New York, 1996.

13. Kolář, I., Michor, P.W., Slovák, J., *Natural Operations in Differential Geometry*, Springer-Verlag, Berlin, 1993.
14. McCarthy, J.M., *An Introduction to Theoretical Kinematics*, MIT Press, Cambridge, MA, 1990.
15. Miller, W., Jr., *Symmetry Groups and Their Applications*, Academic Press, New York, 1972.
16. Murray, R.M., Li, Z., Sastry, S.S., *A Mathematical Introduction to Robotic Manipulation*, CRC Press, Boca Raton, FL, 1994.
17. Park, F.C., *The Optimal Kinematic Design of Mechanisms*, Ph.D. thesis, Division of Engineering and Applied Sciences, Harvard University, Cambridge, MA, 1991.
18. Selig, J.M., *Geometrical Methods in Robotics*, 2nd ed., Springer, New York, 2005.
19. Tapp, K., *Matrix Groups for Undergraduates*, American Mathematical Society, Providence, RI, 2005.
20. Varadarajan, V.S., *Lie Groups, Lie Algebras, and their Representations*, Springer-Verlag, New York, 1984.

11

Lie Groups II: Differential-Geometric Properties

This chapter discusses how a natural extension of the concept of directional derivatives in $\mathbb{R}^n$ can be defined for functions on Lie groups.[1] This "Lie derivative" is closely related to the differential geometric properties of the group. Functions on a Lie group can be expanded in a Taylor series using Lie derivatives.[2] Explicit expressions for these Lie derivatives in a particular parametrization can be easily obtained for Lie groups using the appropriate concept of a Jacobian matrix as defined in the previous chapter. Differential forms on Lie groups that are invariant under left or right shifts also are computed from this Jacobian and satisfy the so-called Maurer–Cartan equations. This is illustrated for a number of examples. The structure and curvature of Lie groups are then related to these differential forms and expressed in coordinates using the Jacobian matrix.

The main points to take away from this chapter are as follows:

- The derivative of a function on a Lie group can be computed in a concrete way using elementary matrix operations and concepts from multivariable calculus.
- Differential forms for Lie groups satisfy certain conditions (i.e., the Maurer–Cartan equations) which make them easier to work with than general manifolds.
- The structure and curvature of Lie groups can be described in terms of these differential forms and computed explicitly in any parameterization using the Jacobian matrices from the previous chapter.

This chapter is structured as follows. Section 11.1 defines the concept of directional derivatives in a Lie group and Section 11.2 explores many of its properties. Section 11.3 defines Taylor-series expansions of functions about a point in a Lie group using these directional (Lie) derivatives and Section 11.4 examines how to compute them in coordinates using the Jacobian matrices introduced in the previous chapter. Section 11.5 considers a version of the chain rule related to the computation of Lie derivatives. Section 11.6 views compact Lie groups as Riemannian symmetric spaces and views vector

[1] Here and throughout the remainder of this book the term "Lie group" should be read as "matrix Lie group." When adding prefixes to describe Lie groups such as "connected," "compact," "semi-simple," "unimodular," etc., it will be convenient to eliminate "matrix" from the list since almost all Lie groups that arise in applications have elements that can be represented as finite-dimensional matrices. Therefore, the prefix "matrix" will only be used for emphasis when this feature is particularly important.

[2] The concept of Lie derivative used here for scalar functions is a degenerate case of a more general definition applied to vector fields that can be found in other books.

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_2,

fields in this light. Sections 11.7 and 11.8 respectively examine differential forms and curvature in the context of Lie groups and their coset spaces.

11.1 Defining Lie Derivatives

The *directional derivative* of an analytic function[3] $f : \mathbb{R}^n \rightarrow \mathbb{R}$ in the direction $\mathbf{v}$ is defined as

$$(D_{\mathbf{v}} f)(\mathbf{x}) = \frac{d}{dt} f(\mathbf{x} + t\mathbf{v})\bigg|_{t=0}. \tag{11.1}$$

In the special case when $\mathbf{v} = \mathbf{e}_i$ (the ith unit basis vector in $\mathbb{R}^n$), then

$$(D_{\mathbf{e}_i} f)(\mathbf{x}) = \frac{\partial f}{\partial x_i}.$$

It can be shown that

$$(D_{\mathbf{v}} f)(\mathbf{x}) = \sum_{i=1}^{n} v_i \frac{\partial f}{\partial x_i}. \tag{11.2}$$

In the following subsections, the generalization of this concept for functions of Lie-group-valued argument is explained and demonstrated.

11.1.1 Left Versus Right

In the context of Lie groups, there is a very similar concept. Let $X \in \mathcal{G}$, the Lie algebra of the group G, and let $f : G \rightarrow \mathbb{R}$ be an analytic function. This can be guaranteed by restricting an analytic function $f : \mathbb{R}^{N \times N} \rightarrow \mathbb{R}$ to arguments $g \in G \subset \mathbb{R}^{N \times N}$. Two kinds of directional derivatives can be defined:[4]

$$(\tilde{X}^r f)(g) \doteq \frac{d}{dt} f(g \circ \exp(tX))\bigg|_{t=0} \quad \text{and} \quad (\tilde{X}^l f)(g) \doteq \frac{d}{dt} f(\exp(-tX) \circ g)\bigg|_{t=0}. \tag{11.3}$$

These definitions are completely equivalent to

$$\boxed{(\tilde{X}^r f)(g) = \lim_{t \rightarrow 0} \frac{f(g \circ \exp(tX)) - f(g)}{t} \quad \text{and} \quad (\tilde{X}^l f)(g) = \lim_{t \rightarrow 0} \frac{f(\exp(-tX) \circ g) - f(g)}{t}.} \tag{11.4}$$

In this text, $(\tilde{X}^r f)(g)$ will be called the *right Lie derivative* of $f(g)$ with respect to (or in the direction of) X, and $(\tilde{X}^l f)(g)$ likewise will be called the *left Lie derivative.* The reason for the choice of these names used here is that they denote on which side of the argument of the function the perturbation is made.

[3] That is, a smooth function for which the Taylor series computed about each point is convergent in an open neighborhood around that point.

[4] The "l" and "r" convention used here is opposite that used in much of the mathematics literature in which "l" and "r" denote which operators commute under left or right shifts. Here, $(\tilde{X}^r f)(g)$, which is generated by an infinitesimal shift on the right side, commutes with arbitrary left shifts and $(\tilde{X}^l f)(g)$, which is generated by an infinitesimal shift on the left side, commutes with arbitrary right shifts.

Note that left Lie derivatives commute with right shifts and right Lie derivatives commute with left shifts. In other words, if $(L(h)f)(g) \doteq f(h^{-1} \circ g)$ and $(R(h)f)(g) = f(g \circ h)$ for $h, g \in G$, then

$$(\tilde{X}^r L(h)f)(g) = (L(h)\tilde{X}^r f)(g) = \frac{d}{dt} f(h^{-1} \circ g \circ \exp(tX))\bigg|_{t=0} \tag{11.5}$$

and

$$(\tilde{X}^l R(h)f)(g) = (R(h)\tilde{X}^l f)(g) = \frac{d}{dt} f(\exp(-tX) \circ g \circ h)\bigg|_{t=0}. \tag{11.6}$$

If E_i is a basis for the Lie algebra $\mathcal{G}$, then, for reasons analogous to those behind the derivation of (11.2), it can be shown that if $X = \sum_{i=1}^n x_i E_i$, then

$$(\tilde{X}^r f)(g) = \sum_{i=1}^n x_i (\tilde{E}_i^r f)(g) \quad \text{and} \quad (\tilde{X}^l f)(g) = \sum_{i=1}^n x_i (\tilde{E}_i^l f)(g).$$

If $\{E_i\}$ is an orthonormal basis analogous to the natural basis for $\mathbb{R}^n$, which is denoted as $\{\mathbf{e}_i\}$, then the associated differential operators will be denoted as $\tilde{E}_i^r f$, and likewise for the left case.

11.1.2 Derivatives for $SO(3)$

If $R \in G = SO(3)$, and the basis in (10.83) is used, then the derivatives of a function $f(R)$ can be computed using the definitions presented above. If $R = R(\alpha, \beta, \gamma)$ is the ZXZ parameterization, then

$$\begin{aligned}
\tilde{E}_1^r &= \frac{\sin\gamma}{\sin\beta}\frac{\partial}{\partial\alpha} + \cos\gamma\frac{\partial}{\partial\beta} - \cot\beta\sin\gamma\frac{\partial}{\partial\gamma}, \\
\tilde{E}_2^r &= \frac{\cos\gamma}{\sin\beta}\frac{\partial}{\partial\alpha} - \sin\gamma\frac{\partial}{\partial\beta} - \cot\beta\cos\gamma\frac{\partial}{\partial\gamma}, \\
\tilde{E}_3^r &= \frac{\partial}{\partial\gamma}.
\end{aligned}$$

The operators $\tilde{E}_i^l$ can be derived in a completely analogous way. Explicitly in terms of ZXZ Euler angles,

$$\begin{aligned}
\tilde{E}_1^l &= \sin\alpha\cot\beta\frac{\partial}{\partial\alpha} - \cos\alpha\frac{\partial}{\partial\beta} - \frac{\sin\alpha}{\sin\beta}\frac{\partial}{\partial\gamma}, \\
\tilde{E}_2^l &= -\cos\alpha\cot\beta\frac{\partial}{\partial\alpha} - \sin\alpha\frac{\partial}{\partial\beta} + \frac{\cos\alpha}{\sin\beta}\frac{\partial}{\partial\gamma}, \\
\tilde{E}_3^l &= -\frac{\partial}{\partial\alpha}.
\end{aligned}$$

In Section 11.4, a trick is revealed for easily computing such expressions for derivatives when Jacobians are known. First, the general properties of these derivatives that are independent of coordinates are described.

11.2 Important Properties of Lie Derivatives

In classical calculus in $\mathbb{R}^n$, and its applications such as mechanics, the product rule and chain rule are indispensable tools. In this section it is shown that the Lie derivative inherits these properties.

11.2.1 The Product Rule

Let $f(g)$ and $h(g)$ be two functions on a unimodular group G and assume that $(\tilde{X}^r f)(g)$ and $(\tilde{X}^r h)(g)$ exist for all $g \in G$. Let

$$(f \cdot h)(g) = f(g)h(g).$$

This is nothing more than the pointwise multiplication of the values of the functions at any value of their arguments.

It then follows from the definition of $\tilde{X}^r$ that

$$\begin{aligned}(\tilde{X}^r(f \cdot h))(g) &= \frac{d}{dt}[f(g \circ \exp(tX))h(g \circ \exp(tX))]\bigg|_{t=0} \\ &= \left[\frac{d[f(g \circ \exp(tX))]}{dt} h(g \circ \exp(tX)) \right. \\ &\qquad \left. + f(g \circ \exp(tX)) \frac{d[h(g \circ \exp(tX))]}{dt}\right]_{t=0} \\ &= h(g)(\tilde{X}^r f)(g) + f(g)(\tilde{X}^r h)(g).\end{aligned}$$

To summarize,

$$\boxed{\tilde{X}^r(f \cdot h) = h \cdot \tilde{X}^r f + f \cdot \tilde{X}^r h} \tag{11.7}$$

(where $\cdot$ is just scalar multiplication of functions).

11.2.2 The Chain Rule (Version 1)

Let $\mathbf{h} : G \to \mathbb{R}^n$ be a vector-valued function of group-valued argument that has continuous Lie derivatives at all values of its argument. Let $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^m$ be a function with continuous partial derivatives. Let $\mathbf{k}(g) = \mathbf{f}(\mathbf{h}(g))$. In some situations it will be useful to compute the Lie derivative of $\mathbf{f}(\mathbf{h}(g)) = (\mathbf{f} \circ \mathbf{h})(g)$ (where $\circ$ is composition of functions),

$$\tilde{X}^r \mathbf{k} = [\tilde{X}^r k_1, \tilde{X}^r k_2, \ldots, \tilde{X}^r k_m]^T,$$

when the Lie derivatives of $\mathbf{h}(g)$ are already known. This can be achieved using the chain rule:

$$\boxed{\tilde{X}^r[\mathbf{f}(\mathbf{h}(g))] = \frac{\partial \mathbf{f}}{\partial \mathbf{h}^T} \tilde{X}^r \mathbf{h}}, \tag{11.8}$$

where $\partial \mathbf{f}/\partial \mathbf{h}^T$ is an $m \times n$ matrix with entries $[\partial \mathbf{f}/\partial \mathbf{h}^T]_{ij} = \partial f_i/\partial h_j$ and $\tilde{X}^r \mathbf{h}$ is an n-dimensional vector.

Instead of a scalar derivative operation applied to a vector-valued function, it is also possible to define a vector-valued derivative of a scalar-valued function:

$$(\tilde{\mathbf{X}}^r f)(g) = [(\tilde{X}_1^r f)(g), \ldots, (\tilde{X}_n^r f)(g)]. \tag{11.9}$$

Unlike $\tilde{X}^r \mathbf{k}$ described above, this is a row vector, reflecting that it belongs to the dual (cotangent) space of the Lie group rather than in a shifted copy of the Lie algebra (tangent space).

A different (and more interesting) form of the chain rule in (11.8) is discussed in Section 11.5.

11.3 Taylor Series on Lie Groups

The Taylor series of functions on $\mathbb{R}^n$ is a central concept in classical calculus and its applications. The concept extends naturally to functions of Lie-group-valued arguments. In Section 11.3.1 a brief review of the classical Taylor series is presented for completeness. This is followed by the natural extension to the Lie-group setting in Section 11.3.2.

11.3.1 Classical Taylor Series and Polynomial Approximation in $\mathbb{R}^n$

The One-Dimensional Case

Consider the set of functions on a closed interval of the real line $[a, b]$ that can be described as a weighted sum of the form

$$f_N(x) = \sum_{k=0}^{N} a_k x^k,$$

where $a_k \in \mathbb{R}$ for all $k \in \{0, 1, 2, \ldots\}$.

Classical calculus is concerned with the convergence properties of such series at each point $x \in [a, b]$ as $N \to \infty$. If the limit

$$f(x) = \lim_{N\to\infty} f_N(x)$$

exists for all $x \in [a, b]$, then $f(x)$ is called a real *analytic* function on $[a, b]$.

Furthermore, if $f(x)$ is assumed to be smooth, then, by definition, all of its derivatives must exist, and using the notation $f^{(k)}(x)$ for $d^k f/dx^k$, it is therefore possible to write the cascade of equations

$$\begin{aligned}
f(x) &= a_0 + a_1\, x + a_2\, x^2 + a_3\, x^3 + a_4\, x^4 + \cdots \\
f^{(1)}(x) &= a_1 + 2\cdot a_2\, x + 3\cdot a_3\, x^2 + 4\cdot a_4\, x^3 + \cdots \\
f^{(2)}(x) &= 2\cdot a_2 + 3\cdot 2\cdot a_3\, x + 4\cdot 3\cdot a_4\, x^2 + \cdots \\
f^{(3)}(x) &= 3\cdot 2\cdot a_3 + 4\cdot 3\cdot a_4\, x + \cdots \\
&\vdots \\
f^{(n)}(x) &= n!\, a_n + \cdots .
\end{aligned}$$

Evaluating both sides at $x = 0$ results in

$$f^{(k)}(0) = k!\, a_k, \tag{11.10}$$

and so for real-valued analytic functions on the real line,

$$f(x) = f(0) + f^{(1)}(0)\, x + \frac{1}{2!} f^{(2)}(0)\, x^2 + \frac{1}{3!} f^{(3)}(0)\, x^3 + \cdots = \sum_{k=0}^{\infty} \frac{1}{k!}\, f^{(k)}(0)\, x^k. \tag{11.11}$$

While in principle it is possible to sum up an infinite number of terms to reproduce the exact value $f(x)$ analytically, in practice when evaluating numerically on a computer, the sum always is truncated at a finite value. When truncated at $k = N$, the result is a polynomial, $f_N(x)$, that locally approximates $f(x)$.

Since the accuracy of the approximation obviously will depend on the distance of x from the point 0 where the approximation becomes exact, it is useful to shift the focus to the point of interest. If this point is $x = a$, then $g(x) = f(x + a)$ will have the important point at $x = 0$. Expanding $g(x)$ in a series of the form (11.11) gives

$$g(x) = f(a) + f^{(1)}(a)\,x + \frac{1}{2!}f^{(2)}(a)\,x^2 + \frac{1}{3!}f^{(3)}(a)\,x^3 + \cdots .$$

Then making the change of variables $x \to x - a$ gives the expansion of $g(x - a) = f(x)$:

$$f(x) = f(a) + f^{(1)}(a)\,(x-a) + \frac{1}{2!}f^{(2)}(a)\,(x-a)^2 + \frac{1}{3!}f^{(3)}(a)\,(x-a)^3 + \cdots . \quad (11.12)$$

Why can this be done? Because the local “shape” of the graph of a function is completely determined by its derivatives and if all points on a graph are simultaneously shifted by the same amount, the shape of the plot does not change—that is, if the derivatives of a function are computed at $x = 0$ and then all of this information is shifted to a new location on the real line, the function constructed using this shifted information will be the same as if the original function were shifted.

Note that this is not the only way to approximate functions on the interval $[a, b]$ using the basis $\{1, x, x^2, x^3, \ldots\}$. For example, instead of using condition (11.10) to constrain the values of $\{a_k\}$, it might be desirable to approximate $f(x)$ with the polynomial

$$\tilde{f}_N(x) = \sum_{k=0}^{N} \tilde{a}_k x^k \quad \text{such that} \quad \tilde{a}_k = \arg\min_{\alpha_k} \int_a^b |f(x) - \sum_{k=0}^{N} \alpha_k x^k|^2 w(x)\,dx$$

for a chosen weighting function $w(x) \geq 0$ for all $x \in [a, b]$. Since the above minimization of a quadratic cost function can be carried out in closed form, the *mean-squared approximation* $\tilde{f}_N(x)$ would require solving a system of equations of the form

$$M\tilde{\mathbf{a}} = \mathbf{b}, \quad \text{where } M_{kl} = \int_a^b x^{k+l} w(x)\,dx; \qquad b_k = \int_a^b x^k f(x) w(x)\,dx.$$

Alternatively, if $\{p_n(x)\}$ is a complete set of polynomials orthonormal with respect to the weight $w(x)$, then $\tilde{f}_N(x) = \sum_{k=0}^{N} \tilde{a}'_k p_k(x)$ and the coefficients $\{\tilde{a}'_k\}$ can be obtained without matrix inversion.

The Multi-dimensional Case

In the same way that any real analytic function $f(x)$ on an interval can be expanded in the polynomial basis $\{1, x, x^2, x^3, \ldots\}$, any function of two variables $f(x, y)$ on $[a_1, b_1] \times [a_2, b_2]$ can be expanded in a basis consisting of products of $\{1, x, x^2, x^3, \ldots\}$ and $\{1, y, y^2, y^3, \ldots\}$. In other words, a real analytic function on a planar region is one for which it is possible to write

$$f(x, y) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} a_{mn} x^m y^n.$$

Taking partial derivatives of both sides and evaluating at $\mathbf{x} = [x, y]^T = \mathbf{0}$ constrains the coefficients $\{a_{mn}\}$ as

$$a_{mn} = \frac{1}{m!}\frac{1}{n!}\left.\frac{\partial^{m+n} f}{\partial x^m \partial y^n}\right|_{\mathbf{x}=\mathbf{0}}.$$

The extension to higher dimensions follows in a natural way.

Usually, in multi-dimensional Taylor-series expansions, only terms up to quadratic order in the components of $\mathbf{x}$ are retained. This is written for $\mathbf{x} \in \mathbb{R}^n$ as

$$f(\mathbf{x}) = f(\mathbf{0}) + \sum_{i=1}^{n} \left.\frac{\partial f}{\partial x_i}\right|_{\mathbf{x}=\mathbf{0}} \cdot\ x_i + \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} \left.\frac{\partial^2 f}{\partial x_i \partial x_j}\right|_{\mathbf{x}=\mathbf{0}} \cdot\ x_i x_j + O(\|\mathbf{x}\|^3). \tag{11.13}$$

11.3.2 Taylor Series on Lie Groups

In a sense, Lie groups were “built” to allow for Taylor series. This is because Lie groups are “analytic manifolds” with an “analytic group operation.” This all boils down to allowing for Taylor series approximation in a small neighborhood around any group element, as well as the Taylor-series approximation of the product of two group elements that are both slightly perturbed from their original values.

Two concepts are often confused: analyticity and smoothness. A Lie group is smooth because through any point $g_0 \in G$, a curve can be defined by the smooth functions $g_0 \to g_0 \circ \exp(tX)$ and $g_0 \to \exp(tX) \circ g_0$ for arbitrary $X \in \mathcal{G}$. The results of these functions can be called $g_1(t)$ and $g_2(t)$, respectively. The “velocities” $\Omega_i^r = g_i^{-1}(dg_i/dt)$ and $\Omega_i^l = (dg_i/dt)g_i^{-1}$ and all of their derivatives, $d^n\Omega_i^r/dt^n$ and $d^n\Omega_i^l/dt^n$, exist for all $n = 1, 2, \ldots$. Analytic functions are smooth functions that have the additional property that their Taylor series are convergent at any point. Exactly what is meant by a Taylor series of a function on a Lie group is defined below. With this in hand, the concept of analytic functions and analytic group operation that appear in the formal definition of a Lie group can be more easily understood. For a more complete and rigorous treatment, see [2].

Let $f : \mathbb{R}^{n\times n} \to \mathbb{R}$ be an analytic function. Since $\mathbb{R}^{n\times n}$ can be identified with $\mathbb{R}^{n^2}$, it is already clear how to define f as an infinite series of polynomials. Now, if G is a group consisting of $n \times n$ real matrices, then $G \subset \mathbb{R}^{n\times n}$, and, naturally, $f : G \to \mathbb{R}$ is well defined. Since elements of a Lie group in a sufficiently small neighborhood of the identity can be expanded in the convergent Taylor series

$$\exp(tX) = I + \sum_{k=1}^{\infty} \frac{t^k}{k!} X^k$$

and since f is an analytic function and the group operation is analytic, it follows that

$$f(g \circ \exp(tX)) = \sum_{n=0}^{\infty} a_n(g) t^n.$$

This is a one-dimensional Taylor series in $t \in \mathbb{R}$. It follows from the one-dimensional Taylor formula (11.11) that

$$a_n(g) = \frac{1}{n!}\frac{d^n}{dt^n} f(g \circ \exp tX)\bigg|_{t=0}$$

and so

$$f(g \circ \exp tX) = f(g) + \left.\frac{d}{ds} f(g \circ \exp sX)\right|_{s=0} t + \frac{1}{2!} \left.\frac{d^2}{ds^2} f(g \circ \exp sX)\right|_{s=0} t^2 + \cdots . \tag{11.14}$$

However, this can be written in a different form. Consider $a_2(g)$ and write

$$\begin{aligned} a_2(g) &= \frac{1}{2} \frac{d}{dt_2} \left[\left. \frac{d}{dt_1} f(g \circ \exp t_1 X \circ \exp t_2 X) \right|_{t_1=0} \right] \Bigg|_{t_2=0} \\ &= \frac{1}{2} \frac{d}{dt_2} \left[\left. \frac{d}{dt_1} f(g \circ \exp t_2 X \circ \exp t_1 X) \right|_{t_1=0} \right] \Bigg|_{t_2=0} \\ &= \frac{1}{2} \frac{d}{dt_2} \left[(\tilde{X}^r f)(g \circ \exp t_2 X) \right] \Bigg|_{t_2=0} \\ &= \frac{1}{2} (\tilde{X}^r f)^2 (g), \end{aligned} \tag{11.15}$$

where $\tilde{X}^r f$ was defined in (11.3), and due to the property that $\tilde{X}^r f = \sum_{k=1}^{d} x_k \tilde{E}_k^r f$, the Taylor series on G can be written about $g \in G$ to second order in the "small" coefficients $\{x_i\}$ as

$$\boxed{f(g \circ \exp tX) = f(g) + t \sum_{k=1}^{d} (\tilde{E}_k^r f)(g)\, x_k + \frac{1}{2} t^2 \sum_{i=1}^{d} \sum_{j=1}^{d} (\tilde{E}_i^r \tilde{E}_j^r f)(g)\, x_k x_l + O(\|\mathbf{x}\|^3 t^3).} \tag{11.16}$$

Everything follows in an analogous way when expanding in a "left" Taylor series:

$$\boxed{f(\exp(-tX) \circ g) = f(g) + t \sum_{k=1}^{d} (\tilde{E}_k^l f)(g)\, x_k + \frac{1}{2} t^2 \sum_{i=1}^{d} \sum_{j=1}^{d} (\tilde{E}_i^l \tilde{E}_j^l f)(g)\, x_k x_l + O(\|\mathbf{x}\|^3 t^3).} \tag{11.17}$$

11.4 Relationship Between the Jacobian and Lie Derivatives

In practice, when computing the Lie derivatives $(\tilde{E}_i^r f)(g)$ and $(\tilde{E}_i^l f)(g)$, the function $f(g)$ will be expressed in terms of the particular parameterization $g = g(\mathbf{q})$ that is being used. Therefore, it is convenient to have expressions that allow for the computation of the Lie derivatives in terms of operations involving $\mathbf{q}$. The way to do this is explained in this subsection for general $X \in \mathcal{G}$ rather than for a particular basis element $E_i \in \mathcal{G}$.

The explicit forms of the operators $(\tilde{X}^l f)(g(\mathbf{q}))$ and $(\tilde{X}^r f)(g(\mathbf{q}))$ in any n-parameter description of $g \in G$ can be found as follows. Start with $(\tilde{X}^r f)(g(\mathbf{q}))$. Since $f(g)$ and the parameterization $g(\mathbf{q})$ are both assumed to be analytic, expanding the composed mapping $\tilde{f}(\mathbf{q}) = f(g(\mathbf{q}))$ in a Taylor series is possible and gives

$$(\tilde{X}^r f)(g(\mathbf{q})) = \sum_{i=1}^{n} \left. \frac{\partial \tilde{f}}{\partial q_i} \frac{dq_i^r}{dt} \right|_{t=0} ,$$

where $\{q_i^r\}$ are the parameters such that $g(\mathbf{q}) \circ \exp(tX) = g(\mathbf{q}^r(t))$.

The coefficients $\left.\frac{dq_i^r}{dt}\right|_{t=0}$ are determined by observing two different-looking, though equivalent, ways of writing $g(\mathbf{q}) \circ \exp(tX)$ for small values of t:

$$g + tgX \approx g \circ \exp(tX) \approx g + t \sum_{i=1}^{n} \frac{\partial g}{\partial q_i} \left.\frac{dq_i^r}{dt}\right|_{t=0}.$$

These approximation signs become exact as t becomes infinitesimally small. We then have that

$$X = \sum_{i=1}^{n} g^{-1} \frac{\partial g}{\partial q_i} \left.\frac{dq_i^r}{dt}\right|_{t=0},$$

or

$$(X)^{\vee} = \sum_{i=1}^{n} \left(g^{-1} \frac{\partial g}{\partial q_i} \right)^{\vee} \left.\frac{dq_i^r}{dt}\right|_{t=0},$$

which is written as[5]

$$(X)^{\vee} = J_r \left.\frac{d\mathbf{q}^r}{dt}\right|_{t=0}.$$

This allows us to solve for

$$\left.\frac{d\mathbf{q}^r}{dt}\right|_{t=0} = J_r^{-1} (X)^{\vee}.$$

The final result is then

$$(\tilde{X}^r f)(g(\mathbf{q})) = \sum_{i=1}^{n} \frac{\partial \tilde{f}}{\partial q_i} \mathbf{e}_i^T J_r^{-1} (X)^{\vee}. \tag{11.18}$$

This can also be written in matrix form as

$$\boxed{(\tilde{X}^r f)(g(\mathbf{q})) = \sum_{j=1}^{n} x_j \mathbf{e}_j^T J_r^{-T} \frac{\partial \tilde{f}}{\partial \mathbf{q}},} \tag{11.19}$$

where $x_j = \mathbf{e}_j^T (X)^{\vee}$ and $X = \sum_j x_j E_j$.

Analogous calculations for the left Lie derivative give

$$(\tilde{X}^l f)(g(\mathbf{q})) = -\sum_{i=1}^{n} \frac{\partial \tilde{f}}{\partial q_i} \mathbf{e}_i^T J_l^{-1} (X)^{\vee}. \tag{11.20}$$

This can also be written in matrix form as

$$\boxed{(\tilde{X}^l f)(g(\mathbf{q})) = -\sum_{j=1}^{n} x_j \mathbf{e}_j^T J_l^{-T} \frac{\partial \tilde{f}}{\partial \mathbf{q}}.} \tag{11.21}$$

As an example of these equations, refer back to Section 11.1.2 where the derivatives for $SO(3)$ were given for $X = E_j$ for $j = 1, 2,$ and 3. The "body" Jacobian J_r for $SO(3)$ has an inverse of the form given in (10.90). Taking the transpose and multiplying by the gradient vector $[\partial/\partial\alpha, \partial/\partial\beta, \partial/\partial\gamma]^T$ as in (11.19) then gives $[\tilde{E}_1^r, \tilde{E}_2^r, \tilde{E}_3^r]^T$. For the special case of $SO(3)$, the relationship $J_l = R J_r$ holds, and so $J_l^{-1} = J_r^{-1} R^T$ can

[5] As usual, $J_r = J_r(\mathbf{q})$, but in the expressions that follow, the dependence on $\mathbf{q}$ is suppressed to avoid clutter.

be used to easily to compute J_l^{-1} once J_r^{-1} is known. The resulting J_l^{-1} is given in (10.90). Then (11.21) can be used to easily obtain the derivatives $[\tilde{E}_1^l, \tilde{E}_2^l, \tilde{E}_3^l]^T$ listed in Section 11.1.2.

11.5 The Chain Rule for Lie Groups (Version 2)

Given a mapping $\boldsymbol{\phi} : \mathbb{R}^n \times \mathbb{R}_{\geq 0} \to \mathbb{R}^n$ and a function $F : \mathbb{R}^n \times \mathbb{R}_{\geq 0} \to \mathbb{R}$, the classical chain rule states

$$\frac{\partial}{\partial t}\left[F(\boldsymbol{\phi}(\mathbf{x},t),t)\right] = \left.\frac{\partial F(\mathbf{k},t)}{\partial \mathbf{k}^T}\right|_{\mathbf{k}=\boldsymbol{\phi}(\mathbf{x},t)} \frac{\partial \boldsymbol{\phi}}{\partial t} + \left.\frac{\partial F(\mathbf{k},t)}{\partial t}\right|_{\mathbf{k}=\boldsymbol{\phi}(\mathbf{x},t)} \tag{11.22}$$

or, equivalently,

$$\frac{\partial}{\partial t}\left[F(\boldsymbol{\phi}(\mathbf{x},t),t)\right] = \left.\frac{\partial F(\mathbf{k},t)}{\partial t}\right|_{\mathbf{k}=\boldsymbol{\phi}(\mathbf{x},t)} + \sum_{i=1}^{n} \frac{\partial \phi_i}{\partial t} \left.\frac{\partial F(\mathbf{k},t)}{\partial k_i}\right|_{\mathbf{k}=\boldsymbol{\phi}(\mathbf{x},t)}. \tag{11.23}$$

Given a Lie group G and defining $\mathbf{x} = (\log g)^\vee$, then one instance of the above that is relevant to the context of Lie groups is when

$$\boldsymbol{\phi}(\mathbf{x},t) = [\log(m^{-1}(t) \circ g)]^\vee, \quad \text{where } m^{-1}(t) \doteq [m(t)]^{-1},$$

g is a fixed element of G, and $m(t)$ is a path in G parameterized by time t. Although the logarithm map may not be defined for all $g \in G$, for the groups of most interest in applications, it will be defined for all $g \in G$ except possibly a set of measure zero.

A function $f : G \times \mathbb{R}_{\geq 0} \to \mathbb{R}$ can be expressed as one in exponential coordinates as

$$F(\mathbf{x},t) = f(g,t), \quad \text{where } g = \exp X \quad \text{and} \quad \mathbf{x} = X^\vee. \tag{11.24}$$

In many applications that will follow in subsequent chapters, $f(g,t)$ will be a time-evolving family of probability density functions (pdfs) on G, and we will be interested in the integral of this function over subsets of G. Although the details of how to integrate over G are left to the next chapter, it is sufficient for the purposes of the current discussion to know that since G is a manifold, it is possible to integrate on G using concepts from Chapter 8 of Volume 1.

If for each fixed value of t, the support of $f(g,t)$ in G is confined to a small ball around m, then when computing integrals over G, only values for which $d(m,g) = \|\log(m^{-1} \circ g)\| \ll 1$ will contribute. Thus, for such "concentrated" pdfs, these are the only values of $g \in G$ that really matter. This means that even though $m(t)$ may not be small (in the sense of being close to the identity of G), we can focus our attention on values of g where $\|m^{-1} \circ g - \mathbb{I}\|$ will be small and make the convenient approximation

$$\log(m^{-1} \circ g) \approx m^{-1} \circ g - \mathbb{I}. \tag{11.25}$$

Therefore, since the $\vee$ and $\partial/\partial t$ operators are both linear and they commute, when the above approximation holds,

$$\frac{\partial \boldsymbol{\phi}}{\partial t} = \left(\frac{dm^{-1}}{dt} g\right)^\vee = -\left(m^{-1}\frac{dm}{dt} m^{-1} g\right)^\vee.$$

If $m(t)$ is defined by a system of ordinary differential equations (ODEs) of the form

$$\frac{dm}{dt} = mA(t) \quad \text{or} \quad \frac{dm}{dt} = S(t)m, \quad \text{where } m(0) = m_0$$

(as would be the case for a body-fixed or space-fixed description of free rigid-body motion), then, using (11.25),

$$\frac{\partial \phi}{\partial t} = -\left(Am^{-1}g\right)^{\vee} \approx -\left(A[\mathbb{I} + \log(m^{-1} \circ g)]\right)^{\vee} = -\mathbf{a} - \left(A \log(m^{-1} \circ g)\right)^{\vee}$$

or

$$\begin{aligned}\frac{\partial \phi}{\partial t} &= -\left(m^{-1}Sg\right)^{\vee} = -\left((m^{-1}Sm)(m^{-1} \circ g)\right)^{\vee} \approx -\left((m^{-1}Sm)[\mathbb{I} + \log(m^{-1} \circ g)]\right)^{\vee} \\ &= -Ad(m^{-1})\mathbf{s} - \left((m^{-1}Sm)\log(m^{-1} \circ g)\right)^{\vee}.\end{aligned}$$

However, if $\|\log(m^{-1} \circ g)\|$ is small, then the second term in each of the above two equations is insignificant compared to the first, and we can write the (approximate) equalities

$$\boxed{\frac{\partial \phi}{\partial t} \approx -\mathbf{a} \quad \text{and} \quad \frac{\partial \phi}{\partial t} \approx -Ad(m^{-1})\mathbf{s}.} \tag{11.26}$$

As a special case, if A is constant of the form

$$A = \sum_{i=1}^{n} a_i E_i \qquad \text{and} \qquad m(t) = \exp\left(t \sum_{i=1}^{n} a_i E_i\right),$$

then $m^{-1}Am = A$, and both expressions in (11.26) reduce to the same thing. Furthermore, if both $\|(\log g)^{\vee}\|$ and $\|(\log m)^{\vee}\|$ are small, then

$$\log(m^{-1} \circ g) \approx (\log g)^{\vee} - (\log m)^{\vee}$$

and

$$\frac{\partial \phi}{\partial t} \approx -\frac{d}{dt}(\log m)^{\vee} \approx -\mathbf{a},$$

which is consistent with, although not a necessary condition for, (11.26) to hold.

In any case, since (11.26) holds and since near the identity $e \in G$

$$\tilde{E}_i^r f \approx -\tilde{E}_i^l f \approx \frac{\partial F}{\partial x_i},$$

where the relationship between f and F is given in (11.24), it follows that (11.22) can be adapted to the Lie group setting involving concentrated functions as

$$\boxed{\frac{\partial}{\partial t}\left[f(m^{-1}(t) \circ g, t)\right] \approx \left.\frac{\partial f(k,t)}{\partial t}\right|_{k=m^{-1}\circ g} - \sum_{i=1}^{n} a_i \cdot \left.(\tilde{E}_i^r f)\right|_{k=m^{-1}\circ g}} \tag{11.27}$$

or

$$\boxed{\frac{\partial}{\partial t}\left[f(m^{-1}(t) \circ g, t)\right] \approx \left.\frac{\partial f(k,t)}{\partial t}\right|_{k=m^{-1}\circ g} + \sum_{i=1}^{n} a_i \cdot \left.(\tilde{E}_i^l f)\right|_{k=m^{-1}\circ g}.} \tag{11.28}$$

11.6 Compact Connected Lie Groups as Riemannian Symmetric Spaces

Let M be a connected Riemannian manifold and let $\gamma_p(t)$ be a geodesic curve in M that passes through $p \in M$ when $t = 0$—that is, $\gamma_p(t) \in M$ for all specified values of t and $\gamma_p(0) = p$. If $\mathcal{X}$ and $\mathcal{Y}$ are vector fields on M and $\mathcal{X}_p$ and $\mathcal{Y}_p$ denote vectors evaluated at $p \in M$, then $\langle \mathcal{X}_p, \mathcal{Y}_p \rangle$ and $R(\mathcal{X}_p, \mathcal{Y}_p)$ respectively denote coordinate-free versions of Riemannian metric and curvature tensors evaluated at $p \in M$. The choice of a metric is not unique, and it influences the value of the curvature tensor.

A *Riemannian symmetric space* is a special kind of Riemannian manifold such that for each point $p \in M$ there is an isometry (distance-preserving mapping) $I_p : M \to M$ for which $I_p(p) = p$ and $I_p(\gamma(t)) = \gamma(-t)$ [9]. An example of I_p was in_p discussed in Section 10.1.6 in the context of homogeneous spaces. A number of books on differential geometry and harmonic analysis focus on symmetric spaces, e.g., [10, 11]. The purpose of this section is to discuss the specific case of compact connected Lie groups. Since these can always be viewed as a subset $G \subset \mathbb{R}^{N \times N} \cong \mathbb{R}^{N^2}$, they always admit a Riemannian metric induced by the ambient space and hence are Riemannian manifolds.

11.6.1 Invariant Vector Fields: The Geometric View

Let G be any compact connected Lie group. If $g \in G$, then left and right shifts by $h \in G$ are defined as $l_h(g) \doteq h \circ g$ and $r_h(g) \doteq g \circ h$. Similarly, if $\mathcal{X}_g$ denotes a vector assigned to $g \in G$, then the collection $\mathcal{X} = \{\mathcal{X}_g | g \in G\}$ defines a vector field on G where each $\mathcal{X}_g$ can be defined according to how it acts on an arbitrary function $f \in C^\infty(G)$ as

$$(\mathcal{X}_g f)(g) \doteq \sum_{i=1}^{n} x_i(g)(\tilde{E}_i^r f)(g). \tag{11.29}$$

Here, each $x_i(g)$ is a smooth scalar function on G which serves as the ith component of the vector in the vector field evaluated at $g \in G$.

This is equivalent to the more general definition of a vector field on a manifold evaluated at a point p in a neighborhood parameterized locally with coordinates $\{q_i\}$,

$$(\mathcal{X}_p f)(p) = \sum_{i=1}^{n} x_i(p) \left. \frac{\partial f}{\partial q_i} \right|_{p(q)=p} .$$

This $\mathcal{X}$ should not be confused with an element of the Lie algebra, $X \in \mathcal{G}$. However, as will be seen shortly, a correspondence between elements of a Lie algebra and *invariant* vector fields can be made in the case when each $x_i(g)$ in (11.29) is independent of g.

The space of all smooth vector fields on G is denoted as $\mathfrak{X}(G)$, and this space contains $\mathcal{X}$. The push forwards of these vector fields associated with the mappings $r_h : G \to G$ and $l_h : G \to G$ are defined in terms of individual vectors respectively as $(r_h)_*(\mathcal{X}_g) \doteq \mathcal{X}_{g \circ h}$ and $(l_h)_*(\mathcal{X}_g) \doteq \mathcal{X}_{h \circ g}$. To avoid proliferation in the number of parenthesis, the shorthand for $(r_h)_*(\mathcal{X}_g)$ and $(l_h)_*(\mathcal{X}_g)$ is $r_{h,*}(\mathcal{X}_g)$ and $l_{h,*}(\mathcal{X}_g)$, respectively. These push forwards applied to *the whole* vector fields are denoted as $r_{h,*}\mathcal{X} = \{r_{h,*}(\mathcal{X}_g) | g \in G\}$ and $l_{h,*}\mathcal{X} = \{l_{h,*}(\mathcal{X}_g) | g \in G\}$. A vector field is called left or right invariant, respectively, if $l_{h,*}\mathcal{X} = \mathcal{X}$ or $r_{h,*}\mathcal{X} = \mathcal{X}$. Of course, these equalities are at the level of a whole vector field, not at the level of individual vectors, the latter of which are generally not invariant under shifts.

For example, consider the group $SO(2) \cong S^1$ embedded as the unit circle in the plane in the usual way. A vector field on the circle can be defined to consist of unit tangent vectors assigned to each point and pointing counterclockwise. The position at an arbitrary planar position assigned to $g(\theta) \in SO(2)$ will be $\mathbf{x}_{g(\theta)} = [\cos\theta, \sin\theta]^T$, and $\mathbf{x}_{g(\theta_1)\circ g(\theta_2)} = \mathbf{x}_{g(\theta_1+\theta_2)}$. The unit tangent vector associated with the group element $g(\theta)$ when written as a vector in $\mathbb{R}^2$ will be $\mathcal{X}_{g(\theta)} = [-\sin\theta, \cos\theta]^T$. Shifting by $h = g(\theta_0) \in SO(2)$ will make $g(\theta) \to g(\theta+\theta_0)$ and $l_{h,*}(\mathcal{X}_{g(\theta)}) = \mathcal{X}_{g(\theta_0)\circ g(\theta)} = R(\theta_0)\mathcal{X}_{g(\theta)}$. Since this is a commutative group, left and right shifts are the same, and so there is no need to address $r_{h,*}$. Viewed graphically, a circle drawn on a plane with counter-clockwise-pointing unit-length tangents emanating from each point will look the same if the whole picture is rotated about the center of the circle by any amount. This is one way to visualize the invariance of this vector field. That does not mean that each tangent vector remains where it started; indeed each vector moves together with each group element. However, the field as a whole is invariant under the rotation. In contrast, if any of the tangent vectors had a length that was different than the others, rotating the picture would result in a different picture. In that case, the vector fields would not be invariant.

11.6.2 Bi-invariant Vector Fields and Associated Metrics

In general, the vector fields $\mathcal{X}$ need not be left or right invariant. However, every left- or right-invariant vector field $\mathcal{X}$ on G can be identified with a Lie algebra basis element as

$$\mathcal{X} \longleftrightarrow X \tag{11.30}$$

by returning to (11.29) and setting

$$x_i(g) = (X, E_i),$$

where $(\cdot,\cdot)$ is the inner product for the Lie algebra $\mathcal{G}$. This is the same as setting $x_i(g) = x_i(e)$. Because of the above correspondence, when the discussion is restricted to left-invariant vector fields on Lie groups, it is possible to make the correspondences

$$l_{g,*}(\mathcal{X}_e) \leftrightarrow gX \quad \text{and} \quad r_{g,*}(\mathcal{X}_e) \leftrightarrow Xg, \tag{11.31}$$

where $X \in \mathcal{G}$ corresponds to $\mathcal{X}_e \in T_eG$.

Suppose that G admits a Riemannian metric $\langle \mathcal{X}_g, \mathcal{Y}_g \rangle$ (which need not be invariant under left or right shifts in the sense that $\langle \mathcal{X}_g, \mathcal{Y}_g \rangle$, $\langle l_{h,*}(\mathcal{X}_g), l_{h,*}(\mathcal{Y}_g) \rangle$, and $\langle r_{h,*}(\mathcal{X}_g), r_{h,*}(\mathcal{Y}_g) \rangle$ can all take different values). This metric need not be the one that results from the fact that $G \subset \mathbb{R}^{N\times N}$.

It turns out that when G is compact, it is always possible to construct a new bi-invariant Riemannian metric from this old one. This is achieved by averaging over the group. The bi-invariant Riemannian metric resulting from averaging is defined as

$$\langle \mathcal{X}_g, \mathcal{Y}_g \rangle_G \doteq \int_G \int_G \langle l_{h,*} r_{k,*} \mathcal{X}_g, l_{h,*} r_{k,*} \mathcal{Y}_g \rangle \, d(h) \, d(k). \tag{11.32}$$

This is because, as we will see in the next chapter, compact Lie groups always admit bi-invariant integration measures and hence are unimodular.[6]

[6] If $g \in G$ (an n-dimensional unimodular Lie group), then in the context of integration $d(g)$ denotes the bi-invariant differential volume element, which is an n-form that we will soon see how to construct. This is not to be confused with dg in (11.34), which is a 1-form. When the context is clear, $d(g)$ is often abbreviated as dg. Although generally it is not good to use the same notation for two very different objects, this should not be a source of confusion since 1-forms and n-forms will rarely be used simultaneously, and the one being discussed will be clear from the context. This is analogous to how $d(\mathbf{x})$ and $d\mathbf{x}$ are used in the context of $\mathbf{x} \in \mathbb{R}^n$, as explained in footnote 7 in Section 2.2 of Volume 1, and how the abbreviation of $d(\mathbf{x})$ as $d\mathbf{x}$ does not usually cause difficulties.

It is left as an exercise to verify that this metric is bi-invariant.

11.6.3 Lie Bracket Versus Jacobi–Lie Bracket

In (6.62) of Volume 1, the Lie bracket of two vector fields, $\mathcal{A}$ and $\mathcal{B}$, on a manifold was defined. In order to distinguish this from the Lie bracket of two Lie algebra elements, $[A, B]$, let us refer to (6.62) here as the *Jacobi–Lie bracket.* When writing $g = g(\mathbf{q})$ and using the shorthand $f(\mathbf{q})$ for $f(g(\mathbf{q}))$, (6.62) can be written in component form for the case of a Lie group as

$$[\mathcal{A}_g, \mathcal{B}_g]f = \sum_{i=1}^{n}\sum_{j=1}^{n}\left(a_j\frac{\partial b_i}{\partial q_j} - b_j\frac{\partial a_i}{\partial q_j}\right)\frac{\partial f}{\partial q_i},$$

where $a_i = a_i(g(\mathbf{q}))$ and $b_i = b_i(g(\mathbf{q}))$ are the coefficient functions that define $\mathcal{A}$ and $\mathcal{B}$.

If the vector fields are left invariant, then the Jacobi–Lie bracket of left-invariant vector fields on a Lie group and the Lie bracket on the Lie algebra are related by the fact that

$$([\mathcal{A}_g, \mathcal{B}_g]f)(g) = \sum_{k=1}^{n}([A, B], E_k)(\tilde{E}_k^r f)(g). \tag{11.33}$$

This follows from the definition in (11.29), the inner product $(\cdot, \cdot)$ on the Lie algebra, and the fact that the differential operators $\{\tilde{E}_k^r f\}$ commute with left shifts. Note that (11.33) is equivalent to

$$\boxed{[\mathcal{A}, \mathcal{B}] \leftrightarrow [A, B] \quad \text{and} \quad \langle[\mathcal{A}_g, \mathcal{B}_g], \mathcal{E}_{g,k}\rangle_G = ([A, B], E_k)}$$

when the normalization[7]

$$\langle\mathcal{E}_{g,k}, \mathcal{E}_{g,k}\rangle_G = (E_k, E_k) = 1$$

is enforced, and the correspondence $\mathcal{E}_k \leftrightarrow E_k$ is analogous to that in (11.30). Since $([A, B], E_k)$ is independent of g, it follows that the Jacobi–Lie bracket of left-invariant vector fields in (11.33) is again left invariant.

If $R_G(\mathcal{X}_g, \mathcal{Y}_g)$ is the Riemannian curvature tensor computed with respect to $\langle\mathcal{X}_g, \mathcal{Y}_g\rangle_G$ at the point $g \in G$, then the following identities involving the (Jacobi)–Lie bracket $[\mathcal{X}_g, \mathcal{Y}_g]$ hold when $\mathcal{X}_g$, $\mathcal{Y}_g$, $\mathcal{Z}_g$, and $\mathcal{W}_g$ are all left invariant [9]:

$$\begin{aligned}
\langle[\mathcal{X}_g, \mathcal{Y}_g], \mathcal{Z}_g\rangle_G &= \langle\mathcal{X}_g, [\mathcal{Y}_g, \mathcal{Z}_g]\rangle_G,\\
R_G(\mathcal{X}_g, \mathcal{Y}_g)\mathcal{Z}_g &= \frac{1}{4}[[\mathcal{X}_g, \mathcal{Y}_g], \mathcal{Z}_g],\\
\langle R_G(\mathcal{X}_g, \mathcal{Y}_g)\mathcal{Z}_g, \mathcal{W}_g\rangle_G &= \frac{1}{4}\langle[\mathcal{X}_g, \mathcal{Y}_g], [\mathcal{Z}_g, \mathcal{W}_g]\rangle_G.
\end{aligned}$$

As a consequence, the sectional curvatures of compact connected Lie groups are always nonnegative:

$$\langle R_G(\mathcal{X}_g, \mathcal{Y}_g)\mathcal{X}_g, \mathcal{Y}_g\rangle_G = \frac{1}{4}\langle[\mathcal{X}_g, \mathcal{Y}_g], [\mathcal{X}_g, \mathcal{Y}_g]\rangle_G \geq 0$$

with equality iff $[\mathcal{X}_g, \mathcal{Y}_g] = \mathbb{O}$.

Interestingly, the geodesics with respect to the bi-invariant Riemannian metric on G that pass through the identity element are the one-parameter subgroups of G [9].

[7] Here, the subscript k is an indexing number and should not be confused with the case when a subscript denotes a specific group element. In E_k, the number k is in $\{1, \ldots, n\}$; in $\mathcal{A}_g$, the subscript is $g \in G$; and in $\mathcal{E}_{g,k}$, the subscripts denote both.

11.7 Differential Forms and Lie Groups

Differential forms for Lie groups are constructed in a very straightforward way. If $g \in G$ is parameterized with some coordinates $\mathbf{q} \in \mathbb{R}^n$, then the derivative of $g(\mathbf{q})$ is well defined as

$$dg \doteq \sum_{i=1}^{n} \frac{\partial g}{\partial q_i} dq_i. \tag{11.34}$$

This is nothing more than the classical chain rule applied to the matrix-valued function $g(\mathbf{q})$.

It is then straightforward to compute the following 1-forms[8]:

$$\Omega_r(g) \doteq g^{-1}\, dg \qquad \text{and} \qquad \Omega_l(g) \doteq dg\, g^{-1}. \tag{11.35}$$

Here, $\Omega_r(g)$ is invariant under left translations of the form $g \to g_0 \circ g$ and $\Omega_l(g)$ is invariant under right translations of the form $g \to g \circ g_0$.

11.7.1 Properties of $\Omega_r(g)$ and $\Omega_l(g)$

Note that $\Omega_r(g)\,,\, \Omega_l(g) \in \mathcal{G}$ and so

$$\Omega_r(g) = \sum_{i=1}^{n} \omega_r^{(i)}(g) E_i \qquad \text{and} \qquad \Omega_l(g) = \sum_{i=1}^{n} \omega_l^{(i)}(g) E_i. \tag{11.36}$$

The corresponding "vectors" are defined as[9]

$$\boldsymbol{\omega}_r(g) = (\Omega_r(g))^\vee = [\omega_r^{(1)}(g), \ldots, \omega_r^{(n)}(g)]^T \in \mathbb{R}^n$$

and

$$\boldsymbol{\omega}_l(g) = (\Omega_l(g))^\vee = [\omega_l^{(1)}(g), \ldots, \omega_l^{(n)}(g)]^T \in \mathbb{R}^n.$$

Instead of evaluating (11.35) at $g = e \circ g = g \circ e$, evaluating at $g_1 = g_0 \circ g$ and $g_2 = g \circ g_0$ provides some insight into the special properties of $\Omega_r(g)$ and $\Omega_l(g)$. In particular, substituting $g_1 = g_0 \circ g$ in for g yields

$$\Omega_r(g_0 \circ g) = g_1^{-1}\, dg_1 = g^{-1} \circ g_0^{-1} \circ g_0\, dg = g^{-1}\, dg = \Omega_r(g) \tag{11.37}$$

and

$$\Omega_l(g_0 \circ g) = dg_1\, g_1^{-1} = g_0\, dg\, g^{-1} \circ g_0^{-1} = g_0\, \Omega_l(g)\, g_0^{-1}, \tag{11.38}$$

and substituting $g_2 = g \circ g_0$ in for g yields

$$\Omega_r(g \circ g_0) = g_2^{-1}\, dg_2 = g_0^{-1} \circ g^{-1} dg\, g_0 = g_0^{-1}\, \Omega_r(g)\, g_0 \tag{11.39}$$

and

$$\Omega_l(g \circ g_0) = dg_2\, g_2^{-1} = dg\, g_0 \circ g_0^{-1} \circ g^{-1} = \Omega_l(g). \tag{11.40}$$

[8] The subscripts l and r are opposite to the usual convention in the literature; Here, they denote on which side ("left" or "right") the differential appears in the expression.

[9] This is one of those rare instances in this book when superscripts are used. The reason for this is so as not to clash with the subscript r and l. The use of parentheses is to avoid confusion between superscripts and powers.

It follows from these expressions that

$$\boldsymbol{\omega}_r(g_0 \circ g) = \boldsymbol{\omega}_r(g), \qquad \boldsymbol{\omega}_l(g_0 \circ g) = [Ad(g_0)]\boldsymbol{\omega}_l(g) \tag{11.41}$$

and

$$\boldsymbol{\omega}_r(g \circ g_0) = [Ad(g_0^{-1})]\boldsymbol{\omega}_r(g), \qquad \boldsymbol{\omega}_l(g \circ g_0) = \boldsymbol{\omega}_l(g); \tag{11.42}$$

that is, the entries in the vector $\boldsymbol{\omega}_r(g)$ are invariant under left shifts and the entries in $\boldsymbol{\omega}_l(g)$ are invariant under right shifts. In fact, these entries form a basis for the space of all differential 1-forms on the group G. All other invariant differential forms can be constructed from these.

Note that these are related to the Jacobian matrices defined in (10.51) as

$$\boldsymbol{\omega}_r(g) = J_r(\mathbf{q})\, d\mathbf{q} \qquad \text{and} \qquad \boldsymbol{\omega}_l(g) = J_l(\mathbf{q})\, d\mathbf{q}$$

and

$$\boldsymbol{\omega}_l(g) = [Ad(g)]\boldsymbol{\omega}_r(g).$$

The corresponding differential 1-forms are

$$\omega_r^{(i)} = \boldsymbol{\omega}_r(g) \cdot \mathbf{e}_i \qquad \text{and} \qquad \omega_l^{(i)} = \boldsymbol{\omega}_l(g) \cdot \mathbf{e}_i. \tag{11.43}$$

From these 1-forms, the rules established for computing products of forms in $\mathbb{R}^n$ are followed to create left-invariant k-forms:

$$a_r^{(k)} \doteq \sum_{i_1 < i_2 < \cdots < i_k} a_{i_1,\ldots,i_k}\, \omega_r^{(i_1)} \wedge \omega_r^{(i_2)} \wedge \cdots \wedge \omega_r^{(i_k)}$$

and likewise for $a_l^{(k)}$. The parenthesis is used to distinguish the superscript that is used to denote the scalar entry of the vector $\omega_r^{(i)} = \boldsymbol{\omega}_r(g) \cdot \mathbf{e}_i$.

11.7.2 The Maurer–Cartan Equations

The application of exterior derivatives to differential forms on Lie groups has a special structure that is captured in the Maurer–Cartan equations defined below.

Derivation

From (11.34) and the rules for computing exterior products,[10]

$$\begin{aligned} d(dg) &= d\left(\sum_{i=1}^{n} \frac{\partial g}{\partial q_i} dq_i\right) \doteq \sum_{i=1}^{n} d\left(\frac{\partial g}{\partial q_i}\right) \wedge dq_i \\ &= \sum_{i=1}^{n}\left(\sum_{j=1}^{n} \frac{\partial^2 g}{\partial q_i \partial q_j}\, dq_i \wedge dq_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} \frac{\partial^2 g}{\partial q_i \partial q_j}\, dq_i \wedge dq_j. \end{aligned} \tag{11.44}$$

[10] The notation d should not be confused with the usual differential. Whereas its meaning does coincide with the usual differential when applied to a 0-form (i.e., a scalar function), it does not follow the same rules as the usual differential when applied to other differential forms. The rules for the exterior derivative d are defined in Chapter 6 of Volume 1.

In the absence of singularities, the partial derivatives with respect to q_i and q_j commute, and due to the anti-symmetry of the wedge product, the last term is equal to 0, and so

$$\boxed{d(dg) = 0.} \tag{11.45}$$

This means that for a Lie group and a parameterization satisfying

$$dg = g\,\Omega_r \qquad \text{and} \qquad dg = \Omega_l\, g,$$

the following equations result:

$$d(dg) = dg\,\Omega_r + gd\Omega_r \qquad \text{and} \qquad d(dg) = d\Omega_l\, g + \Omega_l\, dg.$$

Multiplying by g^{-1} on the left of the first equation above and on the right of the second and using (11.45) yields

$$d\Omega_r + \Omega_r \wedge \Omega_r = 0 \qquad \text{and} \qquad d\Omega_l + \Omega_l \wedge \Omega_l = 0. \tag{11.46}$$

Dropping the subscripts l and r (since the following equations apply to both cases) and substituting in (11.36) gives

$$\begin{aligned}
\Omega \wedge \Omega &= \left(\sum_{i=1}^{n} \omega^{(i)} E_i\right) \wedge \left(\sum_{j=1}^{n} \omega^{(j)} E_j\right)\\
&= \sum_{i=1}^{n}\sum_{j=1}^{n} E_i E_j\, \omega^{(i)} \wedge \omega^{(j)}\\
&= \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} [E_i, E_j]\, \omega^{(i)} \wedge \omega^{(j)}\\
&= \frac{1}{2}\sum_{k=1}^{n}\sum_{i=1}^{n}\sum_{j=1}^{n} C_{ij}^{k} E_k\, \omega^{(i)} \wedge \omega^{(j)}.
\end{aligned}$$

Substituting this result into (11.46) and extracting component gives

$$\boxed{d\omega^{(k)} = -\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} C_{ij}^{k}\, \omega^{(i)} \wedge \omega^{(j)}.} \tag{11.47}$$

These are the *Maurer–Cartan* equations, which hold for both the r and the l case.

Implications for Structure of Jacobians

These equations can be expressed in coordinate-dependent form using the Jacobian matrix. Recall that $\omega^k = \sum_m J_{km} dq_m$ (where here the r and l designations have been suppressed). Identifying the coordinates with Euclidean space,

$$d\omega^k = d\left(\sum_m J_{km} dq_m\right) = \sum_m \left(\sum_r \frac{\partial J_{km}}{\partial q_r} dq_r\right) \wedge dq_m = \sum_m \sum_r \frac{\partial J_{km}}{\partial q_r} dq_r \wedge dq_m.$$

In addition,

$$\omega^{(i)} \wedge \omega^{(j)} = \left(\sum_r J_{ir} dq_r\right) \wedge \left(\sum_m J_{jm} dq_m\right) = \sum_r \sum_m J_{ir} J_{jm} dq_r \wedge dq_m.$$

Substituting these expressions into (11.47) gives

$$\sum_m \sum_r \frac{\partial J_{km}}{\partial q_r} dq_r \wedge dq_m = -\frac{1}{2} \sum_{i,j} C_{ij}^k \sum_r \sum_m J_{ir} J_{jm} dq_r \wedge dq_m.$$

This means that

$$\sum_m \sum_r \left\{ \frac{\partial J_{km}}{\partial q_r} + \frac{1}{2} \sum_{i,j} C_{ij}^k J_{ir} J_{jm} \right\} dq_r \wedge dq_m = 0.$$

If the term in braces is symmetric in r and m, then the above equality will hold for arbitrary infinitesimals $\{dq_m\}$. This localizes the above to

$$\frac{\partial J_{km}}{\partial q_r} + \frac{1}{2} \sum_{i,j} C_{ij}^k J_{ir} J_{jm} = \frac{\partial J_{kr}}{\partial q_m} + \frac{1}{2} \sum_{i,j} C_{ij}^k J_{im} J_{jr}.$$

However, by changing the names of dummy variables and using the fact that $C_{ij}^k = -C_{ji}^k$,

$$\sum_{ij} C_{ij}^k J_{im} J_{jr} = \sum_{ij} C_{ji}^k J_{jm} J_{ir} = -\sum_{ij} C_{ij}^k J_{im} J_{jr}.$$

Therefore, the long equation above reduces to

$$\boxed{\frac{\partial J_{km}}{\partial q_r} - \frac{\partial J_{kr}}{\partial q_m} = -\sum_{i,j} C_{ij}^k J_{ir} J_{jm}.} \tag{11.48}$$

Let J^{ms} denote the $(m-s)$th entry of J^{-1}—that is, $J^{-1} = [J^{ms}]$ and $\sum_m J_{jm} J^{ms} = \delta_{js}$. Therefore, multiplying both sides of (11.48) by J^{ms} and J^{ru} and summing over m and r isolates the structure constants as

$$\boxed{C_{us}^k = -\sum_{m,r} \left(\frac{\partial J_{km}}{\partial q_r} - \frac{\partial J_{kr}}{\partial q_m} \right) J^{ms} J^{ru}.} \tag{11.49}$$

This means that the structure of the Lie algebra can be determined from the Jacobian associated with any parameterization at a point where it is nonsingular.

11.7.3 The Exterior Derivative of Forms on a Lie Group

Let $a^{(k)}$ denote a k-form on a Lie group constructed from 1-forms $\omega^{(i_j)}$ for $j = 1, \ldots, k$ under the usual constraint that $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. All of the $\omega^{(i_j)}$s could be either left or right invariant. For now, the subscripts r and l will be suppressed. The resulting k-form is written as

$$a^{(k)} \doteq \sum_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k}(g) \omega^{(i_1)} \wedge \omega^{(i_2)} \wedge \cdots \wedge \omega^{(i_k)} \tag{11.50}$$

$$= \sum_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k}(g(\mathbf{q})) \, (\mathbf{e}_{i_1}^T J(\mathbf{q}) \, d\mathbf{q}) \wedge \cdots \wedge (\mathbf{e}_{i_k}^T J(\mathbf{q}) \, d\mathbf{q}). \tag{11.51}$$

If $a_{i_1, \ldots, i_k}(g) = a_{i_1, \ldots, i_k}$ is a constant for all values of the indices, then $a^{(k)}$ will have the same invariance as each of the $\omega^{(i_j)}$s. The equality in (11.50) can be taken to be the coordinate-free definition of the form $a^{(k)}$, whereas (11.51) is how it appears in coordinates.

The coordinate-free definition of the exterior derivative of $a^{(k)}$ given below can be expanded in coordinates, where again the r and l subscripts are suppressed:

$$da^{(k)} \doteq \sum_{i_1,\ldots,i_k} \left[\sum_j (\tilde{E}_j \, a_{i_1,\ldots,i_k})(g)\omega^{(j)} \right] \wedge \omega^{(i_1)} \wedge \omega^{(i_2)} \wedge \cdots \wedge \omega^{(i_k)} \tag{11.52}$$

$$= \sum_{i_1,\ldots,i_k} \left[\sum_{j,l} (J^{-T})_{jl} \frac{\partial a_{i_1,\ldots,i_k}(g(\mathbf{q}))}{\partial q_l} \, (\mathbf{e}_j^T J(\mathbf{q}) \, d\mathbf{q}) \right] (\mathbf{e}_{i_1}^T J(\mathbf{q}) \, d\mathbf{q}) \wedge \cdots \wedge (\mathbf{e}_{i_k}^T J(\mathbf{q}) \, d\mathbf{q}) \tag{11.53}$$

$$= \sum_{i_1,\ldots,i_k} \left[\sum_l \frac{\partial a_{i_1,\ldots,i_k}(g(\mathbf{q}))}{\partial q_l} \, dq_l \right] (\mathbf{e}_{i_1}^T J(\mathbf{q}) \, d\mathbf{q}) \wedge \cdots \wedge (\mathbf{e}_{i_k}^T J(\mathbf{q}) \, d\mathbf{q}). \tag{11.54}$$

The reason for the simplification when going from (11.53) to (11.54) is that $\sum_j J_{lj}^{-1} J_{jm} = \delta_{lm}$.

The result in (11.54) is exactly the same result as would have been obtained by treating (11.51) as a differential form on $\mathbb{R}^n$ with Cartesian coordinates $\{q_i\}$ and computing the usual definition of exterior derivative in $\mathbb{R}^n$ in these coordinates. In other words, if all of the parts of Jacobians that appear in the wedge products in (11.51) are consolidated and combined with $a_{i_1,\ldots,i_k}$, and the result is denoted as

$$a^{(k)} = \sum_{i_1,\ldots,i_k} \tilde{a}_{i_1,\ldots,i_k}(\mathbf{q}) \, dq_{i_1} \wedge dq_{i_2} \wedge \cdots \wedge dq_{i_k},$$

then when $a_{i_1,\ldots,i_k}(g) = a_{i_1,\ldots,i_k}$ is constant,

$$da^{(k)} = \sum_{i_1,\ldots,i_k} \left[\frac{\partial \tilde{a}_{i_1,\ldots,i_k}}{\partial q_j} dq_j \right] \wedge dq_{i_1} \wedge dq_{i_2} \wedge \cdots \wedge dq_{i_k}. \tag{11.55}$$

The proof of this fact is left as an exercise.

If G is a unimodular Lie group, the Hodge $*$-operator of a k-form $a^{(k)}$ can be defined in this context as the $(n-k)$-form such that

$$a^{(k)} \wedge *a^{(k)} = dg = |J_r(\mathbf{q})| \, dq_1 \wedge \cdots \wedge dq_n. \tag{11.56}$$

This is the unique (up to arbitrary scaling) invariant volume element with which to integrate functions on unimodular Lie groups. Then, for example,

$$*\omega^{(1)} = \omega^{(2)} \wedge \cdots \wedge \omega^{(n)}.$$

11.7.4 Examples

In this subsection several examples of differential forms on Lie groups that are invariant under left or right shifts are worked out. In some cases, forms are bi-invariant.

Differential Forms for the $ax + b$ Group

Referring back to Section 10.4 in which the left and right Jacobians were computed for the group of affine transformations of the real line, the 1-forms can be read off as

$$\omega_l^{(1)} = a^{-1}\, da \qquad \text{and} \qquad \omega_l^{(2)} = -a^{-1}\, b\, da + db$$

and

$$\omega_r^{(1)} = a^{-1}\, da \qquad \text{and} \qquad \omega_r^{(2)} = a^{-1}\, db.$$

The $\omega_l^{(i)}$ are right invariant and the $\omega_r^{(i)}$ are left invariant. Note that $\omega_l^{(1)} = \omega_r^{(1)}$, indicating that this is a bi-invariant 1-form.

The right- and left-invariant 2-forms are obtained by the wedge products of the 1-forms with these invariance properties as

$$\omega_l^{(1)} \wedge \omega_l^{(2)} = a^{-1}\, da \wedge db = \det J_l(a,b)\, da \wedge db$$

and

$$\omega_r^{(1)} \wedge \omega_r^{(2)} = a^{-2}\, da \wedge db = \det J_r(a,b)\, da \wedge db.$$

Differential Forms for $H(3)$

Reading the 1-forms off from the Jacobian matrices corresponding to the parameterization in (10.67),

$$\omega_r^{(1)} = d\alpha\,, \qquad \omega_r^{(2)} = d\beta - \alpha\, d\gamma\,, \qquad \omega_r^{(3)} = d\gamma$$

and

$$\omega_l^{(1)} = d\alpha\,, \qquad \omega_l^{(2)} = d\beta - \gamma\, d\alpha\,, \qquad \omega_l^{(3)} = d\gamma.$$

Therefore, $\omega_r^{(i)} = \omega_l^{(i)}$ is bi-invariant for $i = 1$ and $i = 3$. The left-invariant 2-forms are

$$\begin{aligned} \omega_r^{(1)} \wedge \omega_r^{(2)} &= d\alpha \wedge d\beta - \alpha\, d\alpha \wedge d\gamma, \\ \omega_r^{(2)} \wedge \omega_r^{(3)} &= d\beta \wedge d\gamma, \\ \omega_r^{(1)} \wedge \omega_r^{(3)} &= d\alpha \wedge d\gamma. \end{aligned}$$

The right-invariant 2-forms are

$$\begin{aligned} \omega_l^{(1)} \wedge \omega_l^{(2)} &= d\alpha \wedge d\beta, \\ \omega_l^{(2)} \wedge \omega_l^{(3)} &= -\gamma\, d\alpha \wedge d\gamma + d\beta \wedge d\gamma, \\ \omega_l^{(1)} \wedge \omega_l^{(3)} &= d\alpha \wedge d\gamma. \end{aligned}$$

Therefore, $\omega_l^{(1)} \wedge \omega_l^{(3)} = \omega_r^{(1)} \wedge \omega_r^{(3)}$ is bi-invariant.

Furthermore,

$$\omega_l^{(1)} \wedge \omega_l^{(2)} \wedge \omega_l^{(3)} = \omega_r^{(1)} \wedge \omega_r^{(2)} \wedge \omega_r^{(3)} = d\alpha \wedge d\beta \wedge d\gamma$$

is bi-invariant and serves as the natural integration measure for $H(3)$.

Differential Forms for $SE(2)$

From the Jacobian matrices in the x_1-x_2-θ parameterization in Section 10.6.2, the left- and right-invariant differential 1-forms can be read off as

$$\omega_r^{(1)} = \cos\theta\, dx_1 + \sin\theta\, dx_2, \quad \omega_r^{(2)} = -\sin\theta\, dx_1 + \cos\theta\, dx_2, \quad \omega_r^{(3)} = d\theta$$

and

$$\omega_l^{(1)} = dx_1 + x_2\, d\theta, \quad \omega_l^{(2)} = dx_2 - x_1\, d\theta, \quad \omega_l^{(3)} = d\theta.$$

From this it is clear that $\omega_r^{(3)} = \omega_l^{(3)}$ is bi-invariant.

The corresponding 2-forms are

$$\begin{aligned} \omega_r^{(1)} \wedge \omega_r^{(2)} &= dx_1 \wedge dx_2, \\ \omega_r^{(2)} \wedge \omega_r^{(3)} &= \cos\theta\, dx_1 \wedge d\theta + \sin\theta\, dx_2 \wedge d\theta, \\ \omega_r^{(1)} \wedge \omega_r^{(3)} &= -\sin\theta\, dx_1 \wedge d\theta + \cos\theta\, dx_2 \wedge d\theta \end{aligned}$$

and

$$\begin{aligned} \omega_l^{(1)} \wedge \omega_l^{(2)} &= dx_1 \wedge dx_2 - x_1\, dx_1 \wedge d\theta - x_2\, dx_2 \wedge d\theta, \\ \omega_l^{(2)} \wedge \omega_l^{(3)} &= dx_2 \wedge d\theta, \\ \omega_l^{(1)} \wedge \omega_l^{(3)} &= dx_1 \wedge d\theta. \end{aligned}$$

None of these appear to be bi-invariant. However, the 3-form is bi-invariant:

$$\omega_l^{(1)} \wedge \omega_l^{(2)} \wedge \omega_l^{(3)} = \omega_r^{(1)} \wedge \omega_r^{(2)} \wedge \omega_r^{(3)} = dx_1 \wedge dx_2 \wedge d\theta.$$

This bi-invariant form serves as the natural integration measure for $SE(2)$.

Differential Forms for $GL(2,\mathbb{R})$

As with the other examples, the left- and right-invariant 1-forms for $GL(2,\mathbb{R})$ are computed from (11.35) and (11.36), and in this case are respectively

$$\begin{aligned} \omega_r^{(1)} &= \frac{1}{\det g}(x_4 dx_1 - x_2 dx_3), \qquad \omega_r^{(2)} = \frac{1}{\det g}(x_4 dx_2 - x_2 dx_4), \\ \omega_r^{(3)} &= \frac{1}{\det g}(-x_3 dx_1 + x_1 dx_3), \qquad \omega_r^{(4)} = \frac{1}{\det g}(-x_3 dx_2 + x_1 dx_4), \end{aligned}$$

and

$$\begin{aligned} \omega_l^{(1)} &= \frac{1}{\det g}(x_4 dx_1 - x_3 dx_2), \qquad \omega_l^{(2)} = \frac{1}{\det g}(-x_2 dx_1 + x_1 dx_2), \\ \omega_l^{(3)} &= \frac{1}{\det g}(x_4 dx_3 - x_3 dx_4), \qquad \omega_l^{(4)} = \frac{1}{\det g}(-x_2 dx_3 + x_1 dx_4). \end{aligned}$$

The bi-invariant 4-form is

$$\omega_l^{(1)} \wedge \omega_l^{(2)} \wedge \omega_l^{(3)} \wedge \omega_l^{(4)} = \omega_r^{(1)} \wedge \omega_r^{(2)} \wedge \omega_r^{(3)} \wedge \omega_r^{(4)} = \frac{1}{|\det g|^2} dx_1 \wedge dx_2 \wedge dx_3 \wedge dx_4.$$

This bi-invariant form serves as the natural integration measure for $GL(2,\mathbb{R})$.

11.8 Sectional Curvature of Lie Groups

Given an arbitrary basis $\{E_i\}$ for the Lie algebra $\mathcal{G}$, the definition of an inner product such that $(E_i, E_j) = \delta_{ij}$ effectively fixes the Riemannian metric that is used. From this inner product, Jacobian matrices J_r and J_l can be defined in any coordinate system. A left-invariant metric tensor is then defined as $G_r = J_r^T J_r$, and a right-invariant one is $G_l = J_l^T J_l$. Generally, $G_l \neq G_r$. Choosing one of them as the Riemannian metric tensor $G = [g_{ij}]$ the Christoffel symbols and Riemannian and Ricci curvature tensors can be computed using the general formulas from Chapters 5 and 7 of Volume 1. In particular, Trofimov [7] reports the following relationship between the Riemannian curvature tensor and structure constants for a compact n-dimensional Lie group:

$$R^i_{j\alpha\beta} = -\frac{1}{4}\sum_{k=1}^{n} C^i_{kj} C^k_{\alpha\beta}.$$

The algebraic structure of Lie groups can be related to their geometry. For example, Milnor derived formulas that relate the Christoffel symbols and sectional curvatures (7.45) of a group manifold to the structure constants of the corresponding Lie algebra when left-invariant metrics are used [4]:

$$\Gamma^k_{ij} = \frac{1}{2}\left(C^k_{ij} - C^i_{jk} + C^j_{ki}\right) \tag{11.57}$$

and

$$\begin{aligned}\kappa(E_i, E_j) = \sum_k \frac{1}{2} C^k_{ij}(-C^k_{ij} + C^i_{jk} + C^j_{ki}) \\ - \frac{1}{4}(C^k_{ij} - C^i_{jk} + C^j_{ki})(C^k_{ij} + C^i_{jk} - C^j_{ki}) - C^i_{ki} C^j_{kj}.\end{aligned} \tag{11.58}$$

Local geometric properties of G, such as the signs of $\kappa(E_i, E_j)$ and its average, can therefore be related to the structure of the Lie algebra $\mathcal{G}$.

11.9 Chapter Summary

This chapter presented a survey of differential-geometric methods developed in previous chapters, applied here to Lie groups. Differential forms and derivatives of functions on Lie groups were defined and examples illustrated how they can be computed explicitly. Since Lie groups have more structure than general manifolds, concrete calculations in coordinates were performed easily using elementary calculus and matrix operations without having to go to a higher level of abstraction. Other books that take a similar approach include [1, 6]. For more general (and therefore abstract) approaches, see [2, 8].

The algebraic and geometric structure of a Lie group were related to equations satisfied by differential forms. These were computed explicitly in parameterizations using the Jacobian matrices defined in the previous chapter. These same Jacobians will appear in the next chapter in the context of integration of functions and differential forms on Lie groups. In addition, the Lie derivatives defined here will play a central role in the invariant definition of Fokker–Planck equations on Lie groups in problems involving stochastic flows in the final two chapters of this volume.

Although the purpose of this chapter was to serve as an introduction to concepts that will be built on and used in later chapters, it is worth noting that without any additional mathematical knowledge, the concepts presented here can be directly applied to engineering problems. For example, the chain rule for $SE(3)$ finds applications in steering flexible needles in medical applications [5]. The differential-geometric properties of the rotation group has applications in the reorientation of microsatellites [3].

11.10 Exercises

11.1. Explain why the factor of 1/2 appears on all terms at second order in (11.13).

11.2. Derive a Taylor formula analogous to (11.16) and (11.17) for the function $f(g)$ shifted from the left and right: $f(\exp(-tX) \circ g \circ \exp(tY))$.

11.3. Verify that matrices of the form

$$g(x,y,z) = \begin{pmatrix} e^x & 0 & y \\ xe^x & e^x & z \\ 0 & 0 & 1 \end{pmatrix}$$

are elements of a Lie group under the operation of matrix multiplication and compute the left- and right-invariant 1-forms, 2-forms, and 3-forms.

11.4. Substitute (10.44) into (10.43) and vice versa to verify that these expressions are the inverse of each other.

11.5. Show that the following is a valid group operation:

$$g(\mathbf{w}, \mathbf{z}, \omega) \circ g(\mathbf{w}', \mathbf{z}', \omega') = g(\mathbf{w} + \mathbf{w}', \mathbf{z} + \mathbf{z}', \omega + \omega' + \tfrac{1}{2}\mathbf{w}' \cdot \mathbf{z}) \tag{11.59}$$

for $\mathbf{w}, \mathbf{z} \in \mathbb{R}^n$ and $\omega \in \mathbb{R}$. This is called the *Weyl group*, $W(n)$. What is the faithful real matrix representation for this group with smallest dimensions?

11.6. (a) Work out the 1-, 2-, and 3-forms for $SO(3)$ in both the exponential and the ZXZ Euler-angle parameterization described in Section 10.6.6. (b) Work out the 1-, 2-,. . ., 6-forms for $SE(3)$ in the T-R parameterization described in Section 10.6.9.

11.7. In Section 11.7.3 it was stated without proof that (11.54) and (11.55) are equal. Prove this fact here. Hint: The Jacobians J_r and J_l both have the property that $\partial J/\partial q_l$ has certain symmetries that lead to the annihilation under the wedge product of all terms that might cause (11.54) and (11.55) to appear to be different from each other.

11.8. Show that $l_k(r_h(g)) = r_h(l_k(g))$ and $l_{k,*}(r_{h,*}(\mathcal{X}_g)) = r_{h,*}(l_{k,*}(\mathcal{X}_g))$.

11.9. Show that

$$\langle l_{h,*}(\mathcal{X}_g), l_{h,*}(\mathcal{Y}_g)\rangle_G = \langle \mathcal{X}_g, \mathcal{Y}_g\rangle_G = \langle r_{h,*}(\mathcal{X}_g), r_{h,*}(\mathcal{Y}_g)\rangle_G.$$

11.10. Using the Jacobians computed in Exercise 10.35 together with (11.19) and (11.21), compute $\tilde{E}_i^r$ and $\tilde{E}_i^l$ for $SO(3)$ in the case of ZYZ Euler angles. Knowing the result for the ZXZ case and the relationship between these parameterizations, is there a shortcut to the answer?

References

1. Arnol'd, V.I., *Mathematical Methods of Classical Mechanics*, Springer-Verlag, New York, 1978.
2. Helgason, S., *Groups and Geometric Analysis*, Academic Press, New York, 1984
3. Koh, S., Chirikjian, G.S., Ananthasuresh, G.K., "A Jacobian-based algorithm for planning attitude maneuvers using forward and reverse rotations," *ASME J. Comput. Nonlinear Dynam.*, 4(1), pp. 1–12, 2009.
4. Milnor, J. "Curvatures of left invariant metrics on Lie groups," *Adv. Math.*, 21, pp. 293–329, 1976.
5. Park, W., Wang, Y., Chirikjian, G.S., "The path-of-probability algorithm for steering and feedback control of flexible needles," *Int. J. Robotics Res.*, 29(7), pp. 813–830, 2010.
6. Sattinger, D.H., Weaver, O.L., *Lie Groups and Algebras with Applications to Physics, Geometry, and Mechanics*, Springer-Verlag, New York, 1986.
7. Trofimov, V.V., *Introduction to Geometry of Manifolds with Symmetry*, Kluwer Academic Publishers, Dordrecht, 1993.
8. Warner, F.W., *Foundations of Differentiable Manifolds and Lie Groups*, Springer-Verlag, New York, 1983.
9. Milnor, J., *Morse Theory*, Princeton University Press, Princeton, NJ, 1963.
10. Helgason, S., *Differential Geometry and Symmetric Spaces*, Academic Press, New York, 1962.
11. Terras, A., *Harmonic Analysis on Symmetric Spaces and Applications I*, Springer-Verlag, New York, 1985.

12

Lie Groups III: Integration, Convolution, and Fourier Analysis

Functions on Lie groups can be integrated almost as easily as functions on $\mathbb{R}^n$. In many applications, a special kind of Lie group arises. This is the *unimodular* Lie group. The integral of functions on unimodular Lie groups has the nice property that it is invariant under shifts of the argument of the function, both from the left and the right. The integral on a Lie group can be decomposed into integrals over a subgroup and a coset space. Other familiar concepts such as integration by parts, convolution, and Fourier transform also extend in a natural way to Lie groups. All of these topics are covered in this chapter and illustrated with concrete examples.

The main points to take away from this chapter are as follows:

- Functions on unimodular Lie groups can be integrated with respect to a volume element that has essentially the same properties as the volume element on $\mathbb{R}^n$. This integral can be computed in coordinates, and the value will be invariant under the choice of coordinates.
- Functions on unimodular Lie groups can be convolved and an integration-by-parts formula holds.
- The integral over a Lie group can be decomposed into an integral over a subgroup and the resulting coset space, and when the group and subgroup are both unimodular, the resulting coset space has an integration measure that is invariant under the action of the group.
- Topological properties of Lie groups and coset spaces can be computed using properties of differential forms.
- A concept of Fourier transform exists that converts the convolution of functions on a Lie group into pointwise products of Fourier matrices in the Fourier (or dual) space.
- Generalizations of Parseval's equality hold that relate the "power" in a function to the analogous quantity in Fourier space, and a function can be reconstructed from the set of all of its Fourier matrices (which is called the *spectrum* of the function).
- Operational properties convert Lie derivatives of functions into the product of Fourier transforms and an associated operator matrix in Fourier space.

This chapter is organized into the following sections. Sections 12.1, 12.2, and 12.3 are respectively concerned with how to compute integrals on Lie groups, how to integrate by parts, and the properties of convolution integrals. Sections 12.4, 12.5, and 12.6 are concerned with how integrals over groups decompose into integrals over subgroups and corresponding homomegeneous spaces, and how this can be used to compute topological invariants of these spaces. Sections 12.7 and 12.8 are concerned with general statements about representation theory and harmonic analysis on unimodular Lie

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_3,

groups. Sections 12.9 and 12.10 address the important example of $SO(3)$. Sections 12.11 and 12.12 respectively address $SE(2)$ and $SE(3)$.

12.1 How to Integrate on Lie Groups

The Jacobian matrices computed for the evaluation of Lie derivatives in the previous chapter also play a central role in expressing invariant integration measures on Lie groups in particular parameterizations. If every element of an n-dimensional Lie group can be captured with a single parameterization, $g(\mathbf{q})$, then the invariant integral for that Lie group is computed in that parameterization simply as[1]

$$\int_G f(g)\,dg \doteq \int_{\mathbf{q}} f(g(\mathbf{q}))\,w(\mathbf{q})\,d\mathbf{q}, \tag{12.1}$$

where

$$w(\mathbf{q}) = c \cdot |\mathrm{det} J(\mathbf{q})|. \tag{12.2}$$

Here, $J(\mathbf{q})$ is either $J_r(\mathbf{q})$ or $J_l(\mathbf{q})$, and c is a normalizing constant that can depend on the choice r or l. Therefore, in general there are two different ways to integrate on a Lie group. However, in the unimodular case, which is of primary interest here, $|\mathrm{det} J_r(\mathbf{q})| = |\mathrm{det} J_l(\mathbf{q})|$, and there is a unique "best" way to integrate over G. Note that when using exponential coordinates, so that $\mathbf{q}$ is replaced with $\mathbf{x}$, the weighting function for a unimodular group is even in the sense that $w(\mathbf{x}) = w(-\mathbf{x})$.

In the compact case, the constant c is often chosen such that $\int_G dg = 1$, although an alternative that can also be convenient (particularly when using exponential coordinates) is $c = 1$. Either choice is equally valid, although one may be preferred over the other depending on the particular context.

For the case of a connected Lie group, (12.1) can often be used directly. In the case of Lie groups that consist of more than one connected component (such as the full orthogonal groups), then integration over the whole group can be broken down into an integral of the form such as in (12.1) for each of these components and summed over all components.

In this book, only functions with integrals that are finite are considered. In particular, with the exception of special cases that will be explicitly stated (such as the Dirac delta function), all functions on G will be assumed to be"nice" in the sense that they belong to

$$\mathcal{N}(G) \doteq (L^1 \cap L^2 \cap \mathcal{A})(G),$$

where

$$f \in L^p(G) \iff \int_G |f(g)|^p dg < \infty$$

and $\mathcal{A}(G)$ denotes the set of all analytic functions on G, meaning that the Taylor series defined in Section 11.3 will always be convergent in a neighborhood around the point where the expansion is made. Additionally, since the iterated application of the derivatives $\tilde{X}^r$ and $\tilde{X}^l$ to a function in $\mathcal{A}(G)$ always results in a function that does not blow up near the point where a Taylor series is being evaluated, it follows that $\mathcal{A}(G) \subset C^\infty(G)$. Although this limits the scope of the discussion in theory, in practice we will be interested in probability density functions that either naturally belong to

[1] Here, as in Chapter 2, dg is shorthand for $d(g)$, the differential volume element, which is an n-form with sign killed by taking an absolute value.

$\mathcal{N}(G)$ (e.g., solutions to a diffusion equation evaluated at a value of time $t > 0$ subject to initial conditions $f(g,0) = \delta(g)$) or can be approximated well in the L^2 sense by functions in $\mathcal{N}(G)$.

If dg is a left-invariant measure, then the right Jacobian, J_r, would be used above, and if dg is a right-invariant measure, then the left Jacobian, J_l, would be used. If G is a unimodular group, then dg will be left and right invariant, and using J_l or J_r for J in (12.1) will produce the same result. If G is compact, it is automatically unimodular. The volume element dg for a compact Lie group is often normalized by multiplication by a constant such that $\int_G f(g)\,dg = 1$.

For an n-dimensional unimodular Lie group, the volume element (or integration measure) dg can be expressed in terms of differential forms as

$$dg = \left(g^{-1}\frac{\partial g}{\partial q_1}\right)^{\vee} \wedge \cdots \wedge \left(g^{-1}\frac{\partial g}{\partial q_n}\right)^{\vee} dq_1 \cdots dq_n \tag{12.3}$$

$$= \left(\frac{\partial g}{\partial q_1}g^{-1}\right)^{\vee} \wedge \cdots \wedge \left(\frac{\partial g}{\partial q_n}g^{-1}\right)^{\vee} dq_1 \cdots dq_n, \tag{12.4}$$

where the coordinates are ordered such that $\det J(\mathbf{q}) \geq 0$.

The reason why integration on unimodular Lie groups is invariant is outlined below. For additional treatment of this issue, see the discussion and references in [11].

12.1.1 Invariance of the Integral on a Unimodular Lie Group

The integral of a real-valued function on the real line for which

$$I = \int_{-\infty}^{\infty} f(x)\,dx < \infty$$

has the property that

$$\int_{-\infty}^{\infty} f(x)\,dx = \int_{-\infty}^{\infty} f(x-a)\,dx = \int_{-\infty}^{\infty} f(-x)\,dx \tag{12.5}$$

regardless of the shape or differentiability of $f(x)$. In other words, the value of the integral is invariant under shifts and inversions of the argument. A generalization of (12.5) holds for the case of *unimodular Lie groups.*

For a unimodular Lie group, the integral defined in (12.1) has the property that

$$\int_G f(g)\,dg = \int_G f(g_0 \circ g)\,dg \tag{12.6}$$

$$= \int_G f(g \circ g_0)\,dg \tag{12.7}$$

$$= \int_G f(g^{-1})\,dg \tag{12.8}$$

for any fixed $g_0 \in G$.

These facts follow from the way the volume element has been defined. For example, making the change of coordinates $g' = g_0 \circ g$, the right-hand side of (12.6) is rewritten as

$$\begin{aligned}
\int_{g\in G} f(g_0 \circ g)\, dg &= \int_{g_0^{-1}\circ g' \in G} f(g')\, d(g_0^{-1} \circ g') \\
&= \int_{g' \in g_0 G} f(g')\, d(g_0^{-1} \circ g') \\
&= \int_{g' \in G} f(g')\, d(g_0^{-1} \circ g').
\end{aligned}$$

Here, the closure of the group has been used in the form $g_0 G \doteq \{g_0 \circ g \mid g \in G\} = G$.

Therefore, if $d(g_0^{-1} \circ g) = d(g)$, the invariance of the integral under left shifts will be proven. If $J_r(\mathbf{q})$ is used in (12.1), this will be the case because the columns of $J_r(\mathbf{q})$ have the property that

$$\left((g_0 \circ g)^{-1} \frac{\partial (g_0 \circ g)}{\partial q_i}\right)^\vee = \left(g^{-1} \circ g_0^{-1} \circ g_0 \frac{\partial g}{\partial q_i}\right)^\vee = \left(g^{-1} \frac{\partial g}{\partial q_i}\right)^\vee .$$

An analogous argument holds for right shifts when J is chosen to be J_l. Additionally, since J_l and J_r are related through multiplication of the adjoint matrix, which has a unit determinant for unimodular Lie groups, $|J| = |J_l| = |J_r|$ is invariant under both left and right shifts.

The invariance of the integral under inversion of the argument of a function on a unimodular Lie group stated in (12.8) also follows from the properties of the Jacobian matrix. This is because by changing variables as $h = g^{-1}$,

$$\begin{aligned}
\int_{g\in G} f(g^{-1})\, dg &= \int_{h^{-1}\in G} f(h)\, d(h^{-1}) \\
&= \int_{h\in G^{-1}} f(h)\, d(h^{-1}) \\
&= \int_{h\in G} f(h)\, d(h^{-1}),
\end{aligned}$$

where $G^{-1} \doteq \{g^{-1} \mid g \in G\} = G$ (since every element of a group has a unique inverse). However, since for a unimodular Lie group $d(g) = d_l(g) = d_r(g)$ we can choose either expression (in this case below it is d_l) and write

$$d(g^{-1}) = \left(\frac{\partial (g^{-1})}{\partial q_1} (g^{-1})^{-1}\right)^\vee dq_1 \wedge \cdots \wedge \left(\frac{\partial (g^{-1})}{\partial q_n} (g^{-1})^{-1}\right)^\vee dq_n,$$

and since $gg^{-1} = e$, the product rule gives

$$\frac{\partial (g^{-1})}{\partial q_k} = -g^{-1} \frac{\partial g}{\partial q_k} g^{-1}.$$

Substituting this in the above expression gives

$$\begin{aligned}
d(g^{-1}) &= \left(-g^{-1} \frac{\partial g}{\partial q_1} g^{-1} \circ g\right)^\vee dq_1 \wedge \cdots \wedge \left(-g^{-1} \frac{\partial g}{\partial q_n} g^{-1} \circ g\right)^\vee dq_n. \\
&= \left(-g^{-1} \frac{\partial g}{\partial q_1}\right)^\vee dq_1 \wedge \cdots \wedge \left(-g^{-1} \frac{\partial g}{\partial q_n}\right)^\vee dq_n. \\
&= |-J_r(\mathbf{q})|\, dq_1 dq_2 \cdots dq_n \\
&= d_r(g) = d(g).
\end{aligned}$$

12.1.2 Example: Integration on the Rotation Group

The proper (invariant) way to integrate a function $f : SO(3) \to \mathbb{R}$ using exponential coordinates is

$$\int_{SO(3)} f(R)\, dR = c \cdot \int_{\|\mathbf{x}\|<\pi} f(R(\mathbf{x}))\, |\det J(\mathbf{x})|\, d\mathbf{x}, \tag{12.9}$$

where $d\mathbf{x} = dx_1\, dx_2\, dx_3$ and J can denote either J_r or J_l. The constant c can either be chosen to ensure that $\int_{SO(3)} 1\, dR = 1$ or it can be taken as $c = 1$

In order to be meaningful, the value of the integral must not depend on the particular parameterization used. For example, if $SO(3)$ is parameterized using Euler angles rather than exponential parameters, then recalling the Euler-angle Jacobians in Section 10.6.6 and their determinants, the resulting integral is

$$\int_{SO(3)} f(R)\, dR = \frac{1}{8\pi^2} \int_0^{2\pi} \int_0^{\pi} \int_0^{2\pi} f(R(\alpha, \beta, \gamma))\, \sin\beta\, d\alpha\, d\beta\, d\gamma, \tag{12.10}$$

where this normalization chosen here is such that $\int_{SO(3)} 1\, dR = 1$.

12.1.3 Example: Integration on the Motion Group

Given a function of motion, $f(g) \in \mathcal{N}(SE(3))$, the proper (invariant) way to integrate using exponential coordinates

$$X = \begin{pmatrix} \Omega & \mathbf{v} \\ \mathbf{0}^T & 0 \end{pmatrix} \in se(3)$$

is

$$\int_{SE(3)} f(g)\, dg = c' \cdot \int_{\mathbf{v}\in\mathbb{R}^3} \int_{\|\boldsymbol{\omega}\|<\pi} f(e^X)\, |\det(J_r(\boldsymbol{\omega}))|^2 d\boldsymbol{\omega}\, d\mathbf{v}, \tag{12.11}$$

where $\boldsymbol{\omega} = \Omega^\vee$ are exponential coordinates for $so(3)$ and $J_r(\boldsymbol{\omega})$ is the $SO(3)$ Jacobian for exponential coordinates. The reason why the square of the determinant appears as a factor is a result of the structure of this group, which is a semi-direct product, which resulted in (10.96). There are multiple ways to define the normalizing constant c'. One way to define it is as $c' = 1$, which is convenient since the exponential parameterization is most useful for functions supported close to the identity, and since $|\det(J_r(\mathbf{0}))| = 1$, the above integral then reduces to a usual integral over a region in Euclidean space.

In contrast, if the T-R parametrization in Section 10.6.9 is used, then

$$\int_{SE(3)} f(g)\, dg = \int_{\mathbb{R}^3} \int_{SO(3)} f(t(\mathbf{a}) \circ r(R))\, dR\, d\mathbf{a}, \tag{12.12}$$

where $d\mathbf{a} = da_1\, da_2\, da_3$ and the integral over $SO(3)$ can be normalized in either of the ways described earlier. Interestingly, the volume element for $SE(3)$ is the same as that for $\mathbb{R}^3 \times SO(3)$. The rotational part can be described with Euler angles or exponential parameters, or other more exotic parameterizations. When a particular problem dictates converting between different parameterizations, some care should be taken that the normalizing constants used are consistent.

12.2 Integration by Parts

Given two differentiable functions $f_1(x)$ and $f_2(x)$ defined on an interval $[a,b] \subset \mathbb{R}$, the rule for integration by parts is

$$\int_a^b \frac{df_1}{dx} f_2 \, dx = f_1(x) f_2(x) \Big|_a^b - \int_a^b f_1 \frac{df_2}{dx} \, dx.$$

In practice, the "surface terms"

$$f_1(x) f_2(x) \Big|_a^b = f_1(b) f_2(b) - f_1(a) f_2(a)$$

disappear in many (but not all) cases. Two such cases are (1) the interval extends over the whole real line, and the functions decay to 0 as $x \to \pm\infty$ and (2) the interval is of the form $[a,b] = [-\pi, \pi]$ and the functions are periodic. Of course, these are not the only two cases when the surface terms disappear. However, it is interesting to note that these cases can be identified with the Lie groups $(\mathbb{R}, +)$ and $SO(2)$. Is this just coincidence, or is there something more general going on? This section addresses this question.

12.2.1 Extension to Unimodular Lie Groups

To see that integration by parts holds, in general all that is required is to use the definition of the Lie derivative and some elementary properties of groups and differentiable functions. In particular, let G be a unimodular Lie group and denote generic elements as $g, g' \in G$. Given functions $f_1(g)$ and $f_2(g)$ with Lie derivatives that exist, then for any fixed $X \in \mathcal{G}$, by definition

$$\begin{aligned}
\int_G (\tilde{X}^r f_1)(g) \, f_2(g) \, dg &= \int_G \frac{d}{dt} f_1(g \circ \exp(tX)) \Big|_{t=0} f_2(g) \, dg && (12.13)\\
&= \frac{d}{dt} \left[\int_G f_1(g \circ \exp(tX)) \, f_2(g) \, dg \right]_{t=0} && (12.14)\\
&= \frac{d}{dt} \left[\int_G f_1(g') \, f_2(g' \circ \exp(-tX)) \, dg' \right]_{t=0} && (12.15)\\
&= \int_G f_1(g') \, \frac{d}{dt} f_2(g' \circ \exp(-tX)) \Big|_{t=0} dg' && (12.16)\\
&= - \int_G f_1(g') \, (\tilde{X}^r f_2)(g') \, dg'. && (12.17)
\end{aligned}$$

At line (12.14) the new variable $g' = g \circ \exp(tX)$ was defined such that the substitution $g = g' \circ \exp(-tX)$ could be made at line (12.15).

The shift invariance of integration on a unimodular group is used at line (12.15). The negative sign on line (12.17) is nothing more than the classical calculus result that

$$\frac{d}{dt} \alpha(-t) \Big|_{t=0} = - \frac{d}{dt} \alpha(t) \Big|_{t=0}.$$

12.2.2 Inner Products of Functions on a Unimodular Lie Group

An inner product between "well-behaved" real-valued function on a group can be defined as

$$\boxed{(f_1, f_2) = \int_G f_1(g)\, f_2(g)\, dg.} \tag{12.18}$$

An obvious prerequisite to being "well behaved" is that the absolute value and square of the functions must integrate to a finite value, and the functions should be differentiable everywhere. This is captured by the concept of the space of nice functions, $\mathcal{N}(G)$.

Using this inner product notation, integration by parts is written as

$$\boxed{(\tilde{X}^r f_1, f_2) = -(f_1, \tilde{X}^r f_2).} \tag{12.19}$$

It follows immediately from (12.19) that if $f_1 = f_2 = f$, then $(\tilde{X}^r f, f) = 0$ or, equivalently,

$$\int_G f\, \tilde{X}^r f\, dg = 0,$$

indicating that a well-behaved function on a unimodular Lie group is always orthogonal to its own Lie derivative.

In a similar way, it is easy to see that if $f_1 = f$ and $f_2 = 1$, then

$$\int_G \tilde{X}^r f\, dg = 0. \tag{12.20}$$

Of course, $f_2 = 1$ is only a well-behaved function on a compact Lie group, because otherwise its integral will blow up.

The equality (12.20) is true for unimodular groups in general (and not only compact ones) because

$$\int_G \tilde{X}^r f\, dg = \frac{d}{dt}\left[\int_G f(g \circ \exp(tX))\, dg\right]_{t=0} \tag{12.21}$$

$$= \frac{d}{dt}\left[\int_G f(g')\, dg'\right]_{t=0} \tag{12.22}$$

$$= 0. \tag{12.23}$$

As a demonstration of the usefulness of (11.7), note that (12.20) could have been used together with this product rule for Lie derivatives to prove (12.19). Furthermore,

$$0 = \int_G \tilde{X}^r(f^{N+1})\, dg = (N+1)\int_G f^N \tilde{X}^r f\, dg.$$

However, there is nothing special about the power N, and so $N = n+p$ can be used together with a regrouping of terms to show that orthogonal functions can be constructed such that

$$(f^n, f^p \tilde{X}^r f) = 0.$$

12.2.3 The Adjoints of $\tilde{X}^r$ and $\tilde{X}^l$ for a Unimodular Lie Group

The discussion of integration by parts in the previous section leads to a natural concept of the adjoint differential operator as

$$\boxed{(\tilde{X}^r)^* \doteq -\tilde{X}^r \quad \text{and} \quad (\tilde{X}^l)^* \doteq -\tilde{X}^l.} \tag{12.24}$$

Building on the coordinate-dependent presentation of $\tilde{X}^r$ and $\tilde{X}^l$ given previously, the adjoint operators $(\tilde{X}^r)^*$ and $(\tilde{X}^l)^*$ can be derived in terms of coordinates.

The coordinate-dependent description of the inner product of two functions on G is

$$(f_1, f_2) = \int_{\mathbb{R}^n} f_1(\mathbf{q}) f_2(\mathbf{q}) |J(\mathbf{q})| \, d\mathbf{q},$$

where again $f(\mathbf{q})$ is shorthand for $f(g(\mathbf{q}))$ that will be used when there is no risk of confusion, and

$$|J(\mathbf{q})| = |\det J_r(\mathbf{q})| = |\det J_l(\mathbf{q})|.$$

These equalities hold, by definition, for unimodular Lie groups in the case when the parameterization is global. When this is not the case, such as when G has more than one connected component, the discussion below will be relevant to each local parameterization.

Using the notation $J_r^{ji} = (J_r^{-1})_{ji}$, substituting in the coordinate-dependent description of $\tilde{X}^r$, and performing integration by parts gives

$$\begin{aligned}
(f_1, \tilde{X}^r f_2) &= \int_{\mathbb{R}^n} f_1 \sum_{i,j=1}^{n} x_i J_r^{ji} \frac{\partial f_2}{\partial q_j} |J| \, d\mathbf{q} \\
&= - \int_{\mathbb{R}^n} f_2 \sum_{i,j=1}^{n} x_i \frac{\partial}{\partial q_j} \left(J_r^{ji} |J| f_1 \right) \, d\mathbf{q} \\
&= - \int_{\mathbb{R}^n} f_2 \frac{1}{|J|} \sum_{i,j=1}^{n} x_i \frac{\partial}{\partial q_j} \left(J_r^{ji} |J| f_1 \right) |J| \, d\mathbf{q}.
\end{aligned}$$

Therefore,

$$(\tilde{X}^r f)^* = - \frac{1}{|J|} \sum_{i,j=1}^{n} x_i \frac{\partial}{\partial q_j} \left(J_r^{ji} |J| f \right). \tag{12.25}$$

However, we know from the coordinate-free formulation that $(\tilde{X}^r f)^* = -\tilde{X}^r f$, and so the following must be true independent of f and x_i:

$$\frac{1}{|J|} \sum_{i,j=1}^{n} x_i \frac{\partial}{\partial q_j} \left(J_r^{ji} |J| f \right) = \sum_{i,j=1}^{n} x_i J_r^{ji} \frac{\partial f}{\partial q_j}.$$

From this, it can be concluded that the Jacobian for a unimodular Lie group must satisfy the condition

$$\boxed{\sum_{j=1}^{n} \frac{\partial}{\partial q_j} \left(J_r^{ji} |J| \right) = 0.} \tag{12.26}$$

12.3 Convolution on Unimodular Lie Groups

A special kind of integral over a unimodular Lie group is the *convolution* of two functions. Given two functions $f_1(g)$ and $f_2(g)$, their convolution is defined as

$$\boxed{(f_1 * f_2)(g) \doteq \int_G f_1(h)\, f_2(h^{-1} \circ g)\, dh.} \tag{12.27}$$

A convolution integral of the form in (12.27) can be written in the following equivalent ways:

$$(f_1 * f_2)(g) = \int_G f_1(z^{-1})\, f_2(z \circ g)\, dz = \int_G f_1(g \circ k^{-1})\, f_2(k)\, dk, \tag{12.28}$$

where the substitutions $z = h^{-1}$ and $k = h^{-1} \circ g$ have been made and the invariance of integration under shifts and inversions is used. This follows from the property of the volume element,

$$d(h \circ g) = d(g \circ h) = d(g^{-1}) = dg,$$

which is a consequence of the definition in (12.2) and the properties of Jacobian matrices for unimodular Lie groups.

Here, as usual in this book, it is assumed that $f_i \in \mathcal{N}(G)$.

Note that unlike the case of the Abelian groups $(\mathbb{R}, +)$, the torus (circle group) $T = \mathbb{R}/(2\pi\mathbb{R})$, and their direct products, for which the convolution product $*$ inherits commutativity from the group operation, $+$, for noncommutative unimodular Lie groups, the convolution product generally will not be commutative:

$$(f_1 * f_2)(g) \neq (f_2 * f_1)(g). \tag{12.29}$$

Having said this, there are special cases. For example, for fixed $h \in G$, the set

$$Cl(h) \doteq \{g \circ h \circ g^{-1} \mid g \in G\} \subset G, \tag{12.30}$$

is called the *conjugacy class* of h in G. A function $\chi(g)$ that is constant on each conjugacy class is called a *class function* and has the property[2]

$$\chi(h) = \chi(g \circ h \circ g^{-1}) \;\Leftrightarrow\; \chi(g \circ h) = \chi(h \circ g) \tag{12.31}$$

for arbitrary $h, g \in G$; then it is straightforward to show that

$$(f * \chi)(g) = (\chi * f)(g)$$

when these convolution integrals exist (which will be the case when $\chi, f \in \mathcal{N}(G)$).

For example, it can be shown that on the group $SO(3)$, functions of the form

$$\chi(\exp X) = \chi_0(\|X\|)$$

are class functions. Additionally, on an arbitrary n-dimensional unimodular Lie group, the Dirac delta function, which can be defined in exponential coordinates as

$$\delta(\exp X) = \prod_{i=1}^{n} \delta(x_i)$$

[2] "Class functions" need not be in the "class of nice functions" $\mathcal{N}(G)$. These should not be confused. Furthermore, $\chi(g)$ is not to be confused with the Euler characteristic, which can be defined for compact Lie groups and is denoted as $\chi(G)$. The Euler characteristic has one value defined for the whole group rather than a value defined on each element $g \in G$.

(where $\delta(x)$ is the usual one-dimensional Dirac delta on the real line, the product of which evaluated in different variables produces the multi-dimensional Dirac delta), is a class function although it is not in $\mathcal{N}(G)$.

If the class of "nice" functions is expanded to include the Dirac delta, then the set $\{\mathcal{N}(G) \cup \{\delta\}\}$ together with the operation of convolution forms a semigroup—namely $\delta(g)$ serves as the identity

$$\delta * f = f * \delta = f$$

and convolution is a binary operation that is associative,

$$(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3).$$

This *convolution semi-group* has no inverse of a given $f_1(g)$ under the operation of convolution. Thus, a convolution equation of the form $(f_1 * f_2)(g) = f_3(g)$ generally cannot be solved exactly to find $f_2(g)$ for arbitrary given $f_1(g)$ and $f_3(g)$. However, functions on a group have the operations of addition and scalar multiplication. Thus, $(\{\mathcal{N}(G) \cup \{\delta\}\}, *, +, \cdot)$ becomes an algebra called the *group algebra*.

12.4 Decomposition of Integrals on Lie Groups

In addition to using the group operation to define the convolution of functions on a group, it is possible to decompose the integral of a function on a group using the natural decomposition of that group into cosets relative to a particular subgroup. This concept, and its extension, called a double-coset decomposition, are explained for Lie groups in the following subsections.

12.4.1 Subgroup-Coset Decompositions

In what follows, it will be convenient to denote a function on G as $f_G(g)$, a function on G/H as $f_{G/H}(gH)$, etc. Let $c_{G/H} : G/H \rightarrow G$ be a mapping that generates one representative per coset; that is, $c_{G/H}(gH) \in gH$. Decomposing each $g \in G$ as $g = c_{G/H}(gH) \circ h$ for some $h \in H$ then means that $f_G(g) = f_G(c_{G/H}(gH) \circ h)$.[3]

Separation of Coordinates

Suppose that G is parameterized such that any group element can be written as

$$\begin{aligned} g(q_1, \ldots, q_n) &= g(0, \ldots, 0, q_{m+1}, \ldots, q_n) \circ g(q_1, \ldots, q_m, 0, \ldots, 0) \\ &\doteq c_{G/H}(gH(q_{m+1}, \ldots, q_n)) \circ h(q_1, \ldots, q_m), \end{aligned}$$

or

$$g(\mathbf{q}_H, \mathbf{q}_{G/H}) = g(\mathbf{0}, \mathbf{q}_{G/H}) \circ g(\mathbf{q}_H, \mathbf{0}) = c_{G/H}(gH(\mathbf{q}_{G/H})) \circ h(\mathbf{q}_H), \tag{12.32}$$

where H is an m-dimensional Lie subgroup of G with $h \in H$ and $gH \in G/H$. For any $\mathbf{q} = [q_1, \ldots, q_n]^T$ resulting in $g(\mathbf{q}) \in G$, the notation $c_{G/H}(gH(\mathbf{q}_{G/H})) =$

[3] It is not required that $G = (G/H) \times H$ for this to be true. For example, the integral over $SO(3)$ decomposes into one over S^2 and one over S^1 even though $SO(3) \neq S^2 \times S$.

$c_{G/H}(gH(q_{m+1},\ldots,q_n))$ stands for the specific coset representative such that (12.32) holds. In what follows, $c_{G/H}(gH(q_{m+1},\ldots,q_n))$ is abbreviated as $c(q_{m+1},\ldots,q_n)$ or $c(\mathbf{q}_{G/H})$.

Using this notation, it follows that

$$\frac{\partial g}{\partial q_k}=\begin{cases} c(q_{m+1},\ldots,q_n)\dfrac{\partial h}{\partial q_k}(q_1,\ldots,q_m) & \text{for } k\in[1,\ldots,m] \\ \dfrac{\partial c}{\partial q_k}(q_{m+1},\ldots,q_n)h(q_1,\ldots,q_m) & \text{for } k\in[m+1,\ldots,n]. \end{cases}$$

Structure of Jacobians and Adjoint Matrices

The associated Jacobian J_r is

$$\begin{aligned} J_r &= \left[\left(g^{-1}\frac{\partial g}{\partial q_1}\right)^{\vee},\ldots,\left(g^{-1}\frac{\partial g}{\partial q_m}\right)^{\vee},\left(g^{-1}\frac{\partial g}{\partial q_{m+1}}\right)^{\vee},\ldots,\left(g^{-1}\frac{\partial g}{\partial q_n}\right)^{\vee}\right] \\ &= \left[\left(g^{-1}\frac{\partial g}{\partial \mathbf{q}_H^T}\right)^{\vee},\left(g^{-1}\frac{\partial g}{\partial \mathbf{q}_{G/H}^T}\right)^{\vee}\right] \\ &= \left[\left(h^{-1}\frac{\partial h}{\partial \mathbf{q}_H^T}\right)^{\vee},[Ad(h^{-1})]\left(c^{-1}\frac{\partial c}{\partial \mathbf{q}_{G/H}}\right)^{\vee}\right]. \end{aligned}$$

In a similar way,

$$\begin{aligned} J_l &= \left[\left(\frac{\partial g}{\partial q_1}g^{-1}\right)^{\vee},\ldots,\left(\frac{\partial g}{\partial q_m}g^{-1}\right)^{\vee},\left(\frac{\partial g}{\partial q_{m+1}}g^{-1}\right)^{\vee},\ldots,\left(\frac{\partial g}{\partial q_n}g^{-1}\right)^{\vee}\right] \\ &= \left[[Ad(c)]\left(\frac{\partial h}{\partial \mathbf{q}_H^T}h^{-1}\right)^{\vee},\left(\frac{\partial c}{\partial \mathbf{q}_{G/H}}c^{-1}\right)^{\vee}\right]. \end{aligned}$$

Note that the Jacobian J_r (which will be denoted here as J_r^G) has the structure

$$J_r^G=\begin{pmatrix} J_r^H & B_1 \\ \mathbb{O} & B_2 \end{pmatrix}, \quad \text{where } J_r^H=\left[\left(h^{-1}\frac{\partial h}{\partial q_1}\right)^{\vee},\ldots,\left(h^{-1}\frac{\partial h}{\partial q_m}\right)^{\vee}\right]$$

is the Jacobian for the subgroup H. It can also be shown that

$$[Ad^G(g)]=\begin{pmatrix} [Ad^H(h)] & A_1 \\ \mathbb{O} & A_2 \end{pmatrix},$$

where $[Ad^G]$ is the adjoint matrix for the group G and $[Ad^H]$ is the adjoint matrix for the subgroup H. Block-by-block inversion of $[Ad^G(g)]$ gives

$$[Ad^G(g)]^{-1}=\begin{pmatrix} [Ad^H(h)]^{-1} & -[Ad^H(h)]^{-1}A_1A_2^{-1} \\ \mathbb{O} & A_2^{-1} \end{pmatrix}$$

If G and H are both unimodular, then the condition $|[Ad^G(g)]|=|[Ad^H(h)]|=1$ forces $|A_2|=1$.

Furthermore,

$$|J_r^G| = |[Ad^G(g)]J_r^G| = |[Ad^H(g)]J_r^H| \cdot |J_r^{gH}| = |J_r^H| \cdot |J_r^{gH}|,$$

where J_r^{gH} is J_r^G evaluated only on representatives of the coset gH.

This means that if $dg \doteq |J_r^G|\, d\mathbf{q}$, $dh \doteq |J_r^H| dq_H$, and $d(gH) \doteq |J_r^{gH}|\, d\mathbf{q}_{G/H}$, then

$$\boxed{dg = dh\, d(gH).} \tag{12.33}$$

The Resulting Decomposition of Integrals

The above discussion leads to the following decomposition of an integral over G:

$$\int_G f_G(g)\, dg = \int_{G/H} \left(\int_H f_G(c_{G/H}(gH) \circ h)\, dh \right) d(gH), \tag{12.34}$$

where dh and $d(gH)$ are unique up to normalization. In the special case when $f_G(g)$ is a left-coset function (i.e., a function that is constant on left cosets), $f_G(c_{G/H}(gH) \circ h_1) = f_G(c_{G/H}(gH) \circ h_2) = f_{G/H}(gH)$ for all $h_1, h_2 \in H$ and (12.34) reduces to

$$\int_G f_G(g)\, dg = \int_{G/H} f_{G/H}(gH)\, d(gH),$$

where it is assumed that dh is normalized so that $\int_H dh = 1$. More generally,

$$f_{G/H}(gH) = \int_H f_G(c_{G/H}(gH) \circ h)\, dh$$

is the value of the function $f_G(g)$ averaging over the subgroup H. Similarly,

$$f_H(h) = \int_{G/H} f_G(c_{G/H}(gH) \circ h)\, d(gH)$$

is the average of $f_G(g)$ taken over the coset gH.

Returning to (12.34), note that if G is unimodular and if dh is normalized such that $\int_H dh = 1$, then the invariance of integration under shifts gives

$$\begin{aligned}\int_G f_G(g)\, dg &= \left(\int_H dh_1 \right) \int_G f_G(g \circ h_1)\, dg \\ &= \int_H \int_G f_G(g \circ h_1)\, dg\, dh_1 = \int_G \int_H f_G(g \circ h_1)\, dh_1\, dg.\end{aligned}$$

Combining this with (12.34) then gives

$$\begin{aligned}\int_G f_G(g)\, dg &= \int_G \int_H f_G(g \circ h_1)\, dh_1\, dg \\ &= \int_{G/H} \int_H \left(\int_H f_G(c_{G/H}(gH) \circ h \circ h_1)\, dh_1 \right) dh\, d(gH) \\ &= \int_{G/H} \int_H \left(\int_H f_G(c_{G/H}(gH) \circ h_1)\, dh_1 \right) dh\, d(gH) \\ &= \int_{G/H} \int_H f_G(c_{G/H}(gH) \circ h_1)\, dh_1\, d(gH).\end{aligned}$$

In other words, the integration over H need not be with respect to the specific $h \in H$ that satisfies $g = c_{G/H}(gH) \circ h$. Then, from the invariance of integration on H under shifts, h can be reintroduced as

$$\int_G f_G(g)\,dg = \int_{G/H}\int_H f_G(c_{G/H}(gH) \circ h \circ h_1)\,dh_1\,d(gH),$$

or

$$\boxed{\int_G f_G(g)\,dg = \int_{G/H}\int_H f_G(g \circ h_1)\,dh_1\,d(gH).} \tag{12.35}$$

Of course, h_1 in the above expression is a dummy variable of integration, and since there is no longer any use $c_{G/H}(gH)$ and hence h no longer has special meaning, h_1 can be called h.

12.4.2 Double-Coset Decompositions

With the definition of double coset given in Chapter 10, the decomposition of the integral of a function on a group can be expressed in terms of two subgroups and a double-coset space. The details of this decomposition are provided here.

Jacobians and Adjoint Matrices When Coordinates Are Separated

First, it is possible to define a mapping $c_{K\backslash G/H} : K\backslash G/H \to G$ such that for any $KgH \in K\backslash G/H$, $c_{K\backslash G/H}(KgH) \in KgH$. Such a function defines a rule for selecting one representative per double coset. Equipped with such a function, it becomes possible to write $g = k \circ c_{K\backslash G/H}(KgH) \circ h$. If coordinates for G are partitioned so that

$$g = g(\mathbf{q}_K, \mathbf{q}_{K\backslash G/H}, \mathbf{q}_H) = h(\mathbf{q}_K) \circ c(\mathbf{q}_{K\backslash G/H}) \circ k(\mathbf{q}_H), \tag{12.36}$$

then the Jacobian for G can be written as

$$J((\mathbf{q}_K, \mathbf{q}_{K\backslash G/H}, \mathbf{q}_H) = \left[\left(g^{-1}\frac{\partial g}{\partial \mathbf{q}_K^T}\right)^\vee, \left(g^{-1}\frac{\partial g}{\partial \mathbf{q}_{K\backslash G/H}^T}\right)^\vee, \left(g^{-1}\frac{\partial g}{\partial \mathbf{q}_H^T}\right)^\vee\right].$$

Using (12.36) then causes this Jacobian to take the form

$$[Ad_G(h^{-1})]\left[[Ad_G(c^{-1})]\left(h^{-1}\frac{\partial h}{\partial \mathbf{q}_K^T}\right)^\vee, \left(c^{-1}\frac{\partial c}{\partial \mathbf{q}_{K\backslash G/H}^T}\right)^\vee, [Ad_G(h)]\left(h^{-1}\frac{\partial h}{\partial \mathbf{q}_H^T}\right)^\vee\right].$$

Then since $|\det[Ad_G(h^{-1})]| = 1$ from the unimodularity of G,

$$|J((\mathbf{q}_K, \mathbf{q}_{K\backslash G/H}, \mathbf{q}_H)| = \begin{vmatrix} [Ad(c^{-1})]_{11}J_K^r(k) & \mathbb{O} & \delta_{H,K}J_H^l(h) \\ [Ad(c^{-1})]_{21}J_K^r(k) & J_{K\backslash G/H}(c) & \mathbb{O} \\ [Ad(c^{-1})]_{31}J_K^r(k) & \mathbb{O} & (1-\delta_{H,K})J_H^l(h) \end{vmatrix}.$$

Here, it is assumed that the basis elements for the Lie algebra of G are ordered so that those belonging to the Lie algebra of K are first, followed by those that belong neither to the Lie algebra of H or K. In the last column of blocks, $\delta_{H,K} = 1$ only if $H = K$ (in which case only the upper term survives), or if $H \neq K$, then $\delta_{H,K} = 0$, in which case only the lowest term survives. In either case,

$$|\det J((\mathbf{q}_K, \mathbf{q}_{K\backslash G/H}, \mathbf{q}_H)| = |Ad_{k1}(c^{-1})| \cdot |J_H(h)| \cdot |J_K(k)| \cdot |J_{K\backslash G/H}(c)|,$$

where $k = 1$ or 3, depending on whether or not $H = K$. Note that the r and l superscripts have been dropped since the determinants of these Jacobians are the same for unimodular Lie groups. By defining $dh \doteq |J_H(h)| d\mathbf{q}_H$, $dk \doteq |J_K(k)| d\mathbf{q}_K$, and $d(KgH) \doteq |Ad_{k1}(c^{-1})| \cdot |J_{K\backslash G/H}(c)| d\mathbf{q}_{K\backslash G/H}$, it follows that

$$\boxed{dg = dh\, dk\, d(KgH).} \tag{12.37}$$

The Resulting Decomposition of Integrals

The above discussion leads to the decomposition

$$\int_G f_G(g)\, dg = \int_{K\backslash G/H} \int_K \int_H f_G(k \circ c_{K\backslash G/H}(KgH) \circ h)\, dh\, dk\, d(KgH). \tag{12.38}$$

A particular example of this is the integral over $SO(3)$, which can be written in terms of Euler angles as

$$\begin{aligned}
&\int_{SO(3)} f(g)\, dg \\
&= \frac{1}{8\pi^2} \int_0^{2\pi} \int_0^{\pi} \int_0^{2\pi} f(R_3(\alpha) R_1(\beta) R_3(\gamma)) \sin\beta\, d\alpha\, d\beta\, d\gamma \\
&= \int_{SO(2)\backslash SO(3)/SO(2)} \int_{SO(2)} \int_{SO(2)} f(h_1(\alpha) \circ c(HgH) \circ h_2(\gamma))\, dh_1\, dh_2\, d(HgH),
\end{aligned}$$

where $h_1(\alpha) = R_3(\alpha), h_2(\gamma) = R_3(\gamma) \in SO(2)$ and $c(HgH) = R_1(\beta)$ is the coset-representative function, and $dh_1 = d\alpha/2\pi$, $dh_1 = d\gamma/2\pi$, and $d(HgH) = \sin\beta d\beta/2$ in this case.

Returning to (12.38), note that if G is unimodular and if dh and dk are both normalized such that $\int_H dh = \int_K dk = 1$, then the invariance of integration under shifts can be used to evaluate $\int_G f_G(g)\, dg$ as

$$\left(\int_K dk_1\right)\left(\int_H dh_1\right) \int_G f_G(k_1 \circ g \circ h_1)\, dg = \int_G \int_K \int_H f_G(k_1 \circ g \circ h_1)\, dh_1\, dk_1\, dg.$$

Combining this with (12.38) then gives

$$\begin{aligned}
&\int_G \int_K \int_H f_G(k_1 \circ g \circ h_1)\, dh_1\, dk_1\, dg \\
&= \int_{K\backslash G/H} \int_{K\times K} \int_{H\times H} f_G(k_1 \circ k \circ c_{K\backslash G/H}(KgH) \circ h \circ h_1)\, dh_1\, dh\, dk_1\, dk\, d(KgH) \\
&= \int_{K\backslash G/H} \int_K \int_H f_G(k_1 \circ c_{K\backslash G/H}(KgH) \circ h_1)\, dh_1\, dk_1\, d(KgH).
\end{aligned}$$

Here, both the left invariance of integration on H and right invariance of integration on K has been used. Then, using the right invariance of integration on H and left invariance of integration on K, h and k can be reintroduced resulting in the integrand $f_G(k_1 \circ k \circ c_{K\backslash G/H}(KgH) \circ h \circ h_1) = f_G(k_1 \circ g \circ h_1)$, and

$$\boxed{\int_G f_G(g)\, dg = \int_{K\backslash G/H} \int_K \int_H f_G(k_1 \circ g \circ h_1)\, dh_1\, dk_1\, dg.} \tag{12.39}$$

As in the case of a single-coset decomposition, the names h_1 and k_1 can be changed at this stage to h and k.

12.4.3 The Weyl Integration Formula for Compact Lie Groups

The Weyl integration formula takes on a variety of different forms. In some books, it is written only for $U(n)$. In others, it is written for more general compact Lie groups. Sometimes it is written for arbitrary functions, and other times it is written only for class functions. This subsection begins with a very concrete and specific example of how the integral of an arbitrary function in $L^1(SO(3))$ can be decomposed. Then it is shown how a similar decomposition holds for the unitary group $U(n)$ and then, finally, the most general statement for arbitrary compact Lie groups is given. In all cases, the functions of interest are general, and it is shown what simplifications happen when these general functions are replaced by class functions.

The Formula for the Case of $SO(3)$

Any element of $SO(3)$ can be written as the matrix exponential $R = \exp(\theta N)$, where $\|N^\vee\| = 1$ and $\theta \in [0, 2\pi)$. (Actually, it is possible to restrict $N^\vee$ to the upper half-sphere or θ to the range $[0, \pi)$. Keeping the above range covers $SO(3)$ twice, but this will be a useful construction in the discussion below.) Without loss of generality, the unit vector $N^\vee = \mathbf{n}$ can be parameterized with spherical coordinates $(\alpha, \beta) \in [0, 2\pi) \times [0, \pi]$. Then the normalized integral over $SO(3)$ can be written as[4]

$$\begin{aligned}\int_{SO(3)} f(R)\, dR &= \frac{1}{4\pi^2} \int_0^{2\pi} \int_0^{\pi} \int_0^{2\pi} f(\theta, \alpha, \beta)\, \sin^2 \frac{\theta}{2}\, \sin\beta\, d\alpha\, d\beta\, d\theta \\ &= \frac{1}{2\pi} \int_0^{2\pi} \left[\frac{1}{4\pi} \int_0^{\pi} \int_0^{2\pi} f(\theta, \alpha, \beta)\, [2 \sin^2 \theta/2]\, \sin\beta\, d\alpha\, d\beta \right] d\theta. \end{aligned} \tag{12.40}$$

The integral over θ in the above expression could have been restricted to $[0, \pi)$, in which case the normalizing factor would have been $1/2\pi^2$ rather than $1/4\pi^2$. The reason for keeping the range $[0, 2\pi)$ is that it can be identified with $SO(2)$.

It is well known that the exponential parametrization can be written as

$$\exp(\theta N) = [\mathbf{a}, \mathbf{b}, \mathbf{n}]\, R_3(\theta)\, [\mathbf{a}, \mathbf{b}, \mathbf{n}]^T,$$

where $\mathbf{a}$ and $\mathbf{b}$ are unit vectors such that $[\mathbf{a}, \mathbf{b}, \mathbf{n}] \in SO(3)$. In other words, these three vectors are mutually orthogonal and form a right-handed coordinate system. The vectors $\mathbf{a}$ and $\mathbf{b}$ are not unique. This is easy to observe this since making the substitution

[4] This should not be confused with the Euler-angle parameterization (α, β, γ), which does not have a $\sin^2 \theta/2$ factor in the volume element, although both parameterizations have the α and β in common.

$$[\mathbf{a}', \mathbf{b}', \mathbf{n}] = [\mathbf{a}, \mathbf{b}, \mathbf{n}]\, R_3(\gamma)$$

in place of $[\mathbf{a}, \mathbf{b}, \mathbf{n}]$ in the above formula will result in exactly the same $\exp(\theta N)$. In other words, $[\mathbf{a}, \mathbf{b}, \mathbf{n}]$ is arbitrary up to membership in the same coset with respect to the subgroup $SO(2)$ consisting of all rotations around the z axis. Without loss of generality, we can take $[\mathbf{a}, \mathbf{b}, \mathbf{n}]$ to be $R_3(\alpha)R_1(\beta)$.

This means that the right-hand side of (12.40) can be written as

$$\int_{SO(2)} \int_{SO(3)/SO(2)} f(R_3(\alpha)R_1(\beta)R_3(\theta)R_1(\beta)^T R_3^T(\alpha))\, d(\mathbf{n}(\alpha,\beta))\, [2\sin^2\theta/2]\, d(R_3(\theta)), \tag{12.41}$$

where $d(\mathbf{n}(\alpha,\beta)) = (4\pi)^{-1}\sin\beta\, d\alpha\, d\beta$ is just the usual volume element for the unit sphere parameterized by α and β and normalized by 4π, and the integral over $SO(2)$ is normalized by 2π so that $d(R_3(\theta)) = d\theta/2\pi$. Slightly more abstractly, the same expression for $\int_{SO(3)} f(R)\, dR$ can be written without coordinates as

$$\int_{SO(2)} \int_{SO(3)/SO(2)} f([R]R_3(\theta)[R]^T)\, d(R \cdot SO(2))\, [2\sin^2\theta/2]\, d(R_3(\theta)), \tag{12.42}$$

where $[R]$ is any representative of the coset $R \cdot SO(2)$ and $d(R \cdot SO(2))$ is the natural integration measure for the coset space containing the coset $R\cdot SO(2)$. Expression (12.42) is one version of the Weyl integration formula for $SO(3)$. Here, $SO(2)$ is a *maximal torus* in $SO(3)$—that is, it is the largest (in terms of volume) Abelian subgroup. One refers to "a" rather than "the" maximal torus because it is not unique. For example, rather than using $R_3(\theta)$, (12.42) could have been written in terms of $R_1(\theta)$, $R_2(\theta)$, or rotation around any fixed axis. In other words, there are an infinite number of maximal tori in $SO(3)$, all of which are conjugate to each other.

This decomposition of the integral of a function on $SO(3)$ into one over a subgroup and its corresponding coset space is different than the double-coset decomposition in Section 12.4.2. Furthermore, since both sides of (12.41) are constants, and introducing an internal rotation around the z axis by γ does not change anything, it is possible to perform an additional normalized integration on both sides over $SO(2)$ without changing anything. This leads to a decompition of $\int_{SO(3)} f(R)\, dR$ of the form

$$\int_{SO(2)} \int_{SO(3)/SO(2)} \int_{SO(2)} f(R(\alpha,\beta,\gamma)R_3(\theta)R^T(\alpha,\beta,\gamma))\, d\mathbf{n}(\alpha,\beta)\, d\gamma\, [2\sin^2\theta/2]\, d\theta,$$

where $R(\alpha,\beta,\gamma)$ can be ZXZ or ZYZ. Recognizing that $d\mathbf{n}(\alpha,\beta)\, d\gamma$ is the volume element for $SO(3)$ in Euler angles, the inner two integrals can be written as an integral over $SO(3)$, and so

$$\boxed{\int_{SO(3)} f(R)\, dR = \int_{SO(2)} \left(\int_{SO(3)} f(R\, R_3(\theta)\, R^T)\, dR \right) [2\sin^2\theta/2]\, d(R_3(\theta)).} \tag{12.43}$$

This is another version of the Weyl integration formula for $SO(3)$. Note that the integrals over $SO(2)$ and $SO(3)$ can be performed in either order.

The Formula for Case of $U(n)$

Any element W of the group $U(n)$ consisting of all $n \times n$ unitary matrices can be written in the form $W = Ve^{\Lambda}V^T$, where $\Lambda = \mathrm{diag}[i\theta_1, i\theta_2, \ldots, i\theta_n]$, $e^{\Lambda} = \mathrm{diag}[e^{i\theta_1}, e^{i\theta_2}, \ldots, e^{i\theta_n}]$, and $V \in U(n)$. The set of all matrices $\{e^{\Lambda}\}$ form an Abelian subgroup of $U(n)$. In fact, this is a maximal torus for $U(n)$, which is denoted as

$$\mathbb{T} = \{e^{\Lambda} \mid (\theta_1, \theta_2, \ldots, \theta_n) \in [0, 2\pi)^n\}.$$

If V is replaced with $V' = Ve^{\Lambda'}$ for some arbitrary $e^{\Lambda'} \in \mathbb{T}$, the resulting W will be exactly the same. Therefore, choosing any coset representative $[V] \in V \cdot \mathbb{T}$, it is possible to write $W = [V]e^{\Lambda}[V]^*$. In principle, we could parameterize the $(n^2 - n)$ homogeneous space $U(n)/\mathbb{T}$ (which plays a role analogous to the sphere in the previous section) and use this together with the n parameters of $\theta_1, \ldots, \theta_n$ to completely parameterize $U(n)$. The integral over $U(n)$ then would be computed using the appropriate Jacobian determinants.

Since $V \cdot \mathbb{T} \in U(n)/\mathbb{T}$, the integral over $U(n)$ can be written as

$$\int_{U(n)} f(W)\, dW = \int_{\mathbb{T}} \int_{U(n)/\mathbb{T}} f([V]\, e^{\Lambda}\, [V]^*)\, |\Delta(e^{\Lambda})|^2\, d(V \cdot \mathbb{T})\, d(e^{\Lambda}), \tag{12.44}$$

where $d(e^{\Lambda}) = (2\pi)^{-n} d\theta_1 \cdots d\theta_n$, $|\Delta(e^{\Lambda})|^2$ is a Jacobian factor, and the volume elements for the coset space, the maximal torus, and $U(n)$ are all normalized so that the integral unity is unity:

$$\int_{U(n)/\mathbb{T}} d(V \cdot \mathbb{T}) = \int_{\mathbb{T}} d(e^{\Lambda}) = \int_{U(n)} dW = 1.$$

It is known that the Jacobian factor can be written explicitly as

$$\Delta(e^{\Lambda}) = \prod_{1 \leq j < k \leq n} (e^{i\theta_k} - e^{i\theta_j}),$$

which is the determinant of a Vandermonde matrix $V = [v_{jk}]$ where $v_{jk} = e^{i(k-1)\theta_j}$. Equation (12.44) is *Weyl's integration formula for* $U(n)$. For class functions, $\chi([V]e^{\Lambda}[V]^*) = \chi(e^{\Lambda})$ and so this simplifies to

$$\int_{U(n)} \chi(W)\, dW = \int_{\mathbb{T}} \chi(e^{\Lambda})\, |\Delta(e^{\Lambda})|^2\, d(e^{\Lambda}).$$

Introducing a transformation of the form $[V] \to [V]e^{\Lambda'}$, which has no effect on the right-hand side of (12.44) due to internal cancellation, and integrating both sides of (12.44) again over $\mathbb{T}$ with respect to the normalized volume element $d((e^{\Lambda'}))$ then gives

$$\boxed{\int_{U(n)} f(W)\, dW = \int_{\mathbb{T}} \int_{U(n)} f(Ve^{\Lambda}V^*)\, |\Delta(e^{\Lambda})|^2\, dV\, d(e^{\Lambda}).} \tag{12.45}$$

This is another version of Weyl's integration formula for $U(n)$, and the integrals on the right-hand side can be written in either order.

The Formula for General Compact Lie Groups

In some sense, Weyl's integration formula for $U(n)$ is already the most general case since every compact Lie group is a subgroup of $U(n)$ for some value of n. Therefore, by restricting the choices of $f(W)$ in the previous section to be those that are nonzero only on the Lie subgroup of interest would be one way to construct a general Weyl integration formula. However, there is a more direct way, which is what is reviewed here.

Suppose G is a compact Lie group and $f \in L^1(G)$. Define a maximal torus $T < G$ to be an Abelian subgroup of maximal volume, which is naturally isomorphic to a torus $\mathbb{R}^k/\mathbb{Z}^k$ for some $k \in \mathbb{Z}_{>0}$. (Here, the notation T is intentionally different than the specific $\mathbb{T} < U(n)$ in the previous subsection.) Given any maximal torus T, the normalizer of T is the subgroup of G defined by

$$N = \{g \in G \,|\, gTg^{-1} = T\}.$$

Necessarily, T is a normal subgroup of N, and so N/T is a group. This group, called the *Weyl group*,[5] is a finite group, and so $|N/T|$ (which is sometimes written as $|W(G,T)|$) is finite.

A natural mapping exists between the product space $G/T \times T$ and G—namely

$$\psi : G/T \times T \to G, \quad \text{where } \psi([g],t) = [g] \circ t \circ [g]^{-1}$$

and where $g \in G$, $t \in T$, and $[g] \in gT \in G/T$. Since G/T, T, and G are orientable Riemannian manifolds, the mapping between the above manifolds has an associated Jacobian determinant when introducing coordinates. Alternatively, Jacobians can be dispensed with and the coordinate-free description of differential geometry expressed in terms of differential forms can be used. Either way, the result is a formula of the form

$$\boxed{\int_G f(g)\,dg = |W(G,T)|^{-1} \int_T |V(t)|^2 \int_{G/T} f([g] \circ t \circ [g]^{-1})\,d(gT)\,dt,} \tag{12.46}$$

where $[g] \in gT$ and $|V(t)|^2$ for $t \in T$ is a Jacobian factor analogous to $|\Delta(e^{\Lambda})|^2$ when $e^{\Lambda} \in U(n)$. Equation (12.46) is one version of Weyl's integration formula for an arbitrary compact Lie group. $V(t)$ could be derived directly from $|\Delta(e^{\Lambda})|^2$ by embedding G in $U(n) \subset \mathbb{R}^{n\times n}$ and performing some additional computations. Alternative (intrinsic) approaches for computing $V(t)$ are described in [6].

Recognizing that any $g \in G$ can be written as $g = [g] \circ t'$ for some $t' \in T$ and since $t' \circ t \circ (t')^{-1} = t$, making this substitution and integrating over $t' \in T$ gives

$$\int_{[g]\in gT \in G/T} \int_{t' \in T} f([g] \circ t' \circ t \circ ([g] \circ t')^{-1})\,dt'\,d(gT) = \int_G f(g \circ t \circ g^{-1})\,dg.$$

Therefore, (12.46) can be rewritten as

$$\boxed{\int_G f(g)\,dg = |W(G,T)|^{-1} \int_T |V(t)|^2 \int_G f(g \circ t \circ g^{-1})\,dg\,dt.} \tag{12.47}$$

The function $V(t)$ in the Weyl integration formula has been computed for broad classes of compact Lie groups in addition to $U(n)$ [7, 50] including (but are not limited to)[6]

[5] No relationship to the group with the same name in Volume 1 (which is called the Weyl–Heisenberg group in this volume).

[6] Here, $R(\theta) \in SO(2)$ is the usual 2×2 rotation matrix. $\mathbb{Z}_2 \wr S_n$ is the wreath product of the groups $\mathbb{Z}_2$ and S_n, which is a new finite group consisting of tuples of the form $(b_1, b_2, \ldots, b_n; \pi)$ for binary numbers $b_k \in \mathbb{Z}_2$ and permutations $\pi \in S_n$. The group operation is $(a_1, \ldots, a_n; \sigma) \diamond (b_1, \ldots, b_n; \pi) = (a_1 +_2 b_{\sigma^{-1}(1)}, \ldots, a_n +_2 b_{\sigma^{-1}(n)}; \sigma\pi)$, where $+_2$ is addition modulo 2. (See [11] for a more general definition.)

$SO(2n)$:

$$T = \{t = R(\theta_1) \oplus R(\theta_2) \oplus \cdots \oplus R(\theta_n) \mid \theta_k \in [0, 2\pi)\},$$
$$V(t) = 2^{n(n-1)} \prod_{1 \le j < k \le n} \sin\left(\frac{\theta_j - \theta_k}{2}\right) \sin\left(\frac{\theta_j + \theta_k}{2}\right),$$
$$|W(SO(2n+1), T)| = |\mathbb{Z}_2 \wr S_n^+| = 2^{n-1} n!$$

$SO(2n+1)$:

$$T = \{t = R(\theta_1) \oplus R(\theta_2) \oplus \cdots \oplus R(\theta_n) \oplus 1 \mid \theta_k \in [0, 2\pi)\},$$
$$V(t) = 2^{n^2} \prod_{1 \le j < k \le n} \sin\left(\frac{\theta_j - \theta_k}{2}\right) \sin\left(\frac{\theta_j + \theta_k}{2}\right) \prod_{1 \le j \le n} \sin\frac{\theta_j}{2},$$
$$|W(SO(2n+1), T)| = |\mathbb{Z}_2 \wr S_n| = 2^n n!$$

$SU(n)$:

$$T = \left\{ t = \mathrm{diag}(e^{i\theta_k}) \;\middle|\; \sum_k \theta_k = 0 \right\},$$
$$V(t) = 2^{n(n-1)/2} \prod_{1 \le j < k \le n} \sin\left(\frac{\theta_j - \theta_k}{2}\right),$$
$$|W(SU(n), T)| = |S_n| = n!$$

For example, using the above information for $SO(2n+1)$ in the case when $n = 1$, the Weyl integration formula is coincident with (12.42), since the product signs vanish, giving $V(t) = 2\sin\theta/2$, or, equivalently, $|V(t)|^2 = 4\sin^2\theta/2$. Additionally, dividing by $|W(SO(3), SO(2))| = 2$ gives the $2\sin^2\theta/2$ in the integrand of (12.42) and (12.43).

12.4.4 Separation of Variables

Other decompositions of integrals on Lie groups with a less group-theoretic flavor are also possible. Let $g(\mathbf{q})$ be any global parametrization (up to a set of singularities of measure zero) of the unimodular Lie group G. If the associated Jacobian determinant[7] is separable as

$$|J(\mathbf{q})| = w_1(\mathbf{q}_1) \cdot w_2(\mathbf{q}_2),$$

where $\mathbf{q} = [\mathbf{q}_1^T, \mathbf{q}_2^T]^T$, and if

$$f(g(\mathbf{q})) = \sum_{i,j} c_{ij} \phi_i(\mathbf{q}_1) \psi_j(\mathbf{q}_2),$$

then

$$\int_G f(g)\, dg = \sum_{i,j} c_{ij} \left(\int_{\mathbf{q}_1} \phi_i(\mathbf{q}_1)\, w_1(\mathbf{q}_1)\, d\mathbf{q}_1 \right) \cdot \left(\int_{\mathbf{q}_2} \psi_j(\mathbf{q}_2)\, w_2(\mathbf{q}_2)\, d\mathbf{q}_2 \right). \tag{12.48}$$

[7] Recall that for a unimodular Lie group, $|J_r(\mathbf{q})| = |J_l(\mathbf{q})|$ for all values of $\mathbf{q}$, and so the subscripts l and r need not be specified.

12.4.5 Integration on Lie Groups with Multiple Components

It can be the case that a Lie group consists of a countable number of disjoint components. When this number is greater than 1, the components can be given labels in an index set, I, and the integral over the group can be described as an integral within each component and a sum over the different components; that is, $G = \cup_{i \in I} G_i$, where $G_i \cap G_j = \emptyset$ when $i \neq j$ and

$$\int_G f(g)\, dg = \sum_{i \in I} \int_{g_i \in G_i} f(g_i)\, dg_i.$$

Several very practical examples of this kind arise in applications.

For example, the full orthogonal group, $O(n)$, has two components: one corresponding to $SO(n)$, and the other corresponding to reflections. Given a rotation $R \in SO(n)$, a reflection can be generated by multiplication with a matrix of the form $\mathbb{I}_n^- \doteq (-1) \oplus \mathbb{I}_{n-1}$. Therefore, the integral over $O(n)$ can be written as

$$\int_{O(n)} f(O)\, dO = \int_{SO(n)} f(R)\, dR + \int_{SO(n)} f(R\mathbb{I}_n^-)\, dR.$$

As another example, consider the direct product $G = SO(2) \times \mathbb{Z}$. Then each element is a pair of the form $g = (\theta, n)$ and

$$\int_G f(g)\, dg = \sum_{n \in \mathbb{Z}} \int_{SO(2)} f(\theta, n)\, d\theta.$$

A third example is one that the author and his postdoc investigated in the context of robotics and image understanding problems [30–32]. This group is the semi-direct product of $(\mathbb{R}^d, +)$ and proper crystallographic point groups describing rotational symmetries of Platonic solids in $\mathbb{R}^d$. In higher dimensions, such groups have relatively few elements, but in the planar case, the group of planar rotational symmetry operations of the regular n-gon has n elements. As n is allowed to become large, this group approximates $SE(2)$.

12.5 Invariant Integration on Homogenous Spaces

In many practical applications, the manifolds that arise are either those that are embedded in Euclidean space or they arise as the homogenous space[8] of a Lie group with respect to a subgroup. Often the manifolds of interest are both embedded in Euclidean space *and* can be viewed as a homogenous space. The classic example of this is the usual sphere $S^2 \subset \mathbb{R}^3$. It is embedded in $\mathbb{R}^3$ and can be viewed as the coset space $SO(3)/SO(2)$.

12.5.1 Conditions for Invariant Integration

Since homogenous spaces form such an important class of manifolds with greater structure than generic Riemannian manifolds, it is worthwhile to examine how to integrate on them. In particular, since unimodular Lie groups occur often in applications, it is useful to know that as a consequence of a theorem proven by Weil in [62] (and in the first edition of that work which appeared in 1938), we have the following theorem.

[8] Also called the quotient space or coset space.

Theorem 12.1. *If G and H are Lie groups with finite and strictly positive dimensions and if $H < G$, then the following are each necessary and sufficient conditions for the equality*

$$\int_{G/H} f(gH)\, d(gH) = \int_{G/H} f(g_0 \cdot (gH))\, d(gH)$$

to hold:

$$|Ad_G(h)| = |Ad_H(h)|, \quad \forall\, h \in H, \tag{12.49}$$

where Ad_G and Ad_H are the adjoint matrices for G and H, respectively;

$$\sum_{k=m+1}^{n} C_{sk}^{k} = 0 \quad \textit{for } s = 1, \ldots, m \tag{12.50}$$

(where $m = \dim(H)$, $n - m = \dim(G/H)$, and s and k respectively run over the basis elements of the Lie algebra of G that span H and G/H); and

$$d(d(gH)) = 0, \quad \textit{where } d(gH) \doteq \omega_{m+1} \wedge \cdots \wedge \omega_n \tag{12.51}$$

and the outer $d(\cdot)$ denotes the exterior derivative.

See Santaló [49] for the proof. The first condition follows from a theorem by Weil [62], the second is due to Chern [9], and the third is proved in Santaló [49].

Clearly, if H and G are both unimodular, the conditions of the theorem hold because then $|Ad_G(h)| = |Ad_H(h)| = 1$. As an example, when $G = SO(3)$ and $H = SO(2)$, it is clear that the integral of a function on the sphere is invariant under rotation:

$$\int_{S^2} f(R^T \mathbf{u})\, d\mathbf{u} = \int_{S^2} f(\mathbf{u})\, d\mathbf{u}.$$

Additionally, if $G = SE(n)$ and $H = SO(n)$, then $G/H \cong \mathbb{R}^n$ and

$$\int_{\mathbb{R}^n} f(g^{-1} \cdot \mathbf{x})\, d\mathbf{x} = \int_{\mathbb{R}^n} f(\mathbf{x})\, d\mathbf{x}$$

for all $g \in SE(n)$.

12.5.2 Convolution on Homogenous Spaces

The convolution of a function $f_1 : G \to \mathbb{R}$ with one of the form $f_2 : G/H \to \mathbb{R}$ is defined as

$$(f_1 \star f_2)(g'H) \doteq \int_G f_1(g)\, f_2(g^{-1} \cdot (g'H))\, dg. \tag{12.52}$$

The operation $\star$ is different than $*$ in analogy with the difference between the group action $\cdot$ and the group operation $\circ$. In analogy with the way the action satisfies the condition $g_1 \cdot (g_2 \cdot x) = (g_1 \circ g_2) \cdot x$, if f_0 and f_1 are functions on G and f_2 is a function on G/H, then

$$(f_0 * f_1) \star f_2 = f_0 \star (f_1 \star f_2). \tag{12.53}$$

The topic of convolution of special kinds of functions on homogeneous spaces is explained in [25]. Fourier expansions on homogeneous spaces are addressed in [60, 64], and the case when the subgroup H is discrete is addressed in [67].

12.6 Global Geometry and Topology of Compact Connected Lie Groups

Equipped with the concept of a bi-invariant integration measure and bi-invariant differential forms, it becomes possible to compute global geometric and topological invariants on compact Lie groups. In this section several of the fundamental differential-geometric properties of Lie groups are addressed together with associated topological invariants.

12.6.1 Stokes' Theorem for a Compact Lie Group

From Stokes' theorem for a manifold with boundary, it follows that for an n-dimensional compact Lie group (which has no boundary) that the integral of the exterior derivative of an arbitrary $(n-1)$-form $\omega^{(n-1)}$ must vanish:

$$\int_G d\omega^{(n-1)} = 0. \tag{12.54}$$

This result has been reported in [29].

In contrast, if $\omega^{(n-1)}$ is either left or right invariant, then from (11.55) it must be a closed form, and so

$$\int_{\partial M} d\omega_r^{(n-1)} = \int_{\partial M} d\omega_l^{(n-1)} = 0 \tag{12.55}$$

for any smooth orientable manifold ∂M that encloses a finite volume $M \subset G$.

12.6.2 Betti Numbers, Poincaré Polynomials, and Euler Characteristics for Compact Lie Groups

In Chapter 6 of Volume 1 the matrices $\Lambda^k(A)$ were introduced as square matrices of dimension $\binom{n}{k} \times \binom{n}{k}$ when A has dimensions $n \times n$. It can be verified that the trace of these matrices show up in the determinant

$$\det(\lambda\mathbb{I} + A) = \lambda^n + a_1\lambda^{n-1} + \cdots + a_{n-1}\lambda + a_n$$

as

$$a_k = \mathrm{tr}[\Lambda^k(A))].$$

Computing the same determinant with $A = [Ad(g)]$, where $g \in G$, a compact Lie group, results in coefficients that depend on the group. If these coefficients are integrated over the whole group, the result is the *Betti numbers*

$$b_k(G) \doteq \int_G \mathrm{tr}\big[\Lambda^k([Ad(g)])\big]\, dg \quad \text{for } k = 1, \ldots, \dim(G). \tag{12.56}$$

The Betti numbers provide topological information about the Lie group.

The Poincaré polynomial for a Lie group is precisely

$$p(\lambda; G) = \lambda^{\dim(G)} + b_1(G)\lambda^{\dim(G)-1} + \cdots + b_{\dim(G)-1}(G)\lambda + b_{\dim(G)}(G),$$

with $b_0(G) = 1$ serving as the coefficient in front of $\lambda^{\dim(G)}$. These polynomials have been computed for all of the classical compact Lie groups, as reviewed in [16, 22, 26, 43, 63]. For example,

$U(n)$:

$$p(\lambda; U(n)) = (1+\lambda^3)(1+\lambda^5)\cdots(1+\lambda^{2n-1}).$$

$SU(n)$ $(n \geq 2)$:

$$p(\lambda; SU(n)) = \prod_{p=1}^{n-1}(1+\lambda^{2p+1}).$$

$SO(2n+1)$:

$$p(\lambda; SO(2n+1)) = \prod_{p=1}^{n}(1+\lambda^{4p-1}).$$

$SO(2n)$ $(n > 2)$:

$$p(\lambda; SO(2n)) = (1+\lambda^{2n-1})\prod_{p=1}^{n-1}(1+\lambda^{4p-1}).$$

$\mathbb{T}^n$:

$$p(\lambda; \mathbb{T}^n) = (1+\lambda)^n.$$

In general, for a compact connected Lie group, the Betti numbers are symmetrical in the sense that $b_k(G) = b_{\dim(G)-k}(G)$. Furthermore, the Betti numbers of the Cartesian product of two manifolds (or including Lie groups with manifolds that are Cartesian products) are

$$p(\lambda; G_1 \times G_2) = p(\lambda; G_1) \cdot p(\lambda; G_2).$$

The Euler–Poincaré characteristic of a compact connected Lie group is obtained from the Betti numbers as

$$\chi(G) = \sum_{k=0}^{\dim(G)} (-1)^k b_k(G). \tag{12.57}$$

A simple connection between the Euler–Poincaré characteristic and the Poincaré polynomials for a compact Lie group is $\chi(G) = p(-1; G)$.

There are a number of ways to compute Betti numbers and the Euler–Poincaré characteristic. In addition to computing $\chi(G)$ as explained above, it could be obtained by tessellating the compact Lie group into a collection of cells as was done in Chapter 5 of Volume 1 for surfaces and bodies in $\mathbb{R}^2$ and $\mathbb{R}^3$. Algebraic properties can be given to these tesselations, leading to the field of *homology.* Alternatively, the properties of differential forms on a compact manifold can be used to directly determine its topological properties. This approach is called *de Rham cohomology.*[9]

12.6.3 de Rham Cohomology

Let $\Omega^k(G)$ denote the set of all k-forms on G. This forms a vector space of dimension $\binom{\dim(G)}{k}$, and hence $(\Omega^k(G), +)$ is a group. The exterior derivative can be viewed as a

[9] Although the discussion that follows is restricted to compact connected Lie groups, the concepts apply equally well to other compact connected manifolds. For more general discussions, see [17, 40]

mapping $d: \Omega^k(G) \to \Omega^{k+1}(G)$. The set of all closed k-forms on G is denoted as $Z^k(G) < \Omega^k(G)$, and the set of all exact k-forms on G is denoted as $B^k(G) < Z^k(G) < \Omega^k(G)$. These subgroups of $\Omega^k(G)$ can be described as [40]

$$Z^k(G) = Ker(d : \Omega^k(G) \to \Omega^{k+1}(G)) \quad \text{and} \quad B^k(G) = Im(d : \Omega^{k-1}(G) \to \Omega^k(G)). \tag{12.58}$$

Since these are Abelian groups, $B^k(G)$ is naturally a normal subgroup of $Z^k(G)$; hence, the quotient

$$H^k_{DR}(G) \doteq Z^k(G)/B^k(G)$$

is also a group, called the kth *de Rham cohomology group of G*. Interestingly, the kth Betti number and kth de Rham cohomology group are related as

$$b_k(G) = \dim(H^k_{DR}(G)) = \dim(Z^k(G)) - \dim(B^k(G)). \tag{12.59}$$

Remarkably, there is a correspondence between homology and cohomology in that they are both paths that lead to the Betti numbers. For a compact Lie group, the Betti number $b_k(G)$ can be viewed as the dimension of the space of harmonic (i.e., bi-invariant) k-forms. Since methods for computing all left- or right-invariant k-forms was given in Chapter 11, for low-dimensional compact Lie groups it is easy to count how many harmonic forms there are. For example, in Exercise 11.7 it was determined that $SO(3)$ has $b_0(SO(3)) = b_3(SO(3)) = 1$ because the number 1 is a bi-invariant 0-form and the volume element is a bi-invariant 3-form, and these are unique up to scaling. Therefore, using (12.57), $\chi(SO(3)) = 0$. The same result could be obtained from the Poincaré polynomials by setting $\chi(SO(3)) = p(-1; SO(3))$. Although it is possible to go through the tedious coordinate-dependent computations of enumerating all bi-invariant forms for a compact Lie group, a more subtle and powerful argument can be used, as explained below.

Following Goldberg [22], it can be reasoned that the kth Betti number for a compact Lie group G can be written as

$$b_k(G) = \binom{\dim(G)}{k} - n_k - n_{k-1}, \tag{12.60}$$

where $\binom{\dim(G)}{k}$ is the total number of linearly independent left-invariant[10] k-forms on G and n_k is the number of elements in the subset of left-invariant k-forms on G, no linear combination of which is a closed form. The procedure for generating a basis for all left-invariant k-forms on G was given in Chapter 11, and assessing closure is simply a matter of observing whether or not the exterior derivative vanishes. Since the exterior derivative of a $(k-1)$-form produces a special kind of closed k-form (i.e., an exact form), this means that applying the exterior derivative to each left-invariant $(k-1)$-form necessarily produces a closed form. However, application of the exterior derivative does not change a form lacking bi-invariance into one that is bi-invariant. Therefore, any left-invariant k-form can be decomposed into a linear combination of harmonic (bi-invariant) forms, left-invariant k-forms that are not closed, and exact forms (which are closed but not harmonic). This means that the total number of linearly independent left-invariant forms must be decomposable as $\binom{\dim(G)}{k} = b_k(G) + n_k + n_{k-1}$ or, equivalently, (12.60). Therefore, combining this with (12.57) gives

[10] Here and throughout this discussion we could have chosen right-invariant rather than left-invariant forms.

$$\begin{aligned}\chi(G) &= \sum_{k=0}^{\dim(G)} (-1)^k \binom{\dim(G)}{k} - \sum_{k=0}^{\dim(G)} (-1)^k n_k - \sum_{k=0}^{\dim(G)} (-1)^k n_{k-1} \\ &= (-1)^{\dim(G)+1} n_{\dim(G)} - n_0.\end{aligned}$$

However, we know that to within a constant scalar multiple, the only $\dim(G)$-form for a compact Lie group is the volume form, which is bi-invariant, and likewise the only 0-form is a constant scalar, which is also bi-invariant, and so that $n_{\dim(G)} = n_0 = 0$. This means that for a compact connected Lie group,

$$\boxed{\chi(G) = 0.} \tag{12.61}$$

Note that the same result can be observed by evaluating $p(-1; G)$ for all of the compact Lie groups listed earlier.

12.6.4 Hodge Theory

If $\dim(G) = n$, then the Hodge star operator converts a k-form of a Lie group G, $\omega \in \Omega^k(G)$, into an $(n-k)$-form. Applying the Hodge star operator twice returns the original k-form, premultiplied by $(-1)^{k(n-k)}$ as in (6.28). On the other hand, exterior differentiation of $*\omega$ gives an $(n-k+1)$-form, $d(*\omega)$, and if this is again followed by another application of the Hodge star operator, this gives an $n-(n-k+1) = (k-1)$-form, $*d(*\omega)$. Due to the sign changes that result from two applications of the Hodge star operator, it is convenient to define

$$\delta\omega \doteq (-1)^{n(k+1)+1} * d(*\omega).$$

Then it can be shown that the following commutative diagram holds:

$$\begin{tikzcd} \Omega^k(G) \arrow[r, "*"] \arrow[d, "\delta"'] & \Omega^{n-k}(G) \arrow[d, "d"] \\ \Omega^{k-1}(G) \arrow[r, "(-1)^k *"'] & \Omega^{n-k+1}(G) \end{tikzcd} \tag{12.62}$$

The operator δ is the adjoint of d in the sense that $\langle d\omega, \alpha\rangle = \langle \omega, \delta\alpha\rangle$, where the inner product of two k-forms on G is defined as in (6.96), with the domain of integration being G. This fact can be written as $d^* = \delta$ and $\delta^* = d$. The Laplacian of a form then can be defined as $\Delta : \Omega^k(G) \to \Omega^k(G)$, where[11]

$$\Delta\omega \doteq d(\delta\omega) + \delta(d\omega) \quad \text{or} \quad \Delta = d\delta + \delta d.$$

If $\Delta\omega = 0$, then ω is called a *harmonic form.*

The Laplacian of general forms, $\alpha, \beta \in \Omega^k(G)$, for any value of $k \in [0, n]$ has the following properties [40]:

[11] This definition reduces to that given in coordinates in (5.50) when $k = 0$.

$$*(\Delta\alpha) = \Delta(*\alpha) \quad \text{or} \quad *\,\Delta = \Delta*,$$
$$\langle \Delta\alpha, \beta \rangle = \langle \alpha, \Delta\beta \rangle,$$
$$\Delta\omega = 0 \iff d\omega = \delta\omega = 0.$$

The space of all harmonic k-forms on G is denoted as $\mathbb{H}^k(G)$. In other words,

$$\mathbb{H}^k(G) \doteq \{\omega \in \Omega^k(G) \,|\, \Delta\omega = 0\}.$$

Given a closed-form $\omega \in \Omega^k(G)$, it has a corresponding representative $[\omega] \in H^k_{DR}(G)$, called the de Rham cohomology class of ω. The *Hodge theorem* says that each de Rham cohomology class can be represented by a unique harmonic form. In other words, there is an isomorphism [26, 40]

$$\boxed{\mathbb{H}^k(G) \longleftrightarrow H^k_{DR}(G).} \tag{12.63}$$

Thus, if the space of harmonic forms can be characterized, so too can each de Rham cohomology group, therefore elucidating the topological properties of G.

Although the above statements hold for any compact orientable Riemannian manifold, the additional structure provided by Lie groups allows us to say even more. In Section 11.7, left/right-invariant forms were discussed. Let $\mathcal{L}^k(G)$ and $\mathcal{R}^k(G)$ respectively denote these left/right-invariant k-forms. Then

$$\mathcal{B}^k(G) = \mathcal{L}^k(G) \cap \mathcal{R}^k(G)$$

denotes those k-forms that are bi-invariant.

For example, in the case of a compact semi-simple Lie group, G, it is known that the set of harmonic k-forms and the set of all bi-invariant k-forms coincide:

$$\mathbb{H}^k(G) \cong \mathcal{B}^k(G).$$

12.6.5 The Euler–Poincaré Characteristic for Coset Spaces of a Compact Lie Group

The Euler–Poincaré characteristic for a coset space of a compact Lie group with respect to a maximal torus can be obtained more directly as the integral [23]

$$\chi(G/T) = \int_T |V(t)|^2\,dt, \tag{12.64}$$

where $|V(t)|^2$ is the same factor that appears in the Weyl integration formula. This immediately indicates that $\chi(G/T) \geq 0$. The Euler–Poincaré characteristic of more general coset spaces $\chi(G/H)$ can be computed using similar integrals [23, 26].

For example, if $R \in SO(3)$, then $[Ad(R)] = R$ and

$$\det(\lambda\mathbb{I} + R) = \lambda^3 + \mathrm{tr}(\Lambda^1(R))\lambda^2 + \mathrm{tr}(\Lambda^2(R))\lambda + 1.$$

Recall from the definition of $\Lambda^n(R)$ in (6.48) that $\Lambda^1(R) = R$ and $\Lambda^2(R)$ is given in component form in (6.109). Integration over the group using the normalized Haar measure in (12.10), with each matrix element R_{ij} expressed in terms of Euler angles, gives an explicit way to compute the Betti numbers

$$b_1(SO(3)) = 0, \quad b_2(SO(3)) = 0, \quad b_3(SO(3)) = 1.$$

The Euler–Poincaré characteristic is then

$$\chi(SO(3)) = 0.$$

When $G = SO(3)$ and $T = SO(2)$, (12.64) evaluates as

$$\chi(SO(3)/SO(2)) = \frac{1}{2\pi} \int_0^{2\pi} 4 \sin^2 \frac{\theta}{2}\, d\theta = 2.$$

This is the Euler characteristic for the sphere S^2.

12.7 Fourier Analysis on Unimodular Lie Groups

This section begins with definitions of group representations and then explains the generalized Fourier analysis that results.

12.7.1 Group Representations

A group representation can be thought of as an element of an indexed set of matrix-valued functions of a group-valued argument, $U(g, \lambda) \in GL(n_\lambda, \mathbb{C})$, that satisfies the homomorphism property

$$\boxed{U(g_1 \circ g_2, \lambda) = U(g_1, \lambda)\, U(g_2, \lambda).} \tag{12.65}$$

Here, $g \in G$ and $\lambda \in \hat{G}$, which is called the "dual of G." For example, when $G = (\mathbb{R}^n, +)$, the representation matrices are the 1×1-dimensional quantities $\exp(i\boldsymbol{\omega}^T \mathbf{x})$ for $\mathbf{x}, \boldsymbol{\omega} \in \mathbb{R}^n$. In this special case, the dual of $\mathbb{R}^n$ is isomorphic (as a vector space) to $\mathbb{R}^n$. When $G = SO(2)$, representations are of the form $e^{in\theta}$ where $\theta \in SO(2)$ and $n \in \mathbb{Z} = \hat{G}$. Therefore, when considering a general group G and thinking about analogies with classical Fourier analysis, the index λ and dual space $\hat{G}$ can be thought of as generalizations of the frequency parameter and frequency space, respectively.

Irreducibility of a representation $U(g, \lambda)$ means that for any $\lambda \in \hat{G}$ it is not possible to find a similarity transformation of the form $S(\lambda)U(g, \lambda)S^{-1}(\lambda)$, where $S(\lambda) \in GL(n_\lambda, \mathbb{C})$, that simultaneously block-diagonalizes $U(g, \lambda)$ for all values of $g \in G$. In the case of Abelian groups, all irreducible representations are one dimensional, as in the examples given above, but this is not so for noncommutative groups.

A famous result (due to Schur) states that every irreducible representation is *equivalent* to a unitary one. In this context, two representations $U(g, \lambda)$ and $V(g, \lambda)$ are said to be equivalent if they are related by a similarity transform $U(g, \lambda) = S(\lambda)V(g, \lambda)S^{-1}(\lambda)$ for some $S(\lambda) \in GL(n_\lambda, \mathbb{C})$ for each $\lambda \in \hat{G}$. When $S(\lambda) \in U(n_\lambda)$, the representations $U(g, \lambda)$ and $V(g, \lambda)$ are called *unitarily equivalent* and the relationship itself is called unitary equivalence.[12] Most definitions and results in the fields of Harmonic Analysis and Representation Theory are invariant under changes between unitary equivalent representations, which means that there are an infinite number of equally valid ways to define sets of *irreducible unitary representations*, or IURs.

[12] Here, $U(g, \lambda)$ denotes a particular unitary matrix and $U(n_\lambda)$ is the full unitary group that contains all such $n_\lambda \times n_\lambda$ matrices; that is, $\{U(g, \lambda) \mid g \in G\} \subseteq U(n_\lambda)$ with equality rarely holding.

Therefore, without loss of generality we can take $U(g,\lambda)$ to be unitary—that is, $U^{-1}(g,\lambda) = U^{*}(g,\lambda)$, where $*$ denotes the Hermitian conjugate. It then follows that since

$$\mathbb{I} = U(e,\lambda) = U(g^{-1} \circ g, \lambda) = U(g^{-1},\lambda)\, U(g,\lambda),$$

then

$$U(g^{-1},\lambda) = (U(g,\lambda))^{-1} = U^{*}(g,\lambda).$$

From the above discussion, the concepts of irreducibility and unitarity should be clear. A third important concept is that of *completeness* of a set of irreducible representations. This means that every possible reducible representation can be decomposed into a direct sum of the representations in the complete set. In order to understand completeness, it is useful to first consider IURs for the simplest group, $SO(2)$. The completeness relation for the classical Fourier basis on the unit circle is

$$\frac{1}{2\pi}\sum_{n\in\mathbb{Z}} e^{in(\theta_1-\theta_2)} = \delta(\theta_1-\theta_2),$$

where $\delta(\theta)$ is the Dirac delta function with the properties

$$\int_{SO(2)} \delta(\theta)\, d\theta = 1 \quad \text{and} \quad \int_{SO(2)} f(\theta)\, \delta(\theta-\theta_0)\, d\theta = f(\theta_0).$$

This is what allows the classical Fourier reconstruction formula to work. In analogy, in the group context, a set of IURs $\{U(g,\lambda) \mid \lambda \in \hat{G}\}$ is complete if for any $g_0, g_1, g_2 \in G$,

$$\sum_{\lambda\in\hat{G}} U(g_1^{-1}\circ g_2, \lambda) = \delta(g_1^{-1}\circ g_2),$$

where the Dirac delta function has the properties

$$\int_G \delta(g)\, dg = 1 \quad \text{and} \quad \int_G f(g)\, \delta(g^{-1}\circ g_0)\, dg = f(g_0)$$

for any $f \in \mathcal{N}(G)$. For some unimodular Lie groups, the completeness relation written above as a discrete sum can be an integral or a combination of both sums and integrals.

In all examples of interest in this book, the mapping $U : G \to U(n_\lambda)$ for each fixed $\lambda \in \hat{G}$ that defines each $U(g,\lambda)$ is a smooth homomorphism, and so we can differentiate. A definition that will be used extensively in the following sections is

$$\boxed{u(E_i,\lambda) \doteq \frac{d}{dt} U(\exp(tE_i),\lambda)|_{t=0}.} \tag{12.66}$$

Later we develop explicit expressions for $U(g,\lambda)$ and $u(E_i,\lambda)$ using the exponential map and corresponding parameterizations for the groups $SO(3)$, $SE(2)$, and $SE(3)$.

As will be shown shortly, IURs are at the core of a generalized version of Fourier analysis for functions on unimodular Lie groups. In a number of practical applications, data is presented on Lie groups such as the rotation group and group of rigid-body motions. These are noncommutative groups for which the representation theory and harmonic analysis have been fully worked out (see, e.g., [21, 24, 51, 52, 68]). In particular, the method of induced representations [33] was used by Miller for the case of the rigid-body motion group [39]. Connections between group representations, special functions, and applications are explored in [38, 53, 56]. Representations of the rotation group play a central role in Quantum Mechanics [2, 21, 55, 65]. In that application, the Euler angles are used to parameterize rotations. This corresponds to the double-coset decomposition used in [34, 35] for fast Fourier transforms (FFTs) developed for the rotation group, $SO(3)$. Work on FFTs for $SO(3)$ continues to the current day. See, for example, [44].

12.7.2 Harmonic Analysis and the Convolution Theorem

Given functions $f_i(g) \in \mathcal{N}(G)$ for $i = 1, 2$, the unimodular Lie group $(G, \circ)$, we can define the convolution product

$$(f_1 * f_2)(g) \doteq \int_G f_1(h)\, f_2(h^{-1} \circ g)\, dh$$

and the Fourier transform

$$\boxed{\mathcal{F}(f)(\lambda) \doteq \int_G f(g)\, U(g^{-1}, \lambda)\, dg,} \tag{12.67}$$

where $U(\cdot, \lambda)$ is a unitary matrix function (called an irreducible matrix representation) for each value of the parameter λ (where the set of all values of λ is called the dual of the group and is denoted as $\hat{G}$).

The shorthand $\hat{f}(\lambda) \doteq \mathcal{F}(f)(\lambda)$ is often convenient. When a complete set of IURS exists, the Fourier transform defined in this way has corresponding inversion, convolution, and Parseval theorems:

$$\boxed{f(g) = \int_{\lambda \in \hat{G}} \mathrm{trace}[\hat{f}(\lambda)\, U(g, \lambda)]\, d(\lambda),} \tag{12.68}$$

$$\boxed{\mathcal{F}(f_1 * f_2)(\lambda) = \hat{f}_2(\lambda)\, \hat{f}_1(\lambda),} \tag{12.69}$$

and

$$\boxed{\int_G |f(g)|^2 dg = \int_{\lambda \in \hat{G}} ||\hat{f}(\lambda)||^2\, d(\lambda).} \tag{12.70}$$

Here, $||\cdot||$ is the Hilbert–Schmidt (Frobenius) norm and $d(\lambda)$ is the integration measure on the dual space. For compact Lie groups, this is the Dirac measure weighted by the dimension of the matrix $U(g, \lambda)$. In other words, in the compact case,

$$\int_{\lambda \in \hat{G}} \cdot\, d(\lambda) \longrightarrow \sum_{\lambda \in \hat{G}} \cdot\, n_\lambda,$$

where $n_\lambda = \dim U(g, \lambda)$ and "$\cdot$" denotes the quantity being integrated or summed. Much of this is classical mathematics (see, e.g., [42]), which has not been fully embraced by the engineering world until relatively recently [11].

12.7.3 Separation of Variables and FFTs

The classical (Abelian) fast Fourier transform (FFT) algorithm due to Cooley and Tukey [14] is one of the most significant algorithmic advances of the 20th century. It is an efficient way to calculate the discrete Fourier transform (DFT). The DFT can be thought of as a sampled version of the continuous Fourier series on the circle in which samples are taken at regular intervals. This reduces the computation to a DFT on the group of finite rotations of the circle by integer multiples of $2\pi/N$ for some positive finite integer, N, which is the number of sample points. The FFT is a special implementation of the DFT in which computations are performed in an efficient recursive way. The roots of the FFT go back to calculations that Gauss did to simplify trigonometric sums computed by hand, although this was not known until after it was independently redeveloped in the 1960s [15]. Now, several variations of the FFT exist. Many detailed treatments of this topic can be found in the literature, including [8, 20, 54, 59].

The generalization of the concept of an FFT to the noncommutative context involves the sampling of a Fourier series/transform for a continuous group. In some cases, the sampling pattern might correspond to a finite subgroup, but in most cases, it will not. The resulting discrete calculation is still called an FFT. These generalized FFTs have received considerable attention in recent years, both in abstract settings applicable to wide classes of (mostly finite) groups [1, 12, 18, 34, 35, 45, 46] as well as specific groups such as $SO(3)$ [28, 34, 35] and the Euclidean groups [11, 30–32].

A key trick to use for FFTs on Lie groups is separation of variables. In other words, if a global parameterization of a Lie group exists such that $g(\mathbf{q})$ can be be decomposed into a product of terms of the form $g(0, \ldots, 0, q_i, 0, \ldots, 0)$, then the representation matrices $U(g, p)$ can be reduced to a product, the ith term of which depends on q_i and p. A common example of this is product-of-exponential parameterizations such as the Euler-angle decomposition of $SO(3)$.

If in addition the parameterization is such that the Jacobian determinant reduces to the form $|J(\mathbf{q})| = w_1(q_1)w_2(q_2)\cdots w_n(q_n)$, then the integral in the definition of the Fourier transform matrix can be written as n nested one-dimensional integrals. This is significant because (1) using this separation alone provides significant computational savings and (2) in cases when the resulting one-dimensional integrals involve special functions defined by recurrence relations, the one-dimensional integrals can be computed using existing fast transforms, the benefits of which propagate through the whole multi-dimensional calculation.

The concept of separation of variables has also been used to develop FFTs for finite groups [36], although this is not the topic of the presentation here.

12.7.4 Operational Properties

By the definition of the group Fourier transform $\mathcal{F}[\cdot]$ and operators E_i^r reviewed earlier, one observes that

$$\mathcal{F}[\tilde{E}_i^r f] = \int_G \frac{d}{dt} f(g \circ \exp(tE_i))\bigg|_{t=0} U(g^{-1}, \lambda)\, dg. \tag{12.71}$$

By performing the change of variables $h = g \circ \exp(tE_i)$ and using the homomorphism property of the representations $U(\cdot, \lambda)$, one finds

$$\mathcal{F}[\tilde{E}_i^r f] = \int_G f(h)\ \frac{d}{dt}\left(U(\exp(tE_i)\circ h^{-1},\lambda)\right)\Big|_{t=0} dh \tag{12.72}$$

$$= \left(\frac{d}{dt}U(\exp(tE_i),\lambda)\Big|_{t=0}\right)\int_G f(h)\,U(h^{-1},\lambda)\,dh. \tag{12.73}$$

Then using the definition in (12.66), we write

$$\boxed{\mathcal{F}[\tilde{E}_i^r f] = u(E_i,\lambda)\,\hat{f}(\lambda).} \tag{12.74}$$

This is called an *operational property* because the differential operator is converted into an algebraic operation in Fourier space. An analogous operational property for $\tilde{E}_i^l$ is

$$\boxed{\mathcal{F}[\tilde{E}_i^l f] = -\hat{f}(\lambda)\,u(E_i,\lambda),} \tag{12.75}$$

which is left as an exercise.

12.8 The Exponential Map and Representations

Given an $n_\lambda \times n_\lambda$ matrix representation $U(g,\lambda)$ of G, a representation of the Lie algebra $\mathcal{G}$, $u(X,\lambda)$, results from (12.66). This is called a representation of $\mathcal{G}$ because it inherits the Lie bracket from the Lie algebra:

$$u([X,Y],\lambda) = [u(X,\lambda),u(Y,\lambda)].$$

Here, we develop an explicit relationship between $u(X,\lambda)$ and $U(\exp X,\lambda)$. These results follow from a well-established theorem stated below. This will lead in subsequent sections to expressions for the groups $SO(3)$ and $SE(3)$ that are useful in numerical computations.

Theorem 12.2 *([21, 41, 56]).* *Given a connected unimodular Lie group G, associated Lie algebra $\mathcal{G}$, and finite-dimensional $u(E_i,\lambda)$ as defined in (12.66), then*

$$U(\exp(tE_i),\lambda) = \exp\left[t\,u(E_i,\lambda)\right], \tag{12.76}$$

where $E_i \in \mathcal{G}$. Furthermore, if the matrix exponential parameterization

$$g(x_1,\ldots,x_n) = \exp\left(\sum_{i=1}^{n} x_i E_i\right) \tag{12.77}$$

is surjective, then when the $u(E_i,\lambda)$s are not simultaneously block-diagonalizable,

$$U(g,\lambda) = \exp\left(\sum_{i=1}^{n} x_i\,u(E_i,\lambda)\right) \tag{12.78}$$

is an irreducible representation for all $g \in G$.

Proof. For the exponential parameterization (12.77), one observes

$$g(tx_1,\ldots,tx_n)\circ g(\tau x_1,\ldots,\tau x_n) = g((t+\tau)x_1,\ldots,(t+\tau)x_n)$$

for all $t, \tau \in \mathbb{R}$; that is, the set of all $g(tx_1, \dots, tx_n)$ forms a one-dimensional (Abelian) subgroup of G for fixed values of x_i. From the definition of a representation it follows that

$$\begin{aligned} U(g((t+\tau)x_1, \dots, (t+\tau)x_n), \lambda) &= U(g(tx_1, \dots, tx_n), \lambda)\, U(g(\tau x_1, \dots, \tau x_n), \lambda) \\ &= U(g(\tau x_1, \dots, \tau x_n), \lambda)\, U(g(tx_1, \dots, tx_n), \lambda). \end{aligned}$$

Then differentiating the above expression with respect to τ, setting $\tau = 0$, and using the definition

$$\tilde{U}(x_1, \dots, x_n; \lambda) = U(g(x_1, \dots, x_n), \lambda)$$

gives

$$\frac{d}{dt}\tilde{U}(tx_1, \dots, tx_n; \lambda) = \left.\frac{d}{d\tau}\tilde{U}(\tau x_1, \dots, \tau x_n; \lambda)\right|_{\tau=0} \tilde{U}(tx_1, \dots, tx_n; \lambda).$$

However, since infinitesimal operations commute, it follows from (12.66) that

$$\left.\frac{d}{d\tau}\tilde{U}(\tau x_1, \dots, \tau x_n; \lambda)\right|_{\tau=0} = \sum_{i=1}^{n} x_i\, u(E_i, \lambda).$$

We therefore have the matrix differential equation

$$\frac{d}{dt}\tilde{U}(tx_1, \dots, tx_n; \lambda) = \left(\sum_{i=1}^{n} x_i\, u(E_i, \lambda)\right) \tilde{U}(tx_1, \dots, tx_n; \lambda)$$

subject to the initial conditions

$$\tilde{U}(0, \dots, 0; \lambda) = \mathbb{I}_{n_\lambda}.$$

The solution is therefore

$$\tilde{U}(tx_1, \dots, tx_n; \lambda) = \exp\left(t \sum_{i=1}^{n} x_i\, u(E_i, \lambda)\right).$$

Evaluating at $t = 1$, we find (12.78), and setting all $x_j = 0$ except x_i, we find (12.76). The irreducibility of these representations follows from the assumed properties of $u(E_i)$.

12.9 Irreducible Unitary Representations for $SO(3)$

The basis elements for the Lie algebra $so(3)$ are

$$E_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Exponentiating any linear combination of these basis elements yields an element of the rotation group, $SO(3)$. In particular, the ZYZ Euler-angle parameterization is expressed as

$$R_{ZYZ}(\alpha, \beta, \gamma) = \exp(\alpha E_3) \exp(\beta E_2) \exp(\gamma E_3).$$

Additionally, matrix elements of the IURs of $SO(3)$ in this parameterization are given as[13]

$$U_{mn}(R_{ZYZ}(\alpha,\beta,\gamma),l) = e^{-im\alpha} d^l_{mn}(\cos\beta) e^{-in\gamma}. \tag{12.79}$$

The functions $d^l_{mn}(\cos\beta)$ can be calculated by the integral[14]

$$d^l_{mn}(\cos\beta) = \frac{i^{m-n}}{2\pi}\left[\frac{(l-m)!(l+m)!}{(l-n)!(l+n)!}\right]^{\frac{1}{2}} \int_0^{2\pi} \left(\cos\frac{\beta}{2}e^{i\phi/2} + i\sin\frac{\beta}{2}e^{-i\phi/2}\right)^{l-n}$$
$$\times \left(\cos\frac{\beta}{2}e^{-i\phi/2} + i\sin\frac{\beta}{2}e^{i\phi/2}\right)^{l+n} e^{im\phi}d\phi. \tag{12.80}$$

Expanding the terms in the integrand in (12.80) using the binomial theorem for $\beta = \epsilon \ll 1$ and retaining first-order terms after integration,

$$U_{mn}(R_2(\epsilon),l) = \delta_{mn} + \frac{1}{2}c^l_{-n}\epsilon\delta_{m+1,n} - \frac{1}{2}c^l_n\epsilon\delta_{m-1,n} + O(\epsilon^2), \tag{12.81}$$

where $R_i(\theta) = \exp(\theta E_i)$ as defined in (A.42)–(A.44) in Volume 1 and

$$c^l_n \doteq \sqrt{(l-n)(l+n+1)} \quad \text{for} \quad |n| \leq l \tag{12.82}$$

and zero otherwise.

Then using the general fact that $R_{ZYZ}(\alpha,\beta,\gamma) = R_3(\alpha+\pi/2)R_1(\beta)R_3(\gamma-\pi/2)$ means that in the specific case when $(\alpha,\beta,\gamma) = (0,\epsilon,0)$,

$$i^{n-m}U_{mn}(R_1(\epsilon),l) = U_{mn}(R_2(\epsilon),l) \quad \text{or} \quad U_{mn}(R_1(\epsilon),l) = i^{m-n}U_{mn}(R_2(\epsilon),l).$$

Then from (12.81) it follows that

$$U_{mn}(R_1(\epsilon),l) = \delta_{mn} - \frac{i}{2}c^l_{-n}\epsilon\delta_{m+1,n} - \frac{i}{2}c^l_n\epsilon\delta_{m-1,n} + O(\epsilon^2).$$

It is easy to see that $U_{mn}(R_3(\epsilon),l) = e^{-in\epsilon}\delta_{mn}$. Differentiating each $U_{mn}(R_i(\epsilon),l)$ with respect to ϵ and setting $\epsilon = 0$ yields

$$\begin{aligned} u_{mn}(E_1,l) &= -\frac{i}{2}c^l_{-n}\delta_{m+1,n} - \frac{i}{2}c^l_n\delta_{m-1,n}, \\ u_{mn}(E_2,l) &= +\frac{1}{2}c^l_{-n}\delta_{m+1,n} - \frac{1}{2}c^l_n\delta_{m-1,n}, \\ u_{mn}(E_3,l) &= -in\delta_{m,n}\,. \end{aligned}$$

The matrices $U(R,l)$ and $u(E_i,l)$ both play important roles in Quantum Mechanics [2, 66]. One reason for this is because of how they are related to the *spherical harmonics*,

[13] Here, $U_{mn}(R,l) = D^l_{mn}(R)$ (the Wigner D-functions) as given in [2, 55] and are related to $U^l_{mn}(R)$ given in Chapter 9 of [11] as $U_{mn}(R,l) = (-1)^{m-n}U^l_{mn}(R)$, where $l = 0,1,2,\ldots$ and $\dim(U(R,l)) = 2l+1$ as discussed in [21].

[14] Equally valid definitions for $d^l_{mn}(\cos\beta)$ result when multiplying this expression by arbitrary powers of i^{n-m}, which would result in similarity-transformed versions of the $U(R,l)$ and $u(E_i,l)$ given here.

$Y_l^m(\mathbf{u})$, where $\mathbf{u} \in S^2$. For detailed expositions of the definitions and properties of spherical harmonics and their relationship to IURs of $SO(3)$, see [27, 55].[15]

In short, one way to define spherical harmonics (normalized according to the Condon and Shortley convention [13]) relative to IURs of $SO(3)$ is

$$Y_l^m(\mathbf{u}(\phi,\theta)) \doteq \sqrt{\frac{2l+1}{4\pi}}\,\overline{U_{m0}(R_3(\phi)R_2(\theta),l)}, \tag{12.83}$$

where $\mathbf{u}(\phi,\theta) = [\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta]^T$. From this definition, it can be shown that these transform under rotation as

$$Y_l^n(R^T\mathbf{u}) = \sum_{m=-l}^{l} Y_l^m(\mathbf{u})\, U_{mn}(R,l). \tag{12.84}$$

12.10 Wigner 3*j* Symbols and Clebsch–Gordon Coefficients

The *Wigner 3j symbols* appear in Quantum Mechanics as angular momentum coupling coefficients [19, 37, 47, 66]. They are scalar coefficients denoted as [37] $\begin{pmatrix} j_1 & j_2 & j_3 \\ m_1 & m_2 & m_3 \end{pmatrix}$, which should not be confused with matrices or permutations. The 3j symbols are computed in $Mathematica^{\mathrm{TM}}$ (see http://mathworld.wolfram.com/Wigner3j-Symbol.html).

Clebsch–Gordan (C-G) coefficients can be defined relative to the 3j symbols with the formula [55]

$$C^{j,m}_{j_1,m_1;j_2,m_2} = (-1)^{m+j_1-j_2}\sqrt{2j+1}\begin{pmatrix} j_1 & j_2 & j \\ m_1 & m_2 & -m \end{pmatrix}. \tag{12.85}$$

They have been studied extensively [55–57]. In the literature, several alternative notations are used for the C-G coefficients including $\langle j_1, m_1; j_2, m_2 | j, m\rangle$ and $\langle j_1 j_2 m_1 m_2 | jm\rangle$, but the notation in (12.85) is used here and throughout this chapter.

In the literature, the function $P^l_{mn}(\cos\Theta) \doteq (-1)^{m-n} d^l_{mn}(\cos\Theta)$ is sometimes used where $d^l_{mn}(\cos\Theta)$ is defined in (12.80). The C-G coefficients appear in the expansion of products of any two functions from the set $\{P^l_{mn}(\cos\Theta) \mid l = 0,1,2\ldots; -l \leq n, m \leq l\}$ in terms of linear combinations of functions from the same set. The functions $P^l_{mn}(\cos\Theta)$ are closely related to the IURs of $SO(3)$, $D^l_{mn}(R)$. From the fact that $D^l_{mn}(R)$ are IURs the following relation can be derived [2, 57]:

$$D^{l_1}_{m_1,n_1}(R) D^{l_2}_{m_2,n_2}(R) = \sum_{l=|l_1-l_2|}^{l_1+l_2} C^{l,m_1+m_2}_{l_1,m_1;l_2,m_2} C^{l,n_1+n_2}_{l_1,n_1;l_2,n_2} D^l_{m_1+m_2,n_1+n_2}(R).$$

Arbitrary $C^{c,\gamma}_{a,\alpha;b;\beta}$ are nonzero only for arguments $a, \alpha, b, \beta, c, \gamma$ that satisfy the following conditions [55]:

1. a, b, c are non-negative integer or half-integer numbers;

[15] A word of caution: In the literature sometimes $Y_l^m(\mathbf{u})$ is written as $Y^l_m(\mathbf{u})$ or $Y_{lm}(\mathbf{u})$ or considered to be an explicit function of angles $Y_l^m(\theta,\phi)$ or $Y_l^m(\phi,\theta)$ rather than a function of unit vectors that are, in turn, parameterized by angles, $Y_l^m(\mathbf{u}(\phi,\theta))$. To make matters worse, there are multiple ways to define spherical harmonics that ensure that they are normalized in the sense that $\int_{S^2} |Y_l^m(\mathbf{u})|^2\, d\mathbf{u} = 1$.

2. α, β, γ are integer or half-integer (positive or negative) numbers;
3. $|\alpha| < a$, $|\beta| < b$, $|\gamma| < c$;
4. $a+\alpha, b+\beta, c+\gamma, a+b+c$ are integer non-negative numbers;
5. $|a-b| \leq c \leq a+b$ and $\alpha+\beta=\gamma$.

For some special values of the arguments, there are explicit forms of the C-G coefficients [55]. In the derivations in this chapter, only the following specific cases are used.

12.10.1 The Case $c = a + b$

The C-G coefficients for the case $c = a + b$ are

$$C_{a,\alpha;b,\beta}^{a+b,\alpha+\beta} = \left(\frac{(2a)!(2b)!(a+b+\alpha+\beta)!(a+b-\alpha-\beta)!}{(2a+2b)!(a+\alpha)!(a-\alpha)!(b+\beta)!(b-\beta)!} \right)^{1/2} . \tag{12.86}$$

Using the above formula,

$$\begin{aligned} C_{l-1,m-1;1,1}^{l,m} &= \left(\frac{(l+m)(l+m-1)}{2l(2l-1)} \right)^{1/2} , \\ C_{l-1,m;1,0}^{l,m} &= \left(\frac{l^2-m^2}{l(2l-1)} \right)^{1/2} , \\ C_{l-1,m+1;1,-1}^{l,m} &= \left(\frac{(l-m)(l-m-1)}{2l(2l-1)} \right)^{1/2} . \end{aligned}$$

12.10.2 The Case $c = a + b - 1$

The C-G coefficients for the case $c = a + b - 1$ are of the form

$$C_{a,\alpha;b,\beta}^{a+b-1,\alpha+\beta} = 2(b\alpha - a\beta) \times \\ \left(\frac{(2a+2b-1)(2a-1)!(2b-1)!(a+b+\alpha+\beta-1)!(a+b-\alpha-\beta-1)!}{(a+\alpha)!(a-\alpha)!(b+\beta)!(b-\beta)!(2a+2b)!} \right)^{1/2} . \tag{12.87}$$

Using the above formula,

$$\begin{aligned} C_{l,m-1;1,1}^{l,m} &= - \left(\frac{(l+m)(l-m+1)}{2l(l+1)} \right)^{1/2} , \\ C_{l,m;1,0}^{l,m} &= \frac{m}{\sqrt{l(l+1)}} , \\ C_{l,m+1;1,-1}^{l,m} &= \left(\frac{(l-m)(l+m+1)}{2l(2l+1)} \right)^{1/2} . \end{aligned}$$

12.10.3 The Case $c = a - b$ $(b \leq a)$

The C-G coefficients for the case $c = a - b$ are of the form

$$C_{a,\alpha;b,\beta}^{a-b,\alpha+\beta} = (-1)^{b+\beta} \left(\frac{(a+\alpha)!(a-\alpha)!(2b)!(2a-2b+1)!}{(2a+1)!(b+\beta)!(b-\beta)!(a-b+\alpha+\beta)!(a-b-\alpha-\beta)!} \right)^{1/2} . \tag{12.88}$$

Using the above formula,

$$\begin{aligned} C^{l,m}_{l+1,m-1;1,1} &= \left(\frac{(l-m+2)(l-m+1)}{(2l+3)(2l+2)}\right)^{1/2}, \\ C^{l,m}_{l+1,m;1,0} &= -\left(\frac{(l+1)^2-m^2}{(l+1)(2l+3)}\right)^{1/2}, \\ C^{l,m}_{l+1,m+1;1,-1} &= \left(\frac{(l+m+2)(l+m+1)}{(2l+3)(2l+2)}\right)^{1/2}. \end{aligned}$$

12.11 Irreducible Unitary Representations for $SE(2)$

Since $SE(2)$ is neither compact nor commutative, the representation matrices will be infinite dimensional. Therefore, it will be more convenient to show the irreducibility of the operator $U(g,p)$ rather than the corresponding matrix. To this end, we examine one parameter subgroups generated by exponentiating linearly independent basis elements of the Lie algebra $se(2)$. Using the basis

$$E_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

it follows that

$$\exp(tE_1) = \begin{pmatrix} 1 & 0 & t \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \exp(tE_2) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}, \quad \exp(tE_3) = \begin{pmatrix} \cos t & -\sin t & 0 \\ \sin t & \cos t & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The IURs for $SE(2)$ were derived many years ago in the physics literature. A detailed recount of the derivation can be found in [11]. The matrix elements of these IURs for $SE(2)$ can be stated in terms of the parameters (r,ϕ,θ) using trigonometric functions and Bessel functions $J_k(\cdot)$ as[16]

$$U_{mn}(g(r,\phi,\theta),p) = i^{n-m} e^{-i[n\theta+(m-n)\phi]} J_{n-m}(p\cdot r) \tag{12.89}$$

for $0 \leq \phi, \theta \leq 2\pi$, $0 \leq r, p \leq \infty$, and $m, n \in \mathbb{Z}$, where

$$g(r,\phi,\theta) = \begin{pmatrix} \cos\theta & -\sin\theta & r\cos\phi \\ \sin\theta & \cos\theta & r\sin\phi \\ 0 & 0 & 1 \end{pmatrix}.$$

The matrix elements of $U(\exp(tE_3),p)$ can be obtained from (12.89) by setting $\phi = 0$, $r = 0$, and $\theta = t$:

$$U_{mn}(\exp(tE_1),p) = U_{mn}(g(0,0,t),p) = e^{-imt}\delta_{m,n}.$$

The fact that

$$J_{m-n}(0) = \begin{cases} 1 & \text{for } m-n=0 \\ 0 & \text{for } m-n \neq 0 \end{cases}$$

[16] Here, $J_k(\cdot)$ is the classical kth-order Bessel function used in polar-coordinate expansions of functions on the plane and should not be confused with a Jacobian matrix or elements thereof.

means that Kronecker delta functions will appear in the expressions for $u(E_i, p)$.

Explicitly,

$$u_{mn}(E_3, p) = \frac{d}{dt} U_{mn}(\exp(tE_3), p)\Big|_{t=0} = -im\delta_{m,n}.$$

The matrix elements of $U(\exp(tE_1), p)$ can be obtained from (12.89) by setting $r = t$, $\phi = 0$, and $\theta = 0$:

$$U_{mn}(\exp(tE_1), p) = U_{mn}(g(t, 0, 0), p) = i^{n-m} J_{n-m}(pt).$$

It is known that

$$\frac{d}{dx} J_m(x) = \frac{1}{2}[J_{m-1}(x) - J_{m+1}(x)].$$

Hence,

$$u_{mn}(E_1, p) = \frac{d}{dt} U_{mn}(\exp(tE_1), p)\Big|_{t=0} = \frac{ip}{2}(\delta_{m,n+1} + \delta_{m,n-1}).$$

The matrix elements of $U(\exp(tE_2), p)$ can be obtained from (12.89) by setting $r = t$, $\phi = \pi/2$, and $\theta = 0$:

$$U_{mn}(\exp(tE_2), p) = U_{mn}(g(t, \pi/2, 0), p) = (-1)^{n-m} J_{n-m}(pt);$$

thus,

$$u_{mn}(E_2, p) = \frac{d}{dt} U_{mn}(\exp(tE_2), p)\Big|_{t=0} = \frac{p}{2}(\delta_{m,n+1} - \delta_{m,n-1}).$$

To summarize the results, we have

$$u_{mn}(E_1, p) = \frac{ip}{2}(\delta_{m,n+1} + \delta_{m,n-1}), \tag{12.90}$$

$$u_{mn}(E_2, p) = \frac{p}{2}(\delta_{m,n+1} - \delta_{m,n-1}), \tag{12.91}$$

$$u_{mn}(E_3, p) = -im\delta_{m,n}. \tag{12.92}$$

12.12 Explicit Results for $SE(3)$

For small translational (rotational) displacements from the identity along (about) the kth coordinate axis, the homogeneous transforms representing infinitesimal motions look like

$$\exp(\epsilon E_k) \approx \mathbb{I}_4 + \epsilon E_k,$$

where

$$E_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad E_3 = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$E_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad E_5 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad E_6 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

12.12.1 Induced Representations for $SE(3)$

Let the pair $(\mathbf{a}, A)$ denote a translation/position $\mathbf{a} \in \mathbb{R}^3$ and a rotation/orientation $A \in SO(3)$. Two such pairs, when viewed as elements of $SE(3)$, satisfy the group operation $(\mathbf{a}_1, A_1) \circ (\mathbf{a}_2, A_2) = (A_1\mathbf{a}_2 + \mathbf{a}_1, A_1A_2)$. Operators for the IURs of $SE(3)$ that act on functions on the sphere can be written in the form

$$(U(\mathbf{a}, A; p, s)\varphi)(\mathbf{u}) = e^{-ip\mathbf{u}\cdot\mathbf{a}}\, \Delta_s(R_{\mathbf{u}}^{-1}\, A\, R_{A^{-1}\mathbf{u}})\, \varphi(A^{-1}\mathbf{u}), \tag{12.93}$$

where $\mathbf{p} = p\mathbf{u}$ and $\mathbf{u}$ is a unit vector. Here, $\varphi(\cdot)$ is defined on the unit sphere and

$$\Delta_s : \quad \phi \to e^{is\phi},\ 0 \leq \phi \leq 2\pi,$$

for $s = 0, \pm 1, \pm 2, \ldots$.

The irreducible representations of the motion group can be built on spaces $\varphi(\mathbf{p}) \in \mathcal{L}^2(S_p)$, with the inner product defined as

$$(\varphi_1, \varphi_2) = \int_{\Theta=0}^{\pi} \int_{\Phi=0}^{2\pi} \overline{\varphi_1(\mathbf{p})}\, \varphi_2(\mathbf{p}) \sin\Theta\, d\Theta\, d\Phi\ , \tag{12.94}$$

where $\mathbf{p} = (p \sin\Theta \cos\Phi,\ p \sin\Theta \sin\Phi,\ p\cos\Theta)$ and $p > 0$, $0 \leq \Theta \leq \pi$, and $0 \leq \Phi \leq 2\pi$.

12.12.2 Matrix Elements of IURs

To obtain the matrix elements of the unitary representations, we use the group property[17]

$$U(\mathbf{a}, A; p, s) = U(\mathbf{a}, \mathbb{I}; p, s)\ \cdot\ U(\mathbf{0}, A; p, s) \tag{12.95}$$

The basis functions used for computing matrix elements of the IURs may be expressed in the form [38, 39]

$$h^l_{m\,s}(\mathbf{u}(\Theta, \Phi)) = Q^l_{s,m}(\cos\,\Theta)\, e^{i(m+s)\Phi}, \tag{12.96}$$

where

$$Q^l_{-s,m}(\cos\,\Theta) = (-1)^{l-s} \sqrt{\frac{2l+1}{4\pi}}\, P^l_{s\,m}(\cos\,\Theta), \tag{12.97}$$

and generalized Legendre polynomials $P^l_{m\,s}(\cos\,\Theta)$ are given as in Vilenkin [56].

Then

$$U_{l',m';l,m}(\mathbf{a}, A; p, s) = (h^{l'}_{m'\,s}, U(g; p, s)h^l_{m\,s}).$$

This can be written as

$$U_{l',m';l,m}(\mathbf{a}, A; p, s) = \sum_{j=-l}^{l} [l', m' \mid p, s \mid l, j](\mathbf{a})\, U_{j\,m}(A, l) \tag{12.98}$$

by using (12.95), where $U_{j\,m}(A, l)$ are the matrix elements of IURs for $SO(3)$ given in (12.79). The translational part of the matrix elements $U_{l',m';l,m}(\mathbf{a}, A; p, s)$ can be written in closed form as [38, 39][18]

[17] The presentation in this section follows that in [11], which, in turn, followed [38, 39].

[18] Here, $j_k(\cdot)$ is the classical kth order spherical Bessel function.

$$[l', m' \mid p, s \mid l, m](\mathbf{a}) \\ = (4\pi)^{1/2} \sum_{k=|\,l'-l\,|}^{l'+l} i^k \sqrt{\frac{(2l'+1)(2k+1)}{(2l+1)}}\, j_k(p\,a)\, C^{l,s}_{k,0;l',s} \\ \cdot C^{l,m}_{k,m-m';l',m'}\, Y_k^{m-m'}(\mathbf{u}(\phi,\theta)), \tag{12.99}$$

where θ and ϕ are polar and azimuthal angles of the translation vector $\mathbf{a} = a\cdot\mathbf{u}(\phi,\theta)$, respectively, and $C^{l,m}_{l'',m'';l',m'}$ are Clebsch–Gordan coefficients (see Section 12.10 and [27]).

The matrix elements of the transform are given in terms of matrix elements (12.98) as

$$\hat{f}_{l',m';l,m}(p,s) = \int_{SE(3)} f(\mathbf{a}, A)\, \overline{U_{l,m;l',m'}(\mathbf{a}, A; p, s)}\, dA\, d\mathbf{a}, \tag{12.100}$$

where we have used the unitarity property.

The inverse Fourier transform is defined by

$$f(g) = \mathcal{F}^{-1}(\hat{f}) = \frac{1}{2\pi^2} \sum_{s=-\infty}^{\infty} \int_0^\infty \operatorname{trace}(\hat{f}(p,s)U(g;p,s))\, p^2\, dp\ . \tag{12.101}$$

Explicitly,

$$f(\mathbf{a}, A) = \frac{1}{2\pi^2} \sum_{s=-\infty}^{\infty} \sum_{l'=|s|}^{\infty} \sum_{l=|s|}^{\infty} \sum_{m'=-l'}^{l'} \sum_{m=-l}^{l} \int_0^\infty p^2\, dp\, \hat{f}_{l,m;l',m'}(p,s) U_{l',m';l,m}(\mathbf{a}, A; p, s). \tag{12.102}$$

Representations (12.93), which can be viewed as infinite-dimensional matrices denoted as $U(g; p, s)$ with elements (12.98), satisfy the homomorphism properties

$$U(g_1 \circ g_2; p, s) = U(g_1; p, s) \cdot U(g_2; p, s)\,,$$

where $\circ$ is the group operation.

The general formulation of operational properties for Lie group Fourier transforms described in Section 12.7.1 are illustrated here concretely. In particular, when $G = SE(3)$,

$$u(E_k; p, s) \doteq \frac{d}{dt} \left(U(\exp(tE_k); p, s)\right)\bigg|_{t=0}. \tag{12.103}$$

Explicit expressions for $u(E_k; p, s)$ are computed below following the steps described in [61].

12.12.3 Explicit Expressions for $u(E_k; p, s)$

Here, we derive in detail the elements of the matrix $u(E_k; p, s)$. The discussion is divided into the cases $k = 1, 2, 3$ (corresponding to the Lie algebra basis elements for infinitesimal rotation) and $k = 4, 5, 6$ (corresponding to infinitesimal translations).

Computing Matrix Elements for Pure Rotation

For the case $k = 1, 2, 3$, the translational vector $\mathbf{a} = \mathbf{0}$. Its IURs are $U^s(A, \mathbf{0}; p, s)$. From (12.98), the matrix elements of $U^s(A, \mathbf{0}; p, s)$ are written as

$$U_{l',m';l,m}(A, \mathbf{0}; p, s) = \sum_{n=-l}^{l} [l', m' \mid p, s \mid l, n](\mathbf{0})\, U_{n\,m}(A, l).$$

Explicitly, we have

$$\begin{aligned}
&[l', m' \mid p\ , s \mid l, m](\mathbf{0}) \\
&\quad = \int_0^{2\pi} e^{-i(m'-m)\Phi} d\Phi \int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta) Q^{l}_{s,m}(\cos\Theta) \sin\Theta \, d\Theta \\
&\quad = 2\pi\delta_{m,m'} \int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta) Q^{l}_{s,m}(\cos\Theta) \sin\Theta \, d\Theta \\
&\quad = 2\pi\delta_{m,m'} \int_0^{\pi} Q^{l'}_{s,m}(\cos\Theta) Q^{l}_{s,m}(\cos\Theta) \sin\Theta \, d\Theta \\
&\quad = \delta_{m,m'} (-1)^{l'+l} \frac{\sqrt{2l'+1}\sqrt{2l+1}}{2} \int_0^{\pi} P^{l'}_{-s,m}(\cos\Theta) P^{l}_{-s,m}(\cos\Theta) \sin\Theta \, d\Theta \\
&\quad = \delta_{m,m'} \delta_{l,l'}
\end{aligned}$$

where the orthogonality property

$$\int_0^{\pi} P^{l}_{m,n}(\cos\Theta) P^{k}_{m,n}(\cos\Theta) \sin\Theta \, d\Theta = \frac{2}{2l+1}\delta_{l,k} \tag{12.104}$$

is used. With the above results, we can rewrite

$$U_{l',m';l,m}(A, \mathbf{0}; p, s) = U_{l',m';l,m}(\exp(X), \mathbf{0}; p, s) = \delta_{l,l'} U_{m',m}(\exp(X), l),$$

where the relationship between $\hat{E}_k$ and E_k is that in (10.92). Hence, we obtain

$$\begin{aligned}
u_{l',m';l,m}(E_k; p, s) &= \frac{d}{dt} U_{l',m';l,m}(\exp(t\hat{E}_k), \mathbf{0}; p, s)\Big|_{t=0} \\
&= \delta_{l,l'} \frac{d}{dt} U_{m',m}(\exp(t\hat{E}_k), l)\Big|_{t=0} \\
&= \delta_{l,l'} \, u_{m',m}(\hat{E}_k, l),
\end{aligned}$$

where IURs of $SO(3)$ evaluated at $\exp(t\hat{E}_k)$ are given in Section 12.9.

Computing Matrix Elements for Pure Translation

For the case $k = 4, 5, 6$, the rotation part is the identity matrix $\mathbb{I}$. Its IURs are $U(\mathbb{I}, \mathbf{a}; p, s)$. The matrix elements of $U(\mathbb{I}, \mathbf{a}; p, s)$ are just the translation matrix elements given in (12.99); that is,

$$U_{l',m';l,m}(\mathbb{I}, \mathbf{a}; p, s) = [l', m' \mid p, s \mid l, m](\mathbf{a}).$$

From this, we have

$$\begin{aligned}
&u_{l',m';l,m}(E_4; p, s) \\
&\quad = \frac{d}{dt} U^{s}_{l',m';l,m}(\mathbb{I}, t\mathbf{e}_1; p)\Big|_{t=0} \\
&\quad = \frac{d}{dt} [l', m' \mid p, s \mid l, m](t\mathbf{e}_1)\Big|_{t=0} \\
&\quad = \frac{d}{dt} \int_0^{2\pi} \int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta) e^{-i(m'-m)\Phi} \, e^{-itp\sin\Theta\cos\Phi} \, Q^{l}_{s,m}(\cos\Theta) \sin\Theta \, d\Theta \, d\Phi\Big|_{t=0}
\end{aligned}$$

$$
\begin{aligned}
&= -ip \int_0^{2\pi} e^{-i(m'-m)\Phi} \cos\Phi \, d\Phi \int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta) Q^{l}_{s,m}(\cos\Theta) \sin^2\Theta \, d\Theta \\
&= -ip\pi(\delta_{m',m+1} + \delta_{m',m-1}) \int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta) Q^{l}_{s,m}(\cos\Theta) \sin^2\Theta \, d\Theta \\
&= -\frac{ip}{4}(-1)^{l'+l}\sqrt{2l'+1}\sqrt{2l+1}\delta_{m',m+1} \int_0^{\pi} P^{l'}_{-s,m+1}(\cos\Theta) P^{l}_{-s,m}(\cos\Theta) \sin^2\Theta \, d\Theta \\
&\quad - \frac{ip}{4}(-1)^{l'+l}\sqrt{2l'+1}\sqrt{2l+1}\delta_{m',m-1} \int_0^{\pi} P^{l'}_{-s,m-1}(\cos\Theta) P^{l}_{-s,m}(\cos\Theta) \sin^2\Theta \, d\Theta .
\end{aligned}
$$

One tricky part to solve the above integrals is to use the relationship [21]

$$\sin\Theta = \sqrt{2} P^1_{0,-1}(\cos\Theta)$$

to replace one $\sin\Theta$ in the first integral and

$$\sin\Theta = -\sqrt{2} P^1_{0,1}(\cos\Theta)$$

to replace one $\sin\Theta$ in the second integral. Then apply the property [39, 58]

$$P^{b_1}_{m_1,k_1}(\cos\Theta) P^{b_2}_{m_2,k_2}(\cos\Theta) = \sum_{b=|b_1-b_2|}^{b_1+b_2} C^{b,m_1+m_2}_{b_1,m_1;b_2,m_2} C^{b,k_1+k_2}_{b_1,k_1;b_2,k_2} P^{b}_{m_1+m_2,k_1+k_2}(\cos\Theta) \tag{12.105}$$

to combine the product of the functions $P^{l'}_{-s,m+1}(\cos\Theta)$ and $P^1_{0,-1}(\cos\Theta)$ into the function $P^b_{-s,m}(\cos\Theta)$ and the product of the functions $P^{l'}_{-s,m-1}(\cos\Theta)$ and $P^1_{0,1}(\cos\Theta)$ into the function $P^b_{-s,m}(\cos\Theta)$. Here, $C^{b,m}_{b_1,m_1;b_2,m_2}$ is a Clebsch–Gordon coefficient [55] (See Section 12.10 for an explanation.) Now, we can solve the integrals as

$$
\begin{aligned}
&\int_0^{\pi} P^{l'}_{-s,m+1}(\cos\Theta) P^{l}_{-s,m}(\cos\Theta) \sin^2\Theta \, d\Theta \\
&\quad = \sqrt{2} \int_0^{\pi} P^{l'}_{-s,m+1}(\cos\Theta) P^1_{0,-1}(\cos\Theta) P^{l}_{-s,m}(\cos\Theta) \sin\Theta \, d\Theta \\
&\quad = \int_0^{\pi} \left(\sum_{b=|l'-1|}^{l'+1} C^{b,-s}_{l',-s;1,0} C^{b,m}_{l',m+1;1,-1} P^{b}_{-s,m}(\cos\Theta) \right) P^{l}_{-s,m}(\cos\Theta) \sin\Theta \, d\Theta
\end{aligned}
$$

and

$$
\begin{aligned}
&\int_0^{\pi} P^{l'}_{-s,m-1}(\cos\Theta) P^{l}_{-s,m}(\cos\Theta) \sin^2\Theta \, d\Theta \\
&\quad = -\sqrt{2} \int_0^{\pi} P^{l'}_{-s,m-1}(\cos\Theta) P^1_{0,1}(\cos\Theta) P^{l}_{-s,m}(\cos\Theta) \sin\Theta \, d\Theta \\
&\quad = \int_0^{\pi} \left(\sum_{b=|l'-1|}^{l'+1} C^{b,-s}_{l',-s;1,0} C^{b,m}_{l',m-1;1,1} P^{b}_{-s,m}(\cos\Theta) \right) P^{l}_{-s,m}(\cos\Theta) \sin\Theta \, d\Theta .
\end{aligned}
$$

These Clebsch–Gordon coefficients in the above equations can be calculated explicitly using the formulaes for special values of the arguments given by [55]. Finally, by employing the orthogonality property (12.104) to simplify the above equations, we obtain the explicit expression

$$\begin{aligned}
&u_{l',m';l,m}(E_4;p,s)\\
&= -\frac{ip}{2}\gamma^s_{l',-m'}\delta_{m',m+1}\delta_{l'-1,l} + \frac{ip}{2}\lambda^s_{l,m}\delta_{m',m+1}\delta_{l',l} + \frac{ip}{2}\gamma^s_{l,m}\delta_{m',m+1}\delta_{l'+1,l}\\
&\quad + \frac{ip}{2}\gamma^s_{l',m'}\delta_{m',m-1}\delta_{l'-1,l} + \frac{ip}{2}\lambda^s_{l,-m}\delta_{m',m-1}\delta_{l',l} - \frac{ip}{2}\gamma^s_{l,-m}\delta_{m',m-1}\delta_{l'+1,l}, \qquad (12.106)
\end{aligned}$$

where

$$\gamma^s_{l,m} = \left(\frac{(l^2-s^2)(l-m)(l-m-1)}{l^2(2l-1)(2l+1)}\right)^{1/2}$$

and

$$\lambda^s_{l,m} = \frac{s\sqrt{(l-m)(l+m+1)}}{l(l+1)}.$$

Now, let us calculate $u_{l',m';l,m}(E_5;p,s)$.

$$\begin{aligned}
&u_{l',m';l,m}(E_5;p,s)\\
&= \frac{d}{dt}U_{l',m';l,m}(\mathbb{I},t\mathbf{e}_2;p,s)\Big|_{t=0}\\
&= \frac{d}{dt}[l',m' \mid p,s \mid l,m](t\mathbf{e}_2)\Big|_{t=0}\\
&= \frac{d}{dt}\int_0^{2\pi}\int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta)e^{-i(m'-m)\Phi}\, e^{-itp\sin\Theta\sin\Phi}\, Q^l_{s,m}(\cos\Theta)\sin\Theta\, d\Theta\, d\Phi\Big|_{t=0}\\
&= -ip\int_0^{2\pi} e^{-i(m'-m)\Phi}\sin\Phi\, d\Phi\int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta)Q^l_{s,m}(\cos\Theta)\sin^2\Theta\, d\Theta\\
&= -p\pi(\delta_{m',m+1}-\delta_{m',m-1})\int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta)Q^l_{s,m}(\cos\Theta)\sin^2\Theta\, d\Theta\\
&= -\frac{p}{4}(-1)^{l'+l}\sqrt{2l'+1}\sqrt{2l+1}\delta_{m',m+1}\int_0^{\pi} P^{l'}_{-s,m+1}(\cos\Theta)P^l_{-s,m}(\cos\Theta)\sin^2\Theta\, d\Theta\\
&\quad + \frac{p}{4}(-1)^{l'+l}\sqrt{2l'+1}\sqrt{2l+1}\delta_{m',m-1}\int_0^{\pi} P^{l'}_{-s,m-1}(\cos\Theta)P^l_{-s,m}(\cos\Theta)\sin^2\Theta\, d\Theta.
\end{aligned}$$

Employing the same techniques used for $u_{l',m';l,m}(E_4;p,s)$ to solve the integrals in the above equation, we can obtain the explicit expression

$$\begin{aligned}
&u_{l',m';l,m}(E_5;p,s)\\
&= -\frac{p}{2}\gamma^s_{l',-m'}\delta_{m',m+1}\delta_{l'-1,l} + \frac{p}{2}\lambda^s_{l,m}\delta_{m',m+1}\delta_{l',l} + \frac{p}{2}\gamma^s_{l,m}\delta_{m',m+1}\delta_{l'+1,l}\\
&\quad - \frac{p}{2}\gamma^s_{l',m'}\delta_{m',m-1}\delta_{l'-1,l} - \frac{p}{2}\lambda^s_{l,-m}\delta_{m',m-1}\delta_{l',l} + \frac{p}{2}\gamma^s_{l,-m}\delta_{m',m-1}\delta_{l'+1,l}. \qquad (12.107)
\end{aligned}$$

Again, for the case $k=6$, we have

$$\begin{aligned}
&u_{l',m';l,m}(E_6;p,s)\\
&= \frac{d}{dt}U_{l',m';l,m}(\mathbb{I},t\mathbf{e}_3;p,s)\Big|_{t=0}\\
&= \frac{d}{dt}[l',m' \mid p,s \mid l,m](t\mathbf{e}_3)\Big|_{t=0}
\end{aligned}$$

$$= \frac{d}{dt}\int_0^{2\pi}\int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta)e^{-i(m'-m)\Phi}\, e^{-itp\cos\Theta}\, Q^{l}_{s,m}(\cos\Theta)\sin\Theta\, d\Theta\, d\Phi\Big|_{t=0}$$

$$= -ip\int_0^{2\pi} e^{-i(m'-m)\Phi} d\Phi \int_0^{\pi} Q^{l'}_{s,m'}(\cos\Theta)Q^{l}_{s,m}(\cos\Theta)\cos\Theta\sin\Theta\, d\Theta$$

$$= -ip2\pi\delta_{m',m}\int_0^{\pi} Q^{l'}_{s,m}(\cos\Theta)Q^{l}_{s,m}(\cos\Theta)\cos\Theta\sin\Theta\, d\Theta$$

$$= -\frac{ip}{2}(-1)^{l'+l}\sqrt{2l'+1}\sqrt{2l+1}\delta_{m',m}\int_0^{\pi} P^{l'}_{-s,m}(\cos\Theta)P^{l}_{-s,m}(\cos\Theta)\cos\Theta\sin\Theta\, d\Theta.$$

For the integral in the above equation, we use the relationship [21]

$$\cos\Theta = P^{1}_{0,0}(\cos\Theta)$$

to take the place of the $\cos\Theta$. Then we apply property (12.105):

$$\int_0^{\pi} P^{l'}_{-s,m}(\cos\Theta)P^{l}_{-s,m}(\cos\Theta)\cos\Theta\sin\Theta\, d\Theta$$

$$= \int_0^{\pi} P^{l'}_{-s,m}(\cos\Theta)P^{1}_{0,0}(\cos\Theta)P^{l}_{-s,m}(\cos\Theta)\sin\Theta\, d\Theta$$

$$= \int_0^{\pi}\left(\sum_{b=|l'-1|}^{l'+1} C^{b,-s}_{l',-s;1,0}C^{b,m}_{l',m;1,0}P^{b}_{-s,m}(\cos\Theta)\right)P^{l}_{-s,m}(\cos\Theta)\sin\Theta\, d\Theta$$

Calculating these Clebsch–Gordon coefficients explicitly and simplifying them using the orthogonality property (12.104), we obtain the explicit expression

$$u_{l',m';l,m}(E_6;p,s) = ip\kappa^{s}_{l',m'}\delta_{m',m}\delta_{l'-1,l} + ip\frac{sm}{l(l+1)}\delta_{m',m}\delta_{l',l} + ip\kappa^{s}_{l,m}\delta_{m',m}\delta_{l'+1,l}, \tag{12.108}$$

where

$$\kappa^{s}_{l,m} = \left(\frac{(l^2-m^2)(l^2-s^2)}{l^2(2l-1)(2l+1)}\right)^{1/2}.$$

Summary of All Matrix Elements

From the above computations, the matrix elements of the Lie algebra representations $u(E_k;p,s)$ for $se(3)$ can be explicitly written as

$$u_{l',m';l,m}(E_1;p,s) = -\frac{i}{2}c^{l}_{-m}\delta_{l,l'}\delta_{m'+1,m} - \frac{i}{2}c^{l}_{m}\delta_{l,l'}\delta_{m'-1,m}, \tag{12.109}$$

$$u_{l',m';l,m}(E_2;p,s) = +\frac{1}{2}c^{l}_{-m}\delta_{l,l'}\delta_{m'+1,m} - \frac{1}{2}c^{l}_{m}\delta_{l,l'}\delta_{m'-1,m}, \tag{12.110}$$

$$u_{l',m';l,m}(E_3;p,s) = -im\delta_{l,l'}\delta_{m',m}, \tag{12.111}$$

$$\begin{aligned} &u_{l',m';l,m}(E_4;p,s)\\ &= -\frac{ip}{2}\gamma^{s}_{l',-m'}\delta_{m',m+1}\delta_{l'-1,l} + \frac{ip}{2}\lambda^{s}_{l,m}\delta_{m',m+1}\delta_{l',l} + \frac{ip}{2}\gamma^{s}_{l,m}\delta_{m',m+1}\delta_{l'+1,l}\\ &\quad + \frac{ip}{2}\gamma^{s}_{l',m'}\delta_{m',m-1}\delta_{l'-1,l} + \frac{ip}{2}\lambda^{s}_{l,-m}\delta_{m',m-1}\delta_{l',l} - \frac{ip}{2}\gamma^{s}_{l,-m}\delta_{m',m-1}\delta_{l'+1,l}, \end{aligned} \tag{12.112}$$

$$
\begin{aligned}
&u_{l',m';l,m}(E_5;p,s)\\
&\quad= -\frac{p}{2}\gamma^s_{l',-m'}\delta_{m',m+1}\delta_{l'-1,l} + \frac{p}{2}\lambda^s_{l,m}\delta_{m',m+1}\delta_{l',l} + \frac{p}{2}\gamma^s_{l,m}\delta_{m',m+1}\delta_{l'+1,l}\\
&\qquad - \frac{p}{2}\gamma^s_{l',m'}\delta_{m',m-1}\delta_{l'-1,l} - \frac{p}{2}\lambda^s_{l,-m}\delta_{m',m-1}\delta_{l',l} + \frac{p}{2}\gamma^s_{l,-m}\delta_{m',m-1}\delta_{l'+1,l},
\end{aligned}
\tag{12.113}
$$

$$
u_{l',m';l,m}(E_6;p,s) = ip\kappa^s_{l',m'}\delta_{m',m}\delta_{l'-1,l} + ip\frac{sm}{l(l+1)}\delta_{m',m}\delta_{l',l} + ip\kappa^s_{l,m}\delta_{m',m}\delta_{l'+1,l},
\tag{12.114}
$$

where

$$
\gamma^s_{l,m} = \left(\frac{(l^2-s^2)(l-m)(l-m-1)}{l^2(2l-1)(2l+1)}\right)^{1/2},
$$

$$
\lambda^s_{l,m} = \frac{s\sqrt{(l-m)(l+m+1)}}{l(l+1)},
$$

and

$$
\kappa^s_{l,m} = \left(\frac{(l^2-m^2)(l^2-s^2)}{l^2(2l-1)(2l+1)}\right)^{1/2},
$$

and c^l_n is defined as in (12.82).

12.13 Chapter Summary

The abstract-sounding concept of integration on Lie groups can be made very concrete by introducing coordinates and using the properties of Jacobian matrices. Lie groups and their homogenous spaces are examples of orientable manifolds that have an additional structure that makes them easier to use than arbitrary abstract manifolds. It was demonstrated how topological properties of Lie groups can be computed. Other classical approaches to the topology of Lie groups can be found in [3–5, 10, 48].

The class of unimodular Lie groups (which includes, but is not limited to, compact Lie groups) is defined by the existence of bi-invariant integrals. The properties of integrals on such groups (and homogeneous spaces of a unimodular group with respect to a unimodular subgroup) are convenient to work with. Concepts such as integration by parts, convolution, and Fubini's theorem (which allows for exchanging the order of nested integrals) all follow in a natural way. Integrals over Lie groups can be nested as integrals over subgroups and homogeneous spaces, or in some cases if a good set of coordinates are chosen, the integrals can be separated into multiple integrals over low-dimensional parametric domains. As with functions on the circle and real line, a concept of Fourier analysis exists for unimodular Lie groups. In this theory, irreducible unitary representation matrices (IURs) $U(g,\lambda)$ take the place of $e^{i\omega x}$, with g replacing x and λ replacing ω. For compact Lie groups, the IURs are all finite dimensional and are enumerated by a discrete parameter. In contrast, for noncompact Lie groups, the IURs have a continuous index set, and, in addition, if the group operations are noncommutative, then the IURs become infinite-dimensional matrices. The IURs for the groups $SO(3)$, $SE(2)$, and $SE(3)$ are provided in this chapter to serve as concrete examples of the general abstract theory. These groups are also quite important in biological and engineering applications.

The discussion of the matrix Lie groups in Chapters 10–12 has been analogous to that of parametric surfaces and embedded manifolds in Chapters 5 and 7. The resulting expressions have been concrete and expressible in terms of coordinates. It is worth mentioning that the extrinsic approach to surfaces discussed in Chapter 5, in which a surface is defined by its constraints, can be applied also to matrix Lie groups. Since all such groups studied here are subgroups of $GL(N,\mathbb{R})$ for sufficiently large N, it is possible to reformulate everything extrinsically. For example, the integral over a Lie group $G < GL(N,\mathbb{R})$ can be written as

$$\int_G f(g)\,dg = \int_{GL(N,\mathbb{R})} f(A)\,\delta(g,A)\,dA,$$

where dA is the Haar measure for $GL(N,\mathbb{R})$ and $\delta(g,A)$ is a function that encodes the conditions defining the elements of the subgroup G. Then, in analogy with the way that the Stokes and divergence theorems in $\mathbb{R}^3$ were written extrinsically in Chapter 5, so too can integrals of interest on Lie groups. This sort of formulation is rare in the literature and will not be pursued here. The reason for mentioning it is that in some application contexts, stochastic differential equations on Lie groups are defined extrinsically, as was illustrated in Chapter 8 and will be revisited in Chapter 20.

12.14 Exercises

12.1. If $f_i(g)$ for $i = 1,2$ are symmetric functions (i.e., $f_i(g) = f_i(g^{-1})$), then is $(f_1 * f_2)(g)$ symmetric?

12.2. If $f_1(g) = f_2(g^{-1})$, will $(f_1 * f_2)(g)$ be symmetric?

12.3. Show that a class function (i.e., a function with the property $\chi(g \circ h) = \chi(h \circ g)$ for all $g,h \in G$) commutes with every function under convolution.

12.4. Let

$$f(x,y,\theta) = e^{-(x^2+y^2)/2} xy \cos\theta$$

and compute the convolution product $(f * f)(x,y,\theta)$ under the following conditions: (a) viewing f as a function on the direct product $\mathbb{R}^2 \times SO(2)$ and (b) viewing f as a function on $SE(2)$.

12.5. Let

$$f(\alpha,\beta,\gamma) = e^{-(\alpha^2+\beta^2+\gamma^2)/2}$$

be a function on the Heisenberg group, $H(3)$. (a) Calculate the integral of this function. (b) Calculate the convolution of this function with itself. (c) Convert to the exponential coordinates x_1, x_2, and x_3 and repeat (a) and (b) in these coordinates.

12.6. Prove the operational property in (12.75).

12.7. Write a computer program to exponentiate the Lie algebra representation matrices for $SO(3)$ and show that the resulting matrices satisfy the homomorphism property.

12.8. Let $A \in GL^+(2,\mathbb{R})$ and $dA = |A|^{-2}\,da_{11}\,da_{12}\,da_{21}\,da_{22}$ be its Haar measure. The QR decomposition of A is $A = QR$ of the form

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} r_{11} & r_{12} \\ 0 & r_{22} \end{pmatrix}.$$

Show that the set of all matrices R with $r_{11} \cdot r_{22} > 0$ forms a group (which will be referred to here as T^+) and compute its left and right Haar measures. Is the group T^+ unimodular? Using the fact that

$$\begin{pmatrix} a_{11} \\ a_{21} \\ a_{12} \\ a_{22} \end{pmatrix} = \begin{pmatrix} r_{11}\cos\theta \\ r_{11}\sin\theta \\ r_{12}\cos\theta - r_{22}\sin\theta \\ r_{12}\sin\theta + r_{22}\cos\theta \end{pmatrix}.$$

Show that

$$da_{11}\, da_{12}\, da_{21}\, da_{22} = |r_{11}|\, dr_{11}\, dr_{12}\, dr_{22}\, d\theta.$$

Show that the Haar measure for $GL^+(2,\mathbb{R})$ can be decomposed into one over $SO(2)$ and over the coset space $SO(2)\backslash GL^+(2,\mathbb{R}) \cong T^+$. How does the measure for $SO(2)\backslash GL^+(2,\mathbb{R})$ compare to the left- and right-invariant integration measures for T^+?

12.9. Let A and dA be as in the previous problem. The polar decomposition $A = PQ$, where $P = P^T > 0$ and Q is orthogonal, can be written in this case as

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} p_{11} & p_{12} \\ p_{12} & p_{22} \end{pmatrix} \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Viewing this as a parameterization of $GL^+(2,\mathbb{R}) \subset \mathbb{R}^{2\times 2}$, compute the Jacobian determinant and find the weighting functions $w_1(P)$ and $w_2(P)$ such that $da_{11}\, da_{12}\, da_{21}\, da_{22} = w_1(P)\, dp_{11}\, dp_{12}\, dp_{22}\, d\theta$ and $dA = w_2(P)\, dp_{11}\, dp_{12}\, dp_{22}\, d\theta$. Viewing the space of all symmetric positive definite 2×2 matrices as $GL^+(2,\mathbb{R})/SO(2)$, decompose the integral over $GL^+(2,\mathbb{R})$ into one over this homogeneous space and the subgroup $SO(2)$. Do the analogous computations with the decomposition $A = QP'$.

12.10. The singular-value decomposition $A = U\Sigma V^*$ for for the special case when $A \in GL^+(2,\mathbb{R})$ can be written as

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \sigma_1 & 0 \\ 0 & \sigma_2 \end{pmatrix} \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix}.$$

Find $w_1(\sigma_1,\sigma_2)$ and $w_2(\sigma_1,\sigma_2)$ such that $da_{11}\, da_{12}\, da_{21}\, da_{22} = w_1(\sigma_1,\sigma_2)\, d\sigma_1\, d\sigma_2\, d\alpha\, d\beta$ and $dA = w_2(\sigma_1,\sigma_2)\, d\sigma_1\, d\sigma_2\, d\alpha\, d\beta$, where dA is the Haar measure for $GL^+(2,\mathbb{R})$. Write the invariant integral over $GL^+(2,\mathbb{R})$ in terms of the subgroup $SO(2)$ and the double coset $SO(2)\backslash GL^+(2,\mathbb{R})/SO(2)$.

12.11. When using exponential coordinates to express the integral over $SO(3)$ in (12.9), it was mentioned that $c = 1$ was an acceptable normalization. However, if we seek dR expressed in exponential coordinates so that $\int_{SO(3)} dR = 1$, how should c be chosen for this parameterization? Similarly, in the case of $SE(3)$, if instead of choosing $c' = 1$, we desire $dg = dR\, d\mathbf{t}$, where R is normalized as above, how should c' be chosen in (12.11)?

12.12 Show that from the definition (12.83) and the homomorphism property

$$U(R_1, l)U(R_2, l) = U(R_1 R_2, l)$$

that (12.84) holds and, moreover, that

$$Y_n^l((R_1R_2)^T\mathbf{u}) = \sum_{m=-l}^{l} Y_m^l(\mathbf{u})U_{mn}(R_1R_2, l).$$

12.13. Using (12.105), show that the Clebsch-Gordon Coefficients and the Wigner D-functions $D^l_{mn}(R) = U_{mn}(R, l)$ given in (12.79) are related as

$$\int_{SO(3)} \overline{D^l_{mn}(R)}\, D^{l_1}_{m_1n_1}(R)\, D^{l_2}_{m_2n_2}(R)\, dR \;=\; \frac{1}{2l+1} C^{lm}_{l_1,m_1;l_2,m_2}\, C^{ln}_{l_1,n_1;l_2,n_2}$$

where $dR = \frac{1}{8\pi^2}\sin\beta d\alpha d\beta d\gamma$ is the normalized Haar measure for $SO(3)$.

References

1. Beth, T., "On the computational complexity of the general discrete Fourier transform," *Theoret. Computer Sci.*, 51, pp. 331–339, 1987.
2. Biedenharn, L.C., Louck, J.D., *Angular Momentum in Quantum Physics: Theory and Application*, Encyclopedia of Mathematics and Its Applications Vol. 8., Addison-Wesley, Reading, MA, 1981.
3. Borel, A., "Topology of Lie groups and characteristic classes," *Bull. Am. Math. Soc.*, 61, 397–432, 1955.
4. Bott, R., "The stable homotopy of the classical groups," *Ann. Math., Second Series*, 70(2), pp. 313–337, 1959.
5. Bott, R., Tu, L.W., *Differential Forms in Algebraic Topology*, Springer-Verlag, New York, 1982.
6. Bröcker, T., tom Dieck, T., *Representations of Compact Lie Groups*, Springer-Verlag, New York, 1985.
7. Bump, D., *Lie Groups*, Springer, New York, 2004.
8. Burrus, C.S., Parks, T.W., *DFT/FFT and Convolution Algorithms*, John Wiley and Sons, New York, 1985.
9. Chern, S.S., "On integral geometry in Klein spaces," *Ann. Math. (2)* 43, pp. 178–189, 1942.
10. Chevalley, C., Eilenberg, S., "Cohomology theory of Lie groups and Lie algebras," *Trans. Am. Math. Soc.*, 63(1), pp. 85–124, 1948.
11. Chirikjian, G.S., Kyatkin, A.B., *Engineering Applications of Noncommutative Harmonic Analysis*, CRC Press, Boca Raton, FL, 2001.
12. Clausen, M., "Fast generalized Fourier transforms," *Theoret. Computer Sci.*, 67, pp. 55–63, 1989.
13. Condon, E.U., Shortley, Q.W., *The Theory of Atomic Spectra*, Cambridge University Press, Cambridge, 1935.
14. Cooley, J.W., Tukey, J., "An algorithm for the machine calculation of complex Fourier series," *Math. Comput.* 19, pp. 297–301, 1965.
15. Cooley, J.W., "The re-discovery of the fast Fourier transform algorithm," *Mikrochim. Acta*, 93(1), pp. 33–45, 1987.
16. de Azcárraga, J.A., Izquierdo, J.M., *Lie Groups, Lie Algebras, Cohomology and Some Applications in Physics*, Cambridge University Press, Cambridge, 1995.
17. de Rham, G., *Variétés Différentiables*, Hermann, Paris, 1955.
18. Diaconis, P., Rockmore, D., "Efficient computation of the Fourier transform on finite groups," *J. Am. Math. Soc.*, 3(2), pp. 297–332, 1990.
19. Edmonds, A. R. *Angular Momentum in Quantum Mechanics*, 2nd ed., Princeton University Press, Princeton, NJ, 1968.

20. Elliott, D.F., Rao, K.R., *Fast Transforms: Algorithms, Analyses, Applications*, Academic Press, New York, 1982.
21. Gel'fand, I. M., Minlos, R.A., Shapiro, Z.Ya., *Representations of the Rotation and Lorentz Groups and Their Applications*, Macmillan, New York, 1963.
22. Goldberg, S.I., *Curvature and Homology*, Academic Press, New York, 1962.
23. Greub, W., Halperin, S., Vanstone, R., *Connections, Curvature, and Cohomology. Vol. II*, Academic Press, New York, 1972.
24. Gurarie, D., *Symmetry and Laplacians: Introduction to Harmonic Analysis, Group Representations and Applications*, Elsevier Science Publisher, Amsterdam, 1992. (Dover edition 2008.)
25. Helgason, S., *Differential Geometry and Symmetric Spaces*, Academic Press, New York, 1962.
26. Hodge, W.V.D., *The Theory and Applications of Harmonic Integrals*, Cambridge University Press, Cambridge, 1941 (and 1989).
27. Jones, M.N., *Spherical Harmonics and Tensors for Classical Field Theory*, Research Studies Press Ltd., London, 1985.
28. Kostelec, P.J., Rockmore, D.N., "FFTs on the Rotation Group," *J. Fourier Anal. Applic.*, 14, pp. 145–179, 2008.
29. Koszul, J.L., "Homologie et cohomologie des algèbres de Lie," *Bull. Soc. Math. France*, 78, pp. 66–127, 1950.
30. Kyatkin, A.B., Chirikjian, G.S., "Pattern matching as a correlation on the discrete motion group, " *Computer Vision Image Understanding*, 74(1), pp. 22–35, 1999.
31. Kyatkin, A.B., Chirikjian, G.S., "Computation of robot configuration and workspaces via the Fourier transform on the discrete motion group," *Int. J. Robotics Res.*, 18(6), pp. 601–615, 1999.
32. Kyatkin, A.B., Chirikjian, G.S., "Algorithms for fast convolutions on motion groups," *Appl. Comput. Harmonic Anal.*, 9, pp. 220–241, 2000.
33. Mackey, G.W., *The Theory of Unitary Group Representations*, The University of Chicago Press, Chicago, 1976.
34. Maslen, D.K., *Fast Transforms and Sampling for Compact Groups*, Ph.D. dissertation, Dept. of Mathematics, Harvard University, Cambridge, MA, 1993.
35. Maslen, D.K., Rockmore, D.N., "Generalized FFTs—a survey of some recent results," *DIMACS Ser. Discr. Math. Theor. Comp. Sci.,* 28, pp. 183–237, 1997.
36. Maslen, D.K., Rockmore, D.N., "Separation of Variables and the Computation of Fourier Transforms on Finite Groups, I," *J. Amer. Math. Soc.,* 10(1), pp. 169–214, 1997.
37. Messiah, A. *Quantum Mechanics, Vol.* 2, North-Holland, Amsterdam, pp. 1054–1060, 1962.
38. Miller, W., Jr., *Lie Theory and Special Functions*, Academic Press, New York, 1968;
39. Miller, W. Jr., "Some applications of the representation theory of the Euclidean group in three-space," *Commun. Pure App. Math.*, 17, pp. 527–540, 1964.
40. Morita, S., *Geometry of Differential Forms*, American Mathematical Society, Providence, RI, 2001.
41. Naimark, M.A., *Linear Representations of the Lorentz Group*, Macmillan, New York, 1964.
42. Peter, F., Weyl, H., "Die Vollständigkeit der primitiven Darstellungen einer geschlossenen kontinuierlichen Gruppe," *Math. Ann.*, 97, pp. 735–755, 1927.
43. Pontryagin, L., "On Betti numbers of compact Lie groups," *C.R. (Doklady) Acad. Sci. SSSR*, 1, pp. 433–437, 1935.
44. Potts, D., Prestin, J., Vollrath, A., "A fast algorithm for nonequispaced Fourier transforms on the rotation group," *Numer. Algorithms*, 52(3), pp. 355–384, 2009.
45. Rockmore, D.N., "Efficient computation of Fourier inversion for finite groups," *J. Assoc. Comput. Mach.*, 41(1), pp. 31–66, 1994.
46. Rockmore, D.N., "Fast Fourier transforms for wreath products," *Appl. Comput. Harmonic Anal.*, 4, pp. 34–55, 1995.
47. Rose, M. E., *Elementary Theory of Angular Momentum*, Dover, New York, 1995.
48. Samelson, H., "Topology of Lie groups," *Bull. Am. Math. Soc.*, 58, pp. 2–37, 1952.

49. Santaló, L., *Integral Geometry and Geometric Probability*, Cambridge University Press, Cambridge, 2004 (originally published in 1976 by Addison-Wesley).
50. Sepanski, M.R., *Compact Lie Groups*, Springer, New York, 2007.
51. Sugiura, M., *Unitary Representations and Harmonic Analysis*, 2nd ed., North-Holland, Amsterdam, 1990.
52. Taylor, M.E., *Noncommutative Harmonic Analysis*, Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 1986.
53. Terras, A., *Harmonic Analysis on Symmetric Spaces and Applications I*, Springer-Verlag, New York, 1985.
54. Van Loan, C., *Computational Frameworks for the Fast Fourier Transform*, SIAM, Philadelphia, 1992.
55. Varshalovich, D.A., Moskalev, A.N., Khersonskii, V.K., *Quantum Theory of Angular Momentum*, World Scientific, Singapore, 1988.
56. Vilenkin, N.Ja. Klimyk, A.U., *Representation of Lie Groups and Special Functions*, Vols. 1–3, Kluwer Academic, Dordrecht, 1991.
57. Vilenkin, N.J., *Special Functions and the Theory of Group Representations*, American Mathematical Society, Providence, RI, 1968.
58. Vilenkin, N.J., Akim, E.L., Levin, A.A., "The matrix elements of irreducible unitary representations of the group of Euclidean three-dimensional space motions and their properties," *Dokl. Akad. Nauk SSSR*, 112, pp. 987–989, 1957 (in Russian).
59. Walker, J.S., *Fast Fourier Transforms*, 2nd ed., CRC Press, Boca Raton, FL, 1996.
60. Wallach, N.R., *Harmonic Analysis on Homogeneous Spaces*, Marcel Dekker, New York, 1973.
61. Wang, Y.F., "Applications of diffusion processes in robotics, optical communications and polymer science," Ph.D. dissertation, Johns Hopkins Univ., Baltimore, MD, 2001.
62. Weil, A., *L'intégration dans les groupes topologiques et ses applications*, 2nd ed., Actualités scientifiques et industrielles no. 1145, Hermann & cie, Paris, 1951.
63. Weyl, H., *The Classical Groups: Their Invariants and Representations*, Princeton University Press, Princeton, NJ, 1946 (reprinted in 1997).
64. Weyl, H., "Harmonics on homogeneous manifolds," *Ann. Math.*, 35, pp. 486–499, 1934.
65. Wigner, E., "On unitary representations of the inhomogeneous Lorentz group," *Ann. Math.*, 40(1), pp. 149–204, 1939.
66. Wigner, E. P. *Group Theory and Its Application to the Quantum Mechanics of Atomic Spectra*, Academic Press, New York, 1959.
67. Williams, F.L., *Lectures on the Sprectum of $L^2(\Gamma\backslash G)$*, Pitman Research Notes in Mathematics Series, 242, Longman Scientific & Technical, London, 1991.
68. Želobenko, D.P., *Compact Lie Groups and their Representations*, Translations of Mathematical Monographs, American Mathematical Society, Providence, RI, 1973.

13

Variational Calculus on Lie Groups

The calculus of variations is concerned with finding extremal paths of functionals in analogy with the way that classical calculus seeks to find critical points of functions. Variational calculus plays a central role in classical mechanics, connecting the "Principle of Least Action" and Lagrange's equations of motion (also called the Euler–Lagrange equations). In that setting, generalized coordinates are introduced to describe the geometric configuration of a mechanical system. In this chapter, classical variational calculus is reviewed and extended to describe systems on Lie groups. Of course, the introduction of coordinates such as Euler angles to describe the orientation of a rigid body can be used to formulate classical variational problems at the expense of introducing singularities. However, it is possible to formulate variational problems on Lie groups *without* coordinates. This results in the Euler–Poincaré equations.

The main goals of this chapter are as follows:

- To become familiar with the use of Lie derivatives as a tool for performing numerical optimization on Lie groups;
- To understand and be able to apply classical variational calculus;
- To be able to use the Euler–Poincaré equation for variational problems on Lie groups.

This chapter begins with the statement of regular (nonvariational) optimization problems on Lie groups in Section 13.1. Section 13.2 then provides proofs of the classical necessary conditions for trajectories that extremize cost functionals. These necessary conditions are the Euler–Lagrange equations. These equations are quite general and can be written in terms of any coordinates. It can be quite hard to prove that the solutions generated by the Euler–Lagrange equations are globally optimal solutions. Furthermore, coordinate-dependent descriptions come with the drawback that they have singularities. A number of variational problems can be formulated in terms of trajectories on matrix Lie groups. This is illustrated in a coordinate-dependent setting in Section 13.3. Section 13.4 takes a detour into a topic rarely addressed in detail in books on variational calculus: When are the solutions guaranteed to be globally optimal? Section 13.5 makes another connection between variational calculus and Lie groups by examining Lie symmetries in Euler–Lagrange equations and other ODEs. A modification of the Euler–Lagrange equations—the Euler–Poincaré equations—is a coordinate-free variational technique that is discussed in Section 13.6. Section 13.7 illustrates this in the context of DNA mechanics. Section 13.8 summarizes this chapter and Section 13.9 provides exercises in both coordinate-dependent and coordinate-free variational problems.

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_4,

13.1 Optimization on Lie Groups

In many problems of practical interest, the quantity to be optimized is an element of a Lie group. For example, consider the hand of a robot arm and the goal of reaching a desired position and orientation. The forward kinematic function for the robot arm can be thought of as a mapping from the joint variables, $\mathbf{q} = [q_1, q_2, \ldots, q_n]^T$, to the group of rigid-body motions, $SE(3)$; that is $g : \mathbb{R}^n \to SE(3)$. If $g_{des} \in SE(3)$ denotes the desired position and orientation of the hand of the robot, then the minimization of measure of distance (or metric) of the form $d(g(\mathbf{q}), g_{des})$ will result in the values of $\mathbf{q}$ that place the hand as close as possible to the desired position and orientation. If g_{des} is within the subset of $SE(3)$ that is reachable by the robot arm, then the minimal value of $d(g(\mathbf{q}), g_{des})$ will be 0. However, how can such a minimization be performed?

One way would be to treat $SE(N)$ as a subspace of $\mathbb{R}^{(N+1)\times(N+1)}$ and simply use the method of Lagrange multipliers to look for solutions that stay on the constraint manifold, which is $SE(N)$. Then classical calculus would be all that is required. A drawback of doing this is that the size of the space will be much larger than needed. Another way would be to use a parameterization of $SE(N)$ and treat the resulting $N(N+1)/2$ parameters as Euclidean space and perform an unconstrained minimization on this space. However, this has the drawback that all parameterizations have singularities. An alternative approach that keeps the problem in a low-dimensional setting is to use the Lie derivatives defined in Chapter 11.

Given a cost function of the form $f(g)$ where $g \in G$ (with G being any Lie group), the necessary conditions that g_0 is an extremum of f are

$$(\tilde{E}_i^r f)(g_0) = 0 \quad \text{for } i = 1, \ldots, \dim(G).$$

In the case when there are additional constraints of the form $\mathbf{h}(g) = [h_1(g), \ldots, h_m(g)]^T = \mathbf{0}$, then a modified cost function can be defined as $c(g) = f(g) + \boldsymbol{\lambda}^T \mathbf{h}(g)$ and the system of equations

$$(\tilde{E}_i^r c)(g_0) = 0 \quad \text{for } i = 1, \ldots, \dim(G) \qquad \text{and} \qquad \frac{\partial c}{\partial \lambda_j} = 0 \quad \text{for } j = 1, \ldots, m \tag{13.1}$$

provides the necessary conditions for an extremum, $g_0 \in G$.

13.2 Derivation of the Euler–Lagrange Equation

Loosely speaking, a variational operator, denoted as δ, finds functions $y(x)$ that yield extremal values of the integral:

$$J = \int_{x_1}^{x_2} f(y(x), y'(x), x)\, dx$$

(where $y' = dy/dx$) for a given function $f(\cdot)$ in the same way that the operator d/dy finds the extremal values of a function $f(y)$. This new problem may be subject to boundary conditions $y(x_1) = y_1$ and $y(x_2) = y_2$, or the boundary conditions can be free. Moreover, Lagrange multipliers can be introduced as in the previous section to enforce constraints of the form

$$\int_{x_1}^{x_2} h_j(y(x), y'(x), x)\, dx = a_j$$

for given real values $\{a_j\}$ for $j = 1, \ldots, m$. In order to do so, a cost function

$$c(y(x), y'(x), x) \doteq f(y(x), y'(x), x) + \sum_j \lambda_j h_j(y(x), y'(x), x)$$

is defined and the same procedure described below is followed with $c(\cdot)$ in place of $f(\cdot)$. The extra freedom built in to $c(\cdot)$ is used to satisfy the integral constraints after the necessary conditions for an optimal solution are obtained. These conditions, which are derived below, are analogous to setting derivatives to 0 in the previous section.

13.2.1 The Concept of a Variational Operator

If we were to *assume* that the optimal solution to the problem is $y(x)$, then the following will *not* be the optimal value of the integral:

$$\hat{J}(\alpha) = \int_{x_1}^{x_2} f(Y, Y', x)\, dx,$$

where

$$Y = Y(x, \alpha) = y(x) + \alpha\, \epsilon(x).$$

Here, $\alpha \in \mathbb{R}$ defines an arbitrary "variation" from the original function, where $\epsilon(x)$ is any continuous function such that

$$\epsilon(x_1) = \epsilon(x_2) = 0. \tag{13.2}$$

The notation $\hat{J}$ is introduced to distinguish between the integral J resulting from the assumed function $y(x)$ and the value of the same integral evaluated with $Y(x, \alpha)$; that is, $J = \hat{J}(0)$ and $Y(x, 0) = y(x)$.

Note that $Y(x)$ satisfies the same boundary conditions as $y(x)$, but by definition it must be the case that $\hat{J}(\alpha) \geq J$. We can introduce the concept of a variational operator as follows:

$$\delta\hat{J} = \left.\frac{\partial \hat{J}}{\partial \alpha}\right|_{\alpha=0} d\alpha. \tag{13.3}$$

α is a variable which is introduced into the calculus of variations problem to distinguish all functions "within the neighborhood" of the desired function and meeting the boundary conditions $Y(x_1, \alpha) = y_1$ and $Y(x_2, \alpha) = y_2$. Here, δ is nothing more than shorthand for the operation in (13.3). It is used like a derivative. There are four properties of δ (which follow naturally from the above equations):

- It commutes with integrals: $\delta \int_{x_1}^{x_2} f(Y, Y', x)\, dx = \int_{x_1}^{x_2} \delta f(Y, Y', x)\, dx$. This follows because δ is basically a derivative, and taking a derivative of an integral when the variables of integration and differentiation are different can be done in any order when the bounds of integration are finite.
- It acts like a derivative on Y and Y' when it is applied to the function $f(Y, Y', x)$ but treats independent variables such as x like constants: $\delta f = \frac{\partial f}{\partial Y}\delta Y + \frac{\partial f}{\partial Y'}\delta Y'$. This is because Y depends on α by definition and x does not.
- It commutes with derivatives: $\delta\left(\frac{\partial Y}{\partial x}\right) = \frac{\partial}{\partial x}(\delta Y)$. This follows because δ is basically a derivative, and derivatives with respect to independent variables commute.
- The variation of $Y(x)$ vanishes at the endpoints : $\delta Y(x_1) = \delta Y(x_2) = 0$. This follows from (13.2).

13.2.2 Variational Calculus Computations

We can use the properties presented above to generate conditions which will yield the extremal solution $y(x)$ that we seek—namely

$$\begin{aligned}\delta\hat{J} = \delta\int_{x_1}^{x_2} f(Y,Y',x)\,dx &= \int_{x_1}^{x_2} \delta f(Y,Y',x)\,dx\\ &= \int_{x_1}^{x_2}\left(\frac{\partial f}{\partial Y}\delta Y + \frac{\partial f}{\partial Y'}\delta Y'\right)dx\\ &= \int_{x_1}^{x_2}\left(\frac{\partial f}{\partial y}\delta Y + \frac{\partial f}{\partial y'}\delta Y'\right)dx. \qquad (13.4)\end{aligned}$$

The last step is true, just by the chain rule.[1]

Now, we will use the third property to rewrite the second part of this expression as

$$\frac{\partial f}{\partial y'}\delta Y' = \frac{\partial f}{\partial y'}\frac{d}{dx}(\delta Y).$$

Using integration by parts,[2] this means

$$\int_{x_1}^{x_2}\frac{\partial f}{\partial y'}\frac{d}{dx}(\delta Y) = \left.\frac{\partial f}{\partial y'}\delta Y\right|_{x_1}^{x_2} - \int_{x_1}^{x_2}\frac{d}{dx}\left(\frac{\partial f}{\partial y'}\right)\delta Y\,dx.$$

Since $\delta Y(x) = \epsilon(x)$ vanishes at endpoints, the first term is 0, and we get

$$\delta\hat{J} = \int_{x_1}^{x_2}\left(\frac{\partial f}{\partial Y}\delta Y - \frac{d}{dx}\left(\frac{\partial f}{\partial Y'}\right)\delta Y\right)dx.$$

This is easily rewritten as

$$\delta\hat{J} = \int_{x_1}^{x_2}\left(\frac{\partial f}{\partial y} - \frac{d}{dx}\left(\frac{\partial f}{\partial y'}\right)\right)\epsilon(x)\,dx. \qquad (13.5)$$

13.2.3 Obtaining the Euler–Lagrange Equations by Localization

A classical mathematical result (called a localization argument) says that if

$$\int_a^b M(x)\epsilon(x)\,dx = 0$$

for all possible differentiable functions $\epsilon(x)$ for which $\epsilon(a) = \epsilon(b) = 0$, then the function $M(x) = 0$, the integrand in (13.5) is 0, and so

$$\frac{\partial f}{\partial y} - \frac{d}{dx}\left(\frac{\partial f}{\partial y'}\right) = 0. \qquad (13.6)$$

This is called the *Euler–Lagrange* equation. Note that if the function f does not depend on y', the second term vanishes, we no longer are able to accommodate boundary conditions, and we get the familiar minimization problem from calculus.

[1] $\partial/\partial y(f(g(y),g'(y'),x)) = (\partial f/\partial g)(\partial g/\partial y)$. In our case, $g = Y$ and $\partial Y/\partial y = 1$. Therefore, $\partial f/\partial y = \partial f/\partial Y$. The same is true for $\partial f/\partial y' = \partial f/\partial Y'$.

[2] $\int_a^b u\,dv = uv|_a^b - \int_a^b v\,du$.

Although we have presented the one-dimensional variational problem, the same methods are used for a functional dependent on many variables:

$$J = \int_a^b f(y_1, \ldots, y_n, y_1', \ldots, y_n', x)\, dx.$$

In this case, a set of simultaneous Euler–Lagrange equations are generated:

$$\frac{\partial f}{\partial y_i} - \frac{d}{dx}\left(\frac{\partial f}{\partial y_i'}\right) = 0. \tag{13.7}$$

Likewise, the treatment of problems in which $f(\cdot)$ depends on higher derivatives of y is straightforward. The derivation above is simply extended by integrating by parts once for each derivative of y. See [6, 21] for further reading on the classical calculus of variations and [28, 35] for the more modern extensions of optimal control and dynamic optimization.

13.3 Examples of Variational Calculus Problems

In this section a number of problems that can be addressed using the classical coordinate-dependent version of variational calculus are formulated.

13.3.1 Geodesics on Manifolds

As was explained in Chapters 5 and 7 of Volume 1, the arc length of a curve on a Riemannian manifold is calculated as

$$L(T) = \int_0^T \left(\dot{\mathbf{q}}^T(t) G(\mathbf{q}(t))\dot{\mathbf{q}}(t)\right)^{\frac{1}{2}} dt,$$

where $\mathbf{q}(t)$ is a path in some coordinates $\mathbf{q}$ parameterized by t, and $G(\mathbf{q})$ is the metric tensor. Given initial and final points in the manifold, $\mathbf{q}(0) = \mathbf{q}_0$ and $\mathbf{q}(T) = \mathbf{q}_T$, the problem of finding the curve of minimal length, $L(T)$, that stays completely inside the manifold and satisfies these end conditions is a *geodesic*. The equation for a geodesic has already been given in (5.60). This can be obtained using the Euler–Lagrange equation when the constraint $L(t) = t$ is imposed.

13.3.2 The Planar Elastica

Euler's elastica is a classical problem. Given an inextensible, shearless, planar elastic filament, with potential energy of bending of the form

$$V = \frac{1}{2}\int_0^L \alpha(s)\kappa^2(s)\, ds$$

(where s is the arc length along the filament and $\alpha(s)$ is its bending stiffness, which can vary along the length), if the two ends are constrained in planar position and orientation, what will the shape of the filament be?

One of the basic principles of mechanics is that in static situations, passive mechanical systems settle down to the state of lowest potential energy. This means that minimization of V subject to end constraints on the curve that describes the filament will provide the answer.

Recalling from Chapter 5 that for a planar curve $\kappa^2 = (d\theta/ds)^2$, where $\theta(s)$ is the angle that the tangent vector to the curve makes with respect to the x_1 axis. The position of the point $\mathbf{x}(L)$ can be written in a reference frame affixed at $s = 0$ with orientation fixed by having the tangent point along the x_1 axis, as

$$\mathbf{x}(L) = \begin{pmatrix} \int_0^L \cos\theta(s)\,ds \\ \int_0^L \sin\theta(s)\,ds \end{pmatrix}.$$

Therefore, the curve that minimizes V subject to the boundary conditions $x_1(0) = x_2(0) = \theta(0) = 0$ and $x_1(L) = x_d$, $x_2(L) = y_d$, and $\theta(L) = \theta_d$ will be the one for which

$$c(\theta,\theta') = \frac{1}{2}\alpha(s)(\theta')^2 + \lambda_1\cos\theta + \lambda_2\sin\theta$$

satisfies

$$\frac{d}{ds}\left(\frac{\partial c}{\partial\theta'}\right) - \frac{\partial c}{\partial\theta} = 0,$$

which is written explicitly as

$$\frac{1}{2}\frac{d}{ds}\left(\alpha(s)(\theta')^2\right) + \lambda_1\sin\theta - \lambda_2\cos\theta = 0$$

subject to the conditions

$$\int_0^L \cos\theta(s)\,ds = x_d, \quad \int_0^L \sin\theta(s)\,ds = y_d, \quad \text{and} \quad \theta(0) = 0 \quad \theta(L) = \theta_d.$$

One way to approach the numerical solution to this problem is to take initial guesses for the values of the Lagrange multipliers, numerically integrate the above ordinary differential equation, and then update the values of the Lagrange multipliers so as to make the constraints satisfied.

This sort of curve has found applications in robotics, including serving as the backbone curves for snakelike, or “hyperredundant,” robot arms [13, 14].

13.3.3 Finding Approximate Solutions to Evolution Equations

Suppose that an evolution equation of the form

$$\frac{\partial f}{\partial t} - \sum_i a_i(\mathbf{q})\frac{\partial f}{\partial q_i} + \sum_{ij} b_{ij}(\mathbf{q})\frac{\partial^2 f}{\partial q_i \partial q_j} = 0\,, \qquad \text{or} \qquad \mathcal{D}f = 0 \tag{13.8}$$

for short, subject to initial conditions $f(\mathbf{q},0) = f_0(\mathbf{q})$, is presented and separation of variables fails. How can a solution be obtained? One way would be to use finite-element techniques, in which the original problem is discretized. Another way to discretize the problem is to choose a basis $\{\phi_k(\mathbf{q})\}$ for the set of square-integrable functions on the domain parameterized by $\mathbf{q}$ and attempt to find coefficients $\{a_k(t)\}$ such that

$$\tilde{f}(\mathbf{q},t) = \sum_{k=1}^{N} a_k(t)\phi_k(\mathbf{q})$$

can approximately solve (13.8). A natural way to quantify how goodness of an approximation $\tilde{f}$ over the period of time $[0,T]$ is by calculating the cost

$$I \doteq \int_0^T \int_{\mathbf{q}} |\mathcal{D}\tilde{f}|^2 d\mathbf{q}\, dt + \alpha^2 \int_{\mathbf{q}} |\tilde{f}(\mathbf{q},0) - f_0(\mathbf{q})|^2 d\mathbf{q},$$

where α^2 is a weighting factor that is introduced in the event that the initial conditions cannot be exactly met and a trade-off between error in the initial conditions and in satisfying the evolution equation must be made.

After the integration over $\mathbf{q}$ is performed, this will be of the form

$$I = \int_0^T c(\mathbf{a}, \dot{\mathbf{a}})\, dt. \tag{13.9}$$

Finding the optimal values of $\mathbf{a}(t)$ over the range $t \in [0,T]$ is then a variational calculus problem.

13.3.4 Equations of Motion of Mechanical Systems

In classical mechanics, a system consisting of N particles, the kth of which has a time-varying position $\mathbf{x}_k(t) \in \mathbb{R}^3$, has a total kinetic energy of the form

$$T = \frac{1}{2}\sum_{k=1}^{N} m_k \dot{\mathbf{x}}_k \cdot \dot{\mathbf{x}}_k.$$

If every geometric configuration of the systems can be described with $n \leq 3N$ generalized coordinates $\mathbf{q} = [q_1, \ldots, q_n]^T$, then using the chain rule, the kinetic energy can be written as

$$T(\mathbf{q}, \dot{\mathbf{q}}) = \frac{1}{2}\dot{\mathbf{q}}^T M(\mathbf{q})\dot{\mathbf{q}}, \qquad \text{where} \qquad [M(\mathbf{q})]_{ij} = \sum_{k=1}^{N} m_k \frac{\partial \mathbf{x}_k}{\partial q_i} \cdot \frac{\partial \mathbf{x}_k}{\partial q_j}.$$

If the system is subjected to conservative forces, then this can be described using a potential energy function $V(\mathbf{q})$.

Hamilton's principle (also called the *principle of least*[3] *action*) states that the integral of the Lagrangian,[4] $L(\mathbf{q}, \dot{\mathbf{q}}) = T(\mathbf{q}, \dot{\mathbf{q}}) - V(\mathbf{q})$, over any period of time should be extremized. From the Euler–Lagrange equations, this gives *Lagrange's equations of motion*:

$$\frac{d}{dt}\left(\frac{\partial L}{\partial \dot{\mathbf{q}}}\right) - \frac{\partial L}{\partial \mathbf{q}} = \mathbf{0}. \tag{13.10}$$

13.4 Sufficient Conditions for Optimality

The Euler–Lagrange equations provide *necessary* conditions for optimality, but there is usually no guarantee that a solution of the Euler–Lagrange equations will be optimal. However, in certain situations, the structure of the function $f(\cdot)$ will guarantee that the solution generated by the Euler–Lagrange equations is a globally optimal solution. We now examine cases in which global optimality of solutions of the Euler–Lagrange equations can be guaranteed.

[3] Whether or not the action is actually minimized is another story.

[4] The time integral of $L(\mathbf{q}, \dot{\mathbf{q}})$ is called the action.

13.4.1 Global optimality in the One-Dimensional Case

Here, we consider a special functional in the one-dimensional case for which it is possible to prove that the solution to the Euler–Lagrange equation is a globally minimal solution. In particular, if

$$f(y, dy/dx, x) = \frac{1}{2} g(y)(dy/dx)^2$$

and $y^*(x)$ denotes the solution obtained by the Euler–Lagrange equations of variational calculus, then when $x \in [0,1]$, $y(0) = 0$, and $y(1) = 1$, the resulting cost is

$$J(y^*) = \left(\int_0^1 g^{\frac{1}{2}}(y^*(x)) \frac{dy^*}{dx} dx \right)^2 = \left(\int_0^1 g^{\frac{1}{2}}(y^*) dy^* \right)^2 .$$

This is because $y^*(0) = 0$, $y^*(1) = 1$ and $dy^*/dx > 0$. Note that this means that the value of the integral in the above expression for $J(y^*)$ is *independent* of the path $y^*(x)$. This does not mean that $J(y^*)$ itself is independent of y^*. Rather, it means that after the form of the candidate optimal path obtained from the Euler–Lagrange equation is substituted back into the cost functional, the resulting value can be written as

$$J(y^*) = \left(\int_0^1 g^{\frac{1}{2}}(y)\, dy \right)^2$$

since the name of the variable of integration is irrelevant. Then from here if we substitute any $y(x)$ with $dy/dx > 0$ and use the Cauchy–Schwarz inequality with $a(x) = g^{\frac{1}{2}}(y(x))\, dy/dx$ and $b(x) = 1$, it follows that

$$J(y^*) \leq J(y) \tag{13.11}$$

for any possible $y(x)$.

Example 1: Optimal Reparameterization of Curves

Suppose that an arc-length parameterized curve $\mathbf{x}(s) \in \mathbb{R}^n$ is given and that the shape of this curve is desirable, but the temporal evolution of the position of a particle along the curve is sought such that the integral of a cost functional $\tilde{f}(\mathbf{x}, \dot{\mathbf{x}}) = \frac{1}{2} \dot{\mathbf{x}}^T A(\mathbf{x}) \dot{\mathbf{x}}$ should be minimized along the curve. From the chain rule, $\dot{\mathbf{x}} = \frac{d\mathbf{x}}{ds} \dot{s}$, and so $f(s, \dot{s}) \doteq \tilde{f}(\mathbf{x}(s), \frac{d\mathbf{x}}{ds} \dot{s}) = \frac{1}{2} \left(\frac{d\mathbf{x}}{ds} \right)^T A(\mathbf{x}(s)) \left(\frac{d\mathbf{x}}{ds} \right) \dot{s}^2 = \frac{1}{2} g(s) \dot{s}^2$. Therefore, the results of the framework above indicate that solving this one-dimensional variational problem will yield a globally optimal reparameterization.

13.4.2 Global Optimality in the Multi-dimensional Case

In the multi-dimensional case it is generally not possible to equate the solution of the Euler–Lagrange equation with global optimality. This is because there can be many possible paths connecting the initial and final values $\mathbf{q}(0)$ and $\mathbf{q}(1)$, respectively. For example, if the cost is of the form $f(\mathbf{q}, \dot{\mathbf{q}}, t) = \dot{\mathbf{q}}^T G(\mathbf{q}) \dot{\mathbf{q}}$, where $G(\mathbf{q})$ is the metric tensor for a Riemannian manifold, then solutions of the Euler–Lagrange equations give the geodesic equations. As is clear even in the simple case of the spheres S^1 and S^2, a geodesic connecting any two points can be either the shorter or the longer of the two great arcs connecting the points. Both are solutions to the variational problem, but only the shorter of the two is a minimal-length path. In the case case of S^2, if the two endpoints are antipodal, an infinite number of great arcs connect them, illustrating the possible nonuniqueness of shortest paths.

Thus, the issue of global optimality is closely tied to the statement of the problem as a boundary value problem. If instead the problem is stated as "find the path starting at $\mathbf{q}(0)$ with specified value of $\dot{\mathbf{q}}(0)$ that minimizes the cost functional $\int_0^1 f(\mathbf{q}, \dot{\mathbf{q}}, t)\, dt$ with $\mathbf{q}(1)$ left unspecified," then the solutions of the Euler–Lagrange equations will be globally optimal. In the one-dimensional case with cost of the form $g(y)(y')^2$ on a domain that is an interval, the distinction between the initial value and boundary value problems is not so important because the paths only have one possible initial direction. In the case of the circle S^1, they have two possible directions. In multi-dimensional problems, the initial directions have a continuous space from which to be chosen, meaning that, in general, the nonlinear mapping between initial conditions and boundary conditions potentially can result in multiple globally suboptimal solutions. Additionally, short of enumerating them all and comparing the cost of each, there is no simple general test to assess global optimality. However, special multi-dimensional cases exist in which global optimality can be proved. For example, when $G(\mathbf{q}) = G_0$ is constant, or dependent on $\mathbf{q}$ but is diagonal, the resulting boundary value problem will be globally minimized by the Euler–Lagrange equations when $\mathbf{q} \in [0,1]^n$. This is verified by solving the Euler–Lagrange equations to obtain $\mathbf{q}^*(t)$ and then evaluating the cost of any $\mathbf{q}(t) = \mathbf{q}^*(t) + \boldsymbol{\epsilon}(t)$, where $\boldsymbol{\epsilon}(0) = \boldsymbol{\epsilon}(1) = \mathbf{0}$. The resulting cost will never be less than that for $\mathbf{q}^*(t)$.

Suppose that, for whatever reason, a globally minimal solution to a variational optimization problem with $f_1(\mathbf{q}, \dot{\mathbf{q}}, t) = \frac{1}{2}\dot{\mathbf{q}}^T G(\mathbf{q})\dot{\mathbf{q}}$ and $\mathbf{q}(0)$ and $\mathbf{q}(1)$ specified has been solved via the Euler–Lagrange equations and minimization over all resulting paths that connect the specified endpoints. This solution then can be used to "bootstrap" a globally optimal solution to a larger variational problem in which

$$f_2(\mathbf{q}, \boldsymbol{\theta}, \dot{\mathbf{q}}, \dot{\boldsymbol{\theta}}, t) = \frac{1}{2}\dot{\mathbf{q}}^T G(\mathbf{q})\dot{\mathbf{q}} + \frac{1}{2}\|\dot{\boldsymbol{\theta}} - A(\mathbf{q})\dot{\mathbf{q}}\|_W^2, \tag{13.12}$$

where $\|B\|_W^2 = \mathrm{tr}(B^T W B)$ is the weighted Frobenius norm where $W = W^T > 0$.

The Euler–Lagrange equations for the original variational problem are of the form

$$\begin{aligned}
&\frac{d}{dt}\left(\frac{\partial f_1}{\partial \dot{\mathbf{q}}}\right) - \frac{\partial f_1}{\partial \mathbf{q}} = \mathbf{0} \\
&\quad\Longrightarrow G(\mathbf{q})\ddot{\mathbf{q}} + \frac{d}{dt}\left[G(\mathbf{q})\right]\dot{\mathbf{q}} - \frac{1}{2}\frac{\partial}{\partial \mathbf{q}}(\dot{\mathbf{q}}^T G(\mathbf{q})\dot{\mathbf{q}}) = \mathbf{0} \\
&\quad\Longrightarrow G(\mathbf{q})\ddot{\mathbf{q}} + \frac{1}{2}\frac{\partial}{\partial \mathbf{q}}(\dot{\mathbf{q}}^T G(\mathbf{q})\dot{\mathbf{q}}) = \mathbf{0}.
\end{aligned} \tag{13.13}$$

Let the solution to this system of equations subject to boundary conditions be denoted as $\mathbf{q}^*(t)$.

The Euler–Lagrange equations for the new system will be

$$\begin{aligned}
&\frac{d}{dt}\left(\frac{\partial f_2}{\partial \dot{\mathbf{q}}}\right) - \frac{\partial f_2}{\partial \mathbf{q}} = \mathbf{0} \\
&\quad\Longrightarrow G(\mathbf{q})\ddot{\mathbf{q}} - \frac{d}{dt}\left[A^T(\mathbf{q})W(\dot{\boldsymbol{\theta}} - A(\mathbf{q})\dot{\mathbf{q}})\right] \\
&\qquad + \frac{1}{2}\frac{\partial}{\partial \mathbf{q}}(\dot{\mathbf{q}}^T G(\mathbf{q})\dot{\mathbf{q}}) + \frac{\partial}{\partial \mathbf{q}}\left[\dot{\mathbf{q}}^T A^T(\mathbf{q})\right] W(\dot{\boldsymbol{\theta}} - A(\mathbf{q})\dot{\mathbf{q}}) = \mathbf{0}
\end{aligned} \tag{13.14}$$

and

$$\begin{aligned}\frac{d}{dt}\left(\frac{\partial f_2}{\partial \dot{\boldsymbol{\theta}}}\right) - \frac{\partial f_2}{\partial \boldsymbol{\theta}} &= \mathbf{0} \\ \Longrightarrow \frac{d}{dt}\left\{W\left[\dot{\boldsymbol{\theta}} - A(\mathbf{q})\dot{\mathbf{q}}\right]\right\} &= \mathbf{0} \\ \Longrightarrow \dot{\boldsymbol{\theta}} - A(\mathbf{q})\dot{\mathbf{q}} &= \mathbf{a}, \end{aligned} \tag{13.15}$$

where $\mathbf{a}$ is a constant vector of integration. Substituting the right-hand side of (13.15) back into (13.14) and using the chain rule,

$$\frac{d}{dt}(A^T(\mathbf{q})W\mathbf{a}) = \dot{\mathbf{q}}^T \frac{\partial}{\partial \mathbf{q}}\left[A^T(\mathbf{q})W\mathbf{a}\right] = \frac{\partial}{\partial \mathbf{q}}\left[\dot{\mathbf{q}}^T A^T(\mathbf{q})\right] W\mathbf{a},$$

means that (13.14) reduces to (13.13), and so the optimal solution for the "$\mathbf{q}$ part" of the problem again will be $\mathbf{q}^*(t)$. The right-hand side of (13.15) means that the candidate optimal solution for this new problem is

$$\boldsymbol{\theta}^*(t) = \mathbf{a}t + \mathbf{b} + \int_0^t A(\mathbf{q}^*(s))\dot{\mathbf{q}}^*(s)\, ds, \tag{13.16}$$

where $\mathbf{a}$ and $\mathbf{b}$ are constant vectors that can be matched to boundary values and $\mathbf{q}^*(t)$ is the solution to the original variational problem with cost $f_1(\mathbf{q}, \dot{\mathbf{q}}, t)$. The global optimality of the solution $(\mathbf{q}^*(t), \boldsymbol{\theta}^*(t))$ is guaranteed by the assumption that optimal $\mathbf{q}^*(t)$ is obtained a priori, and the global optimality of $\boldsymbol{\theta}^*(t)$ in (13.16) can be observed by substituting any $\boldsymbol{\theta}(t) = \boldsymbol{\theta}^*(t) + \boldsymbol{\epsilon}(t)$, where $\boldsymbol{\epsilon}(0) = \boldsymbol{\epsilon}(1) = \mathbf{0}$, into the cost function and observing that this never improves the cost.

This class of problems can be viewed in a slightly different way by rewriting (13.12) as

$$f(\mathbf{q}, \boldsymbol{\theta}, \dot{\mathbf{q}}, \dot{\boldsymbol{\theta}}, t) = \frac{1}{2}\begin{bmatrix}\dot{\mathbf{q}} \\ \dot{\boldsymbol{\theta}}\end{bmatrix}^T \begin{pmatrix} A^T(\mathbf{q})WA(\mathbf{q}) & A^T(\mathbf{q})W \\ WA(\mathbf{q}) & W \end{pmatrix}\begin{bmatrix}\dot{\mathbf{q}} \\ \dot{\boldsymbol{\theta}}\end{bmatrix}. \tag{13.17}$$

This means that if a quadratic cost can be decomposed in this way, then the solution to the larger problem will inherit the global optimality from the original problem.

Example 2: Simultaneous Optimal Reparameterization and Roll Modification

As a concrete application of this class of problems, consider the problem of simultaneous *curve reparameterization and optimal roll distribution.* Start with an initially arc-length-parameterized curve $\mathbf{x}(s)$ for $s \in [0,1]$ and frames defined using the Frenet–Serret apparatus discussed in Chapter 5 of Volume 1. Suppose that in a computer graphics simulation we seek a set of frames that evolve along the curve as evenly as possible. If the Frenet frames are $[\mathbf{x}(s), Q_{FS}(s)]$, then a new set of smoothly evolving reference frames can be defined as $[\mathbf{x}(t), Q(t)] = [\mathbf{x}(s(t)), Q_{FS}(s(t))R_1(\theta(s(t)))]$, where $R_1(\theta)$ is an added twist, or roll, of the Frenet frames about the tangent. A cost function can be formulated as

$$C \doteq \frac{1}{2}\int_0^1 \left\{\frac{1}{2}r^2 \mathrm{tr}(\dot{Q}\dot{Q}^T) + \dot{\mathbf{x}}\cdot\dot{\mathbf{x}}\right\} dt \tag{13.18}$$

$$= \frac{1}{2}\int_0^1 \left\{(r^2\kappa^2(s) + 1)\dot{s}^2 + r^2(\tau(s)\dot{s} + \dot{\theta})^2\right\} dt. \tag{13.19}$$

The integrand here is of the form in (13.12) with s taking the place of $\mathbf{q}$ and θ taking the place of $\boldsymbol{\theta}$. Since the curve reparameterization problem (with the second term in the integral set to 0) is a one-dimensional variational problem with $f(s,\dot{s},t)=\frac{1}{2}g(s)(\dot{s})^2$, global optimality is preserved. Additionally, from the discussion above, this guarantees the global optimality of the composite problem.

As a result, the sorts of simultaneous curve reparameterization and optimal roll distribution to satisfy end constraints obtained from variational calculus in [13, 14] in the context of "hyperredundant" (snakelike) robotic arms are in fact optimal.

13.5 Lie Symmetries in Euler–Lagrange Equations and Other ODEs

Although the spirit of most of this book is the use of Lie groups and associated homogeneous spaces as domains in which deterministic and stochastic trajectories evolve, in the history of mathematics that is not how these mathematical objects originally came to be studied. Sophus Lie studied symmetries of ODEs. Here, we return to these origins of Lie theory because the Euler–Lagrange equations are ODEs. Our path to studying symmetry properties of ODEs has been somewhat circuitous, starting with the presentation in Chapter 2 in which symmetry analysis of partial differential equations (PDEs) was presented. For more direct and general treatments of symmetries of ODEs and the use of these symmetries to reduce and/or solve these equations, see books such as [8, 50].

The theory of symmetries of ODEs begins with a single nth-order ODE of the form

$$y^{(n)}=f(x,y,y',\ldots,y^{(n-1)}),\quad \text{where } y^{(k)}=\frac{d^k y}{dx^k}.$$

From this, it is always possible to define a partial differential operator $\tilde{A}$ that acts on functions $\phi(x,y,y',\ldots,y^{(n-1)})$ as

$$\tilde{A}\phi \doteq \left(\frac{\partial}{\partial x}+y'\frac{\partial}{\partial y}+y''\frac{\partial}{\partial y'}+\cdots+f(x,y,y',\ldots,y^{(n-1)}\frac{\partial}{\partial y^{(n-1)}}\right)\phi.$$

The punch line of the theory is that given a set of partial differential operators $\{\tilde{X}_i\}$ that also act on functions $\phi(x,y,y',\ldots,y^{(n-1)})$, then these will form a Lie algebra corresponding to a local Lie group of symmetries if the following equation is satisfied for some constant scalar λ:

$$\boxed{[\tilde{X}_i,\tilde{A}]\phi=\lambda\tilde{A}\phi.} \tag{13.20}$$

We now illustrate this in the context of geodesics on the sphere. Recall that arc-length-parameterized geodesics can be generated by solving the initial value problem defined in Chapter 5. However, if we seek the geodesic connecting two specified points, this will be a boundary value problem for which we will not have advanced knowledge of the arc-length of the geodesic connecting the points. Therefore, non-arc-length-parameterized curves have value in establishing the curve by solving the boundary value problem resulting form the Euler–Lagrange equation. Then if one desires, the resulting curve can be reparameterized as discussed in Section 13.4.

If $\mathbf{q}=[\phi,\theta]^T$ is the column vector of spherical coordinates, then the metric tensor for the unit sphere is

$$G(\phi,\theta)=\begin{pmatrix}\sin^2\theta & 0\\ 0 & 1\end{pmatrix}.$$

If $\theta = \theta(t)$ and $\phi = \phi(t)$, where t is an arbitrary curve parameter, then minimization of the cost functional with

$$f(\phi, \theta, \dot{\phi}, \dot{\theta}) \doteq \frac{1}{2}\dot{\mathbf{q}}^T G(\mathbf{q})\dot{\mathbf{q}} = \frac{1}{2}\left[\dot{\phi}^2 \sin^2\theta + \dot{\theta}^2\right]$$

subject to end constraints is equivalent to the geodesic problem. The resulting Euler–Lagrange equations are

$$\ddot{\phi} + 2\dot{\phi}\dot{\theta}\cot\theta = 0$$

and

$$\ddot{\theta} - \dot{\phi}^2 \sin\theta\cos\theta = 0,$$

where $\dot{}$ denotes d/dt.

These equations can be combined by eliminating t so that the resulting curve is described as a graph of $\theta = \Theta(\phi)$. Then denoting $' = d/d\phi$, the chain rule gives

$$\dot{\theta} = \Theta'\dot{\phi} \qquad \text{and} \qquad \ddot{\theta} = \Theta''\dot{\phi}^2 + \Theta'\ddot{\phi}.$$

Using these, the original Euler–Lagrange equations can be written as a single equation defining the graph $\theta = \Theta(\phi)$ as

$$\Theta'' = 2(\Theta')^2 \cot\Theta + \sin\Theta\cos\Theta. \tag{13.21}$$

Following [50], it can be shown that the following operators are symmetries of (13.21) in the sense of (13.20):

$$\begin{aligned}
\tilde{X}_1 &= \frac{\partial}{\partial\phi},\\
\tilde{X}_2 &= \cot\Theta\cos\phi\frac{\partial}{\partial\phi} + \sin\phi\frac{\partial}{\partial\Theta} + \left(\cos\phi + \Theta'\cot\Theta\sin\phi + (\Theta')^2\frac{\cos\phi}{\sin^2\Theta}\right)\frac{\partial}{\partial\Theta'},\\
\tilde{X}_3 &= -\cot\Theta\sin\phi\frac{\partial}{\partial\phi} + \cos\phi\frac{\partial}{\partial\Theta} + \left(-\sin\phi + \Theta'\cot\Theta\cos\phi - (\Theta')^2\frac{\sin\phi}{\sin^2\Theta}\right)\frac{\partial}{\partial\Theta'}.
\end{aligned} \tag{13.22}$$

It should come as no surprise that the Lie group corresponding to these symmetries is $SO(3)$, since the sphere can be viewed as the homogenous space $SO(3)/SO(2)$ and, hence, geodesic paths can be moved around by actions of $SO(3)$.

In contrast to the use of Lie theory to characterize the symmetries of equations, as was done here, the following section focuses on coordinate-free formulations of variational calculus problems involving trajectories in Lie groups.

13.6 Parameter-Free Variational Calculus on Matrix Lie Groups

13.6.1 Problem Formulation

The variational calculus problem on matrix Lie groups can be formulated in terms of extremizing functionals of the form

$$J = \int_{t_1}^{t_2} f(g; g^{-1}\dot{g}; t)\, dt, \tag{13.23}$$

where $g(t)$ is an element of a matrix Lie group G and $g^{-1}\dot{g}$ is simply the product of the matrices g^{-1} and $\dot{g}$, the latter of which is not an element of G.

In particular, let $g \in \mathbb{R}^{N\times N}$ with n generators (i.e., it is an element of an n-dimensional group represented as an $N \times N$ matrix). The identity element is the $N \times N$ identity matrix, $\mathbb{I}$, and any small motion around the identity can be expressed as

$$g_{small} = \mathbb{I} + \sum_{i=1}^{n} \gamma_i E_i, \tag{13.24}$$

where $|\gamma_i| \ll 1$ and E_i is a unit basis element of the Lie algebra $\mathcal{G}$, which is also represented as an $N \times N$ matrix. For small deviations from the identity, $g_{small}^{-1} \approx \mathbb{I} - \sum_{i=1}^{n} \gamma_i E_i$. Furthermore, exponentiation of any linear combination of Lie algebra basis elements results in an element of the Lie group G, and (13.24) can be viewed as the truncated version of this exponential for small values of γ_i.

Given a functional of the form (13.23) and constraint equations of the form

$$\int_{t_1}^{t_2} h_k(g)\, dt = C_k, \tag{13.25}$$

one can use the structure of the Lie group G and Lie algebra $\mathcal{G}$ to find a natural analogue of the Euler–Lagrange equations. In this context, the concept of addition (which was used heavily in the previous subsection) is replaced by the group law and certain operations in the Lie algebra. In particular, the expression analogous to $x_i \to x_i + \alpha_i \epsilon_i$ for $i = 1, \ldots, n$ in the classical variational calculus in the Lie group context is

$$g(t) \to g(t) \circ \exp\left(\sum_{i=1}^{n} \alpha_i \epsilon_i(t) E_i\right) \approx g(t) \circ \left(\mathbb{I} + \sum_{i=1}^{n} \alpha_i \epsilon_i(t) E_i\right) \doteq g(\boldsymbol{\alpha}, t),$$

where $\exp(\cdot)$ is the matrix exponential and $g_1 \circ g_2$ is simply matrix multiplication (which will be written as $g_1 g_2$ below). The product rule of elementary calculus then dictates that

$$\dot{g}(t) \to \frac{d}{dt}\left(g(t)\,(\mathbb{I} + \sum_{i=1}^{n} \alpha_i \epsilon_i(t) E_i)\right) = \dot{g}(t)\left(\mathbb{I} + \sum_{i=1}^{n} \alpha_i \epsilon_i(t) E_i\right) + g(t) \sum_{i=1}^{n} \alpha_i \dot{\epsilon}_i(t) E_i.$$

This can be written as

$$\dot{g}(\boldsymbol{\alpha}, t) \doteq \dot{g}(t) + \sum_{i=1}^{n} \alpha_i \{\epsilon_i(t)\dot{g}(t) + \dot{\epsilon}_i(t) g(t)\} E_i.$$

Substituting $g(\boldsymbol{\alpha}, t)$ and $\dot{g}(\boldsymbol{\alpha}, t)$ into the functional (13.23) and incorporating the constraint (13.25) using Lagrange multipliers, the goal becomes the minimization of

$$J'(\boldsymbol{\alpha}; \boldsymbol{\lambda}) = \int_{t_1}^{t_2} f\left(g(\boldsymbol{\alpha}, t); [g(\boldsymbol{\alpha}, t)]^{-1} \dot{g}(\boldsymbol{\alpha}, t); t\right)\, dt + \sum_{k=1}^{m} \lambda_k \left(\int_{t_1}^{t_2} h_k(g(\boldsymbol{\alpha}, t); t)\, dt - C_k\right). \tag{13.26}$$

In this expression, the products of g, $\dot{g}$, and E_i all make sense when interpreted as matrix multiplication. Additionally, since we will be differentiating with respect to entries of the vector $\boldsymbol{\alpha}$ and then setting $\boldsymbol{\alpha}$ to 0 afterward, the term $[g(\boldsymbol{\alpha}, t)]^{-1}\dot{g}(\boldsymbol{\alpha}, t)$ can be linearized in $\boldsymbol{\alpha}$ since those are the only terms that will survive. Then the same steps as in the derivation of the classical Euler–Lagrange equations follow, as described below.

13.6.2 Derivation of the Euler–Poincaré Equation

In analogy with classical variational calculus, we compute

$$\left.\frac{\partial J'}{\partial \alpha_i}\right|_{\alpha_i=0} = 0 \tag{13.27}$$

and

$$\frac{\partial J'}{\partial \lambda_j} = 0 \tag{13.28}$$

for $i = 1, \ldots, n$ and $j = 1, \ldots, m$. Equation (13.28) is nothing more than (13.25).

By defining $f' = f + \sum_k \lambda_k h_k$, integrating by parts, and using the localization argument on (13.27) produces the following ODEs:

$$\tilde{E}_i^r f' + \left(\nabla_{g^{-1}\dot{g}} f', [g^{-1}\dot{g}, E_i]\right) - \frac{d}{dt}\left(\nabla_{g^{-1}\dot{g}} f', E_i\right) = 0 \tag{13.29}$$

where for any function $F \in C^\infty(G)$,

$$\tilde{E}_i^r F(g) = \left.\frac{d}{dt} F(g \circ \exp(tE_i))\right|_{t=0} \tag{13.30}$$

is the "right" derivative of F with respect to the ith Lie algebra basis element. $[\cdot, \cdot]$ is the Lie bracket (which in this case is the matrix commutator $[A, B] = AB - BA$). ∇_X is a directional derivative in the Lie algebra in the direction $X \in \mathcal{G}$. $(\cdot, \cdot)$ is the inner product for the Lie algebra $\mathcal{G}$ such that $(E_i, E_j) = \delta_{ij}$.

By observing that for any Lie group (not only $SO(3)$ or $SE(3)$), we can define $\boldsymbol{\xi} = (g^{-1}\dot{g})^\vee$, then

$$[g^{-1}\dot{g}, E_i] = \left[\sum_{j=1}^n \xi_j E_j, E_i\right] = \sum_{j=1}^n \xi_j [E_j, E_i] = \sum_{j=1}^n \xi_j \left(-\sum_{k=1}^n C_{ij}^k E_k\right),$$

$$(\nabla_{g^{-1}\dot{g}} f, E_i) = \left(\sum_{j=1}^n \frac{\partial f}{\partial \xi_j} E_j, E_i\right) = \sum_{j=1}^n \frac{\partial f}{\partial \xi_j} (E_j, E_i) = \frac{\partial f}{\partial \xi_i},$$

and

$$\begin{aligned}\left(\nabla_{g^{-1}\dot{g}} f, [g^{-1}\dot{g}, E_i]\right) &= \left(\sum_{l=1}^n \frac{\partial f}{\partial \xi_l} E_l, -\sum_{j,k=1}^n \xi_j \, C_{ij}^k E_k\right) \\ &= -\sum_{j,k,l=1}^n \frac{\partial f}{\partial \xi_l} C_{ij}^k \, \xi_j \, (E_l, E_k) \\ &= -\sum_{j,k=1}^n \frac{\partial f}{\partial \xi_k} C_{ij}^k \, \xi_j .\end{aligned}$$

Equation (13.29) can then be written in terms of the functions f and h_k as

$$\boxed{\frac{d}{dt}\left(\frac{\partial f}{\partial \xi_i}\right) + \sum_{j,k=1}^n \frac{\partial f}{\partial \xi_k} C_{ij}^k \, \xi_j = \tilde{E}_i^r \left(f + \sum_{l=1}^m \lambda_l h_l\right).} \tag{13.31}$$

This is a modified version of the *Euler–Poincaré* equation [1, 7, 31, 48]. For $i = 1, \ldots, n$, it forms a system of second-order ordinary differential equations. Generally, these will be nonlinear equations that can be solved numerically subject to boundary conditions. Several special cases are examined in the following subsections.

13.6.3 Cases When the Euler–Poincaré Equation Gives Globally Minimal Solutions

Given a cost function of the form

$$f(g, \boldsymbol{\xi}, t) = \frac{1}{2}\boldsymbol{\xi}^T W \boldsymbol{\xi} = \frac{1}{2}\sum_{i,j=1}^{n} w_{ij}\xi_i\xi_j$$

with $W = W^T > 0$, the Euler–Poincaré equations are of the form

$$\frac{d}{dt}\left(\sum_{j=1}^{n} w_{ij}\xi_j\right) + \sum_{j,k=1}^{n}\left(\sum_{l=1}^{n} w_{kl}\xi_l\right) C_{ij}^{k}\xi_j = 0. \tag{13.32}$$

Let

$$S_{lj}^{i} \doteq \sum_{k=1}^{n} w_{kl} C_{ij}^{k}. \tag{13.33}$$

If $S_{lj}^{i} = -S_{jl}^{i}$, then $\sum_{j,l=1}^{n} S_{lj}^{i}\xi_l\xi_j = 0$ and (13.32) reduces to

$$W\dot{\boldsymbol{\xi}} = \mathbf{0} \Longrightarrow \boldsymbol{\xi}(t) = \boldsymbol{\xi}(0) \Longrightarrow g(t) = g(0) \circ e^{t\hat{\boldsymbol{\xi}}(0)}.$$

This means that when these conditions hold, the shortest path computed from variational calculus connecting $g(0) = g_0$ and $g(1) = g_1$ is

$$\boxed{g(t) = g_0 \circ \exp(t \cdot \log(g_0^{-1} \circ g_1)).} \tag{13.34}$$

Furthermore, this path will be globally optimal because of the structure of the cost function.

However, if $S_{lj}^{i} \neq -S_{jl}^{i}$, then (13.32) does not reduce and the path generated by variational calculus is generally not this geometric one. For example, when $G = SO(3)$ and the cost is kinetic energy due to rotation, Euler's equations of motion result. If the inertia matrix is a multiple of the identity, then the minimal path connecting two rotations is the geometric path in (13.34). However, in cases when the moment of inertia is not isotropic, then computing the optimal path between rotations becomes more complicated. Such problems are relevant in satellite attitude reorientation. See, for example, [34].

In cases when an easy closed-form solution is not available for the optimal path, it is still possible to bound the length of the minimal path using closed-form solutions. An upper bound on the cost always can be obtained using (13.34). Additionally, since matrix Lie groups are naturally embedded in $\mathbb{R}^{n\times n}$, a lower bound on the length of the minimal path can be obtained by the straight-line distance $\|g_1 - g_2\|$. In cases where these upper and lower bounds are not very different from each other, this is an indication that the suboptimal solution obtained from the upper bound can serve as a satisfactory proxy for the optimal solution.

13.6.4 Sub-Riemannian Geometry, Carnot–Carathéodory Distance, and Stochastic Nonholonomic Systems

Throughout the chapter, it has been assumed that the cost function inside of integrals is quadratic with the matrix $G(\mathbf{q})$ being positive definite. This is consistent with Riemannian geometry, and a wide variety of applications fall within that paradigm. However, other systems of interest, including the kinematic cart, do not fall into this framework. If we seek a shortest path for a cart to take between the poses $g(x_0, y_0, \theta_0)$ and $g(x_1, y_1, \theta_1)$, we know that such a path will be of the form

$$\dot{g}(t) = g(t)\left(\sum_{k=1}^{2}\alpha_i(t)X_i\right), \quad \text{where } g(0) = g(x_0, y_0, \theta_0).$$

Here, X_1 and X_2 are the allowable infinitesimal motions in the body-fixed reference frame. In particular, for the cart, the allowable motion is a single translation degree of freedom in the forward/backward direction and a rotation around the z axis. However, no motion is allowed along the direction of the axis connecting the wheels. The fact that the cart can reach any pose from any starting position is a consequence of classical Lie bracket conditions [15]. The shortest path computed under such nonholonomic constraints will obviously be longer than the path computed if there were no such constraints. What is perhaps less obvious is that if the shortest path under such constraints is computed between every pair of points, this defines a bona fide distance/metric function on all pairs of elements (g_0, g_1). The generalization of this concept is the *Carnot–Carathéodory distance*—namely given an n-dimensional Lie group G, integrating the equation

$$\dot{g}(t) = g(t)\left(\sum_{k=1}^{m}\alpha_i(t)X_i\right), \quad \text{where } g(0) = g_0, \tag{13.35}$$

for known $\{\alpha_i(t)\}$ generates a curve segment in G for $t \in [0, 1]$. If the set $\{X_i\}$ for $i = 1, \ldots, m < n$ together with iterated Lie brackets span the whole Lie algebra of G, then it is guaranteed that at least one $\{\alpha_i(t)\}$ can be found such that $g(1) = g_1$. The Carnot–Carathéodory distance is the length of the shortest of all such paths [11, 51]:

$$d_{cc}(g_0, g_1) = \inf_{\{\{\alpha_i\}|g(0)=g_0, g(1)=g_1\}} \int_0^1 \left(\sum_{k=1}^{m}\alpha_i^2(t)\right)^2 dt. \tag{13.36}$$

This satisfies the metric properties (positive definiteness, symmetry, and the triangle inequality) and is invariant under left shifts. Since the infimum is over all possible $\{\{\alpha_i\}$ satisfying the boundary conditions $g(0) = g_0$ and $g(1) = g_1$, the value of $d_{cc}(g_0, g_1)$ depends only on the choice of the subset of basis elements $\{X_i\}$.

In addition to obvious applicability to shortest path problems in nonholonomic systems, the Carnot–Carathéodory distance has been used extensively in the study of how the geometric and algebraic properties of Lie groups are related [27, 44] and how rapidly diffusion processes on Lie groups spread out. Such problems go by names such as "volume growth in Lie groups"—namely if a ball within G centered at the identity is defined under the condition that every element in the ball, $g \in B$, satisfies the condition $d_{cc}(e, g) \leq t$, then the rate at which the volume $V_B(t)$ of this ball grows as $t \to \infty$ says something fundamental about the group. Groups of polynomial growth are those for which the asymptotic behavior of this volume is a polynomial in t. Since compact Lie groups have finite volume, they necessarily fall in this category, whereas some kinds of noncompact Lie groups can exhibit exponential growth. See, for example, [19] for a more detailed discussion of groups that exhibit polynomial volume growth.

The Carnot–Carathéodory distance has also been used to characterize the behavior of diffusion equations on Lie groups. For example, if $\tilde{X}_i^r$ denotes the Lie derivative associated with the Lie algebra basis element X_i, then the diffusion

$$\frac{\partial h}{\partial t} = \frac{1}{2}\sum_{k=1}^{m}(\tilde{X}_k^r)^2 h, \quad \text{where } h(g,0) = \delta(g),$$

will be nondegenerate if it satisfies Hörmander's hypoellipticity conditions [32]. Such equations would result in the example of the cart if it translated forward and backward and around its z axis by Brownian motion. Of relevance to stochastic nonholonomic systems are the following inequalities associated with the time-varying pdfs, $h(g,t)$, on groups G of polynomial growth [52]:

$$\int_{d_{cc}(e,g)\geq r} h(g,t)\,dg \leq Ce^{-r^2/Ct}$$

and

$$ce^{-C[d_{cc}(e,g)]^2/t} \leq h(g,t)\cdot V_B(\sqrt{t}) \leq Ce^{-c[d_{cc}(e,g)]^2/t}$$

for all $t > 0$ and some positive constants c and C.

Such inequalities are relevant to the sorts of diffusion equations that will be studied in Chapter 20. However, in applications, it is often equally important to know the values of the constants c and C, and some degenerate diffusion equations either do not follow Hörmander's condition or are on groups of exponential growth. In either case, the above equations do not apply. For these reasons, we will not be using many of the results of the field of geometric analysis/volume growth on Lie groups. However, readers with an interest in this area can find many results in the references above and [9, 10, 38, 45].

13.7 An Application: Continuum Models of DNA Mechanics

The DNA double helix has been modeled at a variety of levels of coarseness. At the finest level of description, the Cartesian positions of all atomic nuclei are stored. At the next level up, the positions and orientations of individual bases are treated as rigid bodies that are paired and stacked with harmonic potentials. The model reviewed here is even coarser. The stiffness properties of DNA are averaged over several consecutive basepairs in the double helix. The result is a continuous elastic rod model with a minimal energy conformation that has a helical twist. A "backbone curve" together with an arc-length-dependent stiffness matrix then describes the mechanical properties at this course level. Elastic models of DNA mechanics have a long history, and there is a correspondingly immense literature. Here, only a sampling of some of the most modeling-oriented works that are relevant to our current discussion is provided. For more complete lists, including those that focus on experiments, see [12, 36].

A number of recent studies on chiral and uncoupled end-constrained elastic rod models of DNA with circular cross section have been presented [3, 4, 16, 26]. These models use classical elasticity theory of continuum filaments with or without self-contact constraints to model the stable conformations of DNA in plasmids, in chromosomes, and during transcription.

The interpretation of experimental measurements of DNA stiffness parameters have been reported in many works, including [39, 53]. DNA elastic properties and experimental measurements of DNA elastic properties such as twist/stretch coupling have been reported.

Discussion of probabilistic aspects of DNA conformational fluctuations is postponed until Chapter 14. In this section the emphasis is on solving deterministic variational problems, such finding the shape of DNA loops with end constraints. This requires having a model for the elastic properties of DNA.

Recent works involve the modeling of DNA as an anisotropic inextensible rod and also include the effect of electrostatic repulsion for describing the DNA loops bound to the Lac repressor and so forth [3]. Another recent work includes sequence-dependent elastic properties of DNA [16]. All of these aforementioned works are based on Kirchhoff's thin elastic rod theory. This theory, as originally formulated, deals with nonchiral elastic rods with a circular cross section.

Gonzalez and Maddocks devised a method to extract sequence-dependent parameters for a rigid base pair DNA model from molecular dynamics simulation [25]. In their article, they used a force moment balance equation from Kirchhoff's rod theory to extract stiffness and inertia parameters. Another recent work includes the application of Kirchhoffs rod theory to marine cable loop formation and DNA loop formation [26]. Recently, Wiggins et al. developed a theory based on nonlinear elasticity, called the kinkable wormlike chain model, for describing spontaneous kinking of polymers, including DNA [53].

In this section the variational formulation in [36] is reviewed in detail. For associated numerical algorithms and results, the reader is referred to that work.

13.7.1 Elastic Rod Models of DNA

One problem that has been addressed in the literature is that of determining the shape of a DNA filament subjected to constraints on end positions and orientations. This is a natural variational calculus problem in which the energy due to deformation of the filament from its natural double-helical referential conformation can be captured with a helical rod model. Two kinds of elastic-filament models often are used to describe DNA. The first is an extensible model in which the DNA filament is allowed to stretch and shear, as well as to bend and twist. A 6 × 6 stiffness matrix describes the resistance to these motions. The second common model is that of an elastic rod that does not allow shear or stretching/compression. This model has only three degrees of freedom. These two models are described below, and it is explained how variational problems on $SE(3)$ and $SO(3)$ result.

The Extensible Case

A nonuniform extensible elastic filament with unstretched length L has elastic energy of the form[5]

$$E_1 = \int_0^L F(\boldsymbol{\xi}(s), s)\, ds, \quad \text{where } F(\boldsymbol{\xi}(s), s) = \frac{1}{2}[\boldsymbol{\xi}(s) - \boldsymbol{\xi}_0]^T K(s)[\boldsymbol{\xi}(s) - \boldsymbol{\xi}_0]. \qquad (13.37)$$

Here, $\hat{\boldsymbol{\xi}}_0 \in se(3)$ defines the local shape of the minimal energy conformation at each value of curve parameter s, and $K(s)$ is the 6 × 6 stiffness matrix that describes resistance to change in each direction of infinitesimal motion. Off-diagonal terms in this matrix describe couplings that have been observed experimentally. Both $\hat{\boldsymbol{\xi}}(s)$ and $\hat{\boldsymbol{\xi}}_0$

[5] In order to be consistent with recent literature, vectors $X^\vee$, where $X \in se(3)$, will be denoted here as $\boldsymbol{\xi}$.

are body-fixed quantities in the sense that $\hat{\boldsymbol{\xi}}(s) = g^{-1}dg/ds$ and $\hat{\boldsymbol{\xi}}_0 = g_0^{-1}dg_0/ds$ for the one-dimensional set of reference frames $g(s)$ and $g_0(s)$, respectively. Sometimes it is convenient to define

$$\mathbf{k} \doteq K\boldsymbol{\xi}_0.$$

Given $\boldsymbol{\xi}_0(s)$, it is possible to integrate the matrix differential equation

$$\frac{dg_0}{ds} = g_0\, \hat{\boldsymbol{\xi}}_0(s)$$

subject to the initial condition $g(0) = e$ (the identity element of $SE(3)$ is the identity matrix $e = \mathbb{I}_4$) for $s \in [0, L]$ to obtain the minimal energy conformation rooted at the identity. In the case when $\boldsymbol{\xi}_0(s)$ is a constant vector, this will be a helix (with circular arcs and line segments as special cases).

Note that the independent variable is now a curve parameter s rather than time t. Here, the curve parameter s is taken to be the curve parameter of the filament in its undeformed (referential) conformation $g_0(s)$.[6]

As a specific example, if the chain is uniform, inextensible, and shearless, we have the constant stiffness matrix K of the form

$$K = \begin{pmatrix} B_{11} & B_{12} & B_{13} & 0 & 0 & 0 \\ B_{12} & B_{22} & B_{23} & 0 & 0 & 0 \\ B_{13} & B_{23} & B_{33} & 0 & 0 & 0 \\ 0 & 0 & 0 & s_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & s_2 & 0 \\ 0 & 0 & 0 & 0 & 0 & s_3 \end{pmatrix}, \tag{13.38}$$

where s_i are very large numbers. As a result, the diffusion matrix (which when measured in units of $k_B T$) is just the inverse of the stiffness matrix

$$K^{-1} = D \approx \begin{pmatrix} B^{-1} & \mathbb{O} \\ \mathbb{O} & \mathbb{O} \end{pmatrix} \tag{13.39}$$

and if the minimal energy conformation is an arc-length-parameterized helix, we have the constant vector

$$\boldsymbol{\xi}_0^T = [\boldsymbol{\omega}_0^T, \mathbf{e}_3^T]. \tag{13.40}$$

As a specific example of (13.38) and (13.40) that has attracted attention in the recent literature is the Marko–Siggia DNA model [39]

$$B = \begin{pmatrix} a_0 + b_0^2/c_0 & 0 & b_0 \\ 0 & a_0 & 0 \\ b_0 & 0 & c_0 \end{pmatrix}, \quad \boldsymbol{\omega}_0 = \begin{pmatrix} 0 \\ 0 \\ \omega_0 \end{pmatrix}. \tag{13.41}$$

Sometimes it is convenient to define

$$\mathbf{b} \doteq B\omega_0.$$

This model for twist-bend coupling can be used either with extensible or inextensible versions of elastic-filament models of DNA.

[6] In the extensible case, the curve parameter s can be viewed as the arc length in the referential (undeformed) conformation of the filament, which does not necessarily mean that s will be the arc length in the pushed forward (deformed) version of the filament. However, in the inextensible model, s retains its role as the arc length after deformation since deformations are restricted to bending and twisting in that model.

The Inextensible Case

Under the assumption that the molecule is inextensible and shearless and all of the frames of reference are attached to the backbone with their local z axis pointing in the direction of the next frame, the constraint

$$\mathbf{a}(L) = \int_0^L \mathbf{u}(s)\,ds \quad \text{and} \quad \mathbf{u}(s) = R(s)\mathbf{e}_3 \tag{13.42}$$

is observed. This can be viewed as the inextensible filament "growing" along the direction indicated by the tangent for each value of arc length s up to a total length of L.

In this case, the stiffness matrix is 3 × 3 (e.g., of the form in (13.41)), and since stretch and shear degrees of freedom have effectively been frozen out, the resulting problem becomes one of minimizing

$$I = \frac{1}{2}\int_0^L [\boldsymbol{\omega}(s) - \boldsymbol{\omega}_0]^T B[\boldsymbol{\omega}(s) - \boldsymbol{\omega}_0]\,ds \tag{13.43}$$

subject to the constraints (13.42). Here, $\boldsymbol{\omega} = (R^T dR/ds)^\vee$ and $\boldsymbol{\omega}_0 = (R_0^T dR_0/ds)^\vee$ are angular velocities as seen in the body-fixed frame, where the arc length s replaces time as the independent variable.

Unlike the extensible problem, which was an unconstrained variational minimization problem on $SE(3)$, this is a constrained variational problem on $SO(3)$ and will therefore involve the use of Lagrange multipliers. The Euler–Poincaré equations for both cases are worked out in the following subsection.

13.7.2 Minimal Energy Conformations of DNA Loops with End Constraints

Here, the necessary conditions for coordinate-free variational minimization of the energy functionals described in the previous section are established. This is a straightforward application of the Euler–Poincaré equations. In the inextensible and shearless case, the group $G = SO(3)$, and in the extensible case, the group is $G = SE(3)$. In both cases there are six free degrees of freedom to specify the end position and orientation of the elastic filament. In the extensible case, these degrees of freedom correspond to the six scalar components of the initial conditions $\boldsymbol{\xi}(0)$, whereas in the inextensible case, they correspond to three scalar initial conditions $\boldsymbol{\omega}(0)$ and three scalar Lagrange multipliers (components of $\boldsymbol{\lambda}$) corresponding to the three constraints that define $\mathbf{a}(L)$ in (13.42).

Inextensible Case

Considering the case of (13.43) with the kinematic constraint of inextensibility (13.42), one writes (13.31) with $f = U$ for $i = 1, 2, 3$ together as the vector equation

$$B\dot{\boldsymbol{\omega}} + \boldsymbol{\omega} \times (B\boldsymbol{\omega} - \mathbf{b}) = \begin{pmatrix} -\boldsymbol{\lambda}^T A\mathbf{e}_2 \\ \boldsymbol{\lambda}^T A\mathbf{e}_1 \\ 0 \end{pmatrix}, \tag{13.44}$$

where a dot represents differentiation with respect to the arc length s, $\boldsymbol{\lambda} \in \mathbb{R}^3$ is the vector of Lagrange multipliers necessary to enforce the vector constraint in (13.42), and the right-hand side of (13.44) results from the fact that

$$E_i^r(\boldsymbol{\lambda}^T A\mathbf{e}_3) = \frac{d}{dt}\boldsymbol{\lambda}^T A(\mathbb{I} + tE_i)\mathbf{e}_3\bigg|_{t=0} = \boldsymbol{\lambda}^T AE_i\mathbf{e}_3 = \boldsymbol{\lambda}^T A(\mathbf{e}_i \times \mathbf{e}_3).$$

Equation (13.44) is solved iteratively subject to the initial conditions $\boldsymbol{\omega}(0) = \boldsymbol{\mu}$, which are varied together with the Lagrange multipliers until $\mathbf{a}(L)$ and $A(L)$ attain the desired values. $A(s)$ is computed from $\boldsymbol{\omega}(s)$ in (13.44) by integrating the matrix differential equation

$$\dot{A} = A\left(\sum_{i=1}^{3} \omega_i(s) E_i\right),$$

and $\mathbf{a}(L)$ is then obtained from (13.42). Numerical methods for updating $\boldsymbol{\mu}$ and $\boldsymbol{\lambda}$ so as to push the position and orientation of the distal end to specified values are described in [36].

Extensible Rods

From (13.31) and (13.37) one can obtain the following Euler–Lagrange equation for the extensible case:

$$K\dot{\boldsymbol{\xi}} + (K\boldsymbol{\xi} - \mathbf{k}) \wedge \boldsymbol{\xi} = \mathbf{0}, \tag{13.45}$$

where $\wedge$ is the product of infinitesimal rigid-body motions defined by

$$\begin{pmatrix} \boldsymbol{\omega}_1 \\ \mathbf{v}_1 \end{pmatrix} \wedge \begin{pmatrix} \boldsymbol{\omega}_2 \\ \mathbf{v}_2 \end{pmatrix} = \begin{pmatrix} \boldsymbol{\omega}_2 \times \boldsymbol{\omega}_1 + \mathbf{v}_2 \times \mathbf{v}_1 \\ \boldsymbol{\omega}_2 \times \mathbf{v}_1 \end{pmatrix}.$$

This wedge operator is related to the *ad* operator as

$$\boldsymbol{\xi}_1 \wedge \boldsymbol{\xi}_2 = -[ad(\boldsymbol{\xi}_2)]^T \boldsymbol{\xi}_1, \tag{13.46}$$

where $\boldsymbol{\xi}_i = [\boldsymbol{\omega}_i^T, \mathbf{v}_i^T]^T$, $i = 1, 2$, and the matrix of *ad* operator is defined as

$$[ad(\boldsymbol{\xi})] = \begin{pmatrix} \widehat{\boldsymbol{\omega}} & \mathbb{O} \\ \widehat{\mathbf{v}} & \widehat{\boldsymbol{\omega}} \end{pmatrix}.$$

Equation (13.45) is solved subject to the initial conditions $\boldsymbol{\xi}(0) = \boldsymbol{\eta} \in \mathbb{R}^6$. This, together with the kinematic condition

$$\dot{g} = g\left(\sum_{i=1}^{6} \xi_i E_i\right), \tag{13.47}$$

is integrated for $0 \leq s \leq L$ to define $g(\boldsymbol{\xi}, L)$. From this point, everything follows in exactly the same way as for the inextensible case. For any fixed value of $L \in \mathbb{R}^+$, (13.45) and (13.47) can together be thought of as defining a mapping from $\mathbb{R}^6$ (the initial conditions $\boldsymbol{\eta}$) into $SE(3)$. This mapping can be generated by numerically solving these ODEs. It is not a one-to-one mapping, and finding all values of initial conditions that map to a specific end position and orientation of the filament is quite challenging [36].

13.8 Chapter Summary

This chapter served as a brief review of variational calculus. Both the classical coordinate-dependent (Euler–Lagrange) and coordinate-free (Euler–Poincaré) equations were derived. Special emphasis was given to the application of these methods to deriving the necessary conditions for extremal conformations of models of double helical DNA molecules. Very recently, the same techniques have been applied to obtain the minimal energy shapes of concentric elastic tubes that have been proposed for use in minimally invasive surgical applications [49]. Variational calculus also provides a tool for articulating necessary conditions for generating geodesics (shortest paths) in Riemannian manifolds.

An important connection between Lie theory and variational calculus that was not discussed here is *Noether's theorem*, a recent description of which can be found in [46]. Basically, this theorem considers the case when the functional in a variational problem, J, is perturbed by the action of elements of a Lie group, $g = \exp X \in G$, resulting in $J' \doteq g \cdot J$. It states that in the case when $\|X\|$ is small, if $\Delta J \doteq J' - J$ depends on powers of the entries of X that are all higher than linear, then the Euler–Lagrange equations will have associated conservation laws. A classical example of this is the relationship between the conservation of angular momentum in physics and the invariance under changes in reference frame of the integral of rotational kinetic energy over any fixed time interval. Indeed, the search for symmetries has played a large role in physics in general over the past century. Symmetries in the Euler–Lagrange and Euler–Poincaré equations can be analyzed using methods from Lie theory, as was demonstrated for the case of geodesics on the sphere. This theory has been addressed in much more general and abstract contexts, as summarized in [30] in the language of jet bundles.

The emphasis of this chapter has been the formulation of variational problems on Lie groups. A whole other research area is that of accurate numerical solutions of the sorts of ODEs that result from variational calculus and optimal control problems on Lie groups. Although the topic of numerical solution methods is not the subject of this chapter, it nevertheless may be useful to have some pointers to the literature. For example, efforts that seek to integrate ODEs that evolve on rotation and unitary groups include [18, 20], and for rigid-body motion include [42, 43]. Closely related is the problem of evolution on ODEs the Stiefel and Grassmann manifolds [5]. Such problems arise in the study of neural networks [2, 22, 47]. Algorithms for reliably integrating ODEs on general Lie groups and other manifolds can be found in [17, 23, 24, 33, 40, 41]. The recent book by Hairer et al [29] provides a detailed and readable treatment of this subject with many more pointers to the literature than can be provided here.

As was demonstrated in this chapter, variational methods play an important role in mechanics. Lagrange's equations of motion will be encountered again in the next chapter, in the context of statistical mechanics.

13.9 Exercises

13.1. Following the discussion in Section 13.3.1, use the Euler–Lagrange equations to find the conditions describing geodesics on the unit sphere using the usual spherical-coordinate parameterization. Verify that the geodesic curvature is 0 for these curves. Verify that these curves correspond to segments of great circles (i.e., they lie on the circles resulting from intersecting a plane passing through the center of the sphere with the sphere itself).

13.2. Prove that the Euler–Lagrange equations for $f_1 = \frac{1}{2}\sqrt{\dot{\mathbf{q}}^T G(\mathbf{q})\dot{\mathbf{q}}}$ and $f_2 = (f_1)^2 = \frac{1}{4}\dot{\mathbf{q}}^T G(\mathbf{q})\dot{\mathbf{q}}$ reduce to the same thing. Is this true for other powers of f_1?

13.3. How does the Euler–Lagrange equation extend to the case of the extremization of a functional of the form

$$I = \int_a^b f(\mathbf{q}, \dot{\mathbf{q}}, \ddot{\mathbf{q}}, t)\, dt?$$

Hint: Integrate by parts twice.

13.4. Work out the details of the relationship between the function $c(\mathbf{a}, \dot{\mathbf{a}})$ in (13.9) and the original operator $\mathcal{D}f$ in (13.8).

13.5. Chapter 5 discussed, among other things, the differential geometry of arc-length-parameterized curves $\mathbf{x}(s)$. In that discussion, the tangent, normal, and binormal defined the orientation of a Frenet frame $Q_{FS} = [\mathbf{u}(s), \mathbf{n}_1(s), \mathbf{n}_2(s)] \in SO(3)$ attached to an arc-length-parameterized curve. Consider a unit-length curve segment defined by $s \in [0, 1]$. Suppose that $\mathbf{x}(0) = \mathbf{0}$, $Q_{FS}(0) = \mathbb{I}$, and we want to define reference frames relative to $g_{FS}(s) = (Q_{FS}(s), \mathbf{x}(s))$ of the form

$$g(t) = (Q_{FS}(s(t))R_3(\phi(t)), \mathbf{x}(s(t)))$$

that evolve so as to minimize

$$I = \int_0^1 \left\| g^{-1}\frac{dg}{dt} \right\|^2 dt$$

subject to the constraints $s(0) = 0$, $s(1) = 1$ and $\phi(0) = 0$, $\phi(1) = \phi_0$. Using classical variational calculus with coordinates s and ϕ write the Euler–Lagrange equations. Can these equations be solved?

13.6. Let $R \in SO(3)$ and $\boldsymbol{\omega}_r = (R^T\dot{R})^\vee$. The kinetic energy of a rigid body with moment of inertia $\mathcal{I}$ will be $T = \frac{1}{2}\boldsymbol{\omega}_r^T\mathcal{I}\boldsymbol{\omega}_r$. Show that the Euler–Poincaré equations corresponding to the action integral $I = \int_{t_0}^{t_1} T\,dt$ will give Euler's equations of motion for the case of no external moment:

$$\mathcal{I}\dot{\boldsymbol{\omega}} + \boldsymbol{\omega} \times (\mathcal{I}\boldsymbol{\omega}) = \mathbf{0}. \tag{13.48}$$

13.7. Given a rigid body with moment of inertia I, its kinetic energy will be $T = \frac{1}{2}\boldsymbol{\omega}_r^T\mathcal{I}\boldsymbol{\omega}_r$, where $\boldsymbol{\omega}_r = J_r(\mathbf{q})\dot{\mathbf{q}}$. Let $\mathbf{q} = [\alpha, \beta, \gamma]^T$, the ZXZ Euler angles. How do Lagrange's equations in the case when $V = 0$ compare with Euler's equations of motion for the same rigid body (with no external moments applied)?

13.8. In Chapter 10, the logarithm map was used to define a metric (measure of distance) between points in a Lie group. Another such metric on Lie groups is the *Carnot–Carathéodory distance* described in (13.36). Compare and contrast these for the groups $SO(3)$ and $SE(2)$ and choose your own basis elements and functions $\{\alpha_i(t)\}$.

13.9. Make it an exercise to show that when metric tensor is diagonal with $g_{ii}(\mathbf{q})$, a function only of q_i, or if $G(\mathbf{q}) = G_0$ is constant, that the Euler–Lagrange equations will give globally optimal solutions.

13.10. Show that the optimal roll and repramétrization problem can be solved sequentially either by first obtaining the optimal roll for an arc-length-parameterized curve followed by repraméterization of the curve or the curve can first be reparameterized followed by an adjustment to the roll.

13.11. Show that when $s_{ij}^k = -s_{ji}^k$, the geometric path (13.34) not only satisfies the necessary conditions for optimality (i.e., the Euler–Poincaré equation) but is in fact a path of globally minimal cost. Hint: Mimic the proof of Exercise 13.9.

13.12. A number of different forms of stereographic projection exist. In the version in which the horizontal plane intersects the unit sphere at its equator, lines passing through the south pole define a mapping between the open upper hemisphere and the open disk in the plane bounded by the equator of the sphere. In this problem, do the following: (a) Show that this mapping between the unit vector $\mathbf{u} = [u_1, u_2, u_3]^T$ in the upper hemisphere and the Cartesian coordinates $[y_1, y_2]$ in the plane is given by

$$y_1 = \frac{u_1}{1+u_3};\; y_2 = \frac{u_2}{1+u_3}; \Longleftrightarrow u_1 = \frac{2y_1}{1+y_1^2+y_2^2};\; u_2 = \frac{2y_2}{1+y_1^2+y_2^2};\; u_3 = \frac{1-y_1^2-y_2^2}{1+y_1^2+y_2^2}.$$

(b) Compute the metric tensor determinant $|G(y_1, y_2)|$.

13.13. Verify that the differential operators $\{\tilde{X}_i\}$ in (13.22) satisfy the commutation relations for $so(3)$ and show that the following do as well:

$$\begin{aligned}\tilde{Y}_1 &= x\frac{\partial}{\partial y} - y\frac{\partial}{\partial x},\\ \tilde{Y}_2 &= y\frac{\partial}{\partial z} - z\frac{\partial}{\partial y},\\ \tilde{Y}_3 &= x\frac{\partial}{\partial z} - z\frac{\partial}{\partial x}.\end{aligned}$$

Additionally, show that the conversion of these operators from Cartesian coordinates to spherical coordinates results in the operators

$$\begin{aligned}\tilde{Y}_1' &= \frac{\partial}{\partial \phi},\\ \tilde{Y}_2' &= \cot\theta\cos\phi\frac{\partial}{\partial \phi} + \sin\phi\frac{\partial}{\partial \theta},\\ \tilde{Y}_3' &= -\sin\phi\cot\theta\frac{\partial}{\partial \phi} + \cos\phi\frac{\partial}{\partial \theta},\end{aligned}$$

which also satisfy the commutation relations for $so(3)$.

References

1. Abraham, R., Marsden, J.E., *Foundations of Mechanics*, Benjamin/Cummings, San Mateo, CA, 1978.
2. Amari, S., "Natural gradient works efficiently in learning," *Neural Comput.*, 10(2), pp. 251–276, 1998.
3. Balaeff, A., Mahadevan, L., Schulten, K., "Modeling DNA loops using the theory of elasticity," E-print archive arXiv.org (http://arxiv.org/abs/physics/0301006, 2003).
4. Benham, C.J., Mielke, S.P.,"DNA mechanics," *Ann. Rev. Biomed. Engin.*, 7, pp. 21–53, 2005.
5. Bloch, A.M., Crouch, P.E., Sanyal, A.K., "A variational problem on Stiefel manifolds," *Nonlinearity*, 19(10), pp. 2247–2276, 2006.
6. Brechtken-Manderscheid, U., *Introduction to the Calculus of Variations*, Chapman & Hall, New York, 1991.
7. Bloch, A., Krishnaprasad, P.S., Marsden, J.E., Ratiu, T.S., "The Euler–Poincaré equations and double bracket dissipation," *Commun. Math. Phys.*, 175, p. 1, 1996.
8. Bluman, G.W., Anco, S.C., *Symmetry and Integration Methods for Differential Equations*, Applied Mathematical Sciences, Vol. 154, Springer, New York, 2002.
9. Boscain, U., Rossi, F., "Invariant Carnot–Carathéodory metrics on $S^3, SO(3), SL(2)$ and Lens Spaces," *SIAM J. Control Optimiz.*, 47(4), pp. 1851–1878, 2009.
10. Calin, O., Chang, D.-C., *Sub-Riemannian Geometry: General Theory and Examples*, Cambridge University Press, Cambridge, 2009.

11. Carathéodory, C., "Investigations into the foundations of thermodynamics," *Math. Ann.* 67, pp. 355–386, 1909.
12. Chirikjian, G.S., "The stochastic elastica and excluded-volume perturbations of DNA conformational ensembles," *Int. J. Non-Linear Mech.,* 43(10), pp. 1108–1120, 2008.
13. Chirikjian, G.S., *Theory and Applications of Hyper-Redundant Robotic Manipulators*, Division of Engineering and Applied Science, California Institute of Technology, June 1992. Available at http://etd.caltech.edu/etd/available/etd-11082006-132210/unrestricted/Chirikjian_gs_1992.pdf
14. Chirikjian, G.S., Burdick, J.W., "Kinematically optimal hyper-redundant manipulator configurations," *IEEE Trans. Robot. Autom.*, 11, p. 794, 1995.
15. Chow, W.L., "Systeme von linearen partiellen differential Gleichungen erster Ordnung," *Math. Ann.*, 117, pp. 98–105, 1939.
16. Coleman, B.D., Olson, W.K., Swigon, D., "Theory of sequence-dependent DNA elasticity," *J. Chem. Phys.*, 118, pp. 7127–7140, 2003.
17. Crouch, P.E., Grossman, R., "Numerical integration of ordinary differential equations on manifolds," *J. Nonlinear Sci.*, 3, pp. 1–33, 1993.
18. Dieci, L., Russell, R.D., van Vleck, E.S., "Unitary integrators and applications to continuous orthogonalization techniques," *SIAM J. Num. Anal.*, 31, pp. 261–281, 1994.
19. Dungey, N., ter Elst, A.F.M., Robinson, D.W., *Analysis on Lie Groups with Polynomial Growth*, Birkhäuser, Boston, 2003.
20. Edelman, A., Arias, T.A., Smith, S.T., "The geometry of algorithms with orthogonality constraints," *SIAM J. Matrix Anal. Appl.*, 20, pp. 303–353, 1998.
21. Ewing, G.M., *Calculus of Variations with Applications*, W.W. Norton and Co., New York, 1969.
22. Fiori, S., "Formulation and integration of learning differential equations on the Stiefel manifold," *IEEE Trans. Neural Networks* 16(6), pp. 1697–1701, 2005.
23. Forest, E., "Sixth-order Lie group integrators," *J. Comput. Phys.* 99, pp. 209–213, 1992.
24. Ge, Z., Marsden, J.E., "Lie-Poisson Hamilton-Jacobi theory and Lie-Poisson integrators," *Phys. Lett. A*, 133, pp. 134–139, 1988.
25. Gonzalez, O., Maddocks, J.H., "Extracting parameters for base-pair level models of DNA from molecular dynamics simulations," *Theor. Chem. Acc.*, 106(1–2), pp. 76–82, 2001.
26. Goyal, S., Perkins, N.C., Lee, C.L., "Nonlinear dynamics and loop formation in Kirchhoff rods with implications to the mechanics of DNA and cables," *J. Comp. Phys.*, 209, pp. 371–389, 2005.
27. Gromov, M., "Groups of polynomial growth and expanding maps," *Inst. Hautes Études Sci. Publ. Math.*, 53(1), pp. 53–78, 1981.
28. Gruver, W.A., Sachs, E., *Algorithmic Methods in Optimal Control*, Pitman Publishing, Boston, 1980.
29. Hairer, E., Lubich, C., Wanner, G., *Geometric Numerical Integration: Structure-Preserving Algorithms for Ordinary Differential Equations*, 2nd ed., Springer, New York, 2006.
30. Hermann, R., *Geometry, Physics, and Systems*, Marcel Dekker, New York, 1973.
31. Holm, D.D., Marsden, J.E., Ratiu, T.S., "The Euler–Poincaré equations and semidirect products with applications to continuum theories," *Adv. Math.*, 137 p. 1, 1998.
32. Hörmander, L., "Hypoelliptic second-order differential equations," *Acta Math.*, 119, pp. 147–171, 1967.
33. Iserles, A., Munthe-Kaas, H.Z., Nørsett, S.P., Zanna, A., "Lie group methods," *Acta Numerica*, 9, pp. 215–365, 2000.
34. Junkins, J.L., *Optimal Spacecraft Rotational Maneuvers*, Studies in Astronautics Vol. 3, Elsevier, Amsterdam, 1986.
35. Kamien, M.I., Schwartz, N.L., *Dynamic Optimization: The Calculus of Variations and Optimal Control in Economics and Management*, North-Holland, New York, 1991.
36. Kim, J.-S., Chirikjian, G.S., "Conformational analysis of stiff chiral polymers with end constraints," *Mol. Simul.*, 32(14), pp. 1139–1154, 2006.

37. Koh, S., Chirikjian, G.S., Ananthasuresh, G.K., "A Jacobian-based algorithm for planning attitude maneuvers using forward and reverse rotations," *ASME J. Comput. Nonlinear Dynam.*, 4(1), pp. 1–12, 2009.
38. Le Donne, E., *Lecture Notes on sub-Riemannian Geometry.* Available at http://www.math.ethz.ch/∼ledonne/.
39. Marko, J.F., Siggia, E.D., "Bending and twisting elasticity of DNA," *Macromolecules*, 27, pp. 981–988, 1994
40. Marsden, J.E., Pekarsky, S., Shkoller, S., "Discrete Euler–Poincaré and Lie–Poisson equations," *Nonlinearity*, 12, pp. 1647–1662, 1999.
41. Marsden, J.E., West, M., "Discrete mechanics and variational integrators," *Acta Numerica*, 10, pp. 357–514, 2001.
42. McLachlan, R.I., "Explicit Lie–Poisson integration and the Euler equations," *Phys. Rev. Lett.*, 71, pp. 3043–3046, 1993.
43. McLachlan, R.I., Zanna, A., "The discrete Moser–Veselov algorithm for the free rigid body, revisited," *Found. Comput. Math.*, 5, pp. 87–123, 2005.
44. Mitchell, J., "On Carnot–Carathéodory metrics," *J. Diff. Geom.,* 21, pp. 35–45, 1985.
45. Montgomery, R., *A Tour of Sub-Riemannian Geometries, Their Geodesics and Applications*, Math Surveys and Monographs Vol. 91, American Mathematical Society, Providence, RI, 2002.
46. Neuenschwander, D.E., *Emmy Noether's Wonderful Theorem*, Johns Hopkins University Press, Baltimore, 2010.
47. Oja, E., "Neural networks, principal components, and subspaces," *Int. J. Neural Syst.*, 1, pp. 61–68, 1989.
48. Poincaré, H. "Sur une forme nouvelle des equations de la mechanique," *Cr. Hebd. Acad. Sci.*, 132, p. 369, 1901.
49. Rucker, C., Webster, R.J., III, Chirikjian, G.S., Cowan, N.J., "Equilibrium conformations of concentric-tube continuum robots," *Int. J. Robot. Res.*, 29(10), pp. 1263–1280, 2010.
50. Stephani, H., *Differential Equations: Their Solution Using Symmetries*, M. Maccallum, ed., Cambridge University Press, Cambridge, 1989.
51. Varopoulos, N. Th., "Sobolev inequalities on Lie groups and symmetric spaces," *J. Funct. Anal.*, 86, pp. 19–40, 1989.
52. Varopoulos, N. Th., Saloff-Coste, L., Coulhon, T., *Analysis and Geometry on Groups*, Cambridge University Press, Cambridge, 1992.
53. Wiggins, P.A., Phillips, R., Nelson, P.C., "Exact theory of kinkable elastic polymers," E-print archive arXiv.org (arXiv:cond-mat/0409003 v1. 31 Aug. 2004.)

14

Statistical Mechanics and Ergodic Theory

The purpose of this chapter is to tie together a number of concepts that have been presented earlier. Stochastic models and information-theoretic quantities such as entropy are not disjoint concepts. They overlap nicely in the context of statistical mechanics, where stochastic models describe general classes of equations of motion of physical systems.

The concept of entropy used in information theory has a form that is reminiscent of entropy in statistical mechanics. In fact, this is one reason why Shannon used that term. However, the entropy of statistical mechanics demonstrates an invariance under coordinate transformations that does not generally hold for continuous multi-dimensional information-theoretic entropy. This results from the special properties of "phase space" as defined in the Hamiltonian formulation of mechanics.

The main points to take away from this chapter are as follows:

- Equations of motion from classical mechanics, when forced by white noise, lead to Fokker–Planck equations that have the Maxwell–Boltzmann distribution as their steady-state solution.
- Entropy in statistical mechanics, unlike the continuous entropy of information theory, has the special property that it is invariant under coordinate changes. Additionally, this property results from the special nature of so-called phase space.
- The concept of ergodicity encountered in earlier chapters in purely random contexts can be modified to include deterministic phenomena, resulting in a field of study called ergodic theory.
- Information theory and statistical mechanics share more in common than the word "entropy" defined by similar-looking equations, and although care must be taken not to confuse these two different (but related) concepts, there are certain problems (in particular in biology and the thermodynamics of computation and communication) where both apply.

Section 14.1 reviews the classical mechanics of systems driven by conservative forces. In Section 14.2 relationships among classical mechanics, stochastic models, and statistical mechanics are established. Section 14.3 discusses the convergence of Fokker–Planck equations associated with stochastic mechanical models to the Maxwell–Boltzmann distribution of statistical mechanics under special conditions. Section 14.4 discusses a particular problem in the statistical mechanics of rigid molecules forced by Brownian motion. When such molecules interact according to the molecular theory of solvation, the concept of convolution on the group of rigid-body motions arises in a natural way. Section 14.5 uses DNA as an example to demonstrate the general principles articulated

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_5,

in previous sections. Both the statistical mechanics of a continuum elastic filament model and a multi-rigid-body model are discussed. Section 14.6 provides a brief review of ergodic theory and provides pointers to the literature. Finally, in Sections 14.7 and 14.8 the chapter is summarized and exercises are provided.

14.1 Mechanics of Conservative Systems

Statistical Mechanics builds on Classical Mechanics, which is reviewed here.

14.1.1 Lagrangian Mechanics

The kinetic and potential energies of a classical conservative mechanical system are respectively of the form

$$T = \frac{1}{2}\dot{\mathbf{q}}^T M(\mathbf{q})\dot{\mathbf{q}} \quad \text{and} \quad V = V(\mathbf{q}), \tag{14.1}$$

where $\mathbf{q} = [q_1, \ldots, q_n]^T$ is a vector of generalized coordinates and $M(\mathbf{q}) = M^T(\mathbf{q})$ is the positive semi-definite mass matrix that is a function of the coordinates. The *Lagrangian* is defined as

$$L(\mathbf{q}, \dot{\mathbf{q}}) = T(\mathbf{q}, \dot{\mathbf{q}}) - V(\mathbf{q}). \tag{14.2}$$

Lagrange's equations of motion for such a system can be written as

$$\frac{d}{dt}\left(\frac{\partial T}{\partial \dot{q}_i}\right) - \frac{\partial T}{\partial q_i} + \frac{\partial V}{\partial q_i} = 0 \quad \text{or} \quad \frac{d}{dt}\left(\frac{\partial L}{\partial \dot{q}_i}\right) - \frac{\partial L}{\partial q_i} = 0. \tag{14.3}$$

The derivation these equations directly from Newton's laws can be found in many books on Classical Mechanics. Alternatively, it can be viewed as a direct application of the variational methods discussed in the previous chapter via the so-called principle of least action.

As a simple example, consider a pendulum consisting of s massless rod of length L with point mass m concentrated at the distal end. The pendulum is assumed to have a frictionless hingelike fulcrum that only allows planar motion. Denoting the angle that the rod makes with the vertical as θ, the kinetic energy can be written as $T = \frac{1}{2}mL^2\dot{\theta}^2$ and the potential energy is $V = mgL(1 - \cos\theta)$. In this one-degree-of-freedom example, there is a single Lagrange equation of motion of the form $\ddot{\theta} + (g/L)\sin\theta = 0$ (which has been simplified by dividing out the factor of mL^2 in both terms in (14.3) for the case when $q_i = \theta$).

14.1.2 Conjugate Momenta and Hamiltonian Mechanics

Corresponding to the generalized coordinates are quantities called *conjugate momenta*, which are defined as

$$p_i \doteq \frac{\partial T}{\partial \dot{q}_i} \quad \text{or} \quad \mathbf{p} = M(\mathbf{q})\dot{\mathbf{q}}. \tag{14.4}$$

In particular,

$$\frac{\partial T}{\partial q_i} = \frac{1}{2}\sum_{j,k=1}^{n} \frac{\partial m_{jk}}{\partial q_i}\dot{q}_j\dot{q}_k = \frac{1}{2}\dot{\mathbf{q}}^T\frac{\partial M}{\partial q_i}\dot{\mathbf{q}} \tag{14.5}$$

$$= \frac{1}{2}\mathbf{p}^T M^{-1}\frac{\partial M}{\partial q_i}M^{-1}\mathbf{p} = -\frac{1}{2}\mathbf{p}^T\frac{\partial M^{-1}}{\partial q_i}\mathbf{p} \tag{14.6}$$

$$= -\frac{1}{2}\sum_{j,k=1}^{n}\frac{\partial m_{jk}^{-1}}{\partial q_i}p_j p_k. \tag{14.7}$$

The second equality in (14.6) follows from taking the partial derivative of $MM^{-1} = \mathbb{I}$ with respect to q_i. Here, $m_{jk}^{-1} \doteq [M^{-1}]_{jk}$ denotes the jkth element of the matrix M^{-1}.

This means that the original n second-order scalar differential equations of motion in the variable $\mathbf{q}$ can be replaced by $2n$ first-order equations in the variables $\mathbf{p}$ and $\mathbf{q}$. In particular, the *Hamiltonian* is defined as the total system energy written in terms of the variables $\mathbf{p}$ and $\mathbf{q}$:

$$H(\mathbf{p},\mathbf{q}) \doteq T(\mathbf{q}, M^{-1}(\mathbf{q})\mathbf{p}) + V(\mathbf{q}) = \frac{1}{2}\mathbf{p}^T M^{-1}(\mathbf{q})\,\mathbf{p} + V(\mathbf{q}). \tag{14.8}$$

Note that there is a plus sign in (14.8), whereas there is a minus sign in (14.2).

Combining the definition in (14.8) with (14.7) and (14.4) results in *Hamilton's equations of motion*:

$$\boxed{\frac{dp_i}{dt} = -\frac{\partial H}{\partial q_i} \quad \text{and} \quad \frac{dq_i}{dt} = \frac{\partial H}{\partial p_i}.} \tag{14.9}$$

Many interesting properties result from (14.9). For example, the time derivative of a function $f(\mathbf{p},\mathbf{q},t)$ can be computed using a modified version of the usual chain rule as

$$\frac{df}{dt} = \frac{\partial f}{\partial t} + \sum_{i=1}^{n}\left(\frac{\partial f}{\partial q_i}\frac{dq_i}{dt} + \frac{\partial f}{\partial p_i}\frac{dp_i}{dt}\right)$$

$$= \frac{\partial f}{\partial t} + \sum_{i=1}^{n}\left(\frac{\partial f}{\partial q_i}\frac{\partial H}{\partial p_i} - \frac{\partial f}{\partial p_i}\frac{\partial H}{\partial q_i}\right). \tag{14.10}$$

In general, the *Poisson bracket* of two functions $f_1(\mathbf{p},\mathbf{q},t)$ and $f_2(\mathbf{p},\mathbf{q},t)$ is defined as

$$\{f_1, f_2\} \doteq \sum_{i=1}^{n}\left(\frac{\partial f_1}{\partial q_i}\frac{\partial f_2}{\partial p_i} - \frac{\partial f_1}{\partial p_i}\frac{\partial f_2}{\partial q_i}\right) = -\{f_2, f_1\}. \tag{14.11}$$

This means that (14.10) can be written as

$$\frac{df}{dt} = \frac{\partial f}{\partial t} - \{H, f\}. \tag{14.12}$$

The Poisson bracket also satisfies the Jacobi identity

$$\{f_1,\{f_2,f_3\}\} + \{f_2,\{f_3,f_1\}\} + \{f_3,\{f_1,f_2\}\} = 0$$

and the product rule

$$\{f_1, f_2 f_3\} = \{f_1, f_2\}f_3 + f_2\{f_1, f_3\}$$

(where the operator $\{f_1, \cdot\}$ takes the place of the derivative being applied to the product $f_2 f_3$).

The $2n$-dimensional phase space has some interesting properties which make it more convenient to describe dynamical systems than the $2n$-dimensional space consisting of generalized coordinates and their rates. The properties of phase space are explained in the following subsections.

14.1.3 Properties of Volume in Phase Space

Suppose that two different sets of generalized coordinates are used to describe the same mechanical system. Let $\mathbf{q}$ and $\mathbf{q}'$ respectively denote the vectors consisting of these coordinates. The kinetic energy of the system is written as

$$T = \frac{1}{2}\dot{\mathbf{q}}'^T M'(\mathbf{q}')\dot{\mathbf{q}}' = \frac{1}{2}\dot{\mathbf{q}}^T M(\mathbf{q})\dot{\mathbf{q}},$$

which means that

$$M(\mathbf{q}) = J^T(\mathbf{q}) M'(\mathbf{q}'(\mathbf{q})) J(\mathbf{q}),$$

where

$$J(\mathbf{q}) = \frac{\partial \mathbf{q}'}{\partial \mathbf{q}^T}$$

is the Jacobian matrix relating the rates of change of the coordinate vectors:

$$\dot{\mathbf{q}}' = J(\mathbf{q})\,\dot{\mathbf{q}}.$$

Since conjugate momentum is defined as $\mathbf{p} = \partial T/\partial \dot{\mathbf{q}}$, the conjugate momentum in the two different coordinates are related as

$$\mathbf{p} = M(\mathbf{q})\,\dot{\mathbf{q}}, \quad \mathbf{p}' = M'(\mathbf{q}')\,\dot{\mathbf{q}}' = J^{-T}(\mathbf{q}) M(\mathbf{q})\,\dot{\mathbf{q}},$$

which means that

$$\mathbf{p}' = J^{-T}(\mathbf{q})\,\mathbf{p}.$$

Therefore, the volume elements in the two phase spaces are related as

$$d\mathbf{p}'\,d\mathbf{q}' = \begin{vmatrix} J^{-T}(\mathbf{q}) & \partial(J^{-T}(\mathbf{q})\mathbf{p})/\partial \mathbf{q}^T \\ \mathbb{O} & J(\mathbf{q}) \end{vmatrix} d\mathbf{p}\,d\mathbf{q}.$$

The above determinant is equal to 1 since it is upper triangular, and the determinants of the diagonal blocks cancel, and so the very special property of invariance of phase volume with respect to coordinate changes results:

$$\boxed{d\mathbf{p}'\,d\mathbf{q}' = d\mathbf{p}\,d\mathbf{q}.} \tag{14.13}$$

14.1.4 Liouville's Theorem

The emphasis of the previous subsection was that the expression for the volume element in phase space is invariant under the choice of coordinates used. In contrast, *Liouville's theorem* can be viewed as a statement about how regions in phase space flow according to Hamilton's equations of motion. Given an initial ensemble consisting of an infinite number of *noninteracting* copies of the same conservative mechanical system that initially populate an arbitrary region in phase space, then the evolution of the shape of this region over time (with each copy of the mechanical system being governed by Hamilton's equations of motion) will be such that the volume of the region does not change.

Let $\mathbf{p}$ and $\mathbf{q}$ denote the values of conjugate momenta and generalized coordinates at a particular time t. At an instant later, $t' = t + dt$, the corresponding quantities are obtained from Hamilton's equations (14.9) as

$$p_i' = p_i - \frac{\partial H}{\partial q_i}\, dt \qquad \text{and} \qquad q_i' = q_i + \frac{\partial H}{\partial p_i}\, dt.$$

The volume elements are related as

$$dp_1' \cdots dp_n'\, dq_1' \cdots dq_n' = \frac{\partial(p_1', \ldots, p_n'; q_1', \ldots, q_n')}{\partial(p_1, \ldots, p_n; q_1, \ldots, q_n)}\, dp_1 \cdots dp_n\, dq_1 \cdots dq_n. \tag{14.14}$$

The entries in the Jacobian matrix will be of the form

$$\frac{\partial p_i'}{\partial p_j} = \delta_{ij} - \frac{\partial^2 H}{\partial q_i \partial p_j}\, dt, \qquad \frac{\partial q_i'}{\partial p_j} = \frac{\partial^2 H}{\partial p_i \partial p_j}\, dt$$

and

$$\frac{\partial p_i'}{\partial q_j} = -\frac{\partial^2 H}{\partial q_i \partial q_j}\, dt, \qquad \frac{\partial q_i'}{\partial q_j} = \delta_{ij} + \frac{\partial H}{\partial p_i \partial q_j}\, dt.$$

The Jacobian matrix relating $(\mathbf{p}', \mathbf{q}')$ to $(\mathbf{p}, \mathbf{q})$ will then be of the form $J_{ij} = \delta_{ij} + a_{ij}\, dt$, where $A = [a_{ij}]$ consists of all terms that are multiplied by dt. The Jacobian determinant will be of the form $|J| = \text{tr}(A)\, dt + O(dt^2)$. From the above equations, it is clear that $\text{tr}(A) = 0$ and, therefore, (14.14) can be written in the form of (14.13) for each infinitesimal time step, even though (14.13) is for a change of coordinates at a particular time and (14.14) is for the evolution of a system between two different times.

Extending this argument by dt over an infinite number of time steps means that any initial region in phase space will flow and change shape governed by Hamilton's equations, but the volume of that initial region will remain the same under this flow.

14.2 Stochastic Mechanics

In the previous section the only forces considered were those that are conservative. In the case when an ensemble of mechanical systems (such as molecules) are allowed to interact by either directly bumping into each other, or indirectly through the action of surrounding solvent, then energy can be transferred between the different copies of the system. In this context, each individual mechanical system is no longer conservative, but under certain conditions, the energy in the whole system will be conserved. This section examines the modification of equations of motion to include viscous and stochastic forcing in which these two nonconservative forces balance each other and, therefore, drive any initial ensemble to a stable equilibrium distribution.

14.2.1 Stochastic Equations of Motion

If the conservative systems discussed in Section 14.1 are modified to include viscous dissipation, then a *Rayleigh dissipation function* of the form $R = \frac{1}{2}\dot{\mathbf{q}}^T C(\mathbf{q})\dot{\mathbf{q}}$ can be defined, where $C(\mathbf{q}) = C^T(\mathbf{q})$ is a positive semi-definite damping matrix.

Lagrange's equations of motion are modified to include viscous dissipation and other nonconservative forces as

$$\frac{d}{dt}\left(\frac{\partial T}{\partial \dot{q}_i}\right) - \frac{\partial T}{\partial q_i} + \frac{\partial V}{\partial q_i} + \frac{\partial R}{\partial \dot{q}_i} = \tau_i, \tag{14.15}$$

where τ_i is any remaining generalized force (other than conservative and viscous forces) that acts on the coordinate q_i. This generalized force can be thought of as the sum of all projections of physical forces along the direction of motion described by the coordinate. Thus, this generalized force could be a force in the usual sense if the coordinates are Cartesian positions, it could be a torque if the coordinate is an angle defining a rotational motion, or it could be a more exotic and less easily described quantity. Equation (14.15) can be thought of as Newton's equations projected onto an arbitrary coordinate system.

14.2.2 Stochastically Forced Systems

Lagrange's equations of motion with viscous friction and external forcing as written in (14.15) can be recast in the Hamiltonian formulation. Suppose that the generalized forcing corresponds to white noise that is colored by a configuration-dependent matrix, $B(\mathbf{q})$, so that $\tau_i = \sum_j b_{ij} n_j$, where $dw_i = n_i\, dt$. Using the definition of conjugate momenta and multiplying (14.15) by dt and then moving everything except the first term to the right side of the equation results in

$$dp_i = -\frac{1}{2}\sum_{j,k=1}^{n} \frac{\partial m_{jk}^{-1}}{\partial q_i} p_j p_k\, dt - \frac{\partial V}{\partial q_i} dt - \sum_{j,k=1}^{n} c_{ij} m_{jk}^{-1} p_k\, dt + \sum_{j=1}^{n} b_{ij}\, dw_j. \tag{14.16}$$

Multiplying both sides of (14.4) by dt gives

$$dq_i = \sum_{j=1}^{n} m_{ij}^{-1} p_j\, dt. \tag{14.17}$$

Equations (14.16) and (14.17) represent a system of $2n$ nonlinear stochastic differential equations in the generalized coordinates and conjugate momenta.

A natural question to ask is if this is an Itô or Stratonovich stochastic differential equation. Actually, the answer is that this is one of those special cases where it does not matter. The reason is that although the stochastic forcing is weighted by the configuration-dependent matrix $B(\mathbf{q})$, this only appears in the equation defining the evolution of $\mathbf{p}$, and B does not depend on $\mathbf{p}$. Additionally, the equation defining the evolution of $\mathbf{q}$ has no $\mathbf{q}$-dependent stochastic forcing (in fact it has no stochastic forcing at all).

14.3 Fokker–Planck Equations on Phase Space

Equations (14.16) and (14.17) can be written together as

$$\begin{pmatrix} d\mathbf{q} \\ d\mathbf{p} \end{pmatrix} = \begin{pmatrix} \mathbf{a}^{(q)}(\mathbf{p}, \mathbf{q}) \\ \mathbf{a}^{(p)}(\mathbf{p}, \mathbf{q}) \end{pmatrix} dt + \begin{pmatrix} \mathbb{O} & \mathbb{O} \\ \mathbb{O} & B(\mathbf{q}) \end{pmatrix} \begin{pmatrix} d\mathbf{w}' \\ d\mathbf{w} \end{pmatrix} \tag{14.18}$$

(where $d\mathbf{w}'$ could be replaced with any vector rather than unit strength white noises since it multiplies zeros).

The entries in the vector-valued function, $\mathbf{a}^{(q)}$ and $\mathbf{a}^{(p)}$, are respectively

$$a_i^{(q)} \doteq \sum_{j=1}^{n} m_{ij}^{-1} p_j,$$

$$a_i^{(p)} \doteq -\frac{1}{2}\sum_{j,k=1}^{n} \frac{\partial m_{jk}^{-1}}{\partial q_i} p_j p_k - \frac{\partial V}{\partial q_i} - \sum_{j,k=1}^{n} c_{ij} m_{jk}^{-1} p_k.$$

The Fokker–Planck equation corresponding to (14.18), which together with an initial distribution $f_0(\mathbf{q},\mathbf{p})$ defines the family of time-evolving pdfs $f(\mathbf{q},\mathbf{p};t)$, is

$$\frac{\partial f}{\partial t} + \sum_{i=1}^{n} \frac{\partial}{\partial q_i}\left(a_i^{(q)} f\right) + \sum_{i=1}^{n} \frac{\partial}{\partial p_i}\left(a_i^{(p)} f\right) - \frac{1}{2}\sum_{k=1}^{n}\sum_{i,j=1}^{n} \frac{\partial^2}{\partial p_i \partial p_j}\left(b_{ik} b_{kj}^T f\right) = 0. \tag{14.19}$$

14.3.1 The Maxwell–Boltzmann Distribution

A natural question to address is how $f(\mathbf{q},\mathbf{p};t)$, the solution of (14.19), evolves over time. In particular, does it converge to an equilibrium distribution (i.e., one that does not depend on time), and if so, what is the rate of convergence?

The answers to these questions require that the random forces that cause an ensemble of sample paths to diffuse must, in a sense, balance with the conservative forces defined by the potential energy, which tend to drive the paths toward the regions with lowest potential energy. When the matrix $B(\mathbf{q})$ satisfies particular conditions, this tug of war between forces that favor diffusion and those that favor concentration balance exactly. In this case, a stable limiting distribution

$$f_\infty(\mathbf{q},\mathbf{p}) \doteq \lim_{t\to\infty} f(\mathbf{q},\mathbf{p};t)$$

is obtained, which is independent of the initial distribution $f_0(\mathbf{q},\mathbf{p})$.

Using arguments that do not involve stochastic differential equations (SDEs), it is known in the field of statistical mechanics that the equilibrium distribution of an ensemble of identical mechanical systems subjected to a heat bath is the *Maxwell–Boltzmann distribution*:

$$f_\infty(\mathbf{q},\mathbf{p}) = \frac{1}{Z}\exp(-\beta H(\mathbf{p},\mathbf{q}))\,, \tag{14.20}$$

where the shorthand $\beta \doteq 1/k_B T$ is used, k_B is Boltzmann's constant, and T is temperature measured in degrees Kelvin. The *partition function* is defined as

$$Z = \int_{\mathbf{q}}\int_{\mathbf{p}} \exp(-\beta\, H(\mathbf{p},\mathbf{q}))\; d\mathbf{p}\, d\mathbf{q}. \tag{14.21}$$

It is worth noting that this integral is really an approximation to a discrete sum over micro states (as originally formulated by Planck), and the pdf $f_\infty(\mathbf{q},\mathbf{p})$ is an approximation to a probability distribution over these microstates. However, when β is sufficiently small, this continuum approximation can be used without difficulties.

Substituting (14.20) into (14.19) and calculating all of the partial derivatives results in the following condition that must hold in order for the Maxwell–Boltzmann distribution to be the equilibrium solution of (14.19):

$$\boxed{2\cdot C = \beta\cdot BB^T.} \tag{14.22}$$

One form of the *fluctuation-dissipation theorem* states that in order for a stochastic system to attain an equilibrium distribution, the magnitude of the random forcing and viscous dissipation terms must be related. Indeed, (14.22) is just such a statement.

14.3.2 Averages with Respect to the Maxwell–Boltzmann Distribution

Let the equilibrium average of any function on phase space, $a(\mathbf{p},\mathbf{q})$, be defined as

$$\langle a \rangle \doteq \int_{\mathbf{q}} \int_{\mathbf{p}} a(\mathbf{p},\mathbf{q}) f_{\infty}(\mathbf{p},\mathbf{q})\, d\mathbf{p}\, d\mathbf{q}. \tag{14.23}$$

For example, the average of the Hamiltonian is called the *energy* of the system, E, and it can be shown that

$$E \doteq \langle H \rangle = -\frac{\partial(\log Z)}{\partial \beta}. \tag{14.24}$$

The reason why this is written as a partial derivative (rather than a full one) with respect to β is that in thermodynamic applications H, and hence Z, can depend on parameters imposed from outside the system. For example, the volume in a piston can be changed or an external potential field can be applied. Writing this as a partial derivative leaves room for allowing for such variable parameters.

The *Helmholtz free energy* of a system is defined as [92]

$$F \doteq E - TS = -\frac{1}{\beta}\log Z. \tag{14.25}$$

In contrast, the *Gibbs free energy* is defined as

$$G \doteq F + pV, \tag{14.26}$$

where p is the pressure and V is the volume in the container containing the collection of molecules.

Sometimes it is convenient to write the $2n$ phase variables as one long vector, $\mathbf{x} = (\mathbf{p}^T, \mathbf{q}^T)^T = (x_1, \ldots, x_{2n})^T$. The *equipartition theorem* states that [35, 65]

$$\left\langle x_m \frac{\partial H}{\partial x_n} \right\rangle = \frac{1}{\beta}\delta_{mn}. \tag{14.27}$$

It is easy to prove this by integration by parts, and this is left as an exercise. This result is very general.

In the special case when the mass matrix is constant, $M(\mathbf{q}) = M_0$, and the potential is quadratic, $V(\mathbf{q}) = \frac{1}{2}\mathbf{q}^T K_0 \mathbf{q}$, the Maxwell–Boltzmann distribution becomes a Gaussian distribution, and it is possible to use (14.27) to compute

$$\langle H \rangle = \frac{n}{\beta}. \tag{14.28}$$

Furthermore,

$$\langle H \rangle = \langle T \rangle + \langle V \rangle \qquad \text{and} \qquad \langle T \rangle = \langle V \rangle\,. \tag{14.29}$$

The second equality follows from (14.27) because in the Hamiltonian, $H = \frac{1}{2}\mathbf{x}^T(M_0^{-1} \oplus K_0)\mathbf{x}$, the mass and stiffness matrices appear as a direct sum. If the system is composed of N particles each with three translational degrees of freedom, then $n = 3N$. If M_0 is diagonal, T can be separated further into $3n$ individual contributions of kinetic energy: $(T_i)_x$, $(T_i)_y$, and $(T_i)_z$, for $i = 1, \ldots, N$. Since M_0 is diagonal, it follows that $(T_i)_x = (T_j)_y = (T_k)_z$ for $i, j, k = 1, \ldots, N$. If modal coordinates are used (so that K_0 is diagonal), then the energy in each of these coordinates must be equal to each other, and each of these must also be equal to the kinetic energy associated with each coordinate. Thus, the kinetic and potential energies can be subdivided into $6N$ contributions, each of which is equal to the others. Additionally, if these quantities are grouped together in larger collections and added in equal numbers, then the energy in each of these collections will be equal. This statement, which includes (14.29), is a somewhat different statement than (14.28), which is also referred to as the equipartition theorem.

The *Gibbs formula* for entropy of an ensemble described by $f_\infty(\mathbf{p}, \mathbf{q})$ is[1]

$$S = -k_B \int_{\mathbf{q}} \int_{\mathbf{p}} f_\infty(\mathbf{p}, \mathbf{q}) \log f_\infty(\mathbf{p}, \mathbf{q})\, d\mathbf{p}\, d\mathbf{q}. \tag{14.30}$$

It can be shown (and is left as an exercise) that this entropy can be computed from the partition function defined in (14.21) by computing partial derivatives as

$$S = k_B \log Z + \frac{1}{\beta Z} \frac{\partial Z}{\partial T} = k_B \left[\log Z - \beta \frac{\partial (\log Z)}{\partial \beta} \right]. \tag{14.31}$$

14.3.3 Ergodic Properties of Some Stochastic Mechanical Systems

An immediate implication of the convergence of the solution of the Fokker–Planck equation to the Maxwell–Boltzmann distribution when (14.22) holds is that solutions to the stochastic differential equation (14.18) that are run for a sufficiently long time will have the same statistics as the Maxwell–Boltzmann distribution; that is, a single trajectory will meander as if at each step in time a sample is drawn at random from $f(\mathbf{p}, \mathbf{q}; dt)$. According to the solution of the Fokker–Planck equation, after a sufficiently large number of steps, this will converge to the Maxwell–Boltzmann distribution. After that point, the single trajectory can be viewed as a sample of Maxwell–Boltzmann distribution, and if a sufficiently large number of samples are taken in this regime, then the contributions due to samples from earlier in the trajectory will be washed out.

In other words, imagine taking a single very long trajectory and dividing it into an ensemble of shorter (although still very long) trajectories, each starting at a different initial point in phase space corresponding to where the prior subtrajectory finished. The collection of initial values can be used to define a histogram that is normalized as a probability density. This can be considered as an initial distribution $f_0(\mathbf{p}, \mathbf{q})$. At all future times, similar histograms can be constructed and viewed as $f(\mathbf{p}, \mathbf{q}; t)$. It is acceptable to cut up trajectories in this way because the Fokker–Planck equation has autonomous coefficients; that is, the time dependence is only indirect through $\mathbf{p} = \mathbf{p}(t)$ and $\mathbf{q} = \mathbf{q}(t)$, not due to any direct functional dependence of coefficients on time.

If each of the trajectories in the resulting ensemble is long enough, then $f(\mathbf{p}, \mathbf{q}; t)$ will approximate $f_\infty(\mathbf{p}, \mathbf{q})$; that is, there is no difference between recording the locations in phase space visited by a single very long trajectory and chopping this trajectory up into a very large number of shorter (although still very long) trajectories starting from many different initial conditions, and recording the phase states visited. This argument holds because of the existence of a stable limiting distribution. This is an example of ergodicity since the result of multiple sample paths and of a single very long one are the same.

[1] Here, and everywhere in statistical mechanics, $\log = \log_e$ is the natural logarithm function.

The same argument could not be made if, for example, the Fokker–Planck equation corresponded to a purely diffusive process. This is because, in that case, the solution continues to evolve as time goes to infinity. However, even for a purely diffusive process, it is possible to divide a trajectory of length T into N subtrajectories, and if each of these is shifted so that its initial value is identified with, say, $(\mathbf{p}, \mathbf{q}) = (\mathbf{0}, \mathbf{0})$, then the histograms formed along each point in the time interval $0 < t < T/N$ would correspond to the solution of the Fokker–Planck equation for that value of t.

This section has focused on statistical mechanics from the point of view of classical mechanical systems subjected to forcing by Wiener process noise. For other introductions to statistical mechanics (and stochastic mechanics) from several different perspectives, see [10, 20, 22, 28, 33, 41, 43, 52, 57, 60, 70, 86]. The following section will focus on a particular problem in statistical mechanics relating to rigid-body models of molecules.

14.4 Equilibrium Statistical Mechanics of Rigid-Body Molecules

Although the classical theory of statistical mechanics is build on coordinate-dependent descriptions of the state of a system using generalized coordinates and momenta, it is possible to restate statistical mechanics using terminology from the theory of Lie groups (in analogy with what was done with variational calculus in Chapter 13). This is because the configuration spaces of molecular systems can be described as Lie groups. This is equally true for a rigid-body description of a molecule, multi-rigid-body models with rotational and translational degrees of freedom between rigid components, and mixtures of multiple kinds of interacting rigid-body macromolecules.

To start, consider a simple fluid consisting of a single kind of rigid-body molecule. The kinetic energy of a single rigid molecule can be written as

$$T = \frac{1}{2} m \dot{\mathbf{r}} \cdot \dot{\mathbf{r}} + \frac{1}{2} \boldsymbol{\omega}^T I \boldsymbol{\omega},$$

where m is its mass and I is its moment of inertia as seen in a body-fixed frame attached to the center of mass. Here, $\mathbf{r}$ is its position, R is its orientation relative to the lab frame, and $\boldsymbol{\omega} = (R^T \dot{R})^\vee$ is its angular velocity. Using coordinates $\boldsymbol{\phi}$, such as Euler angles, the kinetic energy can be written as $T = \frac{1}{2}[\dot{\mathbf{r}}^T, \dot{\boldsymbol{\phi}}^T] G(\boldsymbol{\phi}) [\dot{\mathbf{r}}^T, \dot{\boldsymbol{\phi}}^T]^T$, where $G(\boldsymbol{\phi}) = (m \mathbb{I}_3) \oplus (J^T(\boldsymbol{\phi}) I J(\boldsymbol{\phi}))$. The conjugate momentum associated with translation is $\mathbf{p}_r = (m^{-1}\mathbb{I}_3)\dot{\mathbf{r}} = m^{-1}\dot{\mathbf{r}}$, and for rotation, it is $\mathbf{p}_\phi \doteq \partial T / \partial \dot{\boldsymbol{\phi}} = J^T(\boldsymbol{\phi}) I J(\boldsymbol{\phi}) \dot{\boldsymbol{\phi}}$. Thus, the coordinate-dependent version of the Boltzmann distribution is

$$f(\mathbf{r}, \boldsymbol{\phi}; \mathbf{p}_r, \mathbf{p}_\phi; \beta) = \frac{1}{Z(\beta)} e^{-\beta\left\{\frac{1}{2}[\mathbf{p}_r^T, \mathbf{p}_\phi^T][G(\boldsymbol{\phi})]^{-1}[\mathbf{p}_r^T, \mathbf{p}_\phi^T]^T + V(\mathbf{r}, \boldsymbol{\phi})\right\}},$$

where the shorthand $\beta \doteq 1/k_B T$ is used and

$$Z(\beta) \doteq \int_{\mathbf{r}} \int_{\phi} \int_{\mathbf{p}_r} \int_{\mathbf{p}_\phi} e^{-\beta\left\{\frac{1}{2}[\mathbf{p}_r^T, \mathbf{p}_\phi^T][G(\boldsymbol{\phi})]^{-1}[\mathbf{p}_r^T, \mathbf{p}_\phi^T]^T + V(\mathbf{r}, \boldsymbol{\phi})\right\}} \, d\mathbf{p}_\phi \, d\mathbf{p}_r \, d\boldsymbol{\phi} \, d\mathbf{r}$$

is the full partition function. Note that dependence on the momenta can be integrated out using knowledge of Gaussian integrals (see Chapter 2), and so the *configurational Boltzmann distribution*

$$f_c(\mathbf{r}, \boldsymbol{\phi}; \beta) \doteq \int_{\mathbf{p}_r} \int_{\mathbf{p}_\phi} f(\mathbf{r}, \boldsymbol{\phi}; \mathbf{p}_r, \mathbf{p}_\phi) \, d\mathbf{p}_\phi \, d\mathbf{p}_r = \frac{1}{Z_c(\beta)} |G(\boldsymbol{\phi})|^{\frac{1}{2}} \cdot e^{-\beta V(\mathbf{r}, \boldsymbol{\phi})}$$

results, where the *configurational partition function* is

$$Z_c(\beta) \doteq \int_{\mathbf{r}} \int_{\phi} e^{-\beta V(\mathbf{r},\boldsymbol{\phi})} |G(\boldsymbol{\phi})|^{\frac{1}{2}} d\boldsymbol{\phi}\, d\mathbf{r}.$$

Note that $|G(\boldsymbol{\phi})|^{\frac{1}{2}} \propto |J(\boldsymbol{\phi})|$.

With these facts in mind, the coordinate-free version of the equilibrium statistical mechanics of gases or dilute solutions of rigid molecules can be written completely independently of coordinates. If $g = (\mathbf{r}, R(\boldsymbol{\phi})) \in SE(3)$ and $\boldsymbol{\xi} = (g^{-1}\dot{g})^{\vee} \in \mathbb{R}^6 \cong se(3)$, then $T = \frac{1}{2}\boldsymbol{\xi}^T \mathcal{I} \boldsymbol{\xi}$, where $\mathcal{I} \doteq (m\mathbb{I}_3) \oplus I$, and the coordinate-free version of conjugate momenta becomes $\boldsymbol{\eta} \doteq \partial T / \partial \boldsymbol{\xi} = \mathcal{I}\boldsymbol{\xi}$. Therefore, $T = \frac{1}{2}\boldsymbol{\eta}^T \mathcal{I}^{-1} \boldsymbol{\eta}$, where $\mathcal{I}^{-1} = [(m\mathbb{I}_3) \oplus I]^{-1} = (m^{-1}\mathbb{I}_3) \oplus I^{-1}$. The coordinate-free Boltzmann distribution is then

$$f(g, \boldsymbol{\eta}; \beta) = \frac{1}{Z(\beta)} e^{-\beta\left\{\frac{1}{2}\boldsymbol{\eta}^T \mathcal{I}^{-1} \boldsymbol{\eta} + V(g)\right\}},$$

where

$$Z(\beta) = \int_{g \in SE(3)} \int_{\boldsymbol{\eta} \in \mathbb{R}^6} e^{-\beta\left\{\frac{1}{2}\boldsymbol{\eta}^T \mathcal{I}^{-1} \boldsymbol{\eta} + V(g)\right\}} d\boldsymbol{\eta}\, dg.$$

Here, of course, dg is the bi-invariant (Haar) measure for $SE(3)$ ($dg = d\mathbf{r}\, dR$, where dR is the normalized Haar measure for $SO(3)$) and $d\boldsymbol{\eta}$ is the Lebesgue measure for $\mathbb{R}^6 \cong se(3)$. The coordinate-free configurational Boltzmann distribution is then

$$f_c(g; \beta) \doteq \int_{\boldsymbol{\eta} \in \mathbb{R}^6} f(g, \boldsymbol{\eta}; \beta)\, d\boldsymbol{\eta} = \frac{1}{Z_c(\beta)} e^{-\beta V(g)},$$

where

$$Z_c(\beta) = \int_{g \in SE(3)} e^{-\beta V(g)}\, dg.$$

Henceforth the subscript c will be dropped when it is clear that the configurational (as opposed to full) Boltzmann distribution is being discussed.

14.4.1 Translational and Rotational Brownian Motion of Rigid-Body Molecules

The Euler–Poincaré equations applied to a total energy (kinetic and potential) of the form $E(g, \boldsymbol{\xi}) = \boldsymbol{\xi}^T \mathcal{I} \boldsymbol{\xi} + V(g)$, where $g = (\mathbf{r}, R)$ and $\mathcal{I} \doteq [(m\mathbb{I}_3) \oplus I]$, gives deterministic equations of motion for a conservative system. These can be decoupled into Newton's and Euler's equations as

$$\dot{\mathbf{p}} = -\nabla_{\mathbf{r}} V \quad \text{and} \quad I\dot{\boldsymbol{\omega}} + \boldsymbol{\omega} \times (I\boldsymbol{\omega}) = -\tilde{\mathbf{X}}^r V,$$

where $\mathbf{p} = m\dot{\mathbf{r}}$ is the classical linear momentum of a particle. If damping and white noise are incorporated and it is assumed that the rotational and translational damping and noise matrices are decoupled,[2] then the resulting system of equations is of the form

$$\dot{\mathbf{x}} = \frac{1}{m}\mathbf{p}, \tag{14.32}$$

$$\dot{\mathbf{p}} = -\nabla_{\mathbf{r}} V - \frac{1}{m} C_1 \mathbf{p} + S_1 \dot{\mathbf{w}}_1, \tag{14.33}$$

$$I\dot{\boldsymbol{\omega}} + \boldsymbol{\omega} \times (I\boldsymbol{\omega}) = -\tilde{\mathbf{X}}^r V - C_2 \boldsymbol{\omega} + S_2 \dot{\mathbf{w}}_2, \tag{14.34}$$

[2] Even if they are not, the formulation proceeds in a similar way.

where $\tilde{\mathbf{X}}^r$ is defined in (11.9). Here, by a slight abuse of notation, $\dot{\mathbf{w}}_i = d\mathbf{w}_i/dt$ is the time derivative of a Wiener process, and multiplication through by dt gives a system of SDEs.[3] The matrices C_i and S_i are all related. Indeed, from the fluctuation-dissipation theorem, $C_i = S_i S_i^T$. A similar result would hold if a more detailed model takes into account coupling between $\mathbf{p}$ and $\boldsymbol{\omega}$, in which case $C \neq C_1 \oplus C_2$ and $S \neq S_1 \oplus S_2$. The nature of such couplings depend on the geometry of the body, the viscosity, and so forth and have been studied in [40, 68].

Using the general formalism of Chapters 4 and 8, it is possible to write the Fokker–Planck equations corresponding to (14.32)–(14.34). Indeed, this was done half a century ago and is surveyed in [13, 23, 27, 36, 56]. The result is an *inertial theory* of Brownian motion, pioneered by Smoluchowski in the translational case at the beginning of the 20th century [80] and in the rotational case by Steele [81]. Applications include fluorescence anisotropy microscopy [84, 91]. Note that due to the structure of these equations, it does not matter if they are interpreted as Itô or Stratonovich. The result is a probability density $f(g, \boldsymbol{\xi}, t)$ which, when C_i, and S_i are all properly balanced, converges to the Boltzmann distribution $Z^{-1}\exp(-\beta E(g, \boldsymbol{\xi}))$ as $t \to \infty$. This serves as a concrete example of a stochastic flow on the tangent bundle for $SE(3)$.

In the *noninertial theory* of Brownian motion (which historically preceded the inertial theory), m and I are assumed to be negligible, and if rotations are parameterized by $\boldsymbol{\phi}$ and $V(g) = V_1(\mathbf{r}) + V_2(R(\boldsymbol{\phi}))$, the result is

$$C_1\dot{\mathbf{x}} = -\nabla_{\mathbf{r}} V_1(\mathbf{r}) + S_1\dot{\mathbf{w}}_1, \tag{14.35}$$

$$C_2 J(\boldsymbol{\phi})\dot{\boldsymbol{\phi}} = -\tilde{\mathbf{X}}^r V_2(R(\boldsymbol{\phi})) + S_2\dot{\mathbf{w}}_2. \tag{14.36}$$

Note that these equations are decoupled from each other and that (14.35) can be interpreted as Itô or Stratonovich and it does not matter. However, (14.36) must be interpreted as a Stratonovich equation because usual calculus was used to replace $\boldsymbol{\omega}$ with $J(\boldsymbol{\phi})\dot{\boldsymbol{\phi}}$. This is equivalent to

$$\dot{\boldsymbol{\phi}} = -J^{-1}(\boldsymbol{\phi})C_2^{-1}\tilde{\mathbf{X}}^r V_2(R(\boldsymbol{\phi})) + J^{-1}(\boldsymbol{\phi})C_2^{-1}S\dot{\mathbf{w}}_2. \tag{14.37}$$

If instead Itô's rule had been used to express $\boldsymbol{\omega}\,dt$, then the resulting equation would have been different than (14.36); that is, it would have included an additional drift term. Then the Itô version of the Fokker–Planck equation corresponding to the Itô SDE and the Statonovich version of the Fokker–Planck equation corresponding to the Statonovich SDE would be the same. Using the methods of Chapters 4 and 8, it is not difficult to write the Fokker–Planck equations, where in this case $|G|^{\frac{1}{2}} = |J|$.

14.4.2 Molecular Theory of Liquids

Consider a dilute solution confined to a container and consisting of N copies of a large rigid molecule dissolved in a solvent of many more small molecules. In this situation, the behavior of each large molecule is expected to act independently of the others and the configurational Boltzmann distribution for all N copies would be the product of those for each individual one. However, as the number density per unit volume of these molecules becomes greater and, in the extreme case, when a pure liquid consisting of these large molecules is considered, then the behavior of each copy is no longer independent.

[3] Although a Wiener process is not differentiable, $d\mathbf{w}_i/dt$ can be interpreted in the sense of finite differences in computer simulations.

Let $C \subset \mathbb{R}^3$ denote the container in which the N molecules are constrained to move and let $D = C \times SO(3)$ be a finite-volume domain within $SE(3)$. In this case, the configurational Boltzmann distribution will be of the form

$$f(g_1, g_2, \ldots, g_N; \beta, D) = \frac{1}{Z_c(\beta, N, D)} e^{-\beta V(g_1, g_2, \ldots, g_N)},$$

where each $g_i \in D$ and

$$Z_c(\beta, N, D) = \int_{D^N \subset SE(3)^N} e^{-\beta V(g_1, g_2, \ldots, g_N)} dg_1\, dg_2 \cdots dg_N.$$

Here, $SE(3)^N$ is shorthand for the N-fold product $SE(3) \times SE(3) \times \cdots \times SE(3)$ and similarly for D^N, and the integration takes place over this finite-volume domain. Alternatively, the shape of the container could be absorbed into the definitions of $f(\cdot)$ by using window functions enforced by an appropriate potential, and then the integral can be extended over all of $SE(3)^N$.

Distribution and Correlation Functions

Since each molecule can exist in each location in this $6N$-dimensional configuration space, it is common to define the *generic distribution function* [29, 32, 34]

$$f'(g_1, g_2, \ldots, g_N; \beta, D) \doteq N!\, f(g_1, g_2, \ldots, g_N; \beta),$$

which reflects that the position and orientation of any molecule can be swapped with any of the others.

If we are only interested in the generic distribution function for the first m of these molecules without regard to the others, then

$$f'(g_1, g_2, \ldots, g_m; \beta, D) = \frac{1}{(N-m)!} \int_{D^{N-m}} f'(g_1, g_2, \ldots, g_N; \beta, D)\, dg_{m+1}\, dg_{m+2} \cdots dg_N.$$

Marginalizing $f(g_1, g_2, \ldots, g_m; \beta, D)$ over all copies except for the ith one gives $f(g_i; \beta, D)$, and $f'(g_i; \beta, D)$ is defined in an analogous way. A quantitative indicator of how independently the N copies of the rigid molecules behave is the value of the so-called *(generic) correlation function*

$$\gamma(g_1, g_2, \ldots, g_m; \beta, D) \doteq \frac{f'(g_1, g_2, \ldots, g_m; \beta, D)}{\prod_{i=1}^{m} f'(g_i; \beta, D)} = K(N, m)\, \frac{f(g_1, g_2, \ldots, g_m; \beta, D)}{\prod_{i=1}^{m} f(g_i; \beta, D)}.$$

Here, for $m \ll N$,

$$K(N, m) \doteq N^{-m}\, \frac{N!}{(N-m)!} \approx 1 - \frac{m(m-1)}{2N},$$

which approaches unity as $N \to \infty$ and m is held fixed. The closer γ is to 1 for all values of the argument, the more independent the behaviors are.

If each molecule has unit mass, then the mass density per unit volume at a given temperature can be computed as [29, 32, 34][4]

$$\begin{aligned}\rho(\mathbf{r};\beta,D) &= \frac{N}{Z_c(\beta,N,D)}\int_{D^{N-1}}\int_{SO(3)} e^{-\beta V(g,g_2,g_3,\ldots,g_N)}\,dR\,dg_2\cdots dg_N \\ &= \left\langle \sum_{i=1}^{N}\delta(g_i^{-1}\circ g)\right\rangle, \end{aligned} \tag{14.38}$$

where $g=(\mathbf{r},R)\in SE(3)$, dR is the normalized Haar measure for $SO(3)$, and $\langle\cdot\rangle$ denotes the average over the Boltzmann-weighted ensemble.

In the case of an isotropic homogeneous fluid, $f'(g_i;\beta,D)=\rho(\beta,D)$—that is, the mass density per unit volume is constant at a particular temperature within the container. In this special case, the (pair) correlation function is written as [29, 32, 34]

$$\begin{aligned}\gamma(g,g';\beta,D) &= \frac{N(N-1)}{\rho^2(\beta)\cdot Z_c(\beta,N,D)}\int_{D^{N-2}} e^{-\beta V(g,g',g_3,\ldots,g_N)}dg_3\cdots dg_N \\ &= \frac{1}{\rho^2(\beta)}\left\langle \sum_{i\neq j}\delta(g_i^{-1}\circ g)\delta(g_j^{-1}\circ g')\right\rangle . \end{aligned} \tag{14.39}$$

Relationship to Convolutions on Groups

The so-called *total correlation function* between two molecules is defined as

$$\tilde{h}(g_1,g_2;\beta,D)\doteq\gamma(g_1,g_2;\beta,D)-1.$$

The *direct correlation function* between two molecules, $\tilde{c}(g_1,g_2;\beta,D)$, is defined to satisfy the equation

$$\tilde{h}(g_1,g_2;\beta,D)=\tilde{c}(g_1,g_2;\beta,D)+\rho\int_{D\subset SE(3)}\tilde{c}(g_1,g_3;\beta,D)\tilde{h}(g_3,g_2;\beta,D)\,dg_3.$$

Each g_i is an absolute motion relative to the lab frame, and all interactions between molecules are *relative*. It follows that the above integral can be written differently by introducing the notation $\tilde{h}(g_1,g_2;\beta,D)=h(g_1^{-1}\circ g_2)$ and $\tilde{c}(g_1,g_2;\beta,D)=c(g_1^{-1}\circ g_2)$, where $h(\cdot)$ and $c(\cdot)$ depend only on relative pose, and the dependence on β,D has been absorbed into how these functions are defined. Moreover, if these functions decay rapidly and if the molecules are not located at the boundary of the container, then integrals over D and $SE(3)$ are indistinguishable. Therefore,

$$h(g_1^{-1}\circ g_2)=c(g_1^{-1}\circ g_2)+\rho\int_{SE(3)}c(g_1^{-1}\circ g_3)h(g_3^{-1}\circ g_2)\,dg_3.$$

Letting $k=g_1^{-1}\circ g_3$, observing that $dk=dg_3$, and $g_3^{-1}\circ g_2=k^{-1}\circ g_1^{-1}\circ g_2$ means that the above equation can be written using the concept of convolution on $SE(3)$ as

$$\boxed{h(g_{12})=c(g_{12})+(c*h)(g_{12}),\quad \text{where } g_{12}\doteq g_1^{-1}\circ g_2.} \tag{14.40}$$

[4] In this field, orientational integrals are usually not normalized, and so an additional multiplicative factor of $\Omega\doteq 8\pi^2$ appears in classical works for molecules without any symmetry.

This form of the Six-dimensional version of the *Ornstein–Zernike* equation [63] and its extensions in the theories of *Percus–Yevick* [66, 67] and *Chandler–Andersen* [15] is not the way it is usually written in the literature [2, 29, 32, 34]. The group-theoretic notation in (14.40) allows it to be more succinctly stated than the way it is in the literature. Furthermore, the $SE(3)$ Fourier transform can be used to solve for h in terms of c (or vice versa) because the convolution theorem gives

$$\hat{h}(p) = [\mathbb{I} + \hat{h}(p)]\hat{c}(p) \implies \hat{c}(p) = [\mathbb{I} + \hat{h}(p)]^{-1}\hat{h}(p) \tag{14.41}$$

or, equivalently,

$$\hat{c}(p) = \hat{h}(p)[\mathbb{I} - \hat{c}(p)] \implies \hat{h}(p) = \hat{c}(p)[\mathbb{I} - \hat{c}(p)]^{-1} \tag{14.42}$$

if the inverses exist.

This formulation by itself does not solve the problem, but it provides a constraint which together with a “closure relation” characterizes the situation. Two popular closure relations are the Percus–Yevick and hyper-netted-chain approximations.

14.5 Conformational Statistics of DNA

In this section the statistical mechanics of DNA is discussed at two different levels of detail. First, a model is presented in which base in the DNA is treated as a rigid body connected to adjacent bases with quadratic potentials described by 6 × 6 stiffness matrices. Then DNA is modeled as a semi-flexible polymer (continuum filament subjected to Brownian motion).

14.5.1 A Multi-Rigid-Body Model of DNA

DNA is the macromolecule that stores genetic information in the form of paired bases. There are four kinds: A, C, G, T. Each of these base is essentially rigid. They are connected sequentially with a phosphate-sugar backbone, and two complementary single-stranded DNA chains merge via hydrogen bonding of the bases. In Watson–Crick base pairings the following possibilities exist: $G - C$, $C - G$, $A - T$, $T - A$.

Suppose that a computer simulation is performed in which a DNA molecule is represented as a ladder of connected rigid bodies, and each base is numbered in the zig-zag fashion illustrated below:

$$\begin{tikzcd}
i+4 \arrow[r] & i+5 \\
i+2 \arrow[r] & i+3 \arrow[ul] \\
i \arrow[r] & i+1 \arrow[ul] \\
i-2 \arrow[r] & i-1 \arrow[ul]
\end{tikzcd}$$

The region of interest is the middle, with the range i to $i+3$, and the others enumerate the nearest neighbors.

Potential Energy of the Rigid-Base Model with Elastic Contacts

Consider a double-helical DNA structure composed of $2N$ rigid bases, each of which can be connected to the others to form a double helix N basepairs long. Let $\overline{g}_i$ denote the position and orientation of the ith such body in a static minimal energy conformation as measured in a reference frame attached to base 0. The relative transformation between body i and body j is then $\overline{g}_i^{-1} \circ \overline{g}_j$.

Let the ith rigid body move by the small amount $\exp(X_i) \approx \mathbb{I}_4 + X_i$ where $X_i = \sum_{l=1}^{6} \chi_l^i E_l$. Then the relative motion between bodies i and j after the small motion is

$$[\overline{g}_i(\mathbb{I}_4 + X_i)]^{-1} \circ [\overline{g}_j(\mathbb{I}_4 + X_j)] = (\mathbb{I}_4 - X_i)(\overline{g}_i^{-1} \circ \overline{g}_j)(\mathbb{I}_4 + X_j).$$

Retaining terms to first order in X, the result can be written as

$$(\overline{g}_i^{-1} \circ \overline{g}_j)[\mathbb{I}_4 + X_j - (\overline{g}_i^{-1} \circ \overline{g}_j^{-1})X_i(\overline{g}_i^{-1} \circ \overline{g}_j)],$$

and the change in relative pose between body i and j is

$$\Delta g_{ij} = \mathbb{I}_4 + X_j - (\overline{g}_i^{-1} \circ \overline{g}_j)^{-1} X_i (\overline{g}_i^{-1} \circ \overline{g}_j).$$

The corresponding 6D vector of small motions is

$$\boldsymbol{\chi}_{ij} = \boldsymbol{\chi}_j - A_{ij}\boldsymbol{\chi}_i, \quad \text{where } A_{ij} \doteq [Ad(\overline{g}_j^{-1} \circ \overline{g}_i)].$$

Given a 6×6 stiffness K_{ij} connecting these two bodies, the corresponding potential energy is

$$V_{ij} = \frac{1}{2}\boldsymbol{\chi}_{ij}^T K_{ij} \boldsymbol{\chi}_{ij} = \frac{1}{2}[\boldsymbol{\chi}_i^T, \boldsymbol{\chi}_j^T] \begin{pmatrix} A_{ij}^T K_{ij} A_{ij} & -A_{ij}^T K_{ij} \\ -K_{ij} A_{ij} & K_{ij} \end{pmatrix} \begin{bmatrix} \boldsymbol{\chi}_i \\ \boldsymbol{\chi}_j \end{bmatrix}, \tag{14.43}$$

and the total potential energy will be

$$V = \sum_{i=0}^{2N-2} \sum_{j=i+1}^{2N-1} V_{ij} = \frac{1}{2}\boldsymbol{\chi}^T K \boldsymbol{\chi}, \tag{14.44}$$

where $\boldsymbol{\chi} \in \mathbb{R}^{12N-6}$ is a composite vector of all small rigid-body motions of the bases in the structure (relative to their equilibrium poses) and K is a composite $(12N - 6) \times (12N - 6)$ stiffness matrix. The dimension is $12N - 6$ rather than $12N$ because the global rigid-body degrees of freedom of the structure have been removed by choosing to measure each $\overline{g}_i$ relative to base 0, rather than relative to an inertial reference frame.

Equation (14.44) shows that the potential energy of the system run at equilibrium is in quadratic form. This is used to obtain the probability density function of the motion. For a macromolecule fluctuating about one conformation which globally minimizes its potential energy, the potential energy function can be expressed as

$$V(\boldsymbol{\chi}) \approx V_0 + \frac{1}{2}\boldsymbol{\chi}^T K \boldsymbol{\chi}, \tag{14.45}$$

where the elements of K are

$$k_{ij} = \left. \frac{\partial^2 V}{\partial \chi_i \partial q \chi_j} \right|_{\boldsymbol{\chi}=\mathbf{0}}$$

and $\boldsymbol{\chi} = \mathbf{0}$ is defined to be the value for which $V(\boldsymbol{\chi}) = V_0$ is the minimum attainable potential energy. By appropriate choice of datum, one can take $V_0 = 0$. Since $\boldsymbol{\chi}(t)$ never strays far from $\mathbf{0}$, it follows that the mass matrix (conformation-dependent inertial tensor) $M(\boldsymbol{\chi})$ is approximated well as the constant matrix $M = M(\mathbf{0})$.

Conformational Boltzmann Distribution

Given the potential energy described above, if one integrates over the momenta, the resulting marginal (or conformational) Boltzmann distribution results:

$$f(\mathbf{q}) = \frac{1}{Z_c} \exp\left(-\frac{1}{2} \beta \boldsymbol{\chi}^T K \boldsymbol{\chi} \right). \tag{14.46}$$

This is a Gaussian distribution, the covariances of which can be related to the stiffness matrix by computing integrals similar to those in Section 2.2.2. This gives

$$\Sigma = \int_{\boldsymbol{\chi} \in \mathbb{R}^N} \boldsymbol{\chi} \boldsymbol{\chi}^T f(\boldsymbol{\chi}) \, d\boldsymbol{\chi} = K^{-1}/\beta.$$

The covariance matrix Σ can be observed from molecular dynamics simulations, from which stiffnesses can be extracted. Or, if stiffnesses are known, then the model presented here can be used to make predictions about how the DNA moves under Brownian motion. This can be used to make predictions about the probability of ring closure and other phenomena.

14.5.2 Continuum Filament Model Subjected to Brownian Motion

Although a model with $12N$ (or $12N - 6$) degrees of freedom for a double helix of length N is substantially coarser than a model that involves the motion of every single atom in the structure (and the surrounding solvent), for some purposes it is sufficient to use an even cruder model. One such model—the continuum filament model—was reviewed in Section 13.7. In that model, DNA is treated as an elastic filament. Whereas the previous goal was to obtain conditions satisfied by the minimal energy conformations of that DNA model, the goal here is to assess how this continuum filament model behaves when subjected to Brownian motion forcing.

Problem Formulation

Consider the equilibrium statistics of a stochastically forced elastic filament. Let the evolution of the probability density of relative pose of reference frames attached to a stochastically forced elastic filament at values of curve parameter 0 and s be denoted as $f(g; 0, s)$. Since it is a probability density, by definition

$$\int_G f(g; 0, s) \, dg = 1. \tag{14.47}$$

Clearly, $f(g; s) \doteq f(g; 0, s)$ must be related in some way to the equilibrium shape of the filament, its stiffness, and the strength of the Brownian motion forcing from the ambient solvent. Additionally, the strength of this noise should be related in some way to the temperature. In fact, since $f(g; 0, s)$ is the function describing the distribution of poses for a filament at equilibrium, it can be represented exactly as a path integral [46] or, equivalently, as a diffusion equation [16]:

$$\frac{\partial f}{\partial s} = \frac{1}{2} \sum_{k,l=1}^{6} D_{lk}(s) \, \tilde{E}_l^r \tilde{E}_k^r f - \sum_{l=1}^{6} (\boldsymbol{\xi}_0(s) \cdot \mathbf{e}_l) \, \tilde{E}_l^r f \tag{14.48}$$

subject to the initial conditions

$$f(g;0,0) = \delta(g).$$

Here, the diffusion matrix is related to the stiffness matrix in (13.37) as $D(s) = (k_B T)K^{-1}(s)$. This equation takes into account anisotropy and inhomogeneity of the elasticity, as well as arbitrary minimal energy shape, and has essentially the same derivation as the homogeneous case presented in [16, 96, 97].

Under the extreme condition that $T \to 0$, no diffusion would take place and $f(g;,0,s) \to \delta(g_0^{-1}(s) \circ g)$. For the biologically relevant case ($T \approx 300$), (14.48) can be solved using the harmonic analysis approach in [16, 96, 97]. If we make the shorthand notation $f_{s_1,s_2}(g) = f(g;s_1,s_2)$, then it will always be the case for $s_1 < s < s_2$ that

$$f_{s_1,s_2}(g) = (f_{s_1,s} * f_{s,s_2})(g) = \int_G f_{s_1,s}(h)\, f_{s,s_2}(h^{-1} \circ g)\, dh. \tag{14.49}$$

This is the convolution of two pose distributions. Here, h is a dummy variable of integration and dh is the bi-invariant integration measure for $SE(3)$. Whereas (14.49) will always hold for semi-flexible phantom chains, for the homogeneous rod there is the additional convenient properties that

$$f(g;s_1,s_2) = f(g;0,s_2 - s_1) \quad \text{and} \quad f(g;s_2,s_1) = f(g^{-1},s_1,s_2). \tag{14.50}$$

The first of these says that for a uniform chain, the pose distribution only depends on the difference of arc length along the chain. The second provides a relationship between the pose distribution for a uniform chain resulting from taking the frame at s_1 to be fixed at the identity and recording the poses visited by s_2, and the distribution of frames that results when s_2 is fixed at the identity. However, neither of these nor (14.49) will hold when excluded-volume interactions are taken into account.

Solving Diffusion Equations on the Euclidean Group

The true benefit of the group-theoretic approach is realized when one observes that in coordinate form, (14.48) is expressed as pages of complicated-looking (but essentially elementary) mathematical expressions. In contrast, it is possible to write out the solution very simply using results from group theory. One numerical approach that works well for dilute solutions of DNA of lengths in the range of 1/2–2 persistence lengths (60–300 basepairs at 300 degrees Kelvin) is based on the group Fourier transform for $SE(3)$. The reason why this approach is most appropriate for this regime is that DNA of this length is flexible enough for Fourier methods (which work better for more spread out distributions than for highly focused ones) to be applicable, and it is short enough that the effects of self-contact can be neglected.

The $SE(3)$ Fourier transform built on the IURs presented in Chapter 12 has operational properties of the form[5]

$$\widehat{\tilde{E}_i^r f} = u_i(p)\hat{f}(p,s)$$

that are directly applicable to solving (14.48), where $u_i(p)$ is an operator matrix. In other words, the group-Fourier transform converts Lie derivatives into matrix operations in

[5] Here, $u_i(p)$ is shorthand for what was written as $u(E_i;p,s)$ in Chapter 12, where the s has been suppressed to avoid confusion with the arc length s used here.

Fourier space. This means that (14.48) can be written as

$$\frac{\partial \hat{f}(p;s)}{\partial s} = \mathcal{B}(s)\hat{f}(p;s), \quad \text{where } \mathcal{B}(s) = \frac{1}{2}\sum_{i,j=1}^{6} D_{ij}(s)u_i(p)u_j(p) - \sum_{k=1}^{6}(\boldsymbol{\xi}_0(s)\cdot\mathbf{e}_k)u_k(p). \tag{14.51}$$

In the case of a referential configuration that is helical and stiffness parameters that are uniform (and therefore independent of s), then $\mathcal{B}(s) = \mathcal{B}_0$ is constant and the solution can be written in Fourier space as $\hat{f}(p;s) = \exp(s\mathcal{B}_0)$ and the inversion formula can be used to recover $f(g;s)$. The details of this procedure have been discussed in a number of the author's papers, together with the use of the convolution theorem for group Fourier transforms to "stitch together" the statistics of several segments of DNA connected by joints and/or kinks [96, 97]. In the case when $\mathcal{B}(s)$ is not constant, the differential equation in (14.51), which is an ODE for each fixed value of $0 \leq p \leq \infty$, can be solved either as a product of exponentials or by numerical integration.

Note that neither of the models presented in Sections 14.5.1 and 14.5.2 take into account the effects of excluded volume, which can be ignored for moderate values of filament length in the case when the DNA is not enclosed in a small compartment. Excluded volume effects can be modeled as described using Lie group ideas as in [17] as well as in lattice models as in [78, 79] The discussion of the principal kinematic formula in Chapter 14 is also motivated by this issue.

14.6 Ergodic Theory

From the discussion in the previous subsection, it should be clear that a single very long sample path corresponding to an SDE for a stochastic mechanical system satisfying (14.22) should result in a sampling of the Maxwell–Boltzmann distribution $f_\infty(\mathbf{p},\mathbf{q})$. Although this sort of ergodic property is extremely important, it should not be confused with an area of mathematics that is known as "ergodic theory."

In ergodic theory, the questions that are addressed are somewhat different than the concept of ergodicity as it appeared in the context of statistical mechanics. Rather than chopping up a single long stochastic trajectory into an ensemble of shorter paths and observing that the statistical properties of each are comparable, in mathematical ergodic theory the convergence properties of iterated one-parameter groups of transformations are studied. This concept will be made concrete with examples in the following subsections.

14.6.1 Ergodic Motions on the Circle and n-Torus: Weyl's Result

Consider a planar rotation $R(\alpha)$ where $0 < \alpha < 2\pi$ is some arbitrary angle. Now, consider an arbitrary nice function on the unit circle, which, by abuse of notation, can be written either as $f(\theta)$ or $f(\mathbf{u}(\theta))$, where $0 \leq \theta < 2\pi$. (Note the subtle difference in the ranges of α and θ). What happens if we calculate

$$\overline{f_N}(\mathbf{u}_0;\alpha) \doteq \frac{1}{N}\sum_{k=0}^{N-1} f(R^k(\alpha)\mathbf{u}_0)$$

for some initial value of $\mathbf{u}_0 = [\cos\theta_0, \sin\theta_0]^T$? Ergodic theory says that if the rotation angle α is an irrational number, then

$$\lim_{N\to\infty} \overline{f_N} = \frac{1}{2\pi}\int_0^{2\pi} f(\phi)\,d\phi. \tag{14.52}$$

In other words, the average taken over a deterministic trajectory generated by a sufficiently large number of iterations of a rotation results in the average of the function over the circle, which is independent of both the starting point θ_0 and the increment of rotation α. This equality was proved by Weyl in [93], who also derived the tube formula in $\mathbb{R}^n$ discussed in Section 5.5.3.

A Fourier-analytic proof of (14.52) follows by representing each sample as a Dirac delta function, expanded in a Fourier series:

$$\delta_\alpha(\theta) \doteq \delta(\theta - \alpha) = \frac{1}{2\pi} \sum_{n=-\infty}^{\infty} e^{in(\theta-\alpha)}.$$

If $f(\theta)$ is any "nice" function on the unit circle, then it can be expanded in a Fourier series as

$$f(\theta) = \frac{1}{2\pi} \sum_{n=-\infty}^{\infty} \hat{f}(n)\, e^{in\theta}.$$

Then

$$\overline{f_N}(\theta_0;\alpha) = \frac{1}{N}\sum_{k=0}^{N-1} f(\theta_0 - k\cdot\alpha) = \frac{1}{N}\sum_{k=0}^{N-1}(f * \delta_{k\cdot\alpha})(\theta_0),$$

which can be expressed as

$$\overline{f_N}(\theta_0;\alpha) = \frac{1}{2\pi N}\sum_{k=0}^{N-1}\sum_{n=-\infty}^{\infty}\hat{f}(n)e^{in(\theta_0 - k\cdot\alpha)} = \frac{1}{2\pi}\sum_{n=-\infty}^{\infty}\hat{f}(n)e^{in\theta_0}\left(\frac{1}{N}\sum_{k=0}^{N-1}e^{-ink\alpha}\right)$$

by virtue of the convolution theorem. However,

$$\sum_{k=0}^{N-1} e^{-ink\alpha} = \frac{e^{-inN\alpha}-1}{e^{-in\alpha}-1} < \infty \quad \text{when } n \neq 0$$

because this is a geometric series which converges as long as α is irrational (otherwise the denominator might become 0). This means that

$$\lim_{N\to\infty}\frac{1}{N}\sum_{k=0}^{N-1}e^{-ink\alpha} \to 0 \quad \text{when } n \neq 0.$$

For any value of N (finite or infinite),

$$\frac{1}{N}\sum_{k=0}^{N-1}e^{-ink\alpha} = 1 \quad \text{when } n = 0.$$

Weyl's result then follows because this means that

$$\lim_{N\to\infty}\overline{f_N}(\theta_0;\alpha) = \frac{1}{2\pi}\hat{f}(0) = \frac{1}{2\pi}\int_0^{2\pi} f(\phi)\,d\phi.$$

It is not difficult to show that given an n-tuple of angles defining a point on the n-torus, $(\theta_0^1, \theta_0^2, \ldots, \theta_0^n) \in T^n$, each of which is an irrational multiple of 2π and none of which are rational multiples of each other, that a similar proof can be used to show that

$$\lim_{N\to\infty}\frac{1}{N}\sum_{k=0}^{N-1} f(\theta_0^1 - k\cdot\alpha_1, \ldots, \theta_0^n - k\cdot\alpha_n) = \frac{1}{(2\pi)^n}\int_0^{2\pi}\cdots\int_0^{2\pi} f(\phi_1,\ldots,\phi_n)\,d\phi_1\cdots d\phi_n. \tag{14.53}$$

Other great mathematicians of the first half of the 20th century also studied ergodic theory, including Birkhoff, von Neumann, and Wiener [9, 88, 89, 94, 95], and ergodic theory is still an active area of mathematical research today (see, e.g., [76, 77, 98]). The following subsection addresses more general topics than motions on the unit circle or torus.

14.6.2 Ergodic Group Actions on Manifolds

From the beginning, strong connections have existed between ergodic theory and group theory. Some of these connections are reviewed in this subsection.

Let M be a compact manifold on which a group G with elements g acts. Then for any nice function $f \in \mathcal{N}(M)$ and $x \in M$, ergodic theory addresses conditions under which for almost any $g \in G$ the limit

$$L = \lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f(g^{-k} \cdot x) \tag{14.54}$$

converges "in some sense." The notation g^k is the k-fold repeated product of g with itself and $g^{-k} = (g^k)^{-1} = (g^{-1})^k$. The limit in (14.54) was proven to exist in the mean-squared sense by von Neumann [88, 89] and in the sense of pointwise convergence by Birkhoff [9], both for the case when the group is a set of *measure-preserving transformations*, meaning that

$$\int_M f(g^{-1} \circ x)\, dV(x) = \int_M f(x)\, dV(x) \tag{14.55}$$

for all $x \in M$ and $g \in G$, where $dV(x)$ is the volume element for M.

While it is always true that when (14.55) holds, then

$$L = \tilde{f}(x_0) \quad \text{and} \quad \int_M f(x)\, dV(x) = \int_M \tilde{f}(x)\, dV(x), \tag{14.56}$$

only in special cases (e.g., the circle and n-torus) is it possible for

$$\tilde{f}(x_0) = \frac{1}{V(M)} \int_M f(x)\, dV(x). \tag{14.57}$$

Here, $V(M)$ is the total volume of M, which can be taken to be $V(M) = 1$ by suitable normalization of $dV(x)$. When (14.57) holds, $\tilde{f}(x_0)$ will not depend on the starting point x_0, and the result will be that the discrete set of transformations $\{g^k \mid k \in \mathbb{Z}^+\}$ results in a uniformly distributed sampling of M. In this case, $g \in G$ is said to be ergodic.

The *von Neumann ergodic theorem* [88] states that if iterated powers of a group element $g \in G$ acting on any point in a compact measurable space, $x \in M$, results in filling that space with a density that is uniform with respect to a volume element $dV(x)$, then[6]

$$\lim_{N\to\infty} \int_M \left(\frac{1}{N} \sum_{k=0}^{N-1} f(g^{-k} \cdot x) - \int_M f(x)\, dV(x) \right)^2 dV(x) = 0. \tag{14.58}$$

[6] The compact manifold M can be replaced with more general measurable spaces, but that greater degree of generality will not be needed here.

Under the same conditions that lead to the above statement, the *Birkhoff ergodic theorem* [9] states that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f(g^{-k} \cdot x) = \int_M f(x)\, dV(x) \tag{14.59}$$

for almost all $x \in M$ (i.e., for all $x \in M$ except possibly a set of measure zero). This comes back to the discussion of the meaning of equality discussed in Chapter 1.

As a first concrete example, consider the case of the group of rotations $SO(n)$ acting on the sphere S^{n-1} in $\mathbb{R}^n$, where it is clear that moving around a function on the surface of the sphere by pure rotations does not affect the total integral of the function:

$$\int_{S^{n-1}} f(R^T\mathbf{u})\, d\mathbf{u} = \int_{S^{n-1}} f(\mathbf{u})\, d\mathbf{u}. \tag{14.60}$$

A second example is the rigid-body motion of a function on $\mathbb{R}^n$, where $g = (R, \mathbf{t})$ with $R \in SO(n)$, $\mathbf{t} \in \mathbb{R}^n$, the action is defined by $g \cdot \mathbf{x} = R\mathbf{x} + \mathbf{t}$ (or equivalently $g^{-1} \cdot \mathbf{x} = R^T(\mathbf{x} - \mathbf{t})$), and

$$\int_{\mathbb{R}^n} f(R^T(\mathbf{x} - \mathbf{t}))\, d\mathbf{x} = \int_{\mathbb{R}^n} f(\mathbf{x})\, d\mathbf{x}. \tag{14.61}$$

So many other such examples exist that it is tempting to believe that (14.55) always holds. However, that is not the case. For example, if $A \in GL(n, \mathbb{R})$, then

$$\int_{\mathbb{R}^n} f(A^{-1}\mathbf{x})\, d\mathbf{x} = |\mathrm{det}A| \cdot \int_{\mathbb{R}^n} f(\mathbf{x})\, d\mathbf{x},$$

where, in general, $0 < |\mathrm{det}A| \neq 1$.

Even though (14.61) is an example of 14.55, $\mathbb{R}^n$ is not compact, and hence (14.58) and (14.59) do not apply. This is intuitively clear since g^{-k} will generate samples along a helix extending to infinity and hence will not fill space. However, S^{n-1} is compact, which together with (14.60) means that both (14.58) and (14.59) hold.

Henceforth the discussion is limited to the case when (14.55) holds. In this context, the equality in (14.54) works for "almost any" $g \in G$ in the same sense that (14.52) is true for almost any $\alpha \in [0, 2\pi)$. Clearly, there are cases when (14.54) works (e.g., if the powers of g form a finite group). However, clearly in that case, (14.57) would not hold.

14.6.3 Mixing and Ergodicity

The transformation $g \in G$ is said to satisfy the *mixing property* if for any two functions $f_1, f_2 \in L^2(M)$,

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \int_M f_1(g^{-k} \cdot x) f_2(x)\, dV(x) = \frac{1}{V(M)} \left(\int_M f_1(x)\, dV(x)\right) \left(\int_M f_2(x)\, dV(x)\right). \tag{14.62}$$

If $f_1(x) = I_A(x)$ is the indicator function for a measurable subset $A \subset M$ and analogously $f_2(x) = I_B(x)$, then since $I_A(x) \cdot I_B(x) = I_{A\cap B}(x)$, (14.62) implies that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} V((g^{-k}A) \cap B) = \frac{V(A) \cdot V(B)}{V(M)}. \tag{14.63}$$

In fact, it can be shown that (14.62) and (14.63) must result from ergodicity (i.e., from (14.57)), and if (14.62) and (14.63) hold for all measurable subsets $A, B \subset M$, then (14.57) must hold. Thus, ergodicity implies mixing, and vice versa.

When (14.63) holds, the discrete dynamical system $\{g^k | k \in \mathbb{Z}_{\geq 0}\}$ is called *strongly mixing*. In contrast, if

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \left| V((g^{-k}A) \cap B) - \frac{V(A) \cdot V(B)}{V(M)} \right|^p = 0, \tag{14.64}$$

then the system is called *weakly mixing* in the L^p sense [4]. Usually $p = 1$ or 2 is considered. Note that a system that is strongly mixing is automatically weakly mixing, but not vice versa [6]. The concept of strong/weak mixing applies equally to continuous-time systems, in which case the sums normalized by $1/N$ would be replaced by integrals from 0 to T, normalized by $1/T$. If M is a compact space (e.g., a ball large enough to contain all possible intersecting configurations of $g^{-k}A$ and B), then the units for measuring the volumes of A and B can be written in units of $V(M)$. Then $V'(A) \doteq V(A)/V(M) < 1$ and likewise for $V'(B)$.

Another important result is that if G is a group of measure-preserving transformations, i.e., (14.55) holds, then the set $\{g^k | k = 0, 1, ..., N-1\}$ generated by $g \in G$ is ergodic if and only if for all $f \in L^2(M)$ for which $\int_M f(x)\, dV(x) = 0$

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} \int_M f(g^{-k} \cdot x)\, \overline{f(x)}\, dV(x) = 0 \tag{14.65}$$

where $\overline{f(x)}$ is the complex conjugate of $f(x)$. The proof of (14.65) can be found in [64].

14.6.4 Ergodic Theory and Dynamical Systems

It is not difficult to imagine a system of differential equations, the solution to which is a continuous trajectory $g(t)$ that forms a one-parameter subgroup of transformations satisfying $g(s) \circ g(t) = g(s+t)$. For such a continuous group of transformations, the discrete sum in (14.54) can be replaced with an integral:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=0}^{N-1} f(g^{-k} \cdot x_0) \qquad \Longrightarrow \qquad \frac{1}{T} \int_0^T f([g(t)]^{-1} \cdot x_0)\, dt.$$

For example, if the trajectory of a conservative mechanical system (i.e., a deterministic system without damping of stochastic forcing) in phase space is allowed to evolve from an initial point $x_0 = (\mathbf{p}(0), \mathbf{q}(0))$, then $g(t) \cdot x_0 = (\mathbf{p}(t), \mathbf{q}(t))$, and this relationship can be iterated to define the group operation and the group action. This establishes a connection between ergodic theory and Hamiltonian mechanics.

On the other hand, if $x \in M$ is a point on a compact manifold and we consider a geodesic curve on M that starts at x with some initial tangent direction, following this path, parameterized by time, defines a *geodesic flow*. In some cases, this flow will ergodically "fill up" M. In other cases, the resulting curve will close back on itself, making it a closed curve. For example, on the sphere, which is a compact space of constant positive curvature, geodesics are closed (i.e., the great circles). On the topological 2-torus, which is a space of zero curvature, some geodesics are closed and some are ergodic. The closed ones are called *invariant tori*. On spaces of negative curvature, the famous *Hedlund–Hopf theorem* states that all geodesic flows are ergodic.

14.6.5 Measure-Theoretic Information

Concepts used in information theory and statistical mechanics have been modified for use in the ergodic theory of deterministic dynamical systems. In this subsection, the concept of measure-theoretic information, as it appears in ergodic theory, is reviewed.

Given any compact space on which a measure can be defined (for the sake of concreteness, think of a compact manifold with associated volume element), it is possible to partition that space into a finite number of disjoint subsets, the union of which is, to within a set of measure zero, the whole space; that is, given a measurable space (e.g., a compact manifold) M, a partition $\alpha = \{A_i\}$ is defined such that

$$A_{i_1} \cap A_{i_2} = \emptyset \quad \text{if} \quad i_1 \neq i_2 \quad \text{and} \quad \bigcup_{i \in I} A_i = M.$$

If $\alpha = \{A_i\}$ and $\beta = \{B_j\}$ with $i \in I$ and $j \in J$ (I and J being index sets) are two such partitions, then a new partition can be defined as[7]

$$\alpha \vee \beta \doteq \{A_i \cap B_j \,|\, i \in I, j \in J\} \quad \text{or} \quad \alpha \vee \beta = \{A \cap B \,|\, A \in \alpha, B \in \beta\}. \tag{14.66}$$

The above are two slightly different notations defining the same quantity, $\alpha \vee \beta$, which will be a finer partition than either of the original two; that is,

$$|\alpha \vee \beta| \geq \max\{|\alpha|, |\beta|\},$$

where, as usual, $|\cdot|$ means the number of elements in a finite set.

The set indicator function,

$$I_A(x) \doteq \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases} \tag{14.67}$$

together with the partition α can be used to define *measure-theoretic information* as

$$\boxed{I_\alpha(x) \doteq -\sum_{A \in \alpha} I_A(x) \log V(A),} \tag{14.68}$$

where $V(A)$ is the volume of A (or, more generally, the measure of A) normalized by the volume of the whole space, M. $I_\alpha(x)$ reflects the amount of "information" that results from discovering that $x \in A$. If A is a very large region, then little information is gained by knowing that $x \in A$. Measure-preserving actions of Lie groups such as rotations and translations do not affect this quantity. If α is a very fine partition, each subset of which has roughly the same volume, then more information is obtained from $I_\alpha(x)$ than if the partition is coarse. Sometimes it is convenient to raise the subscript and write $I(\alpha)(x)$ in place of $I_\alpha(x)$.

The *conditional measure-theoretic information* is defined as

$$I(\alpha \,|\, \beta)(x) \doteq -\sum_{A \in \alpha} I_A(x) \, \log V(A|\beta), \tag{14.69}$$

[7] The use of $\vee$ here is not to be confused with the usage of the same symbol in the context of Lie algebras. They are unrelated.

where

$$V(A|\beta)(x) \doteq \sum_{B\in\beta} I_B(x)V(A\,|\,B) \quad \text{and} \quad V(A\,|\,B) \doteq \frac{V(A\cap B)}{V(B)}. \tag{14.70}$$

It is easy to see that

$$\int_M V(A|\beta)(x)\,dx = \sum_{B\in\beta} V(A\cap B) = V(A).$$

If α and α' are two partitions of the same compact space such that each $A'_{i'} \in \alpha'$ is contained in some $A_i \in \alpha$, then α' will necessarily be at least as fine as α. This is described using the two equivalent notations

$$\alpha \leq \alpha' \qquad \Longleftrightarrow \qquad A'_{i'} \subseteq A_i$$

for some $i' \in I'$ and $i \in I$. As a result, $|I| \leq |I'|$.

Let α, β, and γ be three arbitrary finite and measurable partitions of M and let α' be another finite measurable partition such that $\alpha \leq \alpha'$. It then can be shown (see [64]) that these definitions of information and conditional information satisfy the following equalities:

$$I(\alpha \vee \beta \mid \gamma)(x) = I(\alpha \mid \gamma)(x) + I(\beta \mid \alpha \vee \gamma)(x), \tag{14.71}$$

$$\alpha \leq \alpha' \Longrightarrow I(\alpha \mid \beta)(x) \leq I(\alpha' \mid \beta)(x), \tag{14.72}$$

$$\alpha \leq \alpha' \Longrightarrow I(\alpha \vee \beta \mid \alpha')(x) = I(\beta \mid \alpha')(x). \tag{14.73}$$

14.6.6 Measure-Theoretic Entropy

Measure-theoretic entropy of a partition is defined as

$$\boxed{H(\alpha) \doteq \sum_{A\in\alpha} z(V(A)),} \tag{14.74}$$

where

$$z(\phi) \doteq \begin{cases} -\phi\log\phi & \text{if } 0 < \phi \leq 1 \\ 0 & \text{if } \phi = 0. \end{cases} \tag{14.75}$$

$H(\alpha)$ is related to $I(\alpha)(x)$ through the equality

$$H(\alpha) = \int_M I(\alpha)(x)\,dx.$$

Given two partitions, α and β, the *conditional measure-theoretic entropy* of a partition is defined in an analogous way as

$$H(\alpha\,|\,\beta) \doteq \int_M I(\alpha\,|\,\beta)(x)\,dx \tag{14.76}$$

$$= -\sum_{A\in\alpha}\sum_{B\in\beta}\left(\int_M I_A(x)I_B(x)\,dx\right)\log V(A\,|\,B) \tag{14.77}$$

$$= \sum_{B\in\beta} V(B) \sum_{A\in\alpha} z(V(A\,|\,B)). \tag{14.78}$$

It can be shown (see [76]) that these definitions of entropy and conditional entropy obey the following properties:

$$H(\alpha \vee \beta \mid \beta) = H(\alpha \mid \beta), \tag{14.79}$$

$$H(\alpha \mid \beta) = 0 \quad \text{if and only if} \quad \alpha \leq \beta, \tag{14.80}$$

$$H(\alpha \vee \beta) = H(\beta) + H(\alpha \mid \beta), \tag{14.81}$$

$$\alpha \leq \gamma \Longrightarrow H(\alpha) \leq H(\gamma), \tag{14.82}$$

$$\alpha \leq \gamma \Longrightarrow H(\alpha \mid \beta) \leq H(\gamma \mid \beta), \tag{14.83}$$

$$\alpha \leq \gamma \Longrightarrow H(\beta \mid \gamma) \leq H(\beta \mid \alpha), \tag{14.84}$$

$$H(\alpha \vee \beta \mid \gamma) \leq H(\alpha \mid \gamma) + H(\beta \mid \gamma), \tag{14.85}$$

$$H(\alpha \vee \gamma \vee \beta) + H(\beta) \leq H(\alpha \vee \beta) + H(\gamma \vee \beta), \tag{14.86}$$

$$H(\alpha \vee \beta \mid \gamma) = H(\beta \mid \gamma) + H(\alpha \mid \beta \vee \gamma). \tag{14.87}$$

Even more sophisticated concepts of entropy that are used in the description of dynamical systems have been built on this concept, including the *Kolmogorov–Sinai entropy* [47, 75] and the *topological entropy* of Adler, Konheim, and McAndrew [1]. See, for example, [54] for more details. For further reading on general ergodic theory, see [3, 8, 14, 30, 31, 54, 59, 62, 64, 69, 73, 87]. For works that emphasize the connection between ergodic theory and group theory, see [42, 45, 53, 55, 58, 61, 72, 85, 90]

14.7 Chapter Summary

This chapter established connections between stochastic differential equations and the corresponding Fokker–Planck equations which, when driven to their equilibrium distribution, results in the Maxwell–Boltzmann distribution. Specific examples in the context of DNA statistical mechanics were provided. Both a continuum filament model and multi-rigid-body models of DNA were discussed. The latter is similar to coarse-grained models of proteins and complexes formed from multiple rigid molecules [44]. The molecular theory of solvation was also discussed briefly. The Maxwell–Boltzmann distribution is a probability density on phase space, which for many real systems (including both models of DNA discussed) is a Lie group. Another outgrowth of Lie groups and statistical mechanics is ergodic theory, which was also reviewed in this chapter. The concepts of entropy in statistical mechanics, information theory, and ergodic theory all have some common features.

Although most of the progress in statistical mechanics was made by the classical contributions of Maxwell, Boltzmann, Gibbs, and so forth, more than a century ago, recent years have witnessed a number of extensions of classical statistical mechanics. These have primarily been at the interface of nonequilibrium phenomena and computational modeling of biomolecular systems and include [19, 21, 37, 38, 82, 99]. The molecular theory of solvation continues to be advanced as well [5, 24] In addition, ergodic theory remains an active area [11, 18].

On a historical note, connections between statistical mechanics and information theory have been explored for more than half a century. Brillouin made the case that scientific observation is a communication process with the noisy physical world [12]. Jaynes established connections between information theory and statistical mechanics through the principle of maximum entropy [39]. For a recent unified view of physical noise and information, see [71]. The interplay between statistical-mechanical and information-theoretic entropy have been a source of confusion from the beginning in the form of

Maxwell's demon. For collected papers on this topic, see [50, 51]. Frieden poses many physical phenomena as the extremals of Fisher information [26]. Connections among statistical mechanics, information theory, and the irreversibility of computing have also been explored in the literature [7, 25, 48, 49, 83, 100, 101]. Additionally, "information" has become one of the organizing principles of modern physics, as is epitomized by John A. Wheeler's pithy phrase "It from Bit." Such issues are discussed in a popular way in [74]. In chapters that follow, stochastic phenomena with a geometric flavor involving entropy and Fisher information will be explored. This begins in the next chapter with a quantity called "parts entropy," which is a kind of configurational entropy similar to that in statistical mechanics. One of its applications is to quantify the capabilities of robotic assembly systems, which by their very nature both interact with the physical world and and process information.

14.8 Exercises

14.1. Suppose that a mechanical system is described with two different sets of generalized coordinates $\{q_i\}$ and $\{q_i'\}$ and that the coordinate transformations $\mathbf{q} = \mathbf{q}(\mathbf{q}')$ and $\mathbf{q}' = \mathbf{q}'(\mathbf{q})$ are invertible. (In classical mechanics, changes of variables of this kind are called *point transformations.*) Let $L = L(\mathbf{q}, \dot{\mathbf{q}})$ and $L' = L'(\mathbf{q}', \dot{\mathbf{q}}')$, where $L = L'$. Starting with Lagrange's equations (14.3) defined in the generalized coordinates $\mathbf{q}$ show that Lagrange's equations will hold for L' in the coordinates $\{q_i'\}$.

14.2. In analogy with the above problem, show that Hamilton's equations of motion are also invariant under coordinate changes.

14.3. Substituting (14.20) into (14.19), verify that (14.22) is a sufficient condition for the Maxwell–Boltzmann distribution to be the equilibrium solution.

14.4. Prove (14.27) using integration by parts, assuming that the configuration variables $\mathbf{q}$ exist on direct products of compact manifolds and Euclidean space.

14.5. Verify that (14.31) is equivalent to the Gibbs formula for entropy in (14.30).

14.6. If $G = SO(3)$, the group of rotations in three-dimensional space, and $M = S^2$, the unit sphere, what will the set $\{g^i \cdot x \mid x \in M, g \in G, \forall i \in \mathbb{Z}\}$ converge to? Hint: It depends on how x and g are chosen, and so there are several different cases that need to be considered.

14.7. Two partitions α and β of a compact manifold M are said to be *independent* if for all $A \in \alpha$ and $B \in \beta$,

$$V(A \cap B) = V(A) \cdot V(B)/V(M). \tag{14.88}$$

Show that if α and β are independent, then

$$I(\alpha \vee \beta)(x) = I(\alpha)(x) + I(\beta)(x). \tag{14.89}$$

14.8. Prove (14.71)–(14.73). Hint: When $x \in A \cap B \cap C$ and $A \in \alpha$, $B \in \beta$, and $C \in \gamma$, observe that

$$I(\alpha \wedge \beta \mid \gamma)(x) = -\log \frac{V(A \cap B \cap C)}{V(C)} \quad \text{and} \quad I(\beta \mid \alpha \wedge \gamma)(x) = -\log \frac{V(B \cap A \cap C)}{V(A \cap C)},$$

and when $x \in A \cap C$ for $A \in \alpha$ and $C \in \gamma$,

$$I(\alpha \mid \gamma)(x) = -\log \frac{V(A \cap C)}{V(C)}.$$

14.9. Prove (14.79)–(14.81).

14.10. Prove (14.82)–(14.84). Hint: Use Jensen's inequality in the proof of (14.84).

14.11. Prove (14.85)–(14.87).

References

1. Adler, R.L., Konheim, A.G., McAndrew, M.H., "Topological entropy," *Trans. Am. Math. Soc.*, 114(2), pp. 309–319, 1965.
2. Allen, M.P., Tildesley, D.J., *Computer Simulation of Liquids*, Oxford University Press, Oxford, 1987.
3. Arnol'd, V.I., Avez, A., *Ergodic Problems of Classical Mechanics*, W.A. Benjamin, New York, 1968.
4. Auslander, L., Green, L., Hahn, F., *Flows on Homogeneous Spaces*, Annals of Mathematics Studies, Princeton University Press, Princeton, NJ, 1963.
5. Beck, T.L., Paulaitis, M.E., Pratt, L.R., *The Potential Distribution Theorem and Models of Molecular Solutions*, Cambridge University Press, Cambridge, 2006.
6. Bekka, M.B., Mayer, M., *Ergodic Theory and Topological Dynamics of Group Actions on Homogeneous Spaces*, Cambridge University Press, Cambridge, 2000.
7. Bennett, C.H., "The thermodynamics of computation—a review," *Int. J. Theor. Phys.*, 12, pp. 905–940, 1982.
8. Billingsley, P., *Ergodic Theory and Information*, Robert E. Krieger Publishing Co., Huntington, NY, 1978.
9. Birkhoff, G.D.,"Proof of the ergodic theorem," *Proc. Natl. Acad. Sci. USA* 17, pp. 656–660, 1931.
10. Bismut, J.-M., *Mécanique Aléatoire*, Springer-Verlag, Berlin, 1981.
11. Bowen, R., *Equilibrium States and the Ergodic Theory of Anosov Diffeomorphisms*, 2nd revised ed., Chazottes, J.-R. ed., Lecture Notes in Mathematics 470, Springer, Berlin, 2008.
12. Brillouin, L., *Science and Information Theory*, 2nd ed., Academic Press, New York, 1962.
13. Budó, A., Fischer, E., Miyamoto, S., "Einflußder Molekülform auf die dielektrische Relaxation," *Physikal. Zeitschr.*, 40, pp. 337–345, 1939.
14. Bunimovich, L.A., Dani, S.G., Dobrushin, R.L., Jakobson, M.V., Kornfeld, I.P., Maslova, N.B., Pesin, Ya. B., Sinai, Ya. G., Smillie, J., Sukhov, Yu. M., Vershik, A.M., *Dynamical Systems, Ergodic Theory, and Applications*, 2nd ed., Encyclopaedia of Mathematical Sciences Vol. 100, Springer-Verlag Berlin, 2000.
15. Chandler, D., Andersen, H.C., "Optimized cluster expansions for classical fluids. II. Theory of molecular liquids," *J. Chem. Phys.*, 57(5), pp. 1930–1937, 1972.
16. Chirikjian, G.S., Wang, Y.F., "Conformational statistics of stiff macromolecules as solutions to PDEs on the rotation and motion groups," *Phys. Rev. E*, 62(1), pp. 880–892, 2000.
17. Chirikjian, G.S., "Group theory and biomolecular conformation, I. Mathematical and computational models," *J. Phys.: Condens. Matter.* 22, 323103, 2010.
18. Choe, G.H., *Computational Ergodic Theory*, Springer, New York, 2005.
19. Crooks, G.E., "Entropy production fluctuation theorem and the nonequilibrium work relation for free energy differences," *Phys. Rev. E*, 60, pp. 2721–2726, 1999.

20. Dill, K.A., Bromberg, S., *Molecular Driving Forces: Statistical Thermodynamics in Chemistry and Biology*, Garland Science/Taylor and Francis, New York, 2003.
21. Evans, D.J., Morriss, G., *Statistical Mechanics of Nonequilibrium Liquids*, 2nd ed., Cambridge University Press, Cambridge, 2008
22. Farquhar, I.E., *Ergodic Theory in Statistical Mechanics*, Interscience Publishers/John Wiley and Sons, New York, 1964.
23. Favro, L.D., "Theory of the rotational Brownian motion of a free rigid body," *Phys. Rev.*, 119(1), pp. 53–62, 1960.
24. Feig, M., ed., *Modeling Solvent Environments: Applications to Simulations and Biomolecules*, Wiley–VCH, Weinheim, 2010.
25. Feynman, R.P., *Feynman Lectures on Computation*, T. Hey and R.W. Allen, eds., Westview Press, Boulder, Colorado, 1996.
26. Frieden, B.R., *Physics from Fisher Information*, Cambridge University Press, Cambridge, 1998.
27. Furry, W.H., "Isotropic rotational Brownian motion," *Phys. Rev.*, 107(1), pp. 7–13, 1957.
28. Gibbs, J.W., *Elementary Principles in Statistical Mechanics: Developed with Especial Reference to the Rational Foundation of Thermodynamics*, 1902 (reissued by Kessinger Publishing and BiblioBazaar, 2008).
29. Gray, C.G., Gubbins, K.E., *Theory of Molecular Fluids, Vol. 1: Fundamentals*, Clarendon Press, Oxford, 1984.
30. Gray, R. M., Davisson, L.D., eds., *Ergodic and Information Theory*, Benchmark Papers in Electrical Engineering and Computer Science Vol. 19, Dowden, Hutchinson and Ross, Stroudsburg, PA, 1977.
31. Halmos, P.R., *Lectures on Ergodic Theory*, The Mathematical Society of Japan, Tokyo, 1956.
32. Hansen, J.-P., McDonald, I.R., *Theory of Simple Liquids*, 3rd ed., Academic Press, New York, 2006.
33. Hill, T.L., *An Introduction to Statistical Thermodynamics*, Dover Publications, New York, 1960, 1986.
34. Hirata, F., ed., *Molecular Theory of Solvation*, Kluwer Academic Publishers, Dordrecht, 2003.
35. Huang, K., *Statistical Mechanics*, 2nd ed., John Wiley and Sons, New York, 1987.
36. Hubbard, P.S., "Angular velocity of a nonspherical body undergoing rotational Brownian motion," *Phys. Rev. A*, 15(1), pp. 329–336, 1977.
37. Hummer, G., Szabo, A., "Free energy reconstruction from nonequilibrium single-molecule pulling experiments," *PNAS*, 98(7), pp. 3658–3661, 2001.
38. Jarzynski C., "Nonequilibrium equality for free energy differences," *Phys. Rev. Lett.*, 78, pp. 2690–2693, 1997.
39. Jaynes, E.T., "Information theory and statistical mechanics, I+II," *Phys. Rev.*, 106(4), pp. 620–630, 1957; 108(2), pp. 171–190, 1957.
40. Jeffrey, G.B., "The motion of ellipsoidal particles immersed in a viscous fluid," *Proc. R. Soc. London. Series A*, 102(Nov. 1), pp. 161–179, 1922.
41. Kac, M., *Some Stochastic Problems in Physics and Mathematics*, Colloquium Lectures in the Pure and Applied Sciences, Magnolia Petroleum Company, 1957.
42. Kaniuth, E., *Ergodic and mixing properties of measures on locally compact groups*, Lecture Notes in Mathematics, 1210, pp. 125–129, Springer, Berlin, 1986.
43. Khinchin, A.I., *Mathematical Foundations of Statistical Mechanics*, Dover Publications, New York, 1949.
44. Kim, M.K., Jernigan, R.L., Chirikjian, G.S., "Rigid-cluster models of conformational transitions in macromolecular machines and assemblies," *Biophys. J.*, 89(1), pp. 43–55, 2005.
45. Kleinbock, D., Shah, N., Starkov, A., "Dynamics of subgroup actions on homogeneous spaces of Lie groups and applications to number theory," in *Handbook of Dynamical Systems, Vol. 1A*, B. Hasselblatt and A. Katok, eds., Chapter 11, pp. 813–930, Elsevier, Amsterdam, 2002.

46. Kleinert, H., *Path Integrals in Quantum Mechanics, Statistics, and Polymer Physics*, 2nd ed., World Scientific, Singapore, 1995.
47. Kolmogorov, A.N., "New metric invariant of transitive automorphisms and flows of Lebesgue spaces," *Dokl. Acad. Sci. USSR*, 119(5), pp. 861–864, 1958.
48. Landauer, R., "Irreversibility and heat generation in the computing process," *IBM J. Res. Dev.*, 5, pp. 183–191, 1961.
49. Landauer, R., "Dissipation and noise immunity in computation and communication," *Nature*, 335, pp. 779–784, 1988.
50. Leff, H.S., Rex, A.F., *Maxwell's Demon: Entropy, Information, Computing*, Princeton University Press, Princeton, NJ, 1990.
51. Leff, H.S., Rex, A.F., *Maxwell's Demon 2: Entropy, Classical and Quantum Information, Computing*, Institute of Physics, Bristol, 2003.
52. MacDonald, D.K.C., *Introductory Statistical Mechanics for Physicists*, Dover Publications, Mineola, NY, 2006. (originally published by John Wiley and Sones in 1963).
53. Mackey, G. W., "Ergodic Theory and its significance for statistical mechanics and probability theory," *Adv. Math.*, 12, pp. 178–268, 1974.
54. Mañé, R., *Ergodic Theory and Differentiable Dynamics* (translated from the Portuguese by Silvio Levy), Springer-Verlag, Berlin, 1987.
55. Margulis, G.A., Nevo, A., Stein, E.M., "Analogs of Wiener's ergodic theorems for semisimple groups II," *Duke Math. J.* 103(2), pp. 233–259, 2000.
56. McConnell, J., *Rotational Brownian Motion and Dielectric Theory*, Academic Press, New York, 1980.
57. McLennan, J.A., *Introduction to Non-Equilibrium Statistical Mechanics*, Prentice-Hall, Englewood Cliffs, NJ, 1989.
58. Moore, C.C., "Ergodicity of flows on homogeneous spaces," *Am. J. Math.* 88, pp. 154–178, 1966.
59. Moser, J., Phillips, E., Varadhan, S., *Ergodic Theory (A Seminar)*, Courant Institute, NYU, New York, 1975.
60. Nelson, E., *Dynamical Theories of Brownian Motion*, Princeton University Press, Princeton, NJ, 1967.
61. Nevo, A., Stein, E.M., "Analogs of Wiener's ergodic theorems for semisimple groups I," *Ann. Math., Second Series*, 145(3), pp. 565–595, 1997.
62. Ornstein, D.S., *Ergodic Theory, Randomness, and Dynamical Systems*, Yale University Press, New Haven, CT, 1974.
63. Ornstein, L.S., Zernike, F., "Accidental deviations of density and opalescence at the critical point of a single substance," *Proc. Akad. Sci. (Amst.)*, 17, 793 (1914).
64. Parry, W., *Topics in Ergodic Theory*, Cambridge University Press, Cambridge, 1981.
65. Pathria, R.K., *Statistical Mechanics*, Pergamon Press, Oxford, England, 1972.
66. Percus, J.K., Yevick, G.J., *Phys. Rev.*, 110, 1 (1958).
67. Percus, J.K., *Phys. Rev. Letters*, 8, 462 (1962).
68. Perrin, F., "Étude Mathématique du Mouvement Brownien de Rotation," *Ann. Sci. L' École Norm. Supérieure*, 45, pp. 1–51, 1928.
69. Petersen, K., *Ergodic Theory*, Cambridge University Press, Cambridge, 1983.
70. Prigogine, I., *Non-Equilibrium Statistical Mechanics*, John Wiley and Sons, New York, 1962.
71. Réfrégier, P., *Noise Theory and Applications to Physics: From Fluctuations to Information*, Springer, New York, 2004.
72. Rokhlin, V.A., "Lectures on the entropy theory of transformations with invariant measure," *Usp. Mat. Nauk.* 22, pp. 3–56, 1967; *Russ. Math. Surveys*, 22, pp. 1–52, 1967.
73. Ruelle, D., "Ergodic theory of differentiable dynamical systems," *Publ. IHES*, 50, pp. 275–306, 1979.
74. Seife, C., *Decoding the Universe*, Penguin Books, New York, 2006.
75. Sinai, Ya. G., "On the notion of entropy of dynamical systems," *Dokl. Acad. Sci. USSR*, 124(4), pp. 768–771, 1959.

76. Sinai, Ya. G., *Introduction to Ergodic Theory* (translated by V. Scheffer), Princeton University Press, Princeton, NJ, 1976.
77. Sinai, Ya.G., *Topics in Ergodic Theory*, Princeton University Press, Princeton, NJ, 1994.
78. Skliros, A., Chirikjian, G.S., "Positional and orientational distributions for locally self-avoiding random walks with obstacles," *Polymer*, 49(6), pp. 1701–1715, 2008.
79. Skliros, A., Park, W., Chirikjian, G.S., "Position and orientation distributions for non-reversal random walks using space-group Fourier transforms," *J. Alg. Statist.*, 1(1), pp. 27–46, 2010.
80. Smoluchowski, M. v., "Uber Brownsche Molekular bewegung unter Einwirkung auszerer Krafte und deren Zusammenhang mit der verralgenmeinerten Diffusionsgleichung," *Ann. Phys.*, 48, pp. 1103–1112, 1915.
81. Steele, W.A., "Molecular reorientation in liquids. I. Distribution functions and friction constants. II. Angular autocorrelation functions," *J. Chem. Phys.*, 38(10), pp. 2404–2410, 2411–2418, 1963.
82. Sugita, Y., Okamoto, Y., "Replica-exchange molecular dynamics method for protein folding," *Chem. Phys. Lett.*, 314, pp. 141–151, 1999.
83. Szilard, L., "On the decrease of entropy in a thermodynamic system by the intervention of intelligent beings," *Zeit. Phys.*, 53, pp. 840–856, 1929 (in German, English translation in *Quantum Theory and Measurement*, J.A. Wheeler and W.H. Zurek, eds., pp. 539–548, Princeton University Press, Princeton, NJ, 1983).
84. Tao, T., "Time-dependent fluorescence depolarization and Brownian rotational diffusion coefficients of macromolecules," *Biopolymers*, 8(5), pp. 609–632, 1969.
85. Templeman, A., *Ergodic Theorems for Group Actions: Informational and Thermodynamical Aspects*, Kluwer Academic Publishers, Dordrecht, 1992.
86. Tolman, R.C., *The Principles of Statistical Mechanics*, Dover Publications, New York, 1979.
87. Ulam, S.M., von Neumann, J., "Random ergodic theorems," *Bull. Am. Math. Soc.*, 51(9), p. 660, 1947.
88. von Neumann, J., "Proof of the quasi-ergodic hypothesis," *Proc. Natl. Acad. Sci. USA*, 18, pp. 70–82, 1932.
89. von Neumann, J., "Physical applications of the ergodic hypothesis," *Proc. Natl. Acad. Sci. USA*, 18, pp. 263–266, 1932.
90. Walters, P., *An Introduction to Ergodic Theory*, Springer-Verlag, New York, 1982.
91. Weber, G., "Rotational Brownian motion and polarization of the fluorescence of solutions," *Adv Protein Chem.*, 8, pp. 415–459, 1953.
92. Welecka, J.D., *Fundamentals of Statistical Mechanics: Manuscript and Notes of Felix Bloch*, Imperial College Press/World Scientific Publishing, London/Singapore, 2000.
93. Weyl, H., "Uber die Gleichverteilung von Zahlen mod 1," *Math, Ann.* 77, pp. 313–352, 1916.
94. Wiener, N., "The Ergodic theorem," *Duke Math. J.*, 5, pp. 1–18, 1939.
95. Wiener, N., *Cybernetics: or Control and Communication in the Animal and the Machine*, 2nd ed., The MIT Press, Cambridge, MA, 1961.
96. Zhou, Y., Chirikjian, G.S., "Conformational statistics of semi-flexible macromolecular chains with internal joints," *Macromolecules*, 39(5), pp. 1950–1960, 2006.
97. Zhou, Y., Chirikjian, G.S., "Conformational statistics of bent semiflexible polymers," *J. Chem. Phys.,* 119(9), pp. 4962–4970, 2003.
98. Zimmer, R.J., Morris, D.W., *Ergodic Theory, Groups, and Geometry.* American Mathematical Society, Providence, RI, 2008.
99. Zuckerman, D.M., Woolf, T.B., "Efficient dynamic importance sampling of rare events in one dimension," *Phys. Rev. E*, 63, 016702 (2000).
100. Zurek, W.H. ed., *Complexity, Entropy and the Physics of Information*, Sante Fe Institute Studies in the Sciences of Complexity Vol. 8, Addison-Wesley, Reading, MA, 1990.
101. Zurek, W.H., "Thermodynamic cost of computation, algorithmic complexity, and the information metric," *Nature*, 341, pp. 119–124, 1989.

15

Parts Entropy and the Principal Kinematic Formula

Automated (robotic) assembly systems that are able to function in the presence of uncertainties in the positions and orientations of feed parts are, by definition, more robust than those that are not able to do so. This can be quantified with the concept of "parts entropy," which is a statistical measure of the ensemble of all possible positions and orientations of a single part confined to move in a finite domain. In this chapter the concept of parts entropy is extended to the case of multiple interacting parts. Various issues associated with computing the entropy of ensembles of configurations of parts with excluded-volume constraints are explored. The rapid computation of excluded-volume effects using the "principal kinematic formula" from the field of Integral Geometry is illustrated as a way to potentially avoid the massive computations associated with brute-force calculation of parts entropy when many interacting parts are present.

The most important points to take away from this chapter are as follows:

- The difficulty of assembling a machine composed of rigid parts is related to the shape of the individual parts and how they are brought together to form an assemblage, and the concept of "parts entropy" can be used to quantify the difficulty of automated assembly.
- The principal kinematic formula can be used to evaluate, in closed-form, the volume in $SE(3)$ corresponding to all possible motions that lead to the intersection of two solid bodies.
- Knowing how bodies occlude each other influences the entropy of an ensemble of configurations of a collection of bodies.
- These effects can be bounded by combining the principal kinematic formula and concepts from functional/harmonic analysis on Lie groups.

This chapter is organized as follows. Section 15.1 provides an introduction to the field of automated assembly planning and motivates the use of an entropy concept that shares features from both information theory and statistical mechanics, the so-called "parts entropy." Section 15.2 formulates the problems mathematically. Section 15.3 explains how the principal kinematic formula from the field of stochastic/integral geometry can be used to rapidly evaluate quantities of potential importance in assembly planning. Section 15.4 presents a differential-geometric proof of the principal kinematic formula using nothing more than the basic differential-geometric tools from Chapter 5 of Volume 1. Section 15.5 provides some simple examples to illustrate these formulas. Section 15.6 extends these ideas and derives some new inequalities. Section 15.7 reviews (without proof) generalizations of these formulas to rigid-body motions in higher-dimensional Euclidean spaces that have been presented in the literature. Section 15.8

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_6,

reviews differential-geometric generalizations of the principal kinematic formula where actions of a unimodular Lie group on subsets of homogeneous spaces replaces motions of bodies in $\mathbb{R}^n$ and integration is performed with respect to the Haar measure. Section 15.9 generalizes the classical formula to include non-Haar probability densities. In such cases, it is difficult to obtain formulaes, but inequalities are abundant. Section 15.10 provides bounds on the integral of the square of the Euler characteristic. Sections 15.11, 15.12, and 15.13 consider various extensions to the case of multiple parts connected by joints and illustrate how these methods can be applied to computing (or at least bounding) parts entropy in assembly planning. Finally, Section 15.14 summarizes the chapter and Section 15.15 presents exercises.

15.1 Introduction

In the field of assembly automation it has long been known that the design of machines that assemble parts should take advantage of part geometries [14, 15]. Additionally, robotic systems with minimal sensing can perform assembly operations if information about the parts and environment is known [29]. Systems that shake or otherwise randomize part positions and orientations (i.e., "poses") allow a collection of parts to sample the ensemble of all possible poses. More than 25 years ago, Sanderson quantified the concept of part disorder by defining the concept of "parts entropy" [60]. In his analysis, he considered the tractable problem of noninteracting parts, thereby focusing on individual part entropies. In contrast, in this chapter the concept of parts entropy is extended to the case of multiple interacting parts. Various issues associated with computing the entropy of ensembles of configurations of parts with excluded-volume constraints are explored. The rapid computation of excluded-volume effects using the "principal kinematic formula" from the field of Integral Geometry is illustrated. References in the English language on this topic include [6, 61].

This is all relevant to assembly automation because assembly systems that are able to function in the presence of uncertainties in feed part positions and orientations are more robust than those that are not able to do so. Therefore, having a way to compute the entropy of parts over a statistical ensemble of different feed configurations provides a measure of the capabilities of an assembly automation system. Such metrics quantify the relative effectiveness of such systems and open up new possibilities for quantifiable design principles.

15.2 Problem Formulation

In the first subsection of this section, the concept of the entropy of a single part is reviewed and slightly modified in the context of different terminology. Given N parts that are sparsely scattered in an environment, the total parts entropy can be approximated as the sum of the individual part entropies. This approximation, although always an upper bound, is not accurate when the environment is more cluttered due to excluded volume (noninterpenetration) effects. These issues are addressed in the second subsection.

15.2.1 A Continuous Version of Sanderson's Parts Entropy

Information-theoretic entropy has been used by Sanderson to characterize parts for use in assembly operations [60]. The position and orientation of a part is described by a group element $g \in G$, where $G = SE(3)$ is the group of rigid-body motions. If the part can attain poses with a particular frequency of occurrence at a particular time, which is described by a probability density function $f(g;t)$, then its entropy is defined as

$$S_f(t) = -\int_G f(g;t) \log f(g;t)\, dg, \tag{15.1}$$

where dg is the bi-invariant integration measure (i.e., volume element) with which to integrate (see Chapter 12).

How is $f(g;t)$ defined? Imagine that a single part is placed at random in an environment. Additionally, imagine that this is repeated over many trials. The result can be summarized with a probability density function $f(g;0)$, where 0 indexes the initial time. From each of the random initial conditions that are collectively defined as $f(g;0)$, an assembly task can be attempted. If successful, the assembly task will result in the part being placed at its desired location g_1. Therefore, over the ensemble of trials, the probability will evolve from $f(g;0)$ to $\delta(g_1^{-1} \circ g)$ (a Dirac delta function indicating that the part is placed in its desired location). The evolution of probability of part pose over this ensemble of trials can be described as $f(g;t)$, and the associated part entropy is $S_f(t)$. Clearly, $S_f(t)$ decreases during a successful assembly process. If $\delta(g_1^{-1} \circ g)$ is defined to allow for some small but finite part tolerance, then S_δ will be finite, and as $S_f(t) - S_\delta$ approaches 0, it means that the part is being successfully placed. $S_f(t)$ in (15.1) is essentially Shannon's entropy.

Sanderson adapted concepts from information theory to consider the entropy of rigid parts [60]. In this context, the probability density function, $f(g)$, describes the set of all possible poses of a rigid part ($g \in SE(3)$) as it is randomly placed on a substrate over an ensemble of experiments. The corresponding entropy is called "parts entropy." Sanderson measured parts entropy in bits of information assuming that sensors have a finite resolution in each generalized coordinate used to parameterize rigid-body motion. In contrast, continuous motion is addressed here.

15.2.2 Multiple Parts

An assembly process can be thought of as one in which the initial probability densities for each of the i parts converge to their desired locations $\{g_i\}$:

$$f_i(g;t) \to \delta(g_i^{-1} \circ g) \quad \text{as } t \to T,$$

where T is the total time allowed for the assembly to be completed.

Given n parts, the ith of which is free to be placed arbitrarily in an environment with frequency of occurrence given by $f_i(g_i;t)$, the entropy will be bounded by $S'(t) \leq \sum_{i=1}^{n} S_i(t)$, where S_i is the entropy of the ith part computed independently (i.e., as if that were the only part). If, however, the environment is very cluttered and there is not a significant amount of free space, this bound will not be tight and the entropy of the joint distribution of parts will have to be computed:

$$S'(t) = -\int_{G^n} f' \log f' \, dg_1 \cdots dg_n, \quad \text{where} \int_{G^n} = \int_G \cdots \int_G \tag{15.2}$$

and $f' = f'(g_1, g_2, \ldots, g_n; t)$.

In the independent case,

$$f(g_1, g_2, \ldots, g_n; t) = \prod_{i=1}^{n} f_i(g_i; t), \quad \text{where} \int_G f_i(g_i; t)\, dg_i = 1 \tag{15.3}$$

for each $i = 1, \ldots, n$. In general, this simple form is not realistic and needs to be augmented to reflect the excluded volume of parts since no two parts can occupy the same space at the same time.

To begin, let us consider functions $I_{C_i}(\mathbf{x})$ that take the value of 1 on part C_i and 0 otherwise.[1] For the sake of concreteness, assume that the part is centered on the identity reference frame with its principal axes of inertia aligned with the coordinate axes. Then if body C_i is moved by rigid-body motion g_i, and likewise for body C_j, we can compute their overlap as

$$w_{C_i,C_j}(g_i, g_j) = \int_{\mathbb{R}^3} I_{C_i}(g_i^{-1} \circ \mathbf{x})\, I_{C_j}(g_j^{-1} \circ \mathbf{x})\, d\mathbf{x}.$$

A general property of integration over all of three-dimensional space is that it is invariant under rigid-body motions. Therefore, if we make the change of variables $\mathbf{y} = g_i^{-1} \circ \mathbf{x}$, then we find that

$$w_{C_i,C_j}(g_i, g_j) = w_{C_i,C_j}(e, g_i^{-1} \circ g_j) = w_{C_i,C_j}(g_j^{-1} \circ g_i, e).$$

Clearly, when the two bodies do not overlap, $w_{C_iC_j} = 0$, and if they do overlap, then $w_{C_iC_j} > 0$. This can be "windowed" and made binary. If there is any overlap, let $W_{C_iC_j}(g_i^{-1} \circ g_j) = 1$, and if there is no overlap, let $W_{C_i,C_j}(g_i^{-1} \circ g_j) = 0$. In other words,

$$W_{C_i,C_j}(g_i^{-1} \circ g_j) = u[w_{C_i,C_j}(g_i, g_j)], \tag{15.4}$$

where $u[\cdot]$ is the unit Heaviside step function.

Then the original naive $f(g_1, g_2, \ldots, g_n; t)$ in (15.3), which might reflect the allowable motions of each part constrained by the environment, can be replaced with one of the form

$$f'(g_1, g_2, \ldots, g_n; t) = \alpha \cdot f(g_1, g_2, \ldots, g_n; t) \prod_{i<j}^{n} [1 - W_{C_i,C_j}(g_i^{-1} \circ g_j)], \tag{15.5}$$

which accounts for the fact that pairwise overlaps of bodies is not permitted. Here, α is the normalization required to make f' a probability density function—that is, such that

$$\int_{G^n} f'\, dg_1 \cdots dg_n = 1.$$

Note that the product in (15.5) is not only over sequentially local pairs of bodies, but rather all pairs of bodies, where the "$i < j$" simply avoids double counting. Accounting for all pairwise interactions automatically removes three or more interacting bodies.

In this way we have a tool for assessing the entropy of the unassembled state of parts in a confined environment. The change in entropy from the random ensemble of

[1] The notation C_i will be used throughout this chapter to denote the ith rigid body in a collection of bodies. The letter C comes from the word "corpus." When C is convex, the formulation simplifies, although what is stated is true more generally when convexity is not mentioned.

part conformations to the fully assembled product, $\Delta S = S_{f'} - S_{\delta}$, is a measure of how much disorder the assembly process reduces.

One way to assess the quality of the design of a product to be assembled is how much entropy must be overcome to assemble it from the disassembled ensemble to the final assembly state. In other words, a design for which ΔS is small is easy to assemble and is therefore a good design. In contrast, one measure of how good an assembly automation system is is how large of a ΔS it can handle and still successfully assemble parts.

Naively, the computer-age way to compute probabilities such as f' and the associated entropy $S_{f'}$ would be to uniformly sample all possible positions and orientations of the moving body and to record the ratio of the number of intersects to the total. Computing power is sufficiently large these days that this computation could be done for two (or maybe three) planar bodies. However, for three-dimensional problems, where the space of motions for a rigid body is six dimensional, sampling each spatial dimension results in $O(N^6)$ motions. For each motion, intersections can be assessed by numerical integration (to compute a volume of overlap) or sampling in $O(N^3)$. Therefore, $O(N^9)$ operations would be used. This is a daunting calculation. Additionally, if there are instead m bodies, the result becomes $O(N^{6m+3})$. Fortunately, over the past century, methods have been developed by a small group of pure mathematicians to compute integrals of interest analytically in closed form. In particular, a result called the principal kinematic formula will be used here.

15.3 Principal Kinematic Formulas

The field of Integral Geometry (also called Geometric Probability and Stochastic Geometry) is concerned with properties of random configurations of geometric objects and properties relating to random motions of these objects. Of particular relevance to the current discussion is the principal kinematic formula, which is concerned with evaluating the probability of intersection of two rigid bodies when one body moves uniformly at random relative to another body that his held fixed. Results from this field that are applicable to the computation of parts entropy are adapted here.

15.3.1 The Principal Kinematic Formula

Recall that a body, viewed as a subset of $\mathbb{R}^n$, is convex if the line segment connecting two points in the body is contained in the body for all possible choices of pairs of points. Another way to say this is that if for any $\mathbf{x}, \mathbf{y} \in C \subset \mathbb{R}^n$, then the condition $t\mathbf{x} + (1-t)\mathbf{y} \in C$ for all $t \in [0,1]$ means that C is convex.

The *indicator function* on any measurable body C (not necessarily convex and perhaps not even connected) is defined by

$$\iota(C) \doteq \begin{cases} 1 & \text{if } C \neq \emptyset \\ 0 & \text{for } C = \emptyset. \end{cases}$$

If $g \in G$ is an element of a group that acts on C without shrinking it to the empty set, then $\iota(gC) = \iota(C)$, where

$$gC \doteq \{g \cdot \mathbf{x} | \mathbf{x} \in C\}.$$

For now, let $G = SE(n)$, the group of rigid-body motions in $\mathbb{R}^n$. If $g = (A, \mathbf{a})$ is the rigid-body motion with rotational part $A \in SO(n)$ and translational part $\mathbf{a} \in \mathbb{R}^n$, then recall from Chapter 10 that the action of G on $\mathbb{R}^n$ is $g \cdot \mathbf{x} = A\mathbf{x} + \mathbf{a}$ and, hence, gC is well defined. The indicator function is one of many functions on a body that is invariant under rigid-body motion. Others include the volume of the body and the surface area (or perimeter in the two-dimensional case).

Suppose that we have two convex bodies, C_0 and C_1. Let C_0 be stationary and let C_1 be mobile. The intersection of these two convex bodies is either a convex body or is empty. Furthermore, the rigid-body motion (or even affine deformation) of a convex body does not change the fact that it is convex. Therefore, when $C_0 \cap gC_1$ is not empty, it will be a convex body and

$$f_{C_0,C_1}(g) \doteq \iota(C_0 \cap gC_1)$$

will be a compactly supported function on G that takes the value of 1 when C_0 and the moved version of C_1 (denoted as gC_1) intersect, and it will be 0 otherwise. The function $f_{C_0,C_1}(g)$ has some interesting properties—namely if we shift the whole picture by an amount g_0, then this does not change the value of $f_{C_0,C_1}(g)$. In other words,

$$\iota(g_0(C_0 \cap gC_1)) = \iota(g_0C_0 \, \cap \, (g_0 \circ g)C_1).$$

This means that if we choose $g_0 = g^{-1}$, then

$$f_{C_0,C_1}(g) = \iota((g^{-1}C_0) \cap C_1) = \iota(C_1 \cap g^{-1}C_0) = f_{C_1,C_0}(g^{-1}).$$

In the special case when $C_0 = C_1$ (i.e., they are two copies of the same body), then $f_{C_0,C_0}(g) = f_{C_0,C_0}(g^{-1})$, which is called a symmetric function.

More generally, "counting up" all values of g for which an intersection occurs is then equivalent to computing the integral

$$\mathcal{I}(C_0, C_1) = \int_G \iota(C_0 \cap gC_1)\, dg. \tag{15.6}$$

Note that $\mathcal{I}(C_0, C_1) = \int_G W_{C_0,C_1}(g)\, dg$, where $W_{C_0,C_1}(g)$ is exactly the quantity of interest in the previous section.

A somewhat amazing result is that the integral $\mathcal{I}$ can be computed exactly using only elementary geometric properties of the bodies C_0 and C_1 without actually having to perform an integration over G. Although the general theory has been developed by mathematicians for the case of bodies in $\mathbb{R}^n$ [20] and in manifolds on which some Lie group acts (see [61] and references therein), we are concerned only with the cases of bodies in $\mathbb{R}^2$ and $\mathbb{R}^3$. Furthermore, integrals similar to (15.6) where the integrand is not $\iota(\cdot)$, but other so-called "mixed volumes" can also be computed in closed form [20, 61]. The following subsections review this formula in the cases of planar and spatial bodies.

15.3.2 The Planar Case

A closed arc-length-parameterized curve of length L in the plane can be described (up to rigid-body motion) using the equation

$$\mathbf{x}(s) = \begin{pmatrix} \displaystyle\int_0^s \cos\theta(\sigma)\, d\sigma \\ \displaystyle\int_0^s \sin\theta(\sigma)\, d\sigma \end{pmatrix},$$

where

$$\theta(s) = \int_0^s \kappa(\sigma)\, d\sigma$$

is the counterclockwise-measured angle that the tangent to the curve makes with respect to the x axis and $s \in [0, L]$.

The condition that the curve is closed is given by $\mathbf{x}(L) = \mathbf{0}$, and differentiability of the curve is guaranteed if $\theta(s)$ is continuous on $s \in [0, L]$ and $\theta(L) = 0$ (which ensures that the tangent at $\mathbf{x}(L)$ matches that at $\mathbf{x}(0)$. Continuity of the tangent direction can be relaxed to handle polygonal objects by allowing $\kappa(s)$ to be a sum of shifted Dirac delta functions, which makes $\theta(s)$ piecewise constant.

Regardless, for a convex body, the signed curvature $\kappa(s)$ is always non-negative. For a simple, convex, closed curve, two global intrinsic quantities can be defined: the perimeter L and the area enclosed by the curve, A. The normalized integral of total signed curvature,

$$\chi = \theta(L)/2\pi,$$

is then equal to 1. If this curve bounds a simply connected region, then $\chi = 1$ is both the indicator function and the Euler characteristic of that region. However, in more general cases in which a domain is not connected or not simply connected, then multiple closed curves define the boundaries of the domain and, in these cases, $\chi \neq 1$.

In the planar case, we can write (15.6) explicitly as

$$\mathcal{I}(C_0, C_1) = \int_{-\pi}^{\pi} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \iota(C_0 \cap g(b_1, b_2, \theta) C_1)\, db_1\, db_2\, d\theta, \tag{15.7}$$

where $g = (R, \mathbf{b})$ is described by

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

the vector $\mathbf{b} = [b_1, b_2]^T$, and $g(b_1, b_2, \theta)$ is defined as in (10.75).

Theorem 15.1 *(Blaschke, [11, 12]).* *Given planar convex bodies C_0 and C_1, then (15.7) evaluates as*

$$\mathcal{I}(C_0, C_1) = 2\pi[A(C_0) + A(C_1)] + L(C_0)L(C_1), \tag{15.8}$$

where $A(\cdot)$ is the area and $L(\cdot)$ is the perimeter of the body.

For the proof, see [11, 12, 61] and Section 15.4.1.

In Integral Geometry, the statement of this theorem is in terms of the Euler characteristic rather than the indicator function. Recall that the Euler characteristic of a surface bounding a body C, which is denoted as $\chi(\partial C)$, is a topological invariant of the surface. The Euler characteristic of the corresponding body is denoted as $\chi(C)$. For a simply connected three-dimensional body, $\chi(C) = 1$, whereas $\chi(\partial C) = 2$. In the planar case, the Euler characteristic of a region is just the integral of signed curvature normalized by 2π as defined earlier.

In the nonconvex case, we can bound the integral of interest from below and above by inscribing and circumscribing convex bodies inside and outside of C_0 and C_1. Then computing (15.8) with the convex inscribed/circumscribed bodies will give lower and upper bounds on (15.8) for nonconvex C_0 and C_1.

It is clear from (15.8) that the inscribed convex body should have as large of an area and perimeter as possible in order to obtain a lower bound that is as tight as possible. However, it is not clear what the trade-off between area and perimeter should be. Likewise, for the circumscribed convex body, the tightest upper bound will be obtained by a body of minimal area and perimeter.

15.3.3 The Spatial Case

It follows that if the spatial body C has a continuous piecewise differentiable surface, ∂C, that we can compute:

$$\int_{\partial C} dS = F(C)$$

(the total surface area). Furthermore, if κ denotes the Gaussian curvature at each point on the surface, we can compute (via the Gauss–Bonnet theorem):

$$\int_{\partial C} \kappa \, dS = 2\pi \, \chi(\partial C),$$

where $\chi(\partial C)$ is the Euler characteristic of the bounding surface. As discussed in Chapter 5, in the case of spatial bodies, $\chi(\partial C) = 2 \cdot \chi(C)$. Additionally, for simply connected planar and spatial bodies, $\chi(C) = \iota(C) = 1$.

In differential geometry, a second kind of curvature is defined at every point on a surface. This is the *mean curvature*, m, as discussed in Chapter 5. The total mean sectional curvature is defined as

$$M(C) = \int_{\partial C} m \, dS,$$

and the volume of C is computed as

$$V(C) = \int_{\mathbb{R}^3} I_C(\mathbf{x}) \, d\mathbf{x} = \int_C d\mathbf{x}.$$

If spatial rigid-body motions are parameterized as

$$g(b_1, b_2, b_3; \alpha, \beta, \gamma) = \begin{pmatrix} R(\alpha, \beta, \gamma) & \mathbf{b} \\ \mathbf{0}^T & 1 \end{pmatrix},$$

where $R(\alpha, \beta, \gamma)$ denotes the ZXZ Euler-angle parameterization and $\mathbf{b} \in \mathbb{R}^3$, then the bi-invariant integration measure is, to within an arbitrary scaling constant,

$$dg = \sin \beta \, d\alpha \, d\beta \, d\gamma \, db_1 \, db_2 \, db_3.$$

Theorem 15.2 *(Blaschke, [11, 12]). Given convex bodies C_0 and C_1 in $\mathbb{R}^3$, then*

$$\mathcal{I}(C_0, C_1) = 8\pi^2[V(C_0) + V(C_1)] + 2\pi[F(C_0)M(C_1) + F(C_1)M(C_0)], \tag{15.9}$$

where $F(\cdot)$ and $M(\cdot)$ are respectively the area and integral of mean curvature of the surface enclosing the body and $V(\cdot)$ is the volume of the body.

For the proof, see [11, 12, 61] and Section 15.4.2.

Again, we would really like to be able to compute (15.9) for nonconvex bodies, but it does not apply in that case, although integrals of the Euler characteristic can be obtained in that case.

15.4 Differential-Geometric Derivation of the Principal Kinematic Formula

In this section the principal kinematic formula of Blaschke and Poincaré is derived in the plane and in three-dimensional Euclidean space. This formula relates integrals of geometric quantities such as the volume (or area) inside of a body, its total surface area (or perimeter), and total mean curvature with the properties of intersections of bodies as one is rigidly moved over the other. The proofs provided here use the basic differential geometry of parametric curves and surfaces. Although fully rigorous, this approach is somewhat cumbersome. More elegant and general formulations from the field of Integral Geometry/Geometric Probability/Stochastic Geometry are reviewed in subsequent sections. However, it also will be shown that the parametric approach presented here generalizes in some useful ways not covered by the more elegant methods.

The issue addressed here is the calculation of the integral

$$\begin{aligned}\mathcal{I}(C_0, C_1) &= \int_G \iota(C_0 \cap gC_1)\, dg = \int_G \iota(g^{-1}C_0 \cap C_1)\, dg \\ &= \int_G \iota(gC_0 \cap C_1)\, dg = \int_G \iota(C_1 \cap gC_0)\, dg = \mathcal{I}(C_1, C_0),\end{aligned} \tag{15.10}$$

where C_i are finite bodies in $\mathbb{R}^n$ and $\iota(\cdot)$ is the set indicator function.

Here, $\mathcal{I}(C_0, C_1)$ denotes that C_0 is fixed in space and C_1 is “moved around” under the action of $G = SE(n)$, with gC_1 denoting the version of C_1 that has been moved by $g \in G$. The bi-invariance of the integration measure dg yields the symmetry of the function I in (15.10). It also means that $\mathcal{I}(C_0, C_1) = \mathcal{I}(hC_0, hC_1)$ for any $h \in G$. Therefore, the way that C_0 is fixed in space is irrelevant, as is the choice of which body is considered to be moving and which one is considered to be fixed.

15.4.1 The Planar Case

In this subsection the principal kinematic formula[2] of Blaschke is reviewed. First, some integrals associated with star-shaped regions in the plane are computed. Then these are used to prove the theorem.

Integrals for Planar Star-Shaped Regions

A star-shaped region, or body, in the plane is a shape for which any point can be connected to a special point, referred to here as the center of the region, with a line segment contained in the region. Therefore, all convex bodies are star-shaped, but star-shaped regions need not be convex. Figure 15.1 illustrates a star-shaped planar region together with the coordinates and reference frames used to describe its geometry.

The interior of any smooth star-shaped region in the plane can be parameterized as

$$\mathbf{x}(\rho, \phi) = \begin{pmatrix} r(\rho, \phi) \cos \phi \\ r(\rho, \phi) \sin \phi \end{pmatrix}, \tag{15.11}$$

where $r(\rho, \phi)$ is monotonically increasing in $\rho \in [0, 1]$ and smooth in both arguments. Here, $\mathbf{x} = 0$ is the center defined by $r(0, \phi) = 0$. The collection of all such points is

[2] Also called the fundamental kinematic formula, or simply the kinematic formula

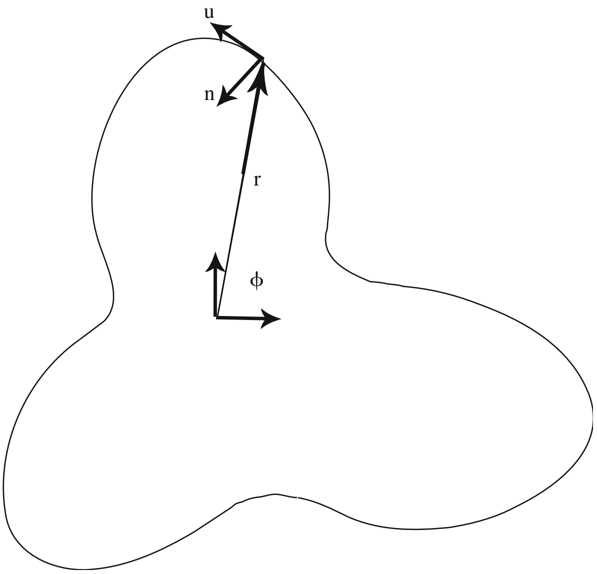


Fig. 15.1. A Planar Star-Shaped Region and Associated Quantities

denoted as C, and its boundary, defined by the condition $\rho = 1$, is parameterized as $\mathbf{x}(1, \phi) \in \partial C$.

The Jacobian associated with this parameterization is

$$J = \begin{bmatrix} \frac{\partial \mathbf{x}}{\partial \rho} & \frac{\partial \mathbf{x}}{\partial \phi} \end{bmatrix} = \begin{bmatrix} \frac{\partial r}{\partial \rho} \cos \phi & \frac{\partial r}{\partial \phi} \cos \phi - r \sin \phi \\ \frac{\partial r}{\partial \rho} \sin \phi & \frac{\partial r}{\partial \phi} \sin \phi + r \cos \phi \end{bmatrix}.$$

Since $|J| = r\partial r/\partial \rho$, it follows that

$$A = \int_0^1 \int_0^{2\pi} r \frac{\partial r}{\partial \rho} \, d\phi \, d\rho. \tag{15.12}$$

In the case when $r(\rho, \phi) = \rho \cdot r(1, \phi)$, (15.12) becomes

$$A = \frac{1}{2} \int_0^{2\pi} [r(1, \phi)]^2 \, d\phi.$$

For each fixed value of ρ, the resulting closed curve will be referred to here as a *shell*. The monotonicity of the function $r(\rho, \phi)$ in the parameter ρ means that C is partitioned into disjoint shells:

$$\bigcup_{\rho \in [0,1]} \partial C(\rho) = C \quad \text{and} \quad \partial C(\rho) \cap \partial C(\rho') = \begin{cases} \partial C(\rho) & \text{if } \rho = \rho' \\ \emptyset & \text{otherwise.} \end{cases} \tag{15.13}$$

The arc length of each closed curve defined by a fixed value of r will be

$$L = \int_0^{2\pi} \left\| \frac{\partial \mathbf{x}}{\partial \phi} \right\| d\phi = \int_0^{2\pi} \left[\left(\frac{\partial r}{\partial \phi} \right)^2 + r^2 \right]^{\frac{1}{2}} d\phi. \tag{15.14}$$

The total curvature of each shell can be calculated by first observing that the unit tangent to each point on a shell is

$$\mathbf{u}(\phi) = \left\| \frac{\partial \mathbf{x}}{\partial \phi} \right\|^{-1} \frac{\partial \mathbf{x}}{\partial \phi}. \tag{15.15}$$

Then the curvature at each point in the shell defined by fixed value of ρ is computed as

$$\kappa = \left\| \frac{\partial \mathbf{u}}{\partial s} \right\| = \left\| \frac{\partial \mathbf{u}}{\partial \phi} \frac{\partial \phi}{\partial s} \right\| = \left\| \frac{\partial \mathbf{x}}{\partial \phi} \right\|^{-1} \left\| \frac{\partial \mathbf{u}}{\partial \phi} \right\|.$$

Substituting the definition of $\mathbf{x}(\rho, \phi)$ in (15.11) into the above two equations results in

$$\kappa = \frac{|r^2 + 2(r')^2 - rr''|}{[r^2 + (r')^2]^{\frac{3}{2}}},$$

where $' = \partial/\partial\phi$. The signed curvature, k, results from removing the absolute value sign in the above equation. The total curvature is then

$$K = \oint k\, ds = \int_0^{2\pi} k \cdot \left\| \frac{\partial \mathbf{x}}{\partial \phi} \right\| d\phi = \int_0^{2\pi} \frac{r^2 + 2(r')^2 - rr''}{r^2 + (r')^2} d\phi = 2\pi$$

when $r > 0$. This follows from the fact that

$$\frac{r^2 + 2(r')^2 - rr''}{1 + (r')^2} = 1 - \frac{(r'r^{-1})'}{1 + (r'r^{-1})^2} = 1 - [\tan^{-1}(r'r^{-1})]',$$

and since $r > 0$ for all values of $\phi \in [0, 2\pi]$, $r(0) = r(2\pi)$, and $r'(0) = r'(2\pi)$, the second term integrates to 0.

Intersections of Moving Planar Star-Shaped Regions

Suppose that there are two regions (or bodies) C_0 and C_1 defined by parametric curves $\mathbf{x}_1$ and $\mathbf{x}_2$ of the form in (15.11), which are, in turn, defined by $r_1(\rho_1, \phi_1)$ and $r_2(\rho_2, \phi_2)$.[3] If these bodies are convex, their intersection will be as well, and given any fixed point on the surface of C_0, it is possible for any point on the surface of C_1 to contact that fixed point without any other part of C_1 intersecting C_0. In general, this will not be true for nonconvex bodies, but there are special cases when it will be. This will be useful in our proof of the principal kinematic formula.

Figure 15.2(left) illustrates a case in which the surfaces of a star-shaped body, C_0, and a convex body, C_1, intersect at a single point. Moreover, if C_1 slides so that another point on its surface comes into contact with C_0 at the original point, it will still be the case that only one point of intersection exists between the bodies. Additionally, if C_1 is decomposed into concentric shells, this will be true for all of these shells as well.

[3] Note that the planar body C_i is described by the boundary curve $\mathbf{x}_{i+1}$, which is in turn described by the function $r_{i+1}(\rho_{i+1}, \phi_{i+1})$.

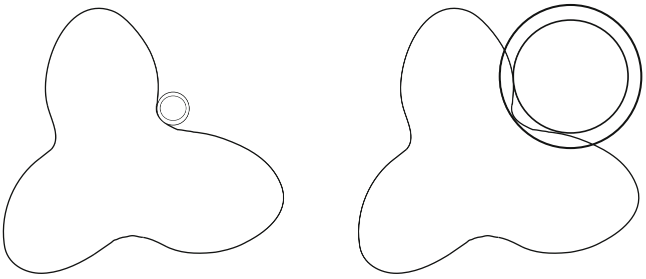


Fig. 15.2. Intersection of a Star-Shaped Body and Convex Body: (left) a Case When the Largest Shell of the Convex Body Can Intersect the Star at Exactly One Point Without Inner Shells Intersecting; (right) a Case When Intersection of Outer Shell at One Point Causes Inner Shells to Make Contacts with the Star

In contrast, Figure 15.2(right) shows a very different picture. In this case, the surface of C_1 cannot make contact with every point on the surface of C_0 without sometimes having multiple contacts. When the surface of C_1 makes a contact, shells from which C_1 is constructed also make contacts. These observations will be useful later in a proof of the principal kinematic formula that does not require the bodies to be convex but does require the situation in Figure 15.2(left) while excluding the one in Figure 15.2(right). The difference between these cases can be described as follows. *When the maximal radius of C_1, $r_{max} = \max_{\phi_2} \|\mathbf{x}_2(1, \phi_2)\|$, is smaller than half the distance between points on any pair of arms of the star, C_0, and if the maximal radius of curvature of C_1, $1/\kappa_2$, is smaller than the smallest radius of curvature of the fillets of the star, then the two bodies can always make contact at a single point, even though one is not convex.* Of course, if both bodies are convex, then these conditions are satisfied trivially since there are no arms or fillets. However, if these conditions do not hold in the nonconvex case, then situations such as in Figure 15.2(right) can result.

Computing (15.10) in the planar case, under the assumption that all intersections are simply connected, can be performed by decomposing all planar rigid-body motions of C_1 into two parts. The first part consists of translating the center of C_1 over all points in C_0. This is guaranteed to result in intersections between C_0 and C_1. Likewise, if C_1 is rotated about its center that has been translated to each of the points in C_0, the intersection between C_0 and C_1 will be nonempty. Therefore, part of the total motions contributing to (15.10) will be $2\pi A(C_0)$, where $A(C_0)$ is the area of C_0 (since C_1 is moved to each point/position in C_0) and 2π indicates that all planar rotations of C_1 pinned to each of these positions result in an intersection.

Now, suppose that C_1 is decomposed into disjoint shells defined by $r_2(\rho_2, \phi_2)$ for each value of $\rho_2 \in [0, 1]$. Imagine that each of these shells is brought into contact with the boundary ∂C_0. If all possible contact states are recorded and if all such contacts result in no intersections between the bodies other than a single point, then this will provide a means to record all possible intersections without double counting. This condition is equivalent to the assumption that all nonempty intersections of C_0 and gC_1 are simply connected. Deriving a closed-form solution for $\mathcal{I}(C_0, C_1)$ in (15.10) for the planar case then follows by "rolling and sliding" each shell of C_1 over the boundary of C_0 and adding the measure of all of these motions to the measure of all motions of the center of C_1 with translations in the interior of C_0, which was already reasoned to be $2\pi A(C_0)$.

Associated with each point on the boundary curve $\mathbf{x}_1(1, \phi_1) \in \partial C_0$ and each point on the shell defined by $\mathbf{x}_2(\rho_2, \phi_2) \in \partial C_1(\rho_2)$ are unit tangent and normal vectors. These vectors can be viewed as the columns of 2×2 rotation matrices, $R_i = [\mathbf{u}_i, \mathbf{n}_i]$, where $\mathbf{u}$ is the unit tangent vector in (15.15) and $\mathbf{n} = [-\mathbf{u} \cdot \mathbf{e}_2, \mathbf{u} \cdot \mathbf{e}_1]^T$. Indices on $\mathbf{u}$, $\mathbf{n}$, and R are used to distinguish between body 1 and body 2. Here, $R_1 = R_1(1, \phi_1)$ and $R_2 = R_2(\rho_2, \phi_2)$.

In order for the shell $\partial C_1(\rho_2)$ to be brought into contact with ∂C_0 at a single point, it is necessary to find the rigid-body motion $(R, \mathbf{b}) \in SE(2)$ such that

$$\mathbf{x}_1(\phi_1) = R \cdot \mathbf{x}_2(\rho_2, \phi_2) + \mathbf{b} \quad \text{and} \quad R \cdot [\mathbf{u}_2, \mathbf{n}_2] = [\mathbf{u}_1, \mathbf{n}_1]\mathrm{rot}[\mathbf{e}_3, \pi].$$

The first of the above conditions ensures contact, and the second ensures that locally the curves $\mathbf{x}_1(\phi_1)$ and $\mathbf{x}_2(\rho_2, \phi_2)$ share common tangent lines (with tangent vectors pointing in opposite directions).

Solving the above equations gives

$$R(\phi_1, \rho_2, \phi_2) = [\mathbf{u}_1, \mathbf{n}_1]\mathrm{rot}[\mathbf{e}_3, \pi][\mathbf{u}_2, \mathbf{n}_2]^{-1} = -R_1(1, \phi_1)R_2^T(\rho_2, \phi_2), \tag{15.16}$$

where

$$R_i(\rho_i, \phi_i) = \begin{bmatrix} \dfrac{r_i'(\rho_i, \phi_i)\cos\phi_i - r_i(\rho_i, \phi_i)\sin\phi_i}{\sqrt{(r_i'(\rho_i, \phi_i))^2 + r_i^2(\rho_i, \phi_i)}} & \dfrac{-r_i'(\rho_i, \phi_i)\sin\phi_i - r_i(\rho_i, \phi_i)\cos\phi_i}{\sqrt{(r_i'(\rho_i, \phi_i))^2 + r_i^2(\rho_i, \phi_i)}} \\ \dfrac{r_i'(\rho_i, \phi_i)\sin\phi_i + r_i(\rho_i, \phi_i)\cos\phi_i}{\sqrt{(r_i'(\rho_i, \phi_i))^2 + r_i^2(\rho_i, \phi_i)}} & \dfrac{r_i'(\rho_i, \phi_i)\cos\phi_i - r_i(\rho_i, \phi_i)\sin\phi_i}{\sqrt{(r_i'(\rho_i, \phi_i))^2 + r_i^2(\rho_i, \phi_i)}} \end{bmatrix}.$$

This expression is a bit cumbersome, and calculations that follow can be facilitated by observing that

$$R_i(\rho_i, \phi_i) = \begin{bmatrix} \alpha_i & -\beta_i \\ \beta_i & \alpha_i \end{bmatrix} \begin{bmatrix} \cos\phi_i & -\sin\phi_i \\ \sin\phi_i & \cos\phi_i \end{bmatrix}, \tag{15.17}$$

where

$$\alpha_i(\rho_i, \phi_i) = r_i'(\rho_i, \phi_i)[(r_i'(\rho_i, \phi_i))^2 + r_i^2(\rho_i, \phi_i)]^{-\frac{1}{2}}$$

and

$$\beta_i(\rho_i, \phi_i) = r_i(\rho_i, \phi_i)[(r_i'(\rho_i, \phi_i))^2 + r_i^2(\rho_i, \phi_i)]^{-\frac{1}{2}}.$$

Note that since the matrices in (15.17) are all planar rotations, they commute. Furthermore, α_i and β_i satisfy the following equalities:

$$\alpha_i^2 + \beta_i^2 = 1, \quad \alpha_i\dot{\alpha}_i + \beta_i\dot{\beta}_i = 0, \quad \alpha_i {\alpha'}_i + \beta_i {\beta'}_i = 0$$

and

$$\begin{gathered} r_i\alpha_i - r_i'\beta_i = 0\,, \quad r_i'\alpha_i + r_i\beta_i = \sqrt{(r_i')^2 + r_i^2}\,, \\ -r_i\alpha_i' + r_i'\beta_i' = \frac{(r_i')^2 - rr''}{\sqrt{(r_i')^2 + r_i^2}}\,, \quad \alpha_i\beta_i' - \beta_i\alpha_i' = \frac{(r_i')^2 - rr''}{(r_i')^2 + r_i^2}\,, \end{gathered} \tag{15.18}$$

where $\cdot\ = \partial/\partial\rho_i$ and $' = \partial/\partial\phi_i$. From (15.18) and the above discussion, it is clear that

$$\int_0^{2\pi} (r_i'\alpha_i + r_i\beta_i)\, d\phi_i = L_i(\rho_i) \quad \text{and} \quad \int_0^{2\pi} (\alpha_i\beta_i' - \beta_i\alpha_i')\, d\phi_i = 0. \tag{15.19}$$

and

$$\begin{aligned} \mathbf{b}(\phi_1, \rho_2, \phi_2) &= \mathbf{x}_1(\phi_1) - R(\phi_1, \rho_2, \phi_2)\mathbf{x}_2(\rho_2, \phi_2) \\ &= \begin{bmatrix} r_1(1, \phi_1)\cos\phi_1 \\ r_1(1, \phi_1)\sin\phi_1 \end{bmatrix} + R_1(1, \phi_1) \begin{bmatrix} r_2(\rho_2, \phi_2)\alpha_2(\rho_2, \phi_2) \\ -r_2(\rho_2, \phi_2)\beta_2(\rho_2, \phi_2) \end{bmatrix}. \end{aligned} \tag{15.20}$$

Computing the Volume in $SE(2)$ Corresponding to Bodies in Collision

If g is described as the 3×3 matrix

$$g(R, \mathbf{b}) = \begin{bmatrix} R & \mathbf{b} \\ \mathbf{0}^T & 1 \end{bmatrix},$$

then

$$J_r(\phi_1, \rho_2, \phi_2) = \left[\left(g^{-1} \frac{\partial g}{\partial \phi_1} \right)^{\vee}, \left(g^{-1} \frac{\partial g}{\partial \rho_2} \right)^{\vee}, \left(g^{-1} \frac{\partial g}{\partial \phi_2} \right)^{\vee} \right]$$

and

$$\mathcal{I}(C_0, C_1) = 2\pi A(C_0) + \int_0^1 \int_0^{2\pi} \int_0^{2\pi} |J_r(\phi_1, \rho_2, \phi_2)| \, d\phi_1 \, d\phi_2 \, d\rho_2. \tag{15.21}$$

Writing out $J_r(\phi_1, \rho_2, \phi_2)$ in terms of its rotational and translational parts separately, and taking a closer look at the determinant $|J_r(\phi_1, \rho_2, \phi_2)|$ using (15.16) reveals that:

$$\begin{aligned} |J_r(\phi_1, \rho_2, \phi_2)| &= \begin{vmatrix} \left(R^T \frac{\partial R}{\partial \phi_1} \right)^{\vee} & \left(R^T \frac{\partial R}{\partial \rho_2} \right)^{\vee} & \left(R^T \frac{\partial R}{\partial \phi_2} \right)^{\vee} \\ R^T \frac{\partial \mathbf{b}}{\partial \phi_1} & R^T \frac{\partial \mathbf{b}}{\partial \rho_2} & R^T \frac{\partial \mathbf{b}}{\partial \phi_2} \end{vmatrix} \\ &= \begin{vmatrix} \left(R_1^T \frac{\partial R_1}{\partial \phi_1} \right)^{\vee} & -\left(\frac{\partial R_2}{\partial \rho_2} R_2^T \right)^{\vee} & -\left(\frac{\partial R_2}{\partial \phi_2} R_2^T \right)^{\vee} \\ R_1^T \frac{\partial \mathbf{b}}{\partial \phi_1} & R_1^T \frac{\partial \mathbf{b}}{\partial \rho_2} & R_1^T \frac{\partial \mathbf{b}}{\partial \phi_2} \end{vmatrix} \\ &= \begin{vmatrix} \omega_{\phi_1} & \omega_{\rho_2} & \omega_{\phi_2} \\ v_1 & w_1 & x_1 \\ v_2 & w_2 & x_2 \end{vmatrix}. \end{aligned} \tag{15.22}$$

The replacement of R^T with R_1^T in the lower rows of the above determinant is valid because multiplication by those rows by any rotation matrix (in this particular case, R_2^T) will not affect the determinant. As for the upper row,

$$\omega_{\phi_1} = \left(R^T \frac{\partial R}{\partial \phi_1} \right)^{\vee} = \left(R_2 R_1^T \frac{\partial R_1}{\partial \phi_1} R_2^T \right)^{\vee} = \left(R_1^T \frac{\partial R_1}{\partial \phi_1} \right)^{\vee}$$

and

$$\begin{aligned} \omega_{\phi_2} &= \left(R^T \frac{\partial R}{\partial \phi_2} \right)^{\vee} = \left(R_2 R_1^T R_1 \frac{\partial R_1^T}{\partial \phi_2} \right)^{\vee} \\ &= \left(R_2 \frac{\partial R_2^T}{\partial \phi_2} \right)^{\vee} = \left(\left[\frac{\partial R_2}{\partial \phi_2} R_2^T \right]^T \right)^{\vee} = -\left(\frac{\partial R_2}{\partial \phi_2} R_2^T \right)^{\vee}. \end{aligned}$$

An exactly analogous argument holds for ω_{ρ_2}.

Explicitly, the following can be observed after some tedious calculations:

$$\begin{gathered} \omega_{\phi_1} = 1 - \alpha_1' \beta_1 + \alpha_1 \beta_1', \quad \omega_{\rho_2} = \dot{\beta}_2 \alpha_2 - \dot{\alpha}_2 \beta_2, \quad \omega_{\phi_2} = 1 - \alpha_2' \beta_2 + \alpha_2 \beta_2', \\ v_1 = \alpha_1 r_1' + \beta_1 r_1 + \beta_2 r_2 + (\alpha_1 \beta_1' - \beta_1 \alpha_1') \beta_2 r_2, \\ v_2 = -\beta_1 r_1' + \alpha_1 r_1 + \alpha_2 r_2 + (\alpha_1 \beta_1' - \beta_1 \alpha_1') \alpha_2 r_2, \\ w_1 = \dot{\alpha}_2 r_2 + \alpha_2 \dot{r}_2, \quad w_2 = -\dot{\beta}_2 r_2 - \beta_2 \dot{r}_2, \\ x_1 = \alpha'{}_2 r_2 + \alpha_2 r'{}_2, \quad x_2 = -\beta'{}_2 r_2 - \beta_2 r'{}_2. \end{gathered}$$

From integration by parts and the continuity of the function r_i in the ϕ_i argument,

$$\int_0^{2\pi} \frac{\partial r_i}{\partial \phi_i} \cos\phi_i \, d\phi_i = r_i(\phi_i)\cos\phi_i \Big|_0^{2\pi} + \int_0^{2\pi} r_i \sin\phi_i \, d\phi_i = \int_0^{2\pi} r_i \sin\phi_i \, d\phi_i .$$

A similar argument holds if $\sin\phi_i$ replaces $\cos\phi_i$ on the left-hand side of the above equations. Therefore,

$$\int_0^{2\pi} \left(\frac{\partial r_i}{\partial \phi_i} \cos\phi_i - r_i \sin\phi_i \right) d\phi_i = 0 \quad \text{and} \quad \int_0^{2\pi} \left(\frac{\partial r_i}{\partial \phi_i} \sin\phi_i + r_i \cos\phi_i \right) d\phi_i = 0. \tag{15.23}$$

Using this together with integrating (15.22) and substituting into (15.21) leads to the *principal kinematic formula*

$$\boxed{\int_G \iota(C_0 \cap gC_1)\, dg = 2\pi[A(C_0) + A(C_1)] + L(C_0)\cdot L(C_1).} \tag{15.24}$$

Note that this has the symmetry in (15.10). In the case when the situation is as in Figure 15.2(right), equality no longer holds. In this case, there is double counting since two shells of gC_1 of different radii can both intersect C_0 with the same $g \in G$, and the right-hand side of (15.24) becomes an upper bound on the left side. A simple lower bound can be computed even when for some or all $g \in G$, it is the case that $C_0 \cap gC_1$ is not simply connected. This bound is obtained by evaluating $2\pi \max\{A(C_0), A(C_1)\}$, which is the volume in G corresponding to the center of one body moving through all points in the interior of the other and visiting all possible orientations. Of course, we choose the greater of these two in order to get the better lower bound. Other lower and upper bounds are explored in Section 15.9.

15.4.2 Spatial Case

In this subsection a sketch of the derivation of the principal kinematic formula in the spatial case is given.

Parameterizing Star-Shaped Bodies

Any star-shaped region in $\mathbb{R}^3$ centered at the origin can be parameterized as

$$\mathbf{x}(\rho,\phi,\theta) = r(\rho,\phi,\theta)\cdot \begin{pmatrix} \cos\phi\sin\theta \\ \sin\phi\sin\theta \\ \cos\theta \end{pmatrix} = r\cdot\mathbf{u}, \quad \text{where } (\rho,\phi,\theta)\in[0,1]\times[0,2\pi]\times[0,\pi]. \tag{15.25}$$

The partial derivatives of the vector $\mathbf{u}(\phi,\theta)$ are

$$\frac{\partial \mathbf{u}}{\partial \phi} = \begin{pmatrix} -\sin\phi\sin\theta \\ \cos\phi\sin\theta \\ 0 \end{pmatrix} \quad \text{and} \quad \frac{\partial \mathbf{u}}{\partial \theta} = \begin{pmatrix} \cos\phi\cos\theta \\ \sin\phi\cos\theta \\ -\sin\theta \end{pmatrix}.$$

A simple calculation shows that

$$\mathbf{u}\cdot\frac{\partial \mathbf{u}}{\partial \phi} = \mathbf{u}\cdot\frac{\partial \mathbf{u}}{\partial \theta} = \frac{\partial \mathbf{u}}{\partial \phi}\cdot\frac{\partial \mathbf{u}}{\partial \theta} = 0,$$
$$\mathbf{u}\cdot\mathbf{u} = \frac{\partial \mathbf{u}}{\partial \theta}\cdot\frac{\partial \mathbf{u}}{\partial \theta} = 1, \quad \frac{\partial \mathbf{u}}{\partial \phi}\cdot\frac{\partial \mathbf{u}}{\partial \phi} = \sin^2\theta,$$

and

$$\mathbf{u} \times \frac{\partial \mathbf{u}}{\partial \phi} = -\sin\theta \frac{\partial \mathbf{u}}{\partial \theta}, \qquad \mathbf{u} \times \frac{\partial \mathbf{u}}{\partial \theta} = \frac{1}{\sin\theta}\frac{\partial \mathbf{u}}{\partial \phi}, \qquad \frac{\partial \mathbf{u}}{\partial \phi} \times \frac{\partial \mathbf{u}}{\partial \theta} = -\sin\theta\, \mathbf{u}.$$

The Jacobian matrix for the parameterization and the absolute value of its determinant are respectively

$$\begin{aligned} J &= \left[\frac{\partial \mathbf{x}}{\partial \rho}, \frac{\partial \mathbf{x}}{\partial \phi}, \frac{\partial \mathbf{x}}{\partial \theta}\right] \\ &= \left[\frac{\partial r}{\partial \rho}\mathbf{u}, \frac{\partial r}{\partial \phi}\mathbf{u} + r\frac{\partial \mathbf{u}}{\partial \phi}, \frac{\partial r}{\partial \theta}\mathbf{u} + r\frac{\partial \mathbf{u}}{\partial \theta}\right] \end{aligned}$$

and

$$|J| = r^2 \frac{\partial r}{\partial \rho}\left|\mathbf{u} \cdot \left(\frac{\partial \mathbf{u}}{\partial \phi} \times \frac{\partial \mathbf{u}}{\partial \theta}\right)\right| = r^2 \frac{\partial r}{\partial \rho} \sin\theta.$$

This means that the volume of the region will be

$$V = \int_0^1 \int_0^\pi \int_0^{2\pi} r^2 \frac{\partial r}{\partial \rho} \sin\theta \, d\phi \, d\theta \, d\rho. \tag{15.26}$$

From the fact that

$$\frac{\partial \mathbf{x}}{\partial \phi} = \frac{\partial r}{\partial \phi}\mathbf{u} + r\frac{\partial \mathbf{u}}{\partial \phi} \quad \text{and} \quad \frac{\partial \mathbf{x}}{\partial \theta} = \frac{\partial r}{\partial \theta}\mathbf{u} + r\frac{\partial \mathbf{u}}{\partial \theta}$$

it follows that

$$\begin{aligned} \frac{\partial \mathbf{x}}{\partial \phi} \times \frac{\partial \mathbf{x}}{\partial \theta} &= r\frac{\partial r}{\partial \phi}\mathbf{u} \times \frac{\partial \mathbf{u}}{\partial \theta} - r\frac{\partial r}{\partial \theta}\mathbf{u} \times \frac{\partial \mathbf{u}}{\partial \phi} + r^2 \frac{\partial \mathbf{u}}{\partial \phi} \times \frac{\partial \mathbf{u}}{\partial \theta} \\ &= \frac{r}{\sin\theta}\frac{\partial r}{\partial \phi}\frac{\partial \mathbf{u}}{\partial \phi} + r\frac{\partial r}{\partial \theta}\sin\theta \frac{\partial \mathbf{u}}{\partial \theta} - r^2 \sin\theta\, \mathbf{u}. \end{aligned} \tag{15.27}$$

Therefore, the surface area for any shell defined by a fixed value of ρ will be

$$\begin{aligned} F &= \int_0^\pi \int_0^{2\pi} \left\| \frac{\partial \mathbf{x}}{\partial \phi} \times \frac{\partial \mathbf{x}}{\partial \theta} \right\| d\phi \, d\theta \\ &= \int_0^\pi \int_0^{2\pi} \left[r^2 \left(\frac{\partial r}{\partial \phi}\right)^2 + r^2 \sin^2\theta \left(\frac{\partial r}{\partial \theta}\right)^2 + r^4 \sin^2\theta \right]^{\frac{1}{2}} d\phi \, d\theta. \end{aligned} \tag{15.28}$$

The metric tensor for each shell is

$$G = \begin{bmatrix} g_{\phi\phi} & g_{\phi\theta} \\ g_{\phi\theta} & g_{\theta\theta} \end{bmatrix} = \begin{bmatrix} \frac{\partial \mathbf{x}}{\partial \phi} \cdot \frac{\partial \mathbf{x}}{\partial \phi} & \frac{\partial \mathbf{x}}{\partial \phi} \cdot \frac{\partial \mathbf{x}}{\partial \theta} \\ \frac{\partial \mathbf{x}}{\partial \phi} \cdot \frac{\partial \mathbf{x}}{\partial \theta} & \frac{\partial \mathbf{x}}{\partial \theta} \cdot \frac{\partial \mathbf{x}}{\partial \theta} \end{bmatrix} = \begin{bmatrix} \left(\frac{\partial r}{\partial \phi}\right)^2 + r^2 \sin^2\theta & \frac{\partial r}{\partial \phi}\frac{\partial r}{\partial \theta} \\ \frac{\partial r}{\partial \phi}\frac{\partial r}{\partial \theta} & \left(\frac{\partial r}{\partial \theta}\right)^2 + r^2 \end{bmatrix}. \tag{15.29}$$

A unit normal can be defined on each point of each shell as

$$\mathbf{n} = |G|^{-\frac{1}{2}} \left(\frac{\partial \mathbf{x}}{\partial \phi} \times \frac{\partial \mathbf{x}}{\partial \theta} \right).$$

From this and the second partial derivatives of $\mathbf{x}$ with respect to ϕ and θ, the matrix of the second fundamental form for each shell can be computed.

Explicitly,

$$\frac{\partial^2 \mathbf{x}}{\partial \phi^2} = \frac{\partial^2 r}{\partial \phi^2}\mathbf{u} + 2\frac{\partial r}{\partial \phi}\frac{\partial \mathbf{u}}{\partial \phi} + r\frac{\partial^2 \mathbf{u}}{\partial \phi^2},$$
$$\frac{\partial^2 \mathbf{x}}{\partial \theta^2} = \frac{\partial^2 r}{\partial \theta^2}\mathbf{u} + 2\frac{\partial r}{\partial \theta}\frac{\partial \mathbf{u}}{\partial \theta} + r\frac{\partial^2 \mathbf{u}}{\partial \theta^2},$$

and

$$\frac{\partial^2 \mathbf{x}}{\partial \phi \partial \theta} = \frac{\partial^2 r}{\partial \phi \partial \theta}\mathbf{u} + \frac{\partial r}{\partial \phi}\frac{\partial \mathbf{u}}{\partial \theta} + \frac{\partial r}{\partial \theta}\frac{\partial \mathbf{u}}{\partial \phi} + r\frac{\partial^2 \mathbf{u}}{\partial \phi \partial \theta}.$$

Since

$$\frac{\partial^2 \mathbf{u}}{\partial \phi^2} = \begin{pmatrix} -\cos\phi\sin\theta \\ -\sin\phi\sin\theta \\ 0 \end{pmatrix}, \quad \frac{\partial^2 \mathbf{u}}{\partial \theta^2} = -\mathbf{u}, \quad \frac{\partial^2 \mathbf{u}}{\partial \phi \partial \theta} = \cot\theta\,\frac{\partial \mathbf{u}}{\partial \phi},$$

it follows that

$$\frac{\partial^2 \mathbf{u}}{\partial \phi^2}\cdot\frac{\partial \mathbf{u}}{\partial \phi} = 0, \;\; \mathbf{u}\cdot\frac{\partial^2 \mathbf{u}}{\partial \theta^2} = -1, \;\; \frac{\partial \mathbf{u}}{\partial \theta}\cdot\frac{\partial^2 \mathbf{u}}{\partial \phi^2} = -\cos\theta,$$
$$\frac{\partial \mathbf{u}}{\partial \phi}\cdot\frac{\partial^2 \mathbf{u}}{\partial \theta^2} = \frac{\partial \mathbf{u}}{\partial \theta}\cdot\frac{\partial^2 \mathbf{u}}{\partial \theta^2} = \frac{\partial \mathbf{u}}{\partial \theta}\cdot\frac{\partial^2 \mathbf{u}}{\partial \phi \partial \theta} = \mathbf{u}\cdot\frac{\partial^2 \mathbf{u}}{\partial \phi \partial \theta} = 0,$$

and

$$\mathbf{u}\cdot\frac{\partial^2 \mathbf{u}}{\partial \theta^2} = -1, \;\; \frac{\partial \mathbf{u}}{\partial \phi}\cdot\frac{\partial^2 \mathbf{u}}{\partial \phi \partial \theta} = \sin\theta\cos\theta.$$

Relationship to First and Second Fundamental Forms

Recall from Chapter 5 that the matrices G and L played an important role in coordinate-dependent differential geometry of surfaces. The equalities presented in the previous section can be used together with the expression in (15.27) to compute

$$L = \begin{bmatrix} l_{\phi\phi} & l_{\phi\theta} \\ l_{\phi\theta} & l_{\theta\theta} \end{bmatrix} = \begin{bmatrix} \mathbf{n}\cdot\frac{\partial^2 \mathbf{x}}{\partial \phi^2} & \mathbf{n}\cdot\frac{\partial^2 \mathbf{x}}{\partial \phi \partial \theta} \\ \mathbf{n}\cdot\frac{\partial^2 \mathbf{x}}{\partial \phi \partial \theta} & \mathbf{n}\cdot\frac{\partial^2 \mathbf{x}}{\partial \theta^2} \end{bmatrix}.$$

Explicitly,

$$l_{\phi\phi} = |G|^{-\frac{1}{2}}\left[2r\left(\frac{\partial r}{\partial \phi}\right)^2\sin\theta - r^2\frac{\partial r}{\partial \theta}\sin^2\theta\cos\theta - r^2\sin\theta\frac{\partial^2 r}{\partial \phi^2} + r^3\sin\theta\right],$$
$$l_{\phi\theta} = |G|^{-\frac{1}{2}}\left[-r^2\sin\theta\frac{\partial^2 r}{\partial \phi \partial \theta} + 2r\frac{\partial r}{\partial \phi}\frac{\partial r}{\partial \theta}\sin\theta + r^2\frac{\partial r}{\partial \phi}\cos\theta\right],$$
$$l_{\theta\theta} = |G|^{-\frac{1}{2}}\left[2r\left(\frac{\partial r}{\partial \theta}\right)^2\sin\theta - r^2\sin\theta\frac{\partial^2 r}{\partial \theta^2} + r^3\sin\theta\right].$$

Additionally, from (15.29) it follows that

$$G^{-1} = |G|^{-1}\cdot\begin{bmatrix} \left(\frac{\partial r}{\partial \theta}\right)^2 + r^2 & -\frac{\partial r}{\partial \phi}\frac{\partial r}{\partial \theta} \\ -\frac{\partial r}{\partial \phi}\frac{\partial r}{\partial \theta} & \left(\frac{\partial r}{\partial \phi}\right)^2 + r^2\sin^2\theta \end{bmatrix},$$

and the mean curvature is calculated at each point as

$$m = \frac{1}{2}\mathrm{tr}(G^{-1}L).$$

Integrating over the shell defined by the value ρ then gives the total mean curvature, M.

By performing calculations that are analogous to the planar case in the previous section (although much more tedious), it is possible to decompose one body into shells and roll another body over each in such a way that the moving body maintains a single point contact with a shell as it is moved over it. If it can be reasoned that during this process the intersection of the two original bodies is always a simply connected region (a sufficient though not necessary condition for which is when the two bodies are convex), then integrating over all motions produces the spatial version of the principal kinematic formula.

15.5 Examples

In this section the application of the principal kinematic formula to computing the entropy of two parts in a bounded environment is illustrated. One part is taken to be fixed at the origin of a coordinate system and another part is placed uniformly at random with its center of mass constrained to be within a sphere of radius R from the origin of the first part. This means that in the absence of the first part, the second has a volume of possible motions in $SE(n)$ given by

$$V = R^n \cdot \mathrm{Vol}(B^n) \cdot \mathrm{Vol}(SO(n)),$$

where $\mathrm{Vol}(B^n)$ is the volume of the ball defined by the interior of a sphere of unit radius in n-dimensional space (which is π in $\mathbb{R}^2$ and $4\pi/3$ in $\mathbb{R}^3$) and $\mathrm{Vol}(SO(n))$ is the volume of the rotation group in n-dimensional space (which is 2π for $SO(2)$ and $8\pi^2$ for $SO(3)$).

Therefore, the positional and orientational distribution of part #2 computed in the absence of part #1 would be

$$f(g) = \frac{1}{V}$$

for $g = (A, \mathbf{a}) \in SE(n)$ with $\|\mathbf{a}\| < R$, and $f(g) = 0$ otherwise.

The entropy of a single isolated part under these conditions is then

$$S_f = \log V.$$

In contrast, the total volume in $SE(n)$ that is available for part #2 to move if part #1 is fixed in the environment, thereby limiting the range of possible motions of part #2, will be

$$V' = V - \int_{SE(n)} \iota(C_0 \cap gC_1)\, dg$$

as long as R is larger than half of the sum of the maximal dimensions of the two parts. Otherwise, the effects of part #1 on limiting the motion may be even greater. With that caveat,

$$S_{f'} = \log V'. \tag{15.30}$$

Therefore, in this case we can completely avoid the computational complexity associated with computing (15.2) and (15.5) by using the principal kinematic formula from Integral Geometry.

15.5.1 Example 1: The Planar Case: Circular Disks in Planar Motion

Let part #1 be a circular disk of radius r_1 fixed at the origin and let part #2 be a circular disk of radius r_2. If part #2 were completely free to rotate and free to translate such that its center stays anywhere in the large circle defined by radius R, then the part entropy would be

$$S = \log(2\pi^2 R^2).$$

In contrast, if all conditions are the same except that the constraint of no interpenetration is imposed, then

$$S' = \log(2\pi^2[R^2 - (r_1 + r_2)^2]),$$

which just removes the disallowed translations defined by the distance of the center of part #2 from the origin in the range $[0, r_1 + r_2]$. This is a simple example that does not require any numerical computation of integrals of motion or even the evaluation of the principal kinematic formula. However, it serves to verify the methodology, since in this case

$$2\pi[A(C_0) + A(C_1)] + L(C_0)L(C_1) = 2\pi[\pi r_1^2 + \pi r_2^2] + (2\pi r_1)(2\pi r_2) = 2\pi^2(r_1 + r_2)^2,$$

which means that the adjustment to the computation of parts entropy from the principal kinematic formula (15.8) will be exactly the same as expected.

15.5.2 Example 2: Spheres and Spatial Motion

As another example, consider the case of two spherical parts: Part #1 has radius r_1 and part #2 has radius r_2. If part #1 is fixed at the origin and part #2 is free to move as long as its center does not go further than a distance R from the origin, then the volume of allowable motion of part #2 in $SE(3)$ will be

$$(8\pi^2)(4\pi/3)[R^3 - (r_1 + r_2)^3].$$

However, (15.30) gives the amount of excluded volume in $SE(3)$ to be

$$\begin{aligned} &8\pi^2[V(C_0) + V(C_1)] + 2\pi[A(C_0)M(C_1) + A(C_1)M(C_1)] \\ &\quad = 8\pi^2[4\pi r_1^3/3 + 4\pi r_2^3/3] + 2\pi[(4\pi r_1^2)(4\pi r_2) + (4\pi r_2^2)(4\pi r_1)] \\ &\quad = (32\pi^3/3)(r_1^3 + r_2^3 + 3r_1^2 r_2 + 3r_1 r_2^2) = (32\pi^3/3)(r_1 + r_2)^3. \end{aligned}$$

This too matches the direct analytical calculation for this simple example.

15.6 Extensions and Limitations

The principal kinematic formula has been used to compute integrals of the form

$$\mathcal{I}(C_0, C_1) = \int_G \iota(C_0 \cap gC_1)\, dg$$

that arise when calculating the entropy of convex parts that can be placed uniformly at random. In Integral Geometry, generalized integrals of the form

$$\mathcal{I}^{\mu}(C_0, C_1) \doteq \int_G \mu(C_0 \cap gC_1)\, dg$$

can be computed in closed form for bodies that are not convex, where μ can be the volume, Euler characteristic, surface area, mean curvature, or Gaussian curvature. This is not directly applicable to the current discussion, although it does open up intriguing possibilities.

15.7 Integral Geometry in $\mathbb{R}^n$

Recall from Chapter 8 that *Steiner's formula* relates the volume of a convex body, $C \subset \mathbb{R}^d$, to the volume within the surface offset from ∂C (along its externally pointing normal) by a distance r. Explicitly, the formula is [8]

$$\mu_d(C + rB^d) = \sum_{m=0}^{d} r^{d-m} \frac{\mathcal{O}_{d-m}}{d-m} \mu_m(C). \tag{15.31}$$

Here, $C + rB^d$ is the Minkowski sum of C with a ball in $\mathbb{R}^d$ of radius r, $\mu_m(C)$ is the mth intrinsic volume, and $\mathcal{O}_d$ is the volume of the unit sphere in $\mathbb{R}^d$, which bounds the unit ball of volume $\mathcal{O}_d/d$ (see the discussion in Section 2.3). In what follows, it is convenient to use the notation

$$(C)_r \doteq C + rB^d.$$

If $I_C(\mathbf{x}) = I(\mathbf{x}; C)$ is the set indicator function[4] for a convex body C, then the indicator function for the unions and intersections of two convex bodies, C_0 and C_1, are related as

$$I(\mathbf{x}; (C_0 \cup C_1)_r) + I(\mathbf{x}; (C_0 \cap C_1)_r) = I(\mathbf{x}; (C_0)_r) + I(\mathbf{x}; (C_1)_r).$$

Integrating over $\mathbb{R}^d$ then gives

$$\mu_d((C_0 \cup C_1)_r) + \mu_d((C_0 \cap C_1)_r) = \mu_d((C_0)_r) + \mu_d((C_1)_r). \tag{15.32}$$

This property (called *additivity*) makes the d-dimensional volume in $\mathbb{R}^d$ an example of a *valuation* in the sense defined in Chapter 1. Evaluating each term in (15.32) using (15.31) for different values of r then means that each $\mu_m(C)$ is additive.

According to *Hadwiger's characterization theorem*, every continuous $SE(d)$-invariant valuation, $\varphi(C)$, can be expressed as

$$\varphi(C) = \sum_{m=0}^{d} \alpha_m \mu_m(C)$$

for some set of constants $\{\alpha_0, \ldots, \alpha_d\}$.

It can be shown that the principal kinematic formula that was derived previously using parametric geometry for $\mu_0(C) = \chi(C) = \iota(C)$ for convex bodies in the case of $d = 2$ and $d = 3$ in Sections 15.4.1 and 15.4.2 generalizes to arbitrary dimensions and arbitrary mixed volumes of intersections of a body C_0 with a rigidly moved version of body C_1 as [64, 65]

$$\boxed{\int_{SE(d)} \mu_j(C_0 \cap gC_1)\, dg = \sum_{k=j}^{d} c_{j,d}^{k,d-k+j}\, \mu_k(C_0)\mu_{d-k+j}(C_1)} \tag{15.33}$$

[4] This function evaluates whether or not $\mathbf{x}$ is in C and should not be confused with $\iota(C)$, which specifies whether or not C is the empty set.

and iterating this formula gives [8, 65]

$$\int_{SE(d)^k} \mu_j(C_0 \cap g_1 C_1 \cap \cdots \cap g_k C_k)\, dg_1 \cdots dg_k$$
$$= \sum_{\substack{m_0,\ldots,m_k=j \\ m_0+\cdots+m_k=kd+j}}^{d} c^{d,m_0,\ldots,m_k}_{j,d,\ldots,d}\, \mu_{m_0}(C_0)\cdots\mu_{m_k}(C_k), \tag{15.34}$$

where in both formulas

$$c^{r_1,\ldots,r_n}_{s_1,\ldots,s_n} = \prod_{i=1}^{n} \frac{(r_i-1)!\mathcal{O}_{r_i}}{(s_i-1)!\mathcal{O}_{s_i}}.$$

Here, the normalization of the Haar measure dg corresponding to $g=(R,\mathbf{b})\in SE(d)$ is defined as

$$dg = dR\, d\mathbf{b}, \quad \text{where} \int_{SO(d)} dR = 1$$

and $d\mathbf{b} = db_1\, db_2 \cdots db_d$ is the usual Lebesgue measure (without any special normalization). One way to generate dR would be to parameterize $SO(d)$ with $d(d-1)/2$ Euler angles, $\boldsymbol{\phi}$, and compute

$$\int_{\boldsymbol{\phi}} |J(\boldsymbol{\phi})|\, d\boldsymbol{\phi} = \text{Vol}(SO(d)) = \prod_{k=2}^{d} \mathcal{O}_k.$$

For example, $\text{Vol}(SO(3)) = (4\pi)\cdot(2\pi)$ is the product of volumes of the surface area of the unit sphere and the unit circle. Then

$$dR = \left(\prod_{k=2}^{d} \mathcal{O}_k\right)^{-1} |J(\boldsymbol{\phi})|\, d\boldsymbol{\phi}. \tag{15.35}$$

Note that in the statement of Theorems 15.1 and 15.2, the unnormalized Haar measures for $SE(2)$ and $SE(3)$ were used.

The results of this section can be related to ergodic theory since $\mu_d(C) = V(C)$ and $c^{d,d}_{d,d} = 1$, and so in the special case when $j = d$, (15.34) becomes

$$\int_{SE(d)} V(C_0 \cap gC_1)\, dg = V(C_0)\, V(C_1).$$

This is like the mixing equation from ergodic theory, with the difference that the space is not finite here and there is no normalization by the volume of the space.

15.8 Differential-Geometric Generalizations of Kinematic Formulas

The concept of tubes circumscribed around curves and surfaces in $\mathbb{R}^3$ was discussed in Chapter 5 and Weyl's tube theorem was demonstrated. The more general version of that theorem asserts that given a smooth closed hyper-surface, ∂C, that encloses a body $C \in \mathbb{R}^n$, the volume enclosed by the tubular hyper-surface with offset distance r exterior to ∂C (denoted here as ∂C_r with r smaller than the smallest radius of curvature of ∂C)

will be given by

$$V((C)_r) = V(C) + \sum_{k=0}^{n-1} \frac{r^{k+1}}{k+1} \int_{\partial C} I_k(G^{-1}L)\, dV_{\partial C}, \tag{15.36}$$

where G is the metric tensor written as an $(n-1) \times (n-1)$ matrix in coordinates and L is the matrix defining the second fundamental form of ∂C, $I_0(A) = 1$, and $I_k(A)$ for $k = 1, \ldots, n-1$ is the kth scalar invariant of an $(n-1) \times (n-1)$ matrix A, as defined in Exercise A.5 in Volume 1 for the $n \times n$ case.

Equation (15.36) can be obtained by starting with a parameterization of the hyper-surface ∂C of the form $\mathbf{x}(\mathbf{q})$, computing an outward-pointing normal to it at each point, $\mathbf{n}(\mathbf{q})$, and defining the offset surface (or tube), $\mathbf{y}(\mathbf{q}) = \mathbf{x}(\mathbf{q}) + r\mathbf{n}(\mathbf{q})$. Then using the divergence theorem for manifolds, the volume inside of this tube can be computed as the sum of the volume of the original body and the surrounding skin of depth r as

$$V((C)_r) = V(C) + \int_0^r \int_{\partial C} \det(\mathbb{I} + tG^{-1}L)\, dV_{\partial C}\, dt,$$

where t is a scalar variable of integration. Expanding the determinant, using the fact that $I_k(tA) = t^k I_k(A)$, and integrating each term over $t \in [0, r]$ then gives (15.36).

The volume element for ∂C is written in coordinates as $dV_{\partial C} = |G(\mathbf{q})|^{\frac{1}{2}} d\mathbf{q}$. It is sometimes convenient to define[5]

$$M_k(\partial C) \doteq \binom{n-1}{k}^{-1} \int_{\partial C} I_k(G^{-1}L)\, dV_{\partial C}, \tag{15.37}$$

which is akin to the total mean curvature. In fact, when $n = 3$ and $k = 2$, this is exactly the total mean curvature defined in (5.68). Steiner's formula for the volume of the Minkowski sum of a body and a ball in $\mathbb{R}^n$ was discussed in Chapter 7. For a body, $C \subset \mathbb{R}^n$, bounded by a smooth hyper-surface, ∂C, the kth quermassintegral, $W_k(C)$, was defined and related to the intrinsic volume $\mu_{n-k}(C)$ in (7.9). By matching (15.36) term-by-term with Steiner's formula (7.8), it becomes clear that the quermassintegrals of smooth bodies and the total mean curvature of the surfaces that envelop them are related as [61]

$$M_k(\partial C) = nW_{k+1}(C). \tag{15.38}$$

With this terminology, (15.33) can be written differently in terms of intersecting hyper-surfaces (rather than the intersecting bodies that they enclose). Observing that, in general,

$$\partial(C_0 \cap C_1) = (\partial C_0 \cap C_1) \cup (C_0 \cap \partial C_1) \cup (\partial C_0 \cap \partial C_1),$$

the fact that the Euler characteristic of a body, C, and the manifold that bounds it, ∂D, are related as[6]

$$2 \cdot \chi(C) = \chi(\partial C) \quad \text{if } \dim(\partial C) = 0 \bmod 2,$$

and the Gauss–Bonnet–Chern theorem gives

$$M_{n-1}(\partial C) = \frac{1}{2}\mathcal{O}_n \chi(\partial C),$$

[5] The matrix invariants $I_k(G^{-1}L)$ should not be confused with the indicator function $I_A(\mathbf{x})$. They are unrelated.

[6] Otherwise, odd-dimensional hyper-surfaces have $\chi(\partial C) = 0$.

which means that for bodies in $\mathbb{R}^n$,

$$\chi(C_0 \cap gC_1) = \frac{1}{\mathcal{O}_n} M_{n-1}(\partial(C_0 \cap gC_1)). \tag{15.39}$$

Using these facts, Santaló [61] gives

$$\int_{SE(n)} M_{n-1}(\partial(C_0 \,\cap\, gC_1))\, dg = \mathcal{O}_n[M_{n-1}(\partial C_0)V(C_1) + M_{n-1}(\partial C_1)V(C_0)] + \frac{1}{n}\sum_{k=0}^{n-2} \binom{n}{k+1} M_k(\partial C_0) M_{n-2-k}(\partial C_1). \tag{15.40}$$

It can also be reasoned that integrals of the other total curvatures M_{q-1} for $q = 1, \ldots, n-1$ can be computed as [61][7]

$$\begin{aligned}\int_{SE(n)} & M_{q-1}(\partial(C_0 \,\cap\, gC_1))\, dg \\ &= M_{q-1}(\partial C_0)V(C_1) + M_{q-1}(\partial C_1)V(C_0) \\ &\quad + \frac{(n-q)\mathcal{O}_q}{\mathcal{O}_{n-q}\mathcal{O}_n} \sum_{k=n-q}^{n-2} \frac{\mathcal{O}_{k+1}\mathcal{O}_{2n-k-q+1}}{(k+1)\mathcal{O}_{n-k+1}\mathcal{O}_{k+q-n+1}} \binom{q-1}{q+k-n} M_{k+q-n}(\partial C_0) \\ &\qquad \times M_{n-2-k}(\partial C_1).\end{aligned} \tag{15.41}$$

Equations (15.40) and (15.41) together are equivalent to (15.33) but written in terms of different quantities. In the sequel, (15.33) will be used.

15.8.1 Non-Euclidean Principal Kinematic Formulae

Spaces of constant curvature (i.e., $\mathbb{R}^n$ and $\mathbb{T}^n$ which have zero curvature, the sphere S^{n-1} which has unit positive curvature, and the hyperbolic space $\mathbb{H}^n$ which has unit negative curvature) are all domains on which principal kinematic formulas can be written. All of these manifolds, M, can be described as homogeneous spaces of Lie groups as $M = G/H$. For example, $S^{n-1} = SO(n)/SO(n-1)$, $\mathbb{R}^n = SE(n)/SO(n)$, and so forth. Both the sphere (or ellipsoid of revolution) and the hyperboloid of one sheet can be embedded in $\mathbb{R}^{n+1}$ as

$$\sum_{k=0}^{n-1} x_k^2 + \epsilon x_n^2 = \epsilon/\mathcal{K},$$

where $\mathcal{K} > 0$ is a curvature parameter. For example, for a sphere of radius r, $\mathcal{K} = 1/r^2$. For a space of positive constant curvature, $\epsilon = +1$, and for a space of negative constant curvature, $\epsilon = -1$.

In spaces of constant curvature, it is possible to define bodies in an analogous way as in $\mathbb{R}^n$. Furthermore, it makes sense to ask whether formulas of the form $\mathcal{I}(C_0, C_1) = \int_G \chi(C_0 \cap gC_1)\, dg$ can be computed where $C_0, C_1 \subset M$ have the same dimension as M, $\dim(M) = n$. Indeed they can. Santaló [61] devoted some effort to review this and display

[7] Note that to be consistent with [20, 52], $\mathcal{O}_n$ is used in place of Santaló's O_{n-1} and the same normalization of the Haar measure in (15.33) is used here, whereas in [61], the version without normalization is used. When $q = 1$, the summation term vanishes.

the results separately when M is even dimensional and when it is odd dimensional. Those results can be summarized here for general dimensions by defining $n = 2m$ or $n = 2m-1$ and writing[8]

$$\begin{aligned}
&\int_G \chi(C_0 \cap gC_1)\, dg \\
&\quad = -\frac{2}{\mathcal{O}_{n+1}} (\epsilon\mathcal{K})^{n/2} V(C_0)V(C_1)[(n-1)\,\mathrm{mod} 2] \\
&\quad + V(C_1)\chi(C_0) + V(C_0)\chi(C_1) + \frac{1}{n\mathcal{O}_n} \sum_{k=0}^{n-2} \binom{n}{k+1} M_k(\partial C_0) M_{n-2-k}(\partial C_1) \\
&\quad + \frac{1}{\mathcal{O}_n} \left[\sum_{i=0}^{m-2} \sum_{k=2(m-i-1)}^{n-2} \binom{n-1}{k} \binom{k}{2(m-i-1)} c(n,m,k,i) a(n,m,k,i) \right],
\end{aligned}$$

where

$$c(n,m,k,i) \doteq \frac{4(m-i-1)\mathcal{O}_{k+1}\mathcal{O}_{n+2m-k-2i-1}}{(k+1)\mathcal{O}_{n-k+1}\mathcal{O}_{2m-2i-2}\mathcal{O}_{2m-2i-1}\mathcal{O}_{2i+k-2m+3}}$$

and

$$a(n,m,k,i) \doteq M_{n-2-k}(\partial C_1) M_{k+2i+2-2m}(\partial C_0) (\epsilon\mathcal{K})^{m-1-i}.$$

Note that when $n = 2$, this reduces to [61]

$$\int_G \chi(C_0 \cap gC_1)\, dg = -\frac{\epsilon}{2\pi}\mathcal{K} A(C_0)A(C_1) + A(C_1)\chi(C_0) + A(C_0)\chi(C_1) + \frac{1}{2\pi} L(C_0)L(C_1),$$

and when $n = 3$, the right-hand side reduces to exactly the principal kinematic formula in $\mathbb{R}^3$ (of course, with volumes, surface areas, and so forth, computed within the 3-manifold, and with a normalization of $8\pi^2$). Thus, the curvature has an indirect influence; in that case, it does not appear explicitly in the formula as it does in the case when $n = 2$.

Other kinematic formulas are also possible in which the integrand is not the Euler characteristic but rather some other intrinsic volume. For example, when the integrand is the volume of intersecting bodies in $M = G/H$ [61],

$$\int_G V(C_0 \cap gC_1)\, dg = V(C_0) \cdot V(C_1). \tag{15.42}$$

This begs the question of how general can the kinematic formula be written. Indeed, it is also possible to compute kinematic formulas for integrals of the form

$$\mathcal{I}(M_q, M_p) = \int_G \chi(M_q \cap gM_p)\, dg,$$

where M_q and M_p are closed submanifolds of $M = G/H$. Such issues are discussed in [17, 43, 52]. This sort of formula is fundamentally different than (15.40) because $\partial(C_0 \cap gC_1) \neq \partial C_0 \cap g\partial C_1$.

[8] The appearance of this formula is substantially different than in Santaló [61] because (1) here, the odd- and even-dimensional cases are combined into one equation and (2) regardless of whether $\epsilon = -1$ or $+1$, the groups $SO(n+1)$ and $SO(n,1)$ both have $SO(n)$ as a subgroup (as does $SE(n)$), and so the integration measure dg can be normalized as in (15.35) with $d = n$.

15.8.2 Integral Geometry of Squared Curvature

Most integral-geometric formulas involve integrals of total curvature (or, equivalently, quermassintegrals or mixed volumes). These are quantities that show up in Hadwiger's characterization theorem. However, these are not the only geometric quantities that can be integrated over a body or surface of intersection.

Other formulas that are not a special case of these were derived by Chen [19] and are stated as follows. Let $\kappa(s)$ be the (signed) curvature of a closed space curve $\mathbf{c}(s)$ as defined in Chapter 5 and let

$$\mathcal{K}^2(c) \doteq \oint_c \kappa^2(s)\, ds$$

denote the integral of the squared curvature over the whole closed curve $\mathbf{c}(s)$. This is called the total square curvature of the curve. Given two closed orientable surfaces, ∂C_0 and ∂C_1, which can be thought of as the boundaries of solid bodies, C_0 and C_1, one of which is moving and the other of which is stationary, the intersection $\partial C_0 \cap g\partial C_1$ will either be empty or result in one or more closed curve. This should not be confused with $C_0 \cap gC_1$, which would result in a volume rather than a curve. Chen's formula states that

$$\int_G \mathcal{K}^2(\partial C_0 \cap g\partial C_1)\, dg = 2\pi^3[3H_0 - K_0]F_1 + 2\pi^3[3H_1 - K_1]F_0, \qquad (15.43)$$

where H_i, F_i, and K_i are respectively the total square of mean curvature, total surface area, and total Gaussian curvature, of surface i. Here, dg is the unnormalized Haar measure for $G = SE(3)$.

15.9 Kinematic Inequalities

The principal kinematic formula can be generalized in several ways. First, the domain in which the bodies are defined need not be $\mathbb{R}^n$. It could be a homogeneous space G/H (e.g., the sphere S^2 with $G = SO(3)$. Second, in some applications it may not be the Haar measure) but rather a different measure that one seeks to use. This section examines these generalizations and establishes approximations and inequalities in this more generalized setting where exact formulas are difficult to come by.

In particular, a quantity that is not directly addressed in Integral Geometry but which is relevant to parts entropy is

$$\mathcal{I}_w(C_0, C_1) = \int_G \iota(C_0 \cap gC_1) w(g)\, dg, \qquad (15.44)$$

where $w(g)$ is a positive weighting function. For example, $w(g)$ could be a probability density function on G or when $w(g) = 1, \mathcal{I}_1(C_0, C_1) = \mathcal{I}(C_0, C_1)$. Being able to compute $\mathcal{I}_w(C_0, C_1)$ would be useful for parts entropy calculations. For this reason, these sorts of formulas are investigated here in the context of individual parts of rigid parts. We will return to collections of parts later.

15.9.1 Kinematic Formulas for Nonconvex Bodies and Non-Haar Measure

The principal kinematic formula can be viewed as an evaluation of the integral in (15.44) for the case when $w(g) = 1$ and each C_i is convex (so that $\iota(C_0 \cap gC_1) = \chi(C_0 \cap gC_1)$). As a practical matter, it may be desirable to compute (or approximate, or bound) $\mathcal{I}_\rho(C_0, C_1)$ in (15.44) for the case when $w(g) \neq 1$ and/or each C_i is not convex. For example, in the statistical mechanics of polymers, a probability density in pose of individual monomers in a phantom chain (i.e., one that does not impose constraints on self-penetration) can be computed easily. However, a real polymer has non-negligible girth, and computing the effects of self-intersection become important. So too is the case for parts entropy of nonconvex parts.

15.9.2 Bounds Based on Hölder's Inequality

A result that appears not to be known in the literature relates to inequalities with the same flavor as those above for the case of nonconvex bodies.

From Hölder's inequality, we have that for integers $1 \leq p, q \leq \infty$,

$$\mathcal{I}_\rho(C_0, C_1) \leq \left(\int_G [i(C_0 \cap gC_1)]^p dg\right)^{\frac{1}{p}} \left(\int_G [\rho(g)]^q dg\right)^{\frac{1}{q}}, \quad \text{where } \frac{1}{p} + \frac{1}{q} = 1.$$

Since $\iota(\cdot)$ takes a value of 1 or 0, $[i(C)]^p = [i(C)]$, and so Hölder's inequality effectively separates the effects of $\rho(g)$ and $\iota(C_0 \cap gC_1)$. This bound can be tightened by minimizing over p. Alternatively, in the special case when $p = q = 2$, this reduces to the Cauchy–Schwarz inequality. This may be useful in some contexts, because then the Parseval/Plancherel equality can be used to compute $\int_G \rho^2(g)\, dg$ in Fourier space.

If C_0 and C_1 are convex, then $\int_G \iota(C_0 \cap gC_1)\, dg$ can be computed directly from the principal kinematic formula. However, convexity of C_0 and C_1 is not a necessary condition for that formula to work. As long as whenever $C_0 \cap gC_1 \neq \emptyset$ the resulting body of intersection is simply connected so that $\iota(C_0 \cap gC_1) = \chi(C_0 \cap gC_1)$, then the formula will work. For example, if C_0 is a large body with boundary that has sufficiently small absolute curvature at each point and if C_1 is convex, then the intersections will be simply connected. In the event that C_1 and C_2 are not convex, upper bounds on $\int_G \iota(C_0 \cap gC_1)]dg$ can be computed in a number of ways. For example, if the bodies are simply connected, then their intersection will have one or more simply connected components, and so

$$\int_G \iota(C_0 \cap gC_1)\, dg \leq \int_G \chi(C_0 \cap gC_1)\, dg,$$

which can be evaluated using the principal kinematic formula.

Alternatively, if C_0 is decomposed as $C_0 = \cup_{i \in I} C_0^i$ into convex components such that $C_0^i \cap C_0^j = \emptyset$ when $i \neq j$, and likewise for C_1, then

$$\int_G \iota(C_0 \cap gC_1)\, dg \leq \sum_{i,j} \int_G \iota(C_0^i \cap gC_1^j)\, dg,$$

where each of the integrals in the sum on the right-hand side can be evaluated using the principal kinematic formula since $\iota(\cdot) = \chi(\cdot)$ when applied to convex bodies. Putting this all together gives

$$\int_G \iota(C_0 \cap gC_1)\, dg \leq \min\left\{\int_G \chi(C_0 \cap gC_1)\, dg\,, \sum_{i,j} \int_G \iota(C_0^i \cap gC_1^j)\, dg\right\}. \tag{15.45}$$

On the other hand, if $\breve{C}_i$ and $\hat{C}_i$ are respectively the largest convex body contained inside of C_i, and the smallest convex body containing C_i, then

$$\int_G \iota(\breve{C}_0 \cap g\breve{C}_1)\, dg \leq \int_G \iota(C_0 \cap gC_1)\, dg \leq \int_G \iota(\hat{C}_0 \cap g\hat{C}_1)\, dg. \tag{15.46}$$

Of course, these bounds will still be valid if each $\breve{C}_i$ is replaced with a smaller convex body and each $\hat{C}_i$ is replaced with a larger one. In principle, the upper bound in (15.46) can be merged with that in (15.45). However, in practice, (15.46) is better than (15.45).

As an example, let $C_0 = C_1$ be a shape that is defined by starting with a 5×5 square and removing a vertical notch of dimensions 1×4 so that the resulting shape can be viewed as the union of rectangles C_0^1, C_0^2, and C_0^3 of dimensions 3×5, 1×1, and 1×5, respectively. The perimeter of this shape is $L(C_0) = 28$ and the area is $A(C_0) = 21$. A straightforward application of the principal kinematic formula gives

$$\int_G \chi(C_0 \cap gC_0)\, dg = 2\pi(42) + (28)^2 \approx 1148.$$

This will be an upper bound for $\mathcal{I}(C_0, C_0)$. An alternative upper bound is

$$\int_G \iota(C_0^1 \cap gC_0^1)\, dg + \int_G \iota(C_0^2 \cap gC_0^2)\, dg + \int_G \iota(C_0^3 \cap gC_0^3)\, dg$$
$$+ 2\int_G \iota(C_0^1 \cap gC_0^2)\, dg + 2\int_G \iota(C_0^1 \cap gC_0^3)\, dg + 2\int_G \iota(C_0^2 \cap gC_0^3)\, dg \approx 1721.$$

Alternatively, taking $\hat{C}_0$ to be a 5×5 square gives $\mathcal{I}(C_0, C_0) < 557.2$ and taking $\breve{C}_0 = C_0^1$ (the 5×3 rectangular component of C_0) gives $\mathcal{I}(C_0, C_0) > 350.1$.

Therefore, (15.46) provides relatively good bounds. As a general rule, convex polyhedra can be constructed that either fit in, or surround, two- and three-dimensional bodies. Additionally, their area and volume can be computed efficiently. It is possible to compute integrals of mean curvature for polyhedral bodies using the methods of convex geometry discussed in Chapter 7. Alternatively, the closed-form formulas for prolate and oblate ellipsoids of revolution are known in closed form, as given in Section 5.4.4.

Other bounds can also be obtained using the same sorts of mathematical tools that are used in information theory. This is examined in the following subsections.

15.9.3 An Upper Bound Based on Jensen's Inequality

An upper bound for (15.44) can be obtained from Jensen's inequality when $w(g) = \rho(g)$ is a pdf. Recognizing that the unit Heaviside step function, $u[x]$, is a (discontinuous) concave function on $\mathbb{R}_{\geq 0}$ (and therefore its negative is convex),

$$\begin{aligned}
\mathcal{I}_\rho(C_0, C_1) &= \int_G \iota(C_0 \cap gC_1)\rho(g)\, dg \\
&= \int_G u\left[\int_{\mathbb{R}^n} I_{C_0}(\mathbf{x}) I_{C_1}(g^{-1} \cdot \mathbf{x})\, d\mathbf{x}\right] \rho(g)\, dg \qquad (15.47) \\
&= \int_G u\left[V(C_0 \cap gC_1)\right] \rho(g)\, dg \\
&\leq u\left[\int_G V(C_0 \cap gC_1)\rho(g)\, dg\right] \\
&\leq 1. \qquad (15.48)
\end{aligned}$$

This upper bound is not very informative since it is the same regardless of the size or geometry of the bodies. Furthermore this does not hold when attempting to compute

$\mathcal{I}_w(C_0, C_1)$ where $w(g)$ is not a pdf. In some cases, if $w(g)$ is not a pdf, it can be normalized and the bound applies. However, in other cases, such as $w(g) = 1$, $\int_G w(g)\,dg$ will be infinite since the group of rigid-body motions, G, is not compact. Thus, defining $\rho(g) = w(g)/\int_G w(g)\,dg$ as a pdf is not useful.

15.9.4 A Lower Bound Inspired by Jensen's Inequality

Rather than applying Jensen's inequality to the integral over G and pulling $u[\cdot]$ outside of that integral, Jensen's inequality can be applied by bringing $u[\cdot]$ inside the integral over $\mathbb{R}^n$, resulting in a lower bound. Then

$$u\left[\int_{\mathbb{R}^n} I_{C_0}(\mathbf{x}) I_{C_1}(g^{-1} \cdot \mathbf{x})\,d\mathbf{x}\right] = u\left[\int_{\mathbb{R}^n} \frac{I_{C_0}(\mathbf{x})}{V(C_0)} \cdot V(C_0) I_{C_1}(g^{-1} \cdot \mathbf{x})\,d\mathbf{x}\right].$$

Here, $I_{C_0}(\mathbf{x})/V(C_0)$ is a pdf on $\mathbb{R}^n$ and $V(C_0)I_{C_1}(g^{-1} \cdot \mathbf{x})$ is some other function. Therefore, from Jensen's inequality and the concavity of $u[\cdot]$,

$$u\left[\int_{\mathbb{R}^n} \frac{I_{C_0}(\mathbf{x})}{V(C_0)} \cdot V(C_0) I_{C_1}(g^{-1} \cdot \mathbf{x})\,d\mathbf{x}\right] \geq \int_{\mathbb{R}^n} \frac{I_{C_0}(\mathbf{x})}{V(C_0)} \cdot u[V(C_0) I_{C_1}(g^{-1} \cdot \mathbf{x})]d\mathbf{x}.$$

However,

$$u[V(C_0) I_{C_1}(g^{-1} \cdot \mathbf{x})] = u[I_{C_1}(g^{-1} \cdot \mathbf{x})] = I_{C_1}(g^{-1} \cdot \mathbf{x}).$$

Therefore,

$$u\left[\int_{\mathbb{R}^n} I_{C_0}(\mathbf{x}) I_{C_1}(g^{-1} \cdot \mathbf{x})\,d\mathbf{x}\right] \geq \frac{1}{V(C_0)} \int_{\mathbb{R}^n} I_{C_0}(\mathbf{x}) I_{C_1}(g^{-1} \cdot \mathbf{x})\,d\mathbf{x} = \frac{V(C_0 \cap gC_1)}{V(C_0)}.$$

The same could have been done if $I_{C_1}(g^{-1} \circ \mathbf{x})/V(C_1)$ were used as the pdf instead of $I_{C_0}(\mathbf{x})/V(C_0)$. The above result also can be obtained with a simple geometric argument. If the smaller body is completely contained in the larger for pose $g \in G$, then $V(C_0 \cap gC_1) = V(C_1)$. Otherwise, $V(C_0 \cap gC_1) < V(C_1)$ with the extreme case of $V(C_0 \cap gC_1) = 0$ when $C_0 \cap gC_1 = \emptyset$. Therefore,

$$\boxed{u[V(C_0 \cap gC_1)] \geq \frac{V(C_0 \cap gC_1)}{\min\{V(C_0), V(C_1)\}}.} \tag{15.49}$$

Returning to (15.47) and substituting (15.49) in then gives

$$\mathcal{I}_w(C_0, C_1) \geq \frac{1}{\min\{V(C_0), V(C_1)\}} \int_G V(C_0 \cap gC_1) w(g)\,dg. \tag{15.50}$$

When $w(g) = 1$, the volume formula (15.42) can be used to give

$$\mathcal{I}(C_0, C_1) \geq \frac{V(C_0) \cdot V(C_1)}{\min\{V(C_0), V(C_1)\}}. \tag{15.51}$$

15.9.5 A Geometric Version of the Cauchy–Schwarz Inequality

If $\mu(\cdot)$ denotes any of the quermassintegrals (e.g., $\chi(\cdot)$, $V(\cdot)$, etc.), then by the Cauchy–Schwarz inequality,

$$\begin{aligned}\int_G \mu(C_0 \cap gC_1)\, dg &= \int_G \mu(C_0 \cap gC_1) \cdot \iota(C_0 \cap gC_1)\, dg \\ &\leq \left(\int_G [\mu(C_0 \cap gC_1)]^2 dg\right)^{\frac{1}{2}} \left(\int_G [\iota(C_0 \cap gC_1)]^2 dg\right)^{\frac{1}{2}}.\end{aligned}$$

Since $[\iota(\cdot)]^2 = \iota(\cdot)$, it follows that

$$\boxed{\frac{\left(\int_G \mu(C_0 \cap gC_1)\, dg\right)^2}{\int_G [\mu(C_0 \cap gC_1)]^2 dg} \leq \mathcal{I}(C_0, C_1).} \tag{15.52}$$

This means that any upper bound developed for $\mathcal{I}(C_0, C_1)$ can be used to develop lower bounds for $\int_G [\mu(C_0 \cap gC_1)]^2\, dg$.

Alternatively, in the special case when $\mu(\cdot) = V(\cdot)$, $\int_G [V(C_0 \cap gC_1)]^2\, dg$ can be bounded from above in closed form using geometric arguments, and this upper bound can then be substituted into (15.52). Specifically, if each of the bodies C_k can be covered with overlapping Gaussian distributions so that

$$I_{C_k}(\mathbf{x}) \leq \sum_i \alpha_i^k \rho(\mathbf{x}; \boldsymbol{\mu}_i^k, \Sigma_i^k),$$

then when $g = (R, \mathbf{t}) \in SE(n)$,

$$\begin{aligned}V(C_0 \cap gC_1) &= \int_{\mathbb{R}^n} I_{C_0}(\mathbf{x}) I_{C_1}(g^{-1} \cdot \mathbf{x})\, d\mathbf{x} \\ &\leq \sum_{i,j} \alpha_j^0 \alpha_j^1 \int_{\mathbb{R}^n} \rho(\mathbf{x}; \boldsymbol{\mu}_i^0, \Sigma_i^0) \rho(R^T(\mathbf{x} - \mathbf{t}); \boldsymbol{\mu}_j^1, \Sigma_j^1)\, d\mathbf{x} \\ &= \sum_{i,j} \alpha_i^0 \alpha_j^1 \int_{\mathbb{R}^n} \rho(\mathbf{x}; \boldsymbol{\mu}_i^0, \Sigma_i^0) \rho(\mathbf{x}; R\boldsymbol{\mu}_j^1 + \mathbf{t}, R\Sigma_j^1 R^T)\, d\mathbf{x} \\ &= \sum_{i,j} \alpha_i^0 \alpha_j^1 \rho(\mathbf{t}; \boldsymbol{\mu}_i^0 + R\boldsymbol{\mu}_j^1, \Sigma_i^0 + R\Sigma_j^1 R^T).\end{aligned} \tag{15.53}$$

This closed-form/series upper bound for $V(C_0 \cap gC_1)$ can then be squared and integrated over $\mathbf{t} \in \mathbb{R}^n$ in closed form using the Gaussian integrals from Chapter 2. The integral over $SO(n)$ can also be computed in closed form using the methods in the following chapter.

Connections between $\int_G [V(C_0 \cap gC_1)]^2\, dg$ and noncommutative harmonic analysis can also be established. Viewing $I_{C_k}(\mathbf{x})$ as a function $\tilde{I}_{C_k}(\mathbf{x}, Q) = I_{C_k}(\mathbf{x})$ that is constant on all $Q \in SO(n)$, then $\tilde{I}_{C_k}(h)$ can be viewed as a function on $(\mathbf{x}, Q) \in SE(n)$. Then if $dh = d\mathbf{x}\, dQ$ is the Haar measure for $SE(n)$ normalized so that $\int_{SO(n)} dQ = 1$,

$$V(C_0 \cap gC_1) = \int_G \tilde{I}_{C_0}(h) \tilde{I}_{C_1}(g^{-1} \circ h)\, dh.$$

This is not quite a convolution on $SE(n)$, but by defining $\tilde{I}_{C_1}^*(g) \doteq \tilde{I}_{C_1}(g^{-1})$ gives

$$V(C_0 \cap gC_1) = (\tilde{I}_{C_0} * \tilde{I}_{C_1}^*)(g). \tag{15.54}$$

Actually, this is an easy way to see that the volume formula $\int_G V(C_0 \cap gC_1)\, dg = V(C_0)V(C_1)$ holds, since, in general, the integral of a convolution is the product of the integrals of the two functions. However, since our goal is to exactly compute or bound $\int_G [V(C_0 \cap gC_1)]^2\, dg$ form above, the convolution theorem and the Parseval/Plancherel equality can be used in the form

$$\begin{aligned}\int_G [V(C_0 \cap gC_1)]^2 dg &= \int_G [(\tilde{I}_{C_0} * \tilde{I}^*_{C_1})(g)]^2\, dg & (15.55)\\ &= \int_{\hat{G}} |\hat{\tilde{I}}_{C_0}(p)\hat{\tilde{I}}^*_{C_1}(p)|^2\, d(p) & (15.56)\\ &\leq \int_{\hat{G}} |\hat{\tilde{I}}_{C_0}(p)|^2 \cdot |\hat{\tilde{I}}^*_{C_1}(p)|^2\, d(p) & (15.57)\\ &\leq \left(\int_{\hat{G}} |\hat{\tilde{I}}_{C_0}(p)|^4\, d(p)\right)^{\frac{1}{2}} \left(\int_{\hat{G}} |\hat{\tilde{I}}_{C_1}(p)|^4\, d(p)\right)^{\frac{1}{2}}. & (15.58)\end{aligned}$$

The last inequality results from the submultiplicative property of the Frobenius norm (see the Appendix in Volume 1) and the Cauchy–Schwarz inequality. The $*$ disappears because the group-Fourier transform of a real-valued function $f^*(g) = f(g^{-1})$ is the Hermitian conjugate of the Fourier transform of $f(g)$. Additionally, the Frobenius norm is invariant under conjugation. The integration measure for $\widehat{SE(n)}$ is of the form $d(p) = c_n p^{n-1}\, dp$, where c_n is a normalizing constant.

15.9.6 Bounds Based on Approximations of $u[\cdot]$

Substituting in place of $u[x]$ any function $\phi(x)$ such that $\phi(x) \leq u[x]$ for all $x \in \mathbb{R}_{\geq 0}$ will provide a lower bound for $\mathcal{I}_w(C_0, C_1)$.

For example, the following can be used:

$$\phi_1(x) = \frac{x}{\sqrt{1+x^2}},$$

the hyperbolic tangent,

$$\phi_2(x) = \tanh x = \frac{e^{2x}-1}{e^{2x}+1},$$

the error function,

$$\phi_3(x) = \operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2}\, dt,$$

and the arctangent/inverse tangent,

$$\phi_4(x) = \frac{2}{\pi} \arctan x.$$

Scaled versions of these functions of the form $\phi_k(ax)$ can be made arbitrarily close to $u[x]$ by increasing $a \in \mathbb{R}_{>0}$.

In addition, other functions that have the property $\phi_k(x) \leq u[x]$ in the range $0 \leq x \leq v$, where

$$v \doteq \min\{V(C_0), V(C_1)\} \qquad (15.59)$$

can be defined and used to generate lower bounds. In other words, since $V(C_0 \cap gV_1)$ never exceeds v, it does not matter how $\phi_k(x)$ behaves when $x > v$. Imposing the additional condition $0 \leq \phi_k(x)$ ensures that the bound does not become negative. For example,

$$\phi_5(x) = 1 - \frac{1}{v^2}(x-v)^2$$

is a parabola that observes the conditions

$$\phi(0) = 0, \quad \min_{0 \le x \le v} \phi(x) \ge 0 \quad \text{and} \quad \max_{0 \le x \le v} \phi(x) = 1. \tag{15.60}$$

Similarly, the functions

$$\phi_6(x) = \sin^p\left(\pi\frac{x}{v}\right), \quad \forall n \in \mathbb{R}_{>0},$$
$$\phi_7(x) = -e \cdot \left(\frac{x}{v}\right)\log_e\left(\frac{x}{v}\right),$$

and

$$\phi_8(x) = \left(\frac{x}{v}\right)^{\frac{1}{n}}, \quad \forall n \in \mathbb{Z}_{>0}$$

observe (15.60).

All of these functions satisfy

$$\mathcal{I}_w(C_0, C_1) \ge \int_G \phi(V(C_0 \cap gC_1))\, w(g)\, dg.$$

For example, if $w(g) = 1$ and the case when $\phi_5(x)$ is used, then

$$\mathcal{I}(C_0, C_1) \ge \frac{2}{v}\int_G V(C_0 \cap gC_1)\, dg - \frac{1}{v^2}\int_G [V(C_0 \cap gC_1)]^2\, dg. \tag{15.61}$$

Substituting an upper bound for $\int_G [V(C_0 \cap gC_1)]^2\, dg$ then provides a lower bound for $\mathcal{I}(C_0, C_1)$. One such bound is (15.59). Another is obtained by observing that the lower bound for $\mathcal{I}(C_0, C_1)$ in (15.61) is of the form $f(v) = 2av^{-1} - bv^{-2}$. Additionally, maximizing $f(v)$ subject to v gives $v = a^2/b$, indicating that when $\mu = V$, (15.61) is never better than (15.52).

15.9.7 Bounds Based on Noncommutative Harmonic Analysis

The integral for $\mathcal{I}_\rho(C_0, C_1)$ in (15.44) can be viewed from the perspective of noncommutative harmonic analysis when $\rho(g)$ is a pdf. Let $f(g) = \iota(C_0 \cap gC_1)$. Then

$$\mathcal{I}_\rho(C_0, C_1) = (f * \rho)(e)$$

is the convolution of f and ρ over G, evaluated at the identity element $e \in G$. Then by the convolution theorem and Fourier reconstruction formula,

$$\mathcal{I}_\rho(C_0, C_1) = \int_{\hat{G}} \operatorname{tr}[\hat{\rho}(\lambda)\hat{f}(\lambda)]\, d\lambda.$$

Various lower and upper bounds on $\operatorname{tr}[\hat{\rho}(\lambda)\hat{f}(\lambda)]$ can then be employed from matrix theory. For example, when $A = A^* > 0$ and $B = B^* > 0$, $\operatorname{tr}(AB) \le \operatorname{tr}(A) \cdot \operatorname{tr}(B)$. Additionally, the Fourier matrices of pdfs that are symmetric functions, $f(g) = f(g^{-1})$, satisfy this condition.

Alternatively, the eigenvalues of $\hat{\rho}(\lambda)$ and $\hat{f}(\lambda)$ can be computed, ordered from smallest to largest, and sums of products of eigenvalues so arranged can be used to provide an upper bound, whereas summing products in reverse order provides a lower bound.

Another sort of problem that can be tackled by noncommutative harmonic and functional analysis is one of the form

$$\mathcal{I}(C_0, C_1, C_2) = \int_G \int_G \iota(C_0 \cap g_1 C_1)\iota(g_1 C_1 \cap g_2 C_2)\, dg_1\, dg_2.$$

By letting $w_1(g) = \iota(C_0 \cap gC_1)$ and $w_2(g) = \iota(C_1 \cap gC_2)$ and observing that $\iota(g_1 C_1 \cap g_2 C_2) = \iota(C_1 \cap (g_1^{-1} \circ g_2) C_2)$, the above integral can be written as

$$\mathcal{I}(C_0, C_1, C_2) = \int_G (w_1 * w_2)(g_2)\, dg_2 = \left(\int_G w_1(g_1)\, dg_1\right)\left(\int_G w_2(g_2)\, dg_2\right). \quad (15.62)$$

Now, in general, Young inequality for a unimodular Lie group states that [31, 34, 81]

$$\|w_2 * w_1\|_{p'} \leq c_G(p', q, r) \cdot \|w_1\|_q \cdot \|w_2\|_r, \quad \text{where } 1 + \frac{1}{p'} = \frac{1}{q} + \frac{1}{r}, \ p', q, r \geq 1, \quad (15.63)$$

where $c_G(p', q, r)$ is a constant bounded from above by unity that depends on the group and

$$\|w_i\|_q = \left(\int_G [w_i(g)]^q\, dg\right)^{\frac{1}{q}}.$$

Setting $p' = 1$ would give exactly what is required to compute an upper bound for $\mathcal{I}(C_0, C_1, C_2)$ although there is no need to do so, since (15.62) is an exact equality. When $p' = \infty$ and $p = q = 2$, an upper bound on the value of $(w_1 * w_2)(g)$ is obtained and the Parseval/Plancherel equality can be used to compute the integrals needed in this bound.

15.9.8 Multi-Gaussian Approximations

Suppose that rather than exact formulae or inequalities, one is interested in approximating the volume of motion corresponding to all intersections of bodies. This can be achieved by approximating the set indicator function of a body, $I_C(\mathbf{x})$, with a weighted sum of Gaussian distributions, $p_C(\mathbf{x})$. This is not limited to the case of convex bodies. However, rather than obtaining a clear "yes" or "no" answer for each intersection, as would be the case in evaluating[9]

$$\iota(C_0 \cap gC_1) = u\left[\int_{\mathbb{R}^n} I_{C_0}(\mathbf{x})\, I_{C_1}(g^{-1} \cdot \mathbf{x})\, d\mathbf{x}\right],$$

in this approximation one obtains a number between 0 and 1 by evaluating the correlation

$$\iota(C_0 \cap gC_1) \approx \iota'(C_0 \cap gC_1) \doteq \frac{\int_{\mathbb{R}^n} p_{C_0}(\mathbf{x}) p_{C_1}(g^{-1} \cdot \mathbf{x})\, d\mathbf{x}}{\left(\int_{\mathbb{R}^n} [p_{C_0}(\mathbf{x})]^2\, d\mathbf{x}\right)^{\frac{1}{2}} \left(\int_{\mathbb{R}^n} [p_{C_1}(\mathbf{x})]^2\, d\mathbf{x}\right)^{\frac{1}{2}}}. \quad (15.64)$$

The fact that $0 \leq \iota'(C_0 \cap gC_1) \leq 1$ follows from the Cauchy–Schwarz inequality, and g is removed from the C_1 term in the denominator due to the invariance of integration over $\mathbb{R}^n$ under rigid-body motion. Each of the integrals in (15.64) can be computed in closed form. Additionally, the resulting dependence of $\iota'(C_0 \cap gC_1)$ on $g \in G$ then allows for a closed-form expression for

$$\mathcal{I}'(C_0, C_1) \doteq \int_G \iota'(C_0 \cap gC_1)\, dg. \quad (15.65)$$

[9] Here, $u[\cdot]$ is the unit Heaviside step function.

15.10 Bounds on Integrals of Powers of the Euler Characteristic

Though not directly relevant to parts entropy, it is interesting to note in passing that integral-geometric inequalities involving powers of the Euler characteristic can be derived easily. Here the same definitions of $\mathcal{X}(C_0, C_1)$ and $\mathcal{I}(C_0, C_1)$ as in the previous section are used.

The *reverse Cauchy-Schwarz inequality* states that for nonnegative sets of numbers $\{a_i\}$, $\{b_i\}$, $\{w_i\}$,

$$p \geq \frac{a_i}{b_i} \geq q \;\forall i \implies \left(\sum_i w_i a_i^2\right)^{\frac{1}{2}} \left(\sum_i w_i b_i^2\right)^{\frac{1}{2}} \leq \frac{p+q}{2\sqrt{pq}} \sum_i w_i a_i b_i. \tag{15.66}$$

Making the substitutions $a_i \to \iota(C_0 \cap gC_1)$, $b_i \to \chi(C_0 \cap gC_1)$, $w_i \to dg$, and $\sum_i \to \int_G$ then gives

$$\mathcal{X}(C_0, C_1) \geq \frac{2\left(\max_{g\in G} \chi(C_0 \cap gC_1)\right)^{\frac{1}{2}}}{1 + \max_{g\in G} \chi(C_0 \cap gC_1)} \cdot [\mathcal{I}(C_0, C_1)]^{\frac{1}{2}} \cdot \left(\int_G [\chi(C_0 \cap gC_1)]^2 dg\right)^{\frac{1}{2}}. \tag{15.67}$$

Given the formula for $\mathcal{X}(C_0, C_1)$, a lower bound for $\mathcal{I}(C_0, C_1)$, and an upper bound for $\max_{g\in G} \chi(C_0 \cap gC_1)$, an upper bound for the integral of $[\chi(C_0 \cap gC_1)]^2$ can be obtained. On the other hand, a lower bound can be obtained as a special case of (15.52) when an upper bound for $\mathcal{I}(C_0, C_1)$ is known.

15.11 Kinematic Formulas for Articulated Bodies

Consider now the case where C_0 is fixed and C_1 is not a single rigid body but rather two rigid bodies connected by a joint or some other constraint; that is, $C_1(g') = C_1^{(1)} \cup g' C_1^{(2)}$, where $g' \in G$ can be thought of as being sampled from a probability density $f(g')$ that describes the allowable motions between the two components of C_1. Then the problem addressed earlier in this chapter is modified as the computation

$$\begin{aligned}
\mathcal{I}_{w,f}\left(C_0, C_1^{(1)}, C_1^{(2)}\right) &\doteq \int_{g'\in G} \left[\int_{g\in G} \iota\left(C_0 \cap g\left[C_1^{(1)} \cup g' C_1^{(2)}\right]\right) w(g)\, dg\right] f(g')\, dg' \\
&= \int_G \int_G \iota\left(C_0 \cap \left[gC_1^{(1)} \cup (g \circ g') C_1^{(2)}\right]\right) w(g) f(g')\, dg\, dg'.
\end{aligned}$$

We now seek to simplify the evaluation of this integral.

Recall from (1.23) of Chapter 1 that the indicator function has the properties

$$I_{A\cup B}(x) = I_A(x) + I_B(x) - I_{A\cap B}(x) \quad \text{and} \quad I_{A\cap B}(x) = I_A(x)\, I_B(x). \tag{15.68}$$

Applying (15.68) and using the fact that $V(A) = \int_{\mathbb{R}^n} I_A(\mathbf{x})\, d\mathbf{x}$ and $\iota(A) = u[V(A)]$ (where in our case, $A = C_0$, $B = gC_1^{(1)}$, and $C = (g \circ g')C_1^{(2)}$) gives

$$V(A \cap [B \cup C]) = V(A \cap B) + V(A \cap C) - V(A \cap B \cap C). \tag{15.69}$$

Then $\iota(A \cap [B \cup C]) = u[V(A \cap [B \cup C])]$. If $u[\cdot]$ is replaced with any of the $\phi_k(\cdot)$ discussed in Section 15.9.6, then a lower bound on $\mathcal{I}_{w,f}\left(C_0, C_1^{(1)}, C_1^{(2)}\right)$ can be obtained. However, with the exception of $\phi_5(\cdot)$ and $\phi_8(\cdot)$ (with $n=1$), these lower bounds may be difficult to compute. Note that the latter of these is equivalent to (15.49). Starting with this,

$$\iota(A \cap [B \cup C]) \geq \frac{V(A \cap [B \cup C])}{\min\{V(A), V(B \cup C)\}} \geq \frac{V(A \cap [B \cup C])}{\min\{V(A), V(B)+V(C)\}}.$$

Since each term in the denominator is independent of how the bodies move, we can focus on the numerator and use (15.69) to write

$$\mathcal{I}_{w,f}\left(C_0, C_1^{(1)}, C_1^{(2)}\right) \cdot \min\{V(A), V(B)+V(C)\} \geq V_1 + V_2 - V_3,$$

where

$$V_1 = \int_G \int_G V\left(C_0 \cap g C_1^{(1)}\right) w(g) f(g')\, dg\, dg' = \int_G V\left(C_0 \cap g C_1^{(1)}\right) w(g)\, dg,$$

$$\begin{aligned} V_2 &= \int_G \int_G V\left(C_0 \cap (g \circ g') C_1^{(2)}\right) w(g) f(g')\, dg\, dg' \\ &= \int_G \int_G V\left(C_0 \cap g_1 C_1^{(2)}\right) w(g) f(g^{-1} \circ g_1)\, dg\, dg_1 \\ &= \int_G V\left(C_0 \cap g_1 C_1^{(2)}\right) (w * f)(g_1)\, dg_1, \end{aligned}$$

and

$$\begin{aligned} V_3 &= \int_G \int_G V\left(C_0 \cap g C_1^{(1)} \cap (g \circ g') C_1^{(2)}\right) w(g) f(g')\, dg\, dg' \\ &= \int_G \int_G V\left(C_0 \cap g C_1^{(1)} \cap g_1 C_1^{(2)}\right) w(g) f(g^{-1} \circ g_1)\, dg\, dg_1 \\ &\geq \left(\max_{(g,g_1) \in G \times G} w(g) f(g^{-1} \circ g_1)\right) \cdot \int_G \int_G V\left(C_0 \cap g C_1^{(1)} \cap g_1 C_1^{(2)}\right) dg\, dg_1. \end{aligned}$$

The last line is simply Hölder's inequality with $p=1$ and $q=\infty$. The term in the integral on that line can be computed as a special case of (15.34).

15.12 Parts Entropy

Imagine that a rigid component (i.e., a part) can be placed at random in a bounded planar or spatial environment. If the environment is empty and there are no potential energies causing the part to move to a minimum, then the part can visit each position and orientation defined by the boundaries with equal probability. If obstacles or other parts limit the allowable motion, then this will change the degree of disorder in the environment, because the number of possible locations that the part can occupy will decrease.

Let $G = SE(n)$ for $n = 2$ or 3 denote the group of rigid-body motions in the plane or in space and let g denote an arbitrary rigid-body motion in G. Let $f(g)$ be a probability density function on G; that is,

$$\int_G f(g)\, dg = 1,$$

where dg is the natural (bi-invariant) integration measure for G.

The entropy of one isolated part was defined by Sanderson [60] as ([60])

$$S = -\int_G f(g) \log f(g)\, dg.$$

It need not be the case that $f(g)$ is uniform and it need not be the case that it is even smooth. For example, we may want to study the entropy of a polyhedral object (which is spatial, and the motions of which are described as elements of $SE(3)$) in terms of all possible ways that it can sit stably on a table. In this case, the distribution $f(g)$ may be singular in the sense that it is only nonzero on a thin set of values along the z axis.

If there are two parts in an environment, then the combinations of all possible ways that they can be simultaneously positioned and oriented without overlap is denoted here as $f'(g_1, g_2)$ It is a probability normalized such that

$$\int_G \int_G f'(g_1, g_2)\, dg_1\, dg_2 = 1$$

and the corresponding parts entropy is

$$S_{12} = -\int_G \int_G f'(g_1, g_2) \log f'(g_1, g_2)\, dg_1\, dg_2.$$

Although the discussion here will be limited to one and two parts, the extension to multiple parts follows in a natural way.

Generally speaking, the entropy of a pdf is bounded from above by the sum of entropies of corresponding marginal densities. For example,

$$S_{12} \leq -\sum_{i=1}^{2} \int_G f_i'(g_i) \log f_i'(g_i)\, dg_i, \tag{15.70}$$

where

$$f_1'(g_1) = \int_G f'(g_1, g_2)\, dg_2 \quad \text{and} \quad f_2'(g_2) = \int_G f'(g_1, g_2)\, dg_1.$$

Equality in (15.70) holds if and only if $f'(g_1, g_2) = f_1(g_1) f_2(g_2)$. Therefore, treating the distributions of two parts separately without regard to their interaction will always overestimate the total parts entropy.

15.13 Entropy of Loosely Connected Parts

Suppose that two rigid parts are connected with a joint or are in some other way coupled but are allowed to exhibit some degree of motion relative to each other. How can the entropy of this articulated part be described? Let the first part have a distribution of allowable motions $f_{0,1}(g)$ defined relative to a frame fixed in space and let the second part have a distribution of allowable motions *relative to the first part*, $f_{1,2}(g)$. This means that $f_{0,1}(g)$ has built into it any effects due to boundaries and obstacles in the environment and that $f_{1,2}(g)$ does not consider this at all. Now, the convolution of these two functions,

$$f_{0,2}(g) = (f_{0,1} * f_{1,2})(g) = \int_G f_{0,1}(h) f_{1,2}(h^{-1} \circ g)\, dh, \tag{15.71}$$

will provide *an overestimate* of the allowable motion of body 2 in space because it does not restrict body two from interpenetrating with obstacles (although by the way $f_{1,2}(g)$ is defined, it would automatically exclude any nonphysical interactions between body 1 and body 2). The way to "fix" $f_{0,2}(g)$ so as to take into account environmental boundaries is to zero it over all values of g that cause an intersection of body 2 with the environment and then rescale the nonzero density that remains so that it is a pdf. Let us call this $\tilde{f}_{0,2}(g)$. It follows that

$$-\int_G \tilde{f}_{0,2}(g)\log\tilde{f}_{0,2}(g)\,dg \leq -\int_G f_{0,2}(g)\log f_{0,2}(g)\,dg$$

because imposing constraints that concentrate probability density will decrease entropy (disorder).

Furthermore, since $f_{0,2}(g_2)$ is the marginal of $f'(g_1,g_2)$ (which is the true joint density taking into account all constraints on the allowable motion of both bodies) over g_1, it follows from the previous subsection that the sum of the entropy of $f_{0,1}(g_1)$ and $\tilde{f}_{0,2}(g_2)$ will be an upper bound on the entropy of $f'(g_1,g_2)$. Additionally, a looser (but easier to compute) bound on the entropy of $f'(g_1,g_2)$ will just be the sum of the entropies of $f_{0,1}(g_1)$ and $f_{0,2}(g_2)$. Therefore, we can bound $f'(g_1,g_2)$ from above by computing and summing the entropies of $f_{0,1}(g_1)$ and $f_{0,2}(g_2)$.

On the other hand, the operation of convolution of two pdfs makes each one more spread out than the original. Therefore, the entropy of $f_{0,2}(g_2)$ is bounded from below by the entropy of $f_{0,1}(g)$ and of $f_{1,2}(g)$. The greater of these entropies can be chosen so as to have the tighter of the two lower bounds.

Due to the special role that convolution plays in probability theory and in the calculation of entropy of articulated parts, the following section addresses some details about convolution on $SE(3)$.

A convolution integral of the form in (15.71) can be written in the following equivalent ways:

$$(f_{0,1} * f_{1,2})(g) = \int_G f_{0,1}(z^{-1})f_{1,2}(z \circ g)\,dz = \int_G f_{0,1}(g \circ k^{-1})f_{1,2}(k)\,dk, \qquad (15.72)$$

where the substitutions $z = h^{-1}$ and $k = h^{-1} \circ g$ have been made, and the invariance of integration under shifts and inversions is used.

It is often convenient to use exponential parameters, $\mathbf{x}$, to describe rigid-body motions (see Section 10.2.3). One can define a Gaussian distribution on the six-dimensional Lie group $SE(3)$ much in the same way as is done on $\mathbb{R}^6$ provided that (1) the covariances are small and (2) the mean is located at the identity. The reason for these conditions is because near the identity, $SE(3)$ resembles $\mathbb{R}^6$, which means that $dg \approx dx_1 \cdots dx_6$, and we can define the Gaussian in the exponential parameters as

$$f(g(\mathbf{x})) = \frac{1}{(2\pi)^3|\Sigma|^{\frac{1}{2}}}\exp\left(-\frac{1}{2}\mathbf{x}^T\Sigma^{-1}\mathbf{x}\right). \qquad (15.73)$$

Given two such distributions that are shifted as $f_{i,i+1}(g_{i,i+1}^{-1} \circ g)$, each with 6×6 covariance $\Sigma_{i,i+1}$, then it can be shown that the mean and covariance of the convolution $f_{0,1}(g_{0,1}^{-1} \circ g) * f_{1,2}(g_{1,2}^{-1} \circ g)$ respectively will be of the form $g_{0,2} = g_{0,1} \circ g_{1,2}$ and [24, 76]

$$\Sigma_{0,2} = [Ad(g_{1,2})]^{-1}\Sigma_{0,1}[Ad(g_{1,2})]^{-T} + \Sigma_{1,2}. \qquad (15.74)$$

This provides a method for computing covariances of two concatenated bodies, and this formula can be iterated to compute covariances of chains without having to compute convolutions directly.

It is well known that the information-theoretic entropy of an n-dimensional Gaussian distribution,

$$f(\mathbf{x}, \Sigma) = \frac{1}{(2\pi)^{n/2}|\Sigma|^{\frac{1}{2}}} \exp\left(-\frac{1}{2}\mathbf{x}^T \Sigma^{-1} \mathbf{x}\right),$$

is

$$S = \log\{(2\pi e)^{n/2}|\Sigma|^{\frac{1}{2}}\}, \tag{15.75}$$

where $\log = \log_e$.

This means that in the absence of any interactions between parts, the entropy of an articulated body can be obtained by using (15.74) and (15.75).

15.14 Chapter Summary

The difficulty of an assembly task can be quantified using the concept of parts entropy. Sanderson's original formulation of this concept was for an individual isolated part. Issues that arise in the context of multiple parts are articulated in this chapter. Methods of integral geometry are adapted in this chapter and shown to be useful as a tool for computing the parts entropy of multiple parts. Although this beautiful theory extends to higher-dimensional Euclidean spaces and to manifolds, the applications discussed here only require the case of bodies in $\mathbb{R}^2$ and $\mathbb{R}^3$. Open issues include how to adapt techniques from integral geometry to cases in which the parts are not distributed uniformly at random but rather have some prior probability densities. In addition, the issue of part entropies for articulated parts, rather than individual rigid parts, remains a challenging problem. For example, formulas or approximations for the following integrals would be desirable in the analysis of parts entropy:

$$\mathcal{I}_w(C_0, C_1) \doteq \int_G \iota(C_0 \cap gC_1)\, w(g)\, dg$$

and

$$\mathcal{I}(C_0, C_0, C_1) \doteq \int_G \int_G \iota(C_0 \cap g_1 C_0)\, \iota(g_1 C_0 \cap g_2 C_1)\, dg_1\, dg_2.$$

Here, $w(g)$ is an arbitrary pdf on G and C_0, C_0, and C_1 are bodies which may or may not be convex. Whereas bounds for these were derived, it would be useful to have either exact formulas or accurate approximations. At the current time, formulas for these quantities, as well as their generalizations to multiple bodies, are unknown to the author.

The author's interest in integral geometry arose from problems in robotics [22, 23] as it relates to assembly planning [28, 29, 49, 79] and has grown to include modeling excluded volume effects in characterizing allowable motions in protein loops [24].

Classical works on convex and integral geometry include [13, 18, 21, 25–27, 30, 32, 40–42, 45, 54, 55]. Comprehensive monographs on this topic include [55, 61, 64], and other related books are [58, 70, 71]. Relatively recent expositions of these topics include [46, 47, 50] and the case where Euclidean space is replaced with a space of constant curvature,[10] such as a sphere [74]. Extensions of the principal kinematic formula

[10] As defined in [80].

where translations replace full rigid-body motions include [33, 35–39, 51, 56, 57, 59, 62, 63, 77, 78]. Related to this are studies of when one body can be completely enclosed in another [44, 82–85]

Generalizations of the concepts presented here and other aspects of stochastic/ integral geometry beyond the principal kinematic formula can be found in [1–3, 5, 7, 9, 10, 16, 48, 53, 66–68, 72–75]. Stochastic geometry in a different sense than that used here has been applied to communication networks [4]

15.15 Exercises

15.1. Derive the principal kinematic formula for convex bodies in the planar case using Cartesian coordinates rather than polar.

15.2. Fill in the details of the derivation of the principal kinematic formula for convex bodies in three-dimensional Euclidean space.

15.3. The concept of convex bodies can be extended to spaces other than $\mathbb{R}^n$. For example, a convex body on the unit sphere S^2 can be defined as one for which the shortest geodesic arc connecting every two pair of points in the body stays in the body. Given two such convex bodies, derive a version of the principal kinematic formula for the sphere where the group acting on the bodies is $SO(3)$ using the same sort of rolling argument used to derive the planar case. In the limit as the bodies become small in comparison to the radius of the sphere, show that your formula reduces to the principal kinematic formula for the Euclidean plane.

15.4. In Chapter 5, closed-form formulas for the volume, surface area, and integral of mean curvature were given for oblate and prolate ellipsoids. As an approximation to an ellipsoid of the form $\mathbf{x}^T A\mathbf{x} = 1$, one can use a Gaussian-like function of the form $f_i(\mathbf{x}) = \exp(-\frac{1}{2}c\mathbf{x}^T A\mathbf{x})$. Pick several uniaxial parameters for pairs of ellipsoids and compare the result of the principal kinematic formula with the closed-form expression that you find for the Gaussian integral

$$I \doteq \int_{SE(3)} f_1(\mathbf{x}) f_2(g^{-1} \cdot \mathbf{x})\, d\mathbf{x}.$$

Tune the constant c so as to get the closest possible match between this Gaussian approximation and the principal kinematic formula over the range of ellipsoids that you test.

15.5. The result in the previous exercise will necessarily never be exact because whatever choice of c is made in $\exp(-\frac{1}{2}b_i x^2)$ will be a poor proxy for the unit pulse function; that is, the function that takes a value of 1 on the range $x \in [0, 1]$ and 0 otherwise. However, if we could approximate a pulse well as a sum of Gaussian-like functions, then various extensions of the principal kinematic formula could be approximated well. Therefore, find constants $\{a_i, b_i\}$ such that

$$f(x; \mathbf{a}, \mathbf{b}) = \sum_{k=1}^{n} a_i \exp\left(-\frac{1}{2} b_i x^2\right)$$

best approximates a unit pulse. Do this by (a) fitting of the parameters $\{a_i, b_i\}$ to given the minimal L^2 error between $f(x; \mathbf{a}, \mathbf{b})$ and the unit pulse function and (b) by matching the moments of this function, $m_k = \int_0^\infty x^k f(x; \mathbf{a}, \mathbf{b})\, dx$, with those for the pulse function and doing a nonlinear least-squares fit.

15.6. Consider two convex bodies in the plane, C_0 and C_1, with $\mathrm{Vol}(C_0) \ll \mathrm{Vol}(C_1)$, the maximal diameter of C_0 smaller than the minimal diameter of C_1, and the maximal curvature of C_1 smaller than the minimal curvature of C_0. Rather than computing the volume in $SE(2)$ corresponding to when two planar bodies intersect, compute the volume in $SE(2)$ corresponding to all possible motions of C_0 contained in C_1. The method of proof is very similar to that for the principal kinematic formula.

15.7. Do the same as in Exercise 15.6 but for bodies on the sphere using the same procedures as in Exercise 15.3.

15.8. Develop a volume of motion for containment formula analogous to that in Exercise 15.6 for the three-dimensional case.

15.9. Numerically verify the principal kinematic formula by selecting several convex bodies such as ellipses and rectangles and evaluating the integral $\int_{SE(2)} \iota(C_0 \cap gC_1)\, dg$ by discretizing it.

15.10. Do the same as in the previous exercise, but now explore what happens when C_0 and C_1 are not convex, as well as when the integral is computed relative to a non-Haar measure: $\int_{SE(2)} \iota(C_0 \cap gC_1) w(g)\, dg$. How do your numerical results compare with the analytical inequalities presented in the chapter?

References

1. Adler, R., Taylor, J., *Random Fields and Geometry*, Springer, New York, 2007.
2. Ambartzumian, R.V., *Combinatorial Integral Geometry with Applications to Mathematical Stereology*, John Wiley and Sons, Somerset, NJ, 1982.
3. Ambartzumian, R.V., “Stochastic geometry from the standpoint of integral geometry,” *Adv. Appl. Probab.*, 9(4), pp. 792–823, 1977.
4. Baccelli, F., Klein, M., Lebourges, M., Zuyev, S., “Stochastic geometry and architecture of communication networks,” *Telecommun. Syst.*, 7, pp. 209–227, 1997.
5. Baddeley, A., “Stochastic geometry: An introduction and reading-list,” *Int. Statist. Rev. / Rev. Int. Statist.*, 50(2), pp. 179–193, 1982.
6. Baddeley, A.J., Jensen, E.B.V., *Stereology for Statisticians*, Monographs on Statistics and Applied Probability Vol. 103. Chapman & Hall/CRC, Boca Raton, FL, 2005.
7. Baryshnikov, Y., Ghrist, R., “Target enumeration in sensor networks via integration with respect to Euler characteristic,” *SIAM J. Appl. Math.* 70, pp. 825–844, 2009.
8. Beneš, V., Rataj, J., *Stochastic Geometry: Selected Topics*, Kluwer Academic, Boston, 2004.
9. Bernig, A., “A Hadwiger-type theorem for the special unitary group,” *Geom. Funct. Anal.*, 19, pp. 356–372, 2009 (also arXiv:0801.1606v4, 2008).
10. Bernig, A., Fu, J.H.G., “Hermitian integral geometry,” *Ann. of Math.*, 173, pp. 907–945, 2011 (also arXiv:0801.0711v9, 2010).
11. Blaschke, W., “Einige Bemerkungen über Kurven und Flächen konstanter Breite,” *Ber. Kgl. Sächs. Akad. Wiss. Leipzig*, 67, pp. 290–297, 1915.
12. Blaschke, W., *Vorlesungen über Integralgeometrie*, Deutscher Verlag der Wissenschaften, Berlin, 1955.
13. Bonnesen, T., Fenchel, W., *Theorie der Konvexen Körper*, Springer Verlag, Heidelberg, 1934.
14. Boothroyd G., *Assembly Automation and Product Design*, 2nd ed., CRC Press, Boca Raton, FL, 2005.

15. Boothroyd, G., Redford, A.H., *Mechanized Assembly: Fundamentals of Parts Feeding, Orientation, and Mechanized Assembly*, McGraw-Hill, London, 1968.
16. Bröcker, L., "Euler integration and Euler multiplication," *Adv. Geom.*, 5(1), pp. 145–169, 2005.
17. Brothers, J.E., "Integral geometry in homogeneous spaces," *Trans. Am. Math. Soc.*, 124, pp. 408–517, 1966.
18. Buffon, G.L.L., "Comte de: Essai d'Arithmétique Morale," In: Histoire naturelle, générale et particulière, Supplément 4, pp. 46–123. Imprimerie Royale, Paris, 1777.
19. Chen, C.-S., " On the kinematic formula of square of mean curvature," *Indiana Univ. Math. J.*, 22, pp. 1163–1169, 1972–3.
20. Chern, S.-S., "On the kinematic formula in the Euclidean space of N dimensions," *Am. J. Math.*, 74(1), pp. 227–236, 1952.
21. Chern, S.-S., "On the kinematic formula in integral geometry," *J. Math. Mech.*, 16(1), pp. 101–118, 1966.
22. Chirikjian, G.S., "Parts entropy, symmetry, and the difficulty of self-replication," *Proceedings of the ASME Dynamic Systems and Control Conference*, Ann Arbor, Michigan, October 20–22, 2008.
23. Chirikjian, G.S., "Parts Entropy and the Principal Kinematic Formula," *Proceedings of the IEEE Conference on Automation Science and Engineering*, pp. 864–869, Washington, DC, August 23–26, 2008.
24. Chirikjian, G.S., "Modeling loop entropy," *Methods Enzymol*, *C*, 487, pp. 101–130, 2011.
25. Crofton, M.W., "Sur quelques théorèmes de calcul intégral," *C.R. Acad. Sci. Paris*, 68, pp. 1469–1470, 1868.
26. Crofton, M.W., "Probability." In: Encyclopedia Britannica, 9th ed., 19, pp. 768–788. Cambridge University Press, Cambridge, 1885.
27. Czuber, E., *Geometrische Wahrscheinlichkeiten und Mittelwerte*, B. G. Teubner, Leipzig, 1884 (reprinted in 2010 by BiblioBazaar/Nabu Press, Charleston, South Carolina, 2010).
28. de Mello, L.S.H., Lee, S., eds., *Computer-Aided Mechanical Assembly Planning*, Kluwer, Boston, 1991.
29. Erdmann, M.A., Mason, M.T., "An exploration of sensorless manipulation", *IEEE J. Robot. Autom.*, 4(4), pp. 369–379, 1988.
30. Federer, H., "Some integralgeometric theorems," *Trans. Am. Math. Soc.*, 72(2), pp. 238–261, 1954.
31. Fournier, J.J.F., "Sharpness in Young's inequality for convolution," *Pacific J. Math.*, 72(2), pp. 383–397, 1977.
32. Fu, J.H.G., "Kinematic formulas in integral geometry," *Indiana Univ. Math. J.*, 39(4), pp. 1115–1154, 1990.
33. Fu, J.H.G., "The two faces of Blaschkean integral geometry," Internet notes, August 22, 2008, http://www.math.uga.edu/∼fu/research/research.html.
34. Führ, H., "Hausdorff–Young inequalities for group extensions," *Can. Math. Bull.*, 49(4), pp. 549–559, 2006.
35. Glasauer, S., "A generalization of intersection formulae of integral geometry," *Geom. Dedicata*, 68, pp. 101–121, 1997.
36. Glasauer, S., "Translative and kinematic integral formulae concerning the convex hull operation," *Math. Z.*, 229, pp. 493–518, 1998.
37. Goodey, P., Weil, W., "Translative integral formulae for convex bodies," *Aequationes Mathematicae*, 34, pp. 64–77, 1987.
38. Goodey, P., Weil, W., "Intersection bodies and ellipsoids," *Mathematika*, 42, pp. 295–304, 1995.
39. Groemer, H., "On translative integral geometry," *Arch. Math.*, 29, pp. 324–330, 1977.
40. Hadwiger, H., *Vorlesungen über Inhalt, Oberfläche und Isoperimetrie.*, Springer-Verlag, Berlin, 1957.
41. Hadwiger, H., *Altes und Neues über Konvexe Körper,* Birkhäuser-Verlag, Basel, 1955.
42. Harding, E.F., Kendall, D.G., *Stochastic Geometry: A Tribute to the Memory of Rollo Davidson*, John Wiley and Sons, London, 1974.

43. Howard, R., “The kinematic formula in Riemannian homogeneous spaces,” *Mem. Am. Math. Soc.*, 106(509), pp. 1–69, 1993.
44. Karnik, M., Gupta, S.K., Magrab, E.B., “Geometric algorithms for containment analysis of rotational parts,” *Computer-Aided Design*, 37(2), pp. 213–230, 2005.
45. Kendall, M.G., Moran, P.A.P., *Geometrical Probability*, Griffin’s Statistical Monographs, London, 1963.
46. Klain, D.A., Rota, G.-C., *Introduction to Geometric Probability*, Cambridge University Press, Cambridge, 1997.
47. Langevin, R., *Integral Geometry from Buffon to Geometers of Today*, Internet notes, 2009, http://math.u-bourgogne.fr/IMB/langevin/09_03_introdintegral.pdf.
48. Langevin, R., Shifrin, T., “Polar varieties and integral geometry,” *Am. J. Math.*, 104(3), pp. 553–605, 1982.
49. Liu, Y., Popplestone, R.J., “Symmetry Groups in Analysis of Assembly Kinematics,” *ICRA 1991*, pp. 572–577, Sacramento, CA, April 1991.
50. Mani-Levitska, P., “A simple proof of the kinematic formula,” *Monatsch. Math.*, 105, pp. 279–285, 1988.
51. Miles, R. E. “The fundamental formula of Blaschke in integral geometry and geometrical probability, and its iteration, for domains with fixed orientations,” *Austral. J. Statist.*, 16, pp. 111–118, 1974.
52. Nijenhuis, A., “On Chern’s kinematic formula in integral geometry,” *J. Diff. Geom.*, 9, pp. 475–482, 1974.
53. Ohmoto, T., “An elementary remark on the integral with respect to Euler characteristics of projective hyperplane sections,” *Rep. Fac. Sci. Kagoshima Univ.*, 36, pp. 37–41, 2003.
54. Poincaré, H., *Calcul de Probabilités*, 2nd ed., Gauthier-Villars, Imprimeur-Libraire, Paris, 1912. (reprinted by BiblioLife in 2009).
55. Pólya, G., “Über geometrische Wahrscheinlichkeiten,” *S.-B. Akad. Wiss. Wien*, 126, pp. 319–328, 1917.
56. Rataj, J., “A translative integral formula for absolute curvature measures,” *Geom. Dedicata*, 84, pp. 245–252, 2001.
57. Rataj, J., Zähle, M., “Mixed curvature measures for sets of positive reach and a translative integral formula,” *Geom. Dedicata*, 57, pp. 259–283, 1995.
58. Ren, D.-L., *Topics in Integral Geometry*, World Scientific Publishing, Singapore, 1994.
59. Rother, W., Zähle, M., “A short proof of the principal kinematic formula and extensions,” *Trans. Am. Math. Soc.*, 321, pp. 547–558, 1990.
60. Sanderson, A.C., “Parts entropy methods for robotic assembly system design,” *Proceedings of the 1984 IEEE International Conference on Robotics and Automation (ICRA ’84)*, Vol. 1, pp. 600–608, March 1984.
61. Santaló, L., *Integral Geometry and Geometric Probability*, Cambridge University Press, Cambridge, 2004 (originally published in 1976 by Addison-Wesley).
62. Schneider, R., “Kinematic measures for sets of colliding convex bodies,” *Mathematika* 25, pp. 1–12, 1978.
63. Schneider, R., Weil, W., “Translative and kinematic integral formulas for curvature measures,” *Math. Nachr.* 129, pp. 67–80, 1986.
64. Schneider, R., Weil, W., *Stochastic and Integral Geometry*, Springer-Verlag, Berlin, 2008.
65. Schneider, R., “Integral geometric tools for stochastic geometry,” in *Stochastic Geometry*, A. Baddeley, I. Bárány, R. Schneider, W. Weil, eds., pp. 119–184, Springer, Berlin, 2007.
66. Shifrin, T., “The kinematic formula in complex integral geometry,” *Trans. Am. Math. Soc.*, 264, pp. 255–293, 1981.
67. Schuster, F.E., “Convolutions and multiplier transformations of convex bodies,” *Trans. Am. Math. Soc.*, 359(11), pp. 5567–5591, 2007.
68. Slavskiĭ, V.V., “On an integral geometry relation in surface theory,” *Siberian Math. J.*, 13(3), pp. 645–658, 1972.
69. Solanes, G., “Integral geometry and the Gauss-Bonnet theorem in constant curvature spaces,” *Trans. Am. Math. Soc.*, 358(3), pp. 1105–1115, 2006.

70. Solomon, H.,*Geometric Probability*, SIAM, Philadelphia, 1978.
71. Stoyan, D., Kendall, W.S., Mecke, J., *Stochastic Geometry and its Applications*, 2nd ed., Wiley Series in Probability and Mathematical Statistics, John Wiley and Sons, Chichester, UK, 1995.
72. Stoyan, D., "Applied stochastic geometry: A survey," *Biomed. J.*, 21, pp. 693–715, 1979.
73. Taylor, J.E., "A Gaussian kinematic formula," *Ann. Probab.*, 34(1), pp. 122–158, 2006.
74. Teufel, V.E., "Integral geometry and projection formulas in spaces of constant curvature," *Abh. Math. Sem. Univ. Hamburg*, 56, pp. 221–232, 1986.
75. Viro, O., "Some integral calculus based on Euler characteristic," *Lecture Notes in Mathematics*, Vol. 1346, pp. 127–138, Springer-Verlag, Berlin, 1988.
76. Wang, Y., Chirikjian, G.S., "Error propagation on the Euclidean group with applications to manipulator kinematics," *IEEE Trans. Robot.*, 22(4), pp. 591–602, 2006.
77. Weil, W., "Translative integral geometry," in *Geobild '89*, A. Hübler et al., eds., pp. 75–86, Akademie-Verlag, Berlin, 1989.
78. Weil, W., "Translative and kinematic integral formulae for support functions," *Geom. Dedicata*, 57, pp. 91–103, 1995.
79. Whitney, D.E., *Mechanical Assemblies*, Oxford University Press, New York, 2004.
80. Wolf, J.A., *Spaces of Constant Curvature*, Publish or Perish Press, Berkeley, CA, 1977.
81. Young, W.H. "On the multiplication of successions of Fourier constants," *Proc. Soc. London A*, 87, pp. 331–339, 1912.
82. Zhang, G., "A sufficient condition for one convex body containing another," *Chin. Ann. Math.*, 9B(4), pp. 447–451, 1988.
83. Zhou, J., "A kinematic formula and analogues of Hadwiger's theorem in space," *Contemporary Mathematics*, Vol. 140, pp. 159–167, American Mathematical Society, 1992.
84. Zhou, J., "When can one domain enclose another in $\mathbb{R}^3$?," *J. Austral. Math. Soc. A*, 59, pp. 266–272, 1995.
85. Zhou, J., "Sufficient conditions for one domain to contain another in a space of constant curvature," *Proc. AMS*, 126(9), pp. 2797–2803, 1998.

16

Multivariate Statistical Analysis and Random Matrix Theory

This chapter is concerned with a number of issues in statistics that have a group-theoretic flavor. Large books can be found that are dedicated to each of the topics that are discussed briefly in the sections that follow. Although the coverage here is meant to be broad and introductory for the most part, effort is taken to elucidate connections between statistics and the theory of Lie groups, perhaps at the expense of completeness. The main topics covered are numerical sampling techniques, multivariate statistical analysis, and theory/numerical procedures associated with random orthogonal, positive definite, unitary, and Hermitian matrices. Integration on Lie groups and their homogeneous spaces ties these topics together. Pointers to classical applications in particle physics as well as more recent applications in complicated wireless communication networks are provided.

Multivariate analysis is concerned in large part with quantifying how close the mean and covariance computed from a set of sampled vectors in $\mathbb{R}^n$ is to the corresponding properties of a Gaussian distribution from which the samples are assumed to have been drawn. Since a covariance matrix is symmetric and positive definite, it can be viewed as an element of the homogeneous space $GL^+(n,\mathbb{R})/SO(n)$. Techniques and terminology from the theory of Lie groups can therefore be used to describe the distribution of sample covariance matrices drawn from a given Gaussian distribution as a function of the number of sample points. Integration of this distribution is relative to the measure defined by the ratio of Haar measures for $GL^+(n,\mathbb{R})$ and $SO(n)$. Therefore, methods for integration, coset decompositions, and so forth that were discussed earlier become immediately relevant.

The main points to take away from this chapter are as follows:

- Samples drawn from a multivariate Gaussian distribution can be used to compute a sample mean and sample covariance which, as the number of samples increases to infinity, converges to the mean and covariance of the underlying distribution.
- In the case of a finite number of samples, the distribution of means that will be obtained under a large number of trial draws, each with the same number of samples, will be approximately Gaussian with a covariance proportional to the covariance of the underlying distribution and inversely proportional to the number of samples.
- The distribution of sample covariance matrices is a probability density on the homogeneous space $GL^+(n,\mathbb{R})/SO(n)$ and is called the *Wishart distribution.*
- Group theory plays additional roles in multivariate analysis when additional symmetries are imposed on problems.

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_7,

- Several different concepts of random matrices exist such as symmetric matrices sampled at random from a Wishart distribution, special orthogonal matrices drawn at random from the uniform distribution of orientations, matrices filled with random entries each sampled from a uniform distribution on a real interval, and so forth.
- Large Hermitian matrices that are filled by sampling from a Gaussian distribution have eigenvalues that approach being distributed according to a specific probability density function, called *Wigner's semi-circle distribution*, as the size of the matrices goes to infinity.
- Closed-form integrals over the unitary group, $U(n)$, and special unitary group, $SU(n)$, play important roles in characterizing the statistical properties of random Hermitian matrices. Such matrices arise in particle physics and in large wireless communication networks.

This chapter is structured as follows. Section 16.1 begins this chapter by connecting the basic concepts from probability theory discussed in Chapters 2 and 3 of Volume 1 to statistics via numerical generation of sampled data. Section 16.2 reviews the basics of sample statistics in $\mathbb{R}^n$. Section 16.3 discusses resampling techniques such as the jacknife and bootstrap. Section 16.4 discusses the concept of maximum likelihood estimation in the context of Gaussian distributions. Section 16.5 connects multivariate statistical analysis and geometry through the concept of integration on matrix Lie groups and their homogeneous spaces. Section 16.6 is a Lie-theoretic treatment of multivariate analysis and the Wishart distribution. Sections 16.7 focuses on invariant integration over the set of symmetric positive-definite matrices and the group of orthogonal matrices. Section 16.8 discusses how the Wishart distribution is applied in multivariate statistical analysis. Whereas most of the chapter has an emphasis on Gaussian statistics, Section 16.9 discusses a class of non-Gaussian distributions, the multi-dimensional t-distributions. Section 16.10 provides a brief introduction to random matrix theory, which is concerned with distributions of eigenvalues of large Hermitian matrices. A complex version of the Wishart distribution appears in this setting, as do a number of closed-form integrals over unitary groups. Section 16.11 summarizes this chapter and Section 16.12 provides exercises.

16.1 Numerical Methods for Sampling from a Given Density

An important capability to have when numerically simulating statistical phenomena is that of generating random samples drawn from any desired pdf. As a starting point, assume that built in to your favorite scientific programming software are two kinds of random number generators that sample uniformly from[1] (1) the uniform distribution on the interval $[0, 1]$ and (2) the Gaussian with zero mean and unit variance. (In fact, it is possible to generate (2) from (1) using the methods described below, but since both are built in to most scientific computing packages, there is no loss of generality in assuming both as a starting point.)

From these two kinds of random number generators we will be able to generate random samples from a wide variety of distributions on closed intervals: the real line, the half-infinite line, and their product spaces. Three basic methods are (a) inversion of the cumulative distribution function (CDF) (b) transformation of samples and

[1] In actuality, a deterministic computer cannot generate truly random samples, but for all reasonable intents and purposes, such samples can be considered random.

(c) imposition of acceptance/rejection criteria. All three of these methods will be demonstrated here. Additionally, as will be shown, they are not mutually exclusive and can be used in combination as may be required by a particular problem. For more detailed discussions of numerical sampling methods, see [25, 40, 56]

16.1.1 The Inverse-CDF Transform Method (ITM)

Given a pdf on some connected subset of the real line, either finite or infinite, it is possible to define a CDF over that subset. For the sake of argument, consider the closed interval $[a, b]$. If the probability density on this interval is $f(x)$, then the corresponding CDF will be

$$F(x) \doteq \int_a^x f(\xi)\, d\xi.$$

This is the probability that a value between a and x will be experienced when sampling from $f(x)$. This probability can be written as $F(x) = P(a \leq X \leq x)$.

In order to use the ITM method presented below, the function $F(x)$ must be invertible. This is a rather mild condition to impose since any pdf can be regularized to make this condition hold at the expense of small distortions to the original pdf. For example, if the pdf is a Dirac delta function located somewhere in (a, b), then $F(x)$ will be a step function, which is not invertible. However, if in place of a Dirac delta we were to use a Gaussian distribution with very small variance, clipped outside of $[a, b]$, and rescaled as discussed in Chapter 2, then the CDF corresponding to the resulting regularized pdf will be invertible.

The procedure to generate samples using the *inverse transform method* (ITM) is then quite simple: First, sample values of s at random from the uniform distribution $u(s) = 1$ on the unit interval $[0, 1]$ (using routines built in to scientific programming software). This produces samples $\{S_1, S_2, \ldots, S_N\}$. Next, evaluate $X_i = F^{-1}(S_i)$ for $i = 1, \ldots, N$. That is, all! The resulting set $\{X_1, \ldots, X_N\}$ will be the desired samples.[2]

The reason why the method works follows from the fact that the probability of a sample, X, being in the subinterval $[x_1, x_2] \subset [a, b]$ is governed by the pdf $f(x)$, and likewise $u(s) = 1$ governs the probability of a sample, S, being in $[s_1, s_2] \subset [0, 1]$. The mapping $F : [a, b] \to [0, 1]$ relates the frequencies of occurrence of $x \in [a, b]$ and $s \in [0, 1]$ through the fact that

$$\int_{x_1}^{x_2} f(x)\, dx = F(x_2) - F(x_1) = s_2 - s_1 = \int_{s_1}^{s_2} u(s)\, ds.$$

This can be written as

$$P(x_1 \leq X \leq x_2) = P(s_1 \leq F_u(S) \leq s_2).$$

Since $F(x_i) = s_i$, it follows that $P(x_1 \leq X \leq x_2) = P(F(x_1) \leq S \leq F(x_2))$, which, in turn, implies from the monotonically increasing nature of $F(x)$ that

$$P(x_1 \leq X \leq x_2) = P(x_1 \leq F^{-1}(S) \leq x_2).$$

This is where the $X_i = F^{-1}(S_i)$ comes from. Figure 16.1 illustrates the method graphically. Samples are drawn uniformly at random from the interval $[0, 1]$, horizontal lines

[2] The set $\{X_1, \ldots, X_N\}$ has elements that are scalars and has nothing to do with Lie algebras, despite the use of the same symbols. There should be no confusion since the contexts are so different.

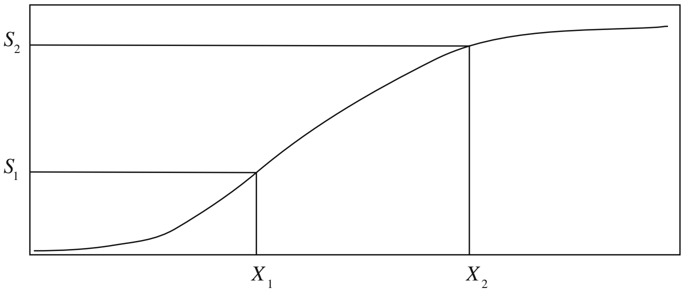


Fig. 16.1. A Graphical Description of the Inverse-CDF Method

are drawn from these sample values until they intersect the CDF, and then vertical lines are drawn down to generate sample values from an arbitrary univariate pdf. The examples below demonstrate the method.

Example 16.1.1.a: Given samples drawn from the uniform distribution $u(s) = 1$ on $[0, 1]$, we can obtain samples drawn from $f(\theta) = \frac{1}{2}\sin\theta$ on $[0, \pi]$ by observing that

$$s = F(\theta) = \frac{1}{2}\int_0^\theta \sin\alpha\, d\alpha = \frac{1}{2}(1 - \cos\theta)$$

and so

$$\theta = F^{-1}(s) = \cos^{-1}(1 - 2s) \tag{16.1}$$

(where, of course, the branch of $\cos^{-1}$ that returns values in the range $[0, \pi]$ is used). Therefore, samples Θ_1, Θ_2,..., Θ_N drawn from $f(\theta) = \frac{1}{2}\sin\theta$ are obtained by substituting the samples S_1,..., S_N drawn from $u(s)$ into (16.1).

Example 16.1.1.b: Given samples drawn from the uniform distribution $u(s) = 1$ on $[0, 1]$, we can obtain samples drawn from $f(x) = \frac{1}{\sqrt{2\pi}}e^{-x^2/2}$ (the Gaussian on the real line with zero mean and unit variance) by observing that

$$s = F(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^x e^{-t^2/2}dt = \frac{1}{2}\left[1 + \mathrm{erf}\left(\frac{x}{\sqrt{2}}\right)\right],$$

where $\mathrm{erf}(\cdot)$ is the standard error function defined in (2.39). Thus,

$$x = F^{-1}(s) = \sqrt{2}\,\mathrm{erf}^{-1}(2s - 1) \tag{16.2}$$

and Gaussian samples $X_1, X_2, \ldots, X_N$ are obtained from samples $S_1, \ldots, S_N$ drawn from $u(s)$ by evaluating $X_i = F^{-1}(S_i)$ in (16.2). As this example shows, it is not necessary to have an independent method for generating Gaussian samples, because they can be obtained from uniformly random samples. However, this does require the evaluation of the error function (and its inverse), which are typically built-in functions in scientific programming packages.

In cases where degrees of freedom can be decoupled (i.e., when random variables X and Y are independent), then $f(x, y) = f_1(x)f_2(y)$ and the ITM method can be used on each coordinate of a multivariate distribution independently. However, for more general multivariate pdfs, the computation and inversion of multivariate versions of CDFs can be problematic, and the methods in the following subsections become applicable.

16.1.2 The Geometric Transformation Method

Given a multivariate pdf $f(\mathbf{y})$ on a simply connected domain $B \subset \mathbb{R}^n$, we know from the classical inverse function theorem (1.38) that if $\mathbf{y} = \boldsymbol{\psi}(\mathbf{x})$ is a diffeomorphism from $\mathbb{R}^n$ onto itself, then $\boldsymbol{\psi}^{-1}(B)$ exists and

$$\int_B f(\mathbf{y})\, d(\mathbf{y}) = \int_{\boldsymbol{\psi}^{-1}(B)} f(\boldsymbol{\psi}(\mathbf{x})) \left| \frac{\partial \boldsymbol{\psi}}{\partial \mathbf{x}^T} \right| d(\mathbf{x}). \tag{16.3}$$

If $\boldsymbol{\phi} = \boldsymbol{\psi}^{-1}$, then this can be written as

$$\int_B f(\mathbf{y})\, d(\mathbf{y}) = \int_{\boldsymbol{\phi}(B)} f\left(\boldsymbol{\phi}^{-1}(\mathbf{x})\right) \left| \frac{\partial \boldsymbol{\phi}}{\partial \mathbf{x}^T} \right|^{-1} d(\mathbf{x}).$$

It is interesting to note in passing that (16.3) can be written in more modern terms by recognizing that functions $f : \mathbb{R}^n \to \mathbb{R}$ can be viewed as 0-forms (i.e., $\omega_0 = f$), and application of the concepts of the Hodge star operator and pull-back as

$$\int_B *\omega_0 = \int_{\boldsymbol{\psi}^{-1}(B)} *(\psi^* \omega_0). \tag{16.4}$$

Whereas modern notation hides Jacobians from plain sight in exchange for appropriately placed asterisks, it is actually the Jacobian determinant that plays the key role in the geometric sampling method. The fact that (16.3) introduces a Jacobian determinant means that data sampled uniformly in B will not be uniformly distributed in $\boldsymbol{\psi}^{-1}(B)$, and vice versa. This provides an opportunity to *choose* diffeomorphisms $\boldsymbol{\psi}(\mathbf{x})$ so as to distort an original sampling to obtain a desired one.

The general geometric transformation method can be stated rather simply in light of (16.3): Suppose that $f(\mathbf{y})$ is a pdf on a domain B for which an existing sampling method exists (e.g., $f(\mathbf{y})$ could be the uniform distribution $u(\mathbf{y}) = 1/\mathrm{Vol}(B)$). If we can find a diffeomorphism $\mathbf{y} = \boldsymbol{\psi}(\mathbf{x})$ such that $D = \boldsymbol{\psi}^{-1}(B)$ is the domain of interest and

$$\tilde{f}(\mathbf{x}) = f(\boldsymbol{\psi}(\mathbf{x})) \left| \frac{\partial \boldsymbol{\psi}}{\partial \mathbf{x}^T} \right|$$

is the pdf of interest on that domain, then $\mathbf{Y}_1$, $\mathbf{Y}_2$,..., $\mathbf{Y}_N$ sampled from $f(\mathbf{y})$ and mapped to D as $\mathbf{X}_i = \boldsymbol{\psi}^{-1}(\mathbf{Y}_i)$ for $i = 1, \ldots, N$ will sample the desired distribution $\tilde{f}(\mathbf{x})$. This method is illustrated below through examples, which can be stated in terms of either $\boldsymbol{\psi}$ or $\boldsymbol{\phi}$.

Example 16.1.2.a: Starting with samples independently drawn from the univariate Gaussian $\rho(y; 0, 1)$, it is easy to construct samples in $\mathbb{R}^n$ drawn from $\rho(\mathbf{y}; \mathbf{0}, \mathbb{I}_n)$. Call these vector samples $\mathbf{Y}_1$, $\mathbf{Y}_2$,..., $\mathbf{Y}_N$. Now, consider that the affine transformation $\mathbf{x} = \boldsymbol{\phi}(\mathbf{y}) = A\mathbf{y} + \mathbf{b}$, which can be used to generate new vector samples $\mathbf{X}_i = A\mathbf{Y}_i + \mathbf{b}$ for $i = 1, \ldots, N$. How will $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_N$ be distributed? Since $\mathbf{y} = \boldsymbol{\phi}^{-1}(\mathbf{x}) = \boldsymbol{\psi}(\mathbf{x}) = A^{-1}(\mathbf{x} - \mathbf{b})$, it follows that $|\partial\boldsymbol{\psi}/\partial\mathbf{x}^T| = |A^{-1}|$ and so

$$\rho(\mathbf{x}; \mathbf{0}, \mathbb{I}_n) \longrightarrow |A|^{-1} \rho(A^{-1}(\mathbf{y} - \mathbf{b}); \mathbf{0}, \mathbb{I}_n) = \rho(\mathbf{y}; \mathbf{b}, AA^T).$$

Example 16.1.2.b: The *Box–Muller transformation* [14] is a geometric alternative to the method presented in Example 16.1.1.b for generating Gaussian samples from a set of random samples uniformly distributed in $[0,1]$. Let x and y be Cartesian coordinates in the plane. Consider the new coordinates $0 \leq s, t \leq 1$ defined by

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \sqrt{-2\ln s}\cos(2\pi t) \\ \sqrt{-2\ln s}\sin(2\pi t) \end{pmatrix} \doteq \boldsymbol{\psi}^{-1}\begin{pmatrix} s \\ t \end{pmatrix}$$

and

$$\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} e^{-(x^2+y^2)/2} \\ \frac{1}{2\pi}\tan^{-1}(y/x) \end{pmatrix} = \boldsymbol{\psi}\begin{pmatrix} x \\ y \end{pmatrix}.$$

It follows that if s and t are sampled uniformly at random from $[0,1]$ resulting in sample pairs (S_i, T_i) for $i = 1, \ldots, N$, then since

$$ds\,dt = \begin{vmatrix} \frac{\partial s}{\partial x} & \frac{\partial s}{\partial y} \\ \frac{\partial t}{\partial x} & \frac{\partial t}{\partial y} \end{vmatrix} dx\,dy = \frac{1}{2\pi}e^{-(x^2+y^2)/2}\,dx\,dy,$$

$\mathbf{X}_i = \boldsymbol{\psi}^{-1}([S_i, T_i]^T)$ will be distributed according to $\rho(\mathbf{x}; \mathbf{0}, \mathbb{I}_2)$. Since the behaviors of x and y are independent, this can be used to generate samples from $\rho(x; 0, 1)$ without using the error function.

A similar phenomenon is observed when using the coordinates (u, v) defined as [25, 65]

$$x = u \cdot \left(\frac{-2\ln(u^2+v^2)}{u^2+v^2}\right)^{\frac{1}{2}},$$

$$y = v \cdot \left(\frac{-2\ln(u^2+v^2)}{u^2+v^2}\right)^{\frac{1}{2}}.$$

The benefit here is that no trigonometric functions are required.

Example 16.1.2.c: Suppose that we want to sample uniformly on the sphere with respect to the usual integration measure $(1/4\pi)\sin\theta\, d\phi\, d\theta$. From Example 16.1.1.a we know how to sample from the distribution $(1/2)\sin\theta$ on $[0,\pi]$, and sampling ϕ from the uniform distribution $1/2\pi$ on the range $[0, 2\pi]$ is easy. Combining them provides a way to sample on $[0,2\pi] \times [0,\pi]$ in a way that reflects the appropriate weighting from the metric tensor determinant. Call these samples (Φ_i, Θ_i) for $i = 1, \ldots, N$. Then these can be mapped to the unit sphere via (5.69) (with $R = 1$) to define samples $\mathbf{X}_i = \mathbf{x}(\Phi_i, \Theta_i)$ that are distributed uniformly at random.

This example begs the question of how to sample on other compact orientable Riemannian manifolds, M. Given an atlas, let us partition M into p nonoverlapping domains, $D_1, \ldots, D_p$, each with volume $V_1, \ldots, V_p$ (computed with respect to the Riemannian metric). Assume that coordinate chart ϕ_k completely covers D_k. Then to sample uniformly at random on M, we first must pick one of the D_k at random, the probability of which should be chosen in proportion to its volume. Suppose that D_k is the one that has been chosen. Let $\mathbf{q}$ denote the coordinates for this chosen domain. Then samples should be drawn from a density

$$f_k(\mathbf{q}) = \frac{1}{V_k}|G(\mathbf{q})|^{\frac{1}{2}}, \quad \text{where } V_k = \int_{D_k} |G(\mathbf{q})|^{\frac{1}{2}} d\mathbf{q}.$$

The geometric transformation method in $\mathbb{R}^n$ can be used to generate samples from $f_k(\mathbf{q})$. These samples, $\mathbf{Q}_1$, $\mathbf{Q}_2, \ldots, \mathbf{Q}_N$, then map to points in the manifold as $\phi_k^{-1}(\mathbf{Q}_i)$

for $i = 1, \ldots, n$; or, if the manifold is embedded, the samples would map to points $\mathbf{x}(\mathbf{Q}_i)$ in Euclidean space, as in the sphere example.

16.1.3 The Acceptance/Rejection/Modification Method

Since uniform sampling on $[0, 1]$ and from Gaussian distributions with zero mean and unit variance are build in to software programs, it is possible to start with these and then either modify or throw away samples in order to obtain samples from a desired distribution. For example, if samples from a clipped Gaussian are desired, it is possible to use the built-in Gaussian sampler, and then throw away those outside of the range defined by the clipping. Or, if sampling from the Gaussian wrapped around the circle is desired, then samples from the build-in Gaussian can be shifted if they lie outside the range $[-\pi, \pi]$ by addition/subtraction of integer multiples of 2π until they fall in the right range. By combining with the methods described previously, this sort of rejection or modification of samples can be applied to any initially supplied distribution, i.e., it is not limited to uniform distributions on unit intervals or unit-variance-zero-mean Gaussians on the line.

Example 16.1.3.a: Consider again the generation of random samples on the unit sphere. Begin by sampling the uniform distribution on $[-1, 1]^3$. If these samples obey the constraint $x_1^2 + x_2^2 + x_3^2 \leq 1$, then keep them. Otherwise throw them away. Then take each remaining sample vector and normalize it. This will project the result onto the unit sphere. The result will be a uniformly random distribution for the sphere. If the samples that lie outside the sphere had not been rejected, they would "pile up" around the directions corresponding to the corners of the bounding cube when projected on the sphere. If the surviving samples are converted to spherical coordinates, then this method can be used indirectly to generate samples for the pdf $\frac{1}{2} \sin\theta$ on the interval $[0, \pi]$ simply by picking off the θ coordinate from each pair of coordinates (ϕ_i, θ_i). Similar constructs can be imagined with other surfaces that bound closed bodies in $\mathbb{R}^n$. Knowing the analytical form of the Jacobian determinants for various hyper-surfaces allows for the appropriate choice.

The drawback of this method is that as the dimensions of the sample space increases, the volume of the sphere (or any other curved body) becomes smaller and smaller compared to the volume of the bounding box. Indeed, in the limit as n goes to infinity, the ratio of the volume of the ball bounded by the unit sphere in $\mathbb{R}^n$ compared to the volume of the cube $[-1, 1]^n$ goes to 0. Thus, the efficiency of sample generation becomes 0 since most samples are thrown away.

By combining several of the sampling methods, the weaknesses of each can be avoided. This is illustrated in the following example.

Example 16.1.3.b: If instead of sampling within a box in $\mathbb{R}^n$ and throwing away samples that lie outside the sphere, independent samples drawn from the univariate Gaussian $\rho(x; 0, 1)$ (which can either be generated as in Example 16.1.1.b or Example 16.1.2.a or can be taken as a primitive function) are used to construct vector samples from $\rho(\mathbf{x}; \mathbf{0}, \mathbb{I}_n)$ in a similar way as was done at the start of Example 16.1.2.a, then the transformation $\mathbf{x} \to \mathbf{x}/\|\mathbf{x}\| = \mathbf{u}$ can be used to convert the Gaussian samples $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_N$ into unit vectors $\mathbf{U}_1, \mathbf{U}_2, \ldots, \mathbf{U}_N$ distributed uniformly on the sphere S^{n-1}. These vectors are uniformly distributed because $\rho(R^T\mathbf{x}; \mathbf{0}, \mathbb{I}_n) = \rho(R^T\mathbf{x}; \mathbf{0}, RR^T) = \rho(\mathbf{x}; \mathbf{0}, \mathbb{I}_n)$ for any $R \in SO(n)$ is a spherically symmetric distribution with the mean at the center of the sphere.

16.1.4 Sampling Using SDEs

In some contexts it is desired to sample from a pdf that solves a Fokker–Planck equation at some value of time, $t = T$. Let $f(\mathbf{x}, T)$ denote such a pdf. Suppose that none of the sampling methods described above provides an adequate method to sample from this pdf. What can be done?

Quite simply, we already know from Chapters 4 and 8 the relationship between SDEs and Fokker–Planck equations in $\mathbb{R}^n$ and on manifolds, respectively. If the pdf that we seek to sample solves a Fokker–Planck equation, then the coefficient functions in the drift and diffusion terms can be picked off and used to define an SDE. This SDE can then be numerically integrated to generate sample paths from $t = 0$ until $t = T$. Each such sample path will then generate a single sample from $f(\mathbf{x}, T)$.

This method can be rather intensive from a computational perspective since a whole stochastic trajectory from $t = 0$ to $t = T$ must be computed in order to record a single point. On the other hand, if the goal is to sample from a family of pdfs $f(\mathbf{x}, t)$ for $t \in [0, T]$, then this method is not wasteful, since calculations that are performed at each time increment result in samples for a specific member of the family.

16.2 Sample Statistics in Euclidean Space

Often it is the case that the pdf associated with a random process is not known a priori. What is known is a set of N measurements $\{\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_N\}$ that are assumed to be drawn from an unknown pdf on $\mathbb{R}^n$. These samples are assumed to be iid (independent and identically distributed), meaning that there is no relationship between the samples other than the fact that they are drawn completely at random from the underlying distribution.

One goal is to recover an estimate of the unknown pdf from these sample measurements without any assumption about the form of the pdf. This is known as *nonparametric pdf estimation.* A more modest (and tractable) goal is to assume that the data is drawn from a distribution of known type (such as a Gaussian), and then the sample mean and covariance can be used to estimate the corresponding properties of the underlying distribution, thereby defining it completely. This is the *parametric* estimation problem.

In the subsections that follow, statistical properties of the sample mean and sample covariance are reviewed in the general (nonparametric) case and then the interpretation of these quantities when they are assumed to be drawn from a Gaussian distribution are addressed.

16.2.1 Properties of the Sample Mean

In this subsection the properties of the sample mean are reviewed. This material can be found in any book on multivariate statistical analysis. In particular, we follow the presentations in [2, 56].

Expected Value of the Sample Mean

Given samples $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_N \in \mathbb{R}^n$, the sample mean is defined as

$$\overline{\mathbf{X}} \doteq \frac{1}{N} \sum_{i=1}^{N} \mathbf{X}_i. \tag{16.5}$$

The *expected value* of this sample mean is

$$\langle \overline{\mathbf{X}} \rangle = \left\langle \frac{1}{N} \sum_{i=1}^{N} \mathbf{X}_i \right\rangle = \frac{1}{N} \sum_{i=1}^{N} \langle \mathbf{X}_i \rangle .$$

However, since the set of samples $\{\mathbf{X}_i\}$ is generated by an iid process, $\langle \mathbf{X}_i \rangle = \boldsymbol{\mu}$, which is the actual mean of the unknown pdf from which the samples are assumed to have been drawn. Therefore, summing up N copies of $\boldsymbol{\mu}$ and dividing by N results in the expression

$$\langle \overline{\mathbf{X}} \rangle = \boldsymbol{\mu}. \tag{16.6}$$

This is very important and allows for the estimation of the mean of the underlying pdf by taking the average of the samples. However, a natural question to ask is, "How close can we expect the sample mean to be to the actual?" This is addressed in the following subsection.

Distribution of the Sample Mean

Note that

$$\overline{\mathbf{X}} - \boldsymbol{\mu} = \frac{1}{N} \sum_{i=1}^{N} \mathbf{X}_i - \boldsymbol{\mu} = \frac{1}{N} \sum_{i=1}^{N} (\mathbf{X}_i - \boldsymbol{\mu}), \tag{16.7}$$

which is true again because if we add N copies of $\boldsymbol{\mu}$ to itself and divide by N, the result is equal to $\boldsymbol{\mu}$.

The covariance matrix of the random variable $\overline{\mathbf{X}}$ is defined as

$$\mathrm{Cov}(\overline{\mathbf{X}}) = \langle (\overline{\mathbf{X}} - \boldsymbol{\mu})(\overline{\mathbf{X}} - \boldsymbol{\mu})^T \rangle .$$

This is a measure of the dispersion of $\overline{\mathbf{X}}$ around $\langle \overline{\mathbf{X}} \rangle = \boldsymbol{\mu}$. From (16.7), this covariance matrix for the mean can be computed as

$$\begin{aligned} \mathrm{Cov}(\overline{\mathbf{X}}) &= \left\langle \left(\frac{1}{N} \sum_{i=1}^{N} (\mathbf{X}_i - \boldsymbol{\mu}) \right) \left(\frac{1}{N} \sum_{j=1}^{N} (\mathbf{X}_j - \boldsymbol{\mu}) \right)^T \right\rangle \\ &= \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} \left\langle [(\mathbf{X}_i - \boldsymbol{\mu})(\mathbf{X}_j - \boldsymbol{\mu})^T \right\rangle . \end{aligned} \tag{16.8}$$

However, since the sampled are assumed to be independent of each other and since this means that each component of one vector is independent of every component of the other vector [56], then when $i \neq j$, the expectation inside the sums will be 0. In particular,

$$\left\langle (\mathbf{X}_i - \boldsymbol{\mu})(\mathbf{X}_j - \boldsymbol{\mu})^T \right\rangle = \delta_{ij} \Sigma$$

since $\langle (\mathbf{X}_i - \boldsymbol{\mu})(\mathbf{X}_i - \boldsymbol{\mu})^T \rangle = \Sigma$ for every sample, which is assumed to be identically distributed. This kills one sum in (16.8) and gives $\mathrm{Cov}(\overline{\mathbf{X}}) = N^{-2} \sum_{i=1}^{N} \Sigma$, which simplifies to

$$\boxed{\mathrm{Cov}(\overline{\mathbf{X}}) = \frac{1}{N} \Sigma.} \tag{16.9}$$

This states that the distribution of the sample mean gets tighter as the number of samples increases, and it depends linearly on the covariance of the underlying distribution.

This is a nonparametric result; that is, no assumption about the form of the pdf had to be made. In the case when the samples are drawn from a Gaussian distribution, not only will the sample mean and covariance behave as described above but also the sample mean will be Gaussian distributed with mean $\boldsymbol{\mu}$ and covariance $\frac{1}{N}\Sigma$. In other words, as the number of trials, each drawing N samples, tends to infinity, the distribution of the mean will be Gaussian.

16.2.2 Properties of the Sample Covariance

As we will see in the following subsections, the assumption that the data is drawn from a Gaussian distribution will be helpful when addressing the distribution of the covariance matrix obtained from sampled data. However, first the unbiased nonparametric estimate of covariance is considered.

The *naive (or biased) sample covariance* is defined as

$$S_N = \frac{1}{N}\sum_{i=1}^{N}(\mathbf{X}_i - \overline{\mathbf{X}})(\mathbf{X}_i - \overline{\mathbf{X}})^T. \tag{16.10}$$

This is not the same as Σ, the covariance of the underlying pdf, but it is natural to assume that as $N \to \infty$, $S_N \to \Sigma$. Below, it is shown why this assumption is justified.

Using the fact that $\sum_{i=1}^{N}(\mathbf{X}_i - \overline{\mathbf{X}}) = \mathbf{0}$, (16.10) can be rewritten as

$$\begin{aligned}
S_N =& \frac{1}{N}\sum_{i=1}^{N}(\mathbf{X}_i - \overline{\mathbf{X}})\mathbf{X}_i^T + \frac{1}{N}\sum_{i=1}^{N}(\mathbf{X}_i - \overline{\mathbf{X}})(-\overline{\mathbf{X}})^T \\
=& \frac{1}{N}\sum_{i=1}^{N}\mathbf{X}_i\mathbf{X}_i^T - \overline{\mathbf{X}}\left(\frac{1}{N}\sum_{i=1}^{N}\mathbf{X}_i\right)^T - \left(\frac{1}{N}\sum_{i=1}^{N}\mathbf{X}_i\right)\overline{\mathbf{X}}^T + \overline{\mathbf{X}}\,\overline{\mathbf{X}}^T \\
=& \frac{1}{N}\sum_{i=1}^{N}\mathbf{X}_i\mathbf{X}_i^T - \overline{\mathbf{X}}\,\overline{\mathbf{X}}^T.
\end{aligned}$$

The expected value of the naive sample covariance is then

$$\begin{aligned}
\langle S_N\rangle =& \left\langle \frac{1}{N}\sum_{i=1}^{N}\mathbf{X}_i\mathbf{X}_i^T - \overline{\mathbf{X}}\,\overline{\mathbf{X}}^T\right\rangle \\
=& \frac{1}{N}\sum_{i=1}^{N}\langle\mathbf{X}_i\mathbf{X}_i^T\rangle - \langle\overline{\mathbf{X}}\,\overline{\mathbf{X}}^T\rangle.
\end{aligned}$$

Now, since $\langle(\mathbf{X}_i - \boldsymbol{\mu})(\mathbf{X}_i - \boldsymbol{\mu})^T\rangle = \Sigma$, it follows from elementary calculations that

$$\langle\mathbf{X}_i\mathbf{X}_i^T\rangle = \Sigma + \boldsymbol{\mu}\boldsymbol{\mu}^T.$$

Similarly, the fact that $\langle(\overline{\mathbf{X}} - \boldsymbol{\mu})(\overline{\mathbf{X}} - \boldsymbol{\mu})^T\rangle = \frac{1}{N}\Sigma$ means that

$$\langle\overline{\mathbf{X}}\,\overline{\mathbf{X}}^T\rangle = \frac{1}{N}\Sigma + \boldsymbol{\mu}\boldsymbol{\mu}^T.$$

Therefore,

$$\langle S_N\rangle = \Sigma + \boldsymbol{\mu}\boldsymbol{\mu}^T - \left(\frac{1}{N}\Sigma + \boldsymbol{\mu}\boldsymbol{\mu}^T\right),$$

which simplifies to

$$\boxed{\langle S_N \rangle = \frac{N-1}{N}\Sigma.} \tag{16.11}$$

This implies that a better (unbiased) estimate of the actual covariance matrix is

$$\boxed{\hat{S}_N \doteq \frac{N}{N-1}S_N = \frac{1}{N-1}\sum_{i=1}^{N}(\mathbf{X}_i - \overline{\mathbf{X}})(\mathbf{X}_i - \overline{\mathbf{X}})^T.} \tag{16.12}$$

In this way, $\langle \hat{S}_N \rangle = \Sigma$.

Whereas it was clear that the probability density for the sample mean corresponding to many trials, each drawing N samples, will be a Gaussian with mean μ and covariance Σ/N, describing the "covariance of sample covariances" and the corresponding probability density of sample covariances is somewhat more difficult. In part this is because unlike the space of mean vectors, the space of covariance matrices is a non-Euclidean space. This will require several sections to explain. However, first, a discussion of modern resampling methods is presented.

16.3 Resampling Methods

When obtaining an estimate of the mean, covariance, or some other quantity from sampled data, a natural question to ask is how sensitive the answer is to the removal of random samples. One way to assess this sensitivity (or variability of the answer) is to perform jackknife and bootstrap calculations. Many good books exist on this subject. In our review, we follow the presentation in [81].

16.3.1 Jackknife

The jackknife method was introduced by Quenouille in 1949 [78] to estimate the bias of an estimator by sequentially deleting one point from the original data set and recomputing the estimate for the $N-1$ depleted data sets. The basic idea, as explained in [81], begins with a scalar function $t(\mathbf{x})$, the average value of which would be computed as

$$\tau = \int_{\mathbb{R}^n} t(\mathbf{x})f(\mathbf{x})\,d\mathbf{x}$$

if the underlying pdf $f(\mathbf{x})$ were known. However, since $f(\mathbf{x})$ is generally not known, τ is estimated by a series of sampled measurements by an estimator $T_N(X_1, \ldots, X_N)$, where $\{X_i\}$ are the sample observations. The bias in the original estimate is then $\text{bias}(T_N) = \langle T_N \rangle - \tau$. In contrast, the jackknife estimate is defined as

$$T_{JACK} \doteq N \cdot T_N - \frac{N-1}{N}\sum_{i=1}^{N} T_{N-1,i}, \tag{16.13}$$

where $T_{N-1,i} = T_{N-1}(\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_{i-1}, \mathbf{X}_{i+1}, \ldots, \mathbf{X}_N)$ is the estimate obtained by removal of sample i. Assuming that the bias in the original estimate decays in an asymptotic series of the form

$$\text{bias}(T_N) = \frac{a}{N} + \frac{b}{N^2} + O\left(\frac{1}{N^3}\right)$$

and that the depleted data sets follow the same form, and so

$$\mathrm{bias}(T_{N-1,i}) = \frac{a}{N-1} + \frac{b}{(N-1)^2} + O\left(\frac{1}{(N-1)^3}\right),$$

then the associated bias in the bootstrap is

$$\begin{aligned}\mathrm{bias}(T_{JACK}) &= N \cdot \mathrm{bias}(T_N) - \frac{N-1}{N}\sum_{i=1}^{N}\mathrm{bias}(T_{N-1,i}) \qquad (16.14)\\ &= -\frac{b}{N(N-1)} + O\left(\frac{1}{(N-1)^3}\right). \qquad (16.15)\end{aligned}$$

In other words, under certain modest assumptions, the bias in the jacknife is smaller than that of the bias in the original estimator that used all of the sample data.

In 1958, Tukey extended the jackknife concept to the estimation of variances [94], where improvements in the estimate of variance can be proven using similar assumptions and arguments as those used above.

16.3.2 Bootstrap Methods

The bootstrap method resamples much more extensively than the jacknife. Although this method was developed by Efron in 1979 [33], elements of the theory were presented prior to that (see Hartigan's work [48]). Recall that given a set with N elements, there are

$$C_{N,k} = \binom{N}{k} = \frac{N!}{k!(N-k)!}$$

ways of removing k entries to result in $C_{N,k}$ sets of sets with $N-k$ entries. Since

$$\sum_{k=0}^{N} C_{N,k} = 2^N,$$

there are $2^N - 1$ nonempty subsets of the original set with which to recompute estimates. Clearly, then, given sufficient computing capabilities, one could compute an estimate of a covariance matrix based on not only the full set of data but also all subsets.

Since, in practice, this becomes prohibitive, a method that is sometimes used is to first obtain the original estimate of the covariance matrix, use that to define a multivariate Gaussian distribution and then randomly sample from this Gaussian distribution. If the distribution in covariances of the samples is consistent with the distribution of covariances obtained from extensive resampling, then greater confidence in the estimate is obtained. Sensitivity to outliers can be reduced by performing jackknifelike computations. More on these methods can be found in [22, 34].

16.4 Maximum Likelihood Estimation with Gaussian Distributions

Chapter 2 was devoted to the multivariate Gaussian distribution

$$\rho(\mathbf{x};\boldsymbol{\mu},\Sigma) \doteq \frac{1}{(2\pi)^{n/2}|\Sigma|^{\frac{1}{2}}}\exp\left\{-\frac{1}{2}(\mathbf{x}-\boldsymbol{\mu})^T\Sigma^{-1}(\mathbf{x}-\boldsymbol{\mu})\right\}. \qquad (16.16)$$

In Chapter 3, general parameterized distributions of the form $f(\mathbf{x};\boldsymbol{\theta})$ were discussed along with the concept of Fisher information, estimators, and the Cramér–Rao bound.

The goal in later chapters is to extend these concepts to Lie groups as $f(g;\boldsymbol{\theta})$ for $g \in G$, where, for example, $\boldsymbol{\theta}$ may be a combination of drift and diffusion parameters, in the context of the present.

The Gaussian distribution in (16.16) is often written in statistical works as $\rho(\mathbf{x} \mid \boldsymbol{\mu}, \Sigma)$. In other words, it is possible to write it as a conditional probability density that is conditioned on knowledge of the mean and covariance. More generally, $f(\mathbf{x};\boldsymbol{\theta})$ can be written as $f(\mathbf{x} \mid \boldsymbol{\theta})$, but this begs the question of what density on the parameter space should be used to describe the *prior*[3] $f(\boldsymbol{\theta})$ in order to obtain the joint density

$$f(\mathbf{x},\boldsymbol{\theta}) = f(\mathbf{x} \mid \boldsymbol{\theta})f(\boldsymbol{\theta}) = f(\boldsymbol{\theta} \mid \mathbf{x})f(\mathbf{x}).$$

For if such a prior exists, then

$$f(\mathbf{x}) = \int_{\boldsymbol{\theta}' \in \Theta} f(\mathbf{x} \mid \boldsymbol{\theta}')f(\boldsymbol{\theta}')\,d\boldsymbol{\theta}'$$

and

$$f(\boldsymbol{\theta} \mid \mathbf{x}) = \frac{f(\mathbf{x} \mid \boldsymbol{\theta})f(\boldsymbol{\theta})}{\int_{\boldsymbol{\theta}' \in \Theta} f(\mathbf{x} \mid \boldsymbol{\theta}')f(\boldsymbol{\theta}')\,d\boldsymbol{\theta}'}. \tag{16.17}$$

This means that based on observed data, $\{\mathbf{X}_1, \ldots, \mathbf{X}_N\}$, a Bayesian estimate of $\boldsymbol{\theta}$, denoted here as $\hat{\boldsymbol{\theta}}$, would be obtained from (16.17) as the value $\hat{\boldsymbol{\theta}} \in \Theta$ such that (16.17) holds as closely as possible for all $\mathbf{x} \in \{\mathbf{X}_1, \ldots, \mathbf{X}_N\}$ when $f(\boldsymbol{\theta})$ is known. Below arguments for obtaining $f(\boldsymbol{\theta})$ are given based on the concept of the likelihood function.

The *likelihood function* (which is not normalized to be a pdf) can be defined as

$$\mathcal{L}(\boldsymbol{\theta} \mid \mathbf{X}_1, \ldots, \mathbf{X}_N) \doteq \prod_{i=1}^{N} f(\mathbf{X}_i \mid \boldsymbol{\theta}). \tag{16.18}$$

A *maximum likelihood estimate* is one that seeks the value of $\boldsymbol{\theta}$ defined by

$$\tilde{\boldsymbol{\theta}} \doteq \arg\max_{\boldsymbol{\theta}} \mathcal{L}(\boldsymbol{\theta} \mid \mathbf{X}_1, \ldots, \mathbf{X}_N). \tag{16.19}$$

This is particularly convenient for the Gaussian distribution, since the product of exponentials results in the exponential of the sum of exponents. The *Gaussian likelihood function* is

$$\begin{aligned}
\mathcal{L}(\boldsymbol{\mu}, \Sigma \mid \mathbf{X}_1, \ldots, \mathbf{X}_N) &= \prod_{i=1}^{N} \rho(\mathbf{X}_i \mid \boldsymbol{\mu}, \Sigma) \qquad (16.20)\\
&= \frac{1}{(2\pi)^{Nn/2}|\Sigma|^{\frac{N}{2}}} \prod_{i=1}^{N} \exp\left\{-\frac{1}{2}(\mathbf{X}_i - \boldsymbol{\mu})^T \Sigma^{-1}(\mathbf{X}_i - \boldsymbol{\mu})\right\}\\
&= \frac{1}{(2\pi)^{Nn/2}|\Sigma|^{\frac{N}{2}}} \prod_{i=1}^{N} e^{-\frac{1}{2}\mathrm{tr}\left\{\Sigma^{-1}(\mathbf{X}_i - \boldsymbol{\mu})(\mathbf{X}_i - \boldsymbol{\mu})^T\right\}}\\
&= \frac{1}{(2\pi)^{Nn/2}|\Sigma|^{\frac{N}{2}}} e^{-\frac{1}{2}\mathrm{tr}\left\{\Sigma^{-1}\left[\sum_{i=1}^{N}(\mathbf{X}_i - \boldsymbol{\mu})(\mathbf{X}_i - \boldsymbol{\mu})^T\right]\right\}}. \qquad (16.21)
\end{aligned}$$

Now, using the definition in (16.5),

$$\mathbf{X}_i - \boldsymbol{\mu} = (\mathbf{X}_i - \overline{\mathbf{X}}) + (\overline{\mathbf{X}} - \boldsymbol{\mu})$$

[3] A priori density (or prior) refers to the fact that this distribution is independent of information obtained from observations.

and so the term inside the trace in (16.21) becomes

$$\sum_{i=1}^{N}(\mathbf{X}_i-\boldsymbol{\mu})(\mathbf{X}_i-\boldsymbol{\mu})^T = N\cdot S_N + N\cdot(\overline{\mathbf{X}}-\boldsymbol{\mu})(\overline{\mathbf{X}}-\boldsymbol{\mu})^T.$$

From the convexity and strictly decreasing nature of the function $\phi(x)=e^{-x/2}$ on $\mathbb{R}_{\geq 0}$, it follows that minimization of x will maximize $\phi(x)$. It can then be reasoned that the maximum likelihood estimate of $(\boldsymbol{\mu},\Sigma)$ is computed as

$$(\tilde{\boldsymbol{\mu}},\tilde{\Sigma}) = (\overline{\mathbf{X}}, S_N), \tag{16.22}$$

where S_N is defined in (16.10). Note that this is *not* the unbiased estimator $\hat{S}_N$ in (16.12). However, as $N\to\infty$, the difference between S_N and $\hat{S}_N$ becomes negligible. It is common to define

$$S \doteq N\cdot S_N = (N-1)\cdot\hat{S}_N.$$

Although S depends on N through the summation (as does $\overline{\mathbf{X}}$), this dependence is suppressed for notational convenience in the presentation that follows.

16.5 Integration and Probability Densities on Spaces of Matrices

In order to make sense of the concept of distributions on the set of all covariance matrices, it is first necessary to understand how to integrate on such a space. This provides a connection to the discussion of differential forms in Chapter 6 and to the Jacobian matrices for Lie groups in Chapter 10.

Differential forms can be used to define a concept of integration over spaces of matrices that may or may not have special structure. In this context, a specialized notation

$$\bigwedge_{i=1}^{n} dx_i \doteq dx_1\wedge dx_2\wedge\cdots\wedge dx_n$$

is introduced as shorthand to reduce the number of symbols that need to be written during derivations, following [71]. Using this notation, the (unoriented) Lebesgue measure on $\mathbb{R}^{m\times n}$ corresponding to the (oriented) volume form is[4]

$$d'X \doteq \left|\bigwedge_{i=1}^{m}\bigwedge_{j=1}^{n} dx_{ij}\right| = \prod_{i=1}^{m}\prod_{j=1}^{n} dx_{ij}, \quad \text{where } X\in\mathbb{R}^{m\times n}. \tag{16.23}$$

Here, the absolute value symbol is used to kill the sign of the form. In contrast, when the same symbol is applied to a matrix, it means the determinant.

Using the properties of the wedge product, it can be shown that if $Y=AXB$, where $X,Y\in\mathbb{R}^{m\times n}$, and $A\in\mathbb{R}^{m\times m}$ and $B\in\mathbb{R}^{n\times n}$ are fixed, then

$$d'Y = |A|^n|B|^m d'X, \tag{16.24}$$

where, as usual, $|A|$ denotes the determinant of A.

[4] The prime inserted in $d'X$ distinguishes it from dX because when $m=n$ and $X\in GL(n,\mathbb{R})$, the plain dX is used to denote the Haar measure for $GL(n,\mathbb{R})$.

16.5.1 $d'X$ Versus dX When $X \in GL(n,\mathbb{R})$

In contrast to $d'X$ as defined in (16.23) in the case when $m = n$, the Haar measure for $X \in GL(n,\mathbb{R})$ can be written as

$$dX = |X|^{-n}\, d'X, \tag{16.25}$$

and so for fixed $A, B \in GL(n,\mathbb{R})$,

$$d(AXB) = |AXB|^{-n}\, d'(AXB) = |X|^{-n}\, d'X = dX. \tag{16.26}$$

This invariance of dX is the rationale for making it the "natural" way to integrate over $GL(n,\mathbb{R})$ and, hence, the use of the simplest notation for this quantity (even though the formula for it is more complicated than that for $d'X$ in (16.23)).

16.5.2 Integration on the Space of $n \times n$ Symmetric Matrices

If $S = S^T \in \mathbb{R}^{n\times n}$, then a natural definition for the integration measure for the space of all such matrices, $\mathbb{S}_n$, is

$$d'S \doteq \left| \bigwedge_{j=1}^{n} \bigwedge_{i=1}^{j} ds_{ij} \right| = \prod_{1\leq i\leq j\leq n} ds_{ij}. \tag{16.27}$$

It can be shown that when $|S| \neq 0$, this measure has the property [71]

$$d'(S^{-1}) = |S|^{-(n+1)} d'S, \tag{16.28}$$

and that if $P = ASA^T$ for any $A \in GL(n,\mathbb{R})$,

$$d'P = |A|^{n+1} d'S. \tag{16.29}$$

The subset of $\mathbb{S}_n$ consisting of all symmetric positive definite $n \times n$ matrices is denoted as

$$\mathbb{S}_n^+ \doteq \{S \in \mathbb{R}^{n\times n} \mid S = S^T, \lambda_i(S) > 0, \forall\, i = 1, \dots, n\}. \tag{16.30}$$

The integral of a function on this space with respect to the measure $d'S$ can be defined as

$$I'(f) = \int_{\mathbb{S}_n^+} f(S)\, d'S.$$

From (16.29), it follows that for any $A \in GL(n,\mathbb{R})$, the action $(A\cdot f)(S) \doteq f(A^{-1}SA^{-T})$ has the property that

$$I'(A \cdot f) = \int_{\mathbb{S}_n^+} f(ASA^T)\, d'S = \int_{\mathbb{S}_n^+} f(P)\, d'(APA^T) = |A|^{n+1} I'(f).$$

In group-theoretic terminology, $d'S$ is called a *relatively invariant* integration measure on $\mathbb{S}_n^+$ with respect to the action of $GL(n,\mathbb{R})$. More abstractly, the concept of relative invariance of an integration measure on some measurable space $\mathcal{X}$ acted on by a group G is the property[5]

[5] The space $\mathcal{X}$ and function $\chi(g)$ should not be confused. Additionally, the dot in $g^{-1} \cdot x$ is a group action, whereas the dot between $\chi(g)$ and the integral is simply scalar multiplication.

$$\int_{\mathcal{X}} f(g^{-1} \cdot x)\, dx = \chi(g) \cdot \int_{\mathcal{X}} f(x)\, dx, \tag{16.31}$$

where $x \in \mathcal{X}$ and $g \in G$.

It is no coincidence that the symbol $\chi(g)$ is used as the scale factor, since repeating the above expression gives that $\chi(g)$ must have the property $\chi(g_1 \circ g_2) = \chi(g_1) \cdot \chi(g_2) = \chi(g_2) \cdot \chi(g_1) = \chi(g_2 \circ g_1)$. In other words, $\chi : G \to \mathbb{R}_{\geq 0}$ is a homomorphism from $(G, \circ)$ into the commutative group $(\mathbb{R}_{\geq 0}, \cdot)$, and therefore it must be a class function. A special case of relative invariance is when the definition of dx forces $\chi(g) = 1$ for all $g \in G$. In this case, dx is truly invariant under G. In general, it is not possible for arbitrary G and $\mathcal{X}$ to construct an invariant measure dx (although there are some special cases), but it is always possible to construct a relatively invariant measure. The case when $G = GL(n, \mathbb{R})$ and $\mathcal{X} = \mathbb{S}_n^+$ is one in which both a relatively invariant measure, $d'S$, and an invariant measure, dS (to be defined shortly), are both possible and useful.

The *multivariate gamma function* is defined as the following specific integral over $\mathbb{S}_n^+$:

$$\Gamma_n(a) \doteq \int_{\mathbb{S}_n^+} e^{-\mathrm{tr}(S)} |S|^{(2a-n-1)/2}\, d'S, \quad \text{where } n \in \mathbb{Z}_{>0} \text{ and } (n+1)/2 < a \in \mathbb{R}. \tag{16.32}$$

This can be related to the usual gamma function in (2.34) of Chapter 2 as in (16.81).

The above definition can extend to $a \in \mathbb{C}$ under the constraint that $\mathrm{Re}(a) > (n+1)/2$, but we will not need this generalization here. It can be shown that [71]

$$\frac{1}{2^{n \cdot a} \Gamma_n(a)} \int_{\mathbb{S}_n^+} e^{-\frac{1}{2}\mathrm{tr}\left(\Sigma^{-1} S\right)} |S|^{(2a-n-1)/2}\, d'S = |\Sigma|^a. \tag{16.33}$$

16.5.3 Integration on the Space of $n \times n$ Skew-Symmetric Matrices

In analogy with the way that an integration measure can be defined for the $n(n+1)/2$-dimensional space of symmetric matrices, for the $n(n-1)/2$-dimensional space consisting of skew-symmetric matrices $\Omega = -\Omega^T \in \mathbb{R}^{n \times n}$,

$$d'\Omega \doteq \prod_{1 \leq i < j \leq n} d\omega_{ij}.$$

This has the property that for any $A \in GL(n, \mathbb{R})$,

$$d'(A\Omega A^T) = |A|^{n-1}\, d'\Omega. \tag{16.34}$$

Unlike the symmetric case, it is not possible to normalize by a determinant when n is odd, since $|\Omega| = 0$ in that case.

16.5.4 Integration on Orthogonal Groups and Stiefel Manifolds

Let $O = [\mathbf{o}_1, \mathbf{o}_2, \ldots, \mathbf{o}_n] \in O(n)$ (the full group orthogonal $n \times n$ matrices); that is, $\mathbf{o}_i \in \mathbb{R}^n$ and $\mathbf{o}_i \cdot \mathbf{o}_j = \delta_{ij}$ for all $i, j \in \{1, \ldots, n\}$. A set of nonsquare matrices of the form $V = [\mathbf{o}_1, \mathbf{o}_2, \ldots, \mathbf{o}_m]$ for some fixed integer m in the range $1 \leq m \leq n$ can also be defined. This will have the property $V^T V = \mathbb{I}_m$, and the set of all such matrices for fixed m and n is denoted as $V_{m,n}$. This set has the properties of an $mn - m(m+1)/2$-dimensional manifold embedded in $\mathbb{R}^{n \times m} \cong \mathbb{R}^{nm}$. It is called the *Stiefel manifold.* As special cases, $V_{1,n} = S^n$, and $V_{n,n} = O(n)$.

The natural volume form with which to integrate on $V_{m,n}$ is [71]

$$\omega_{m,n} \doteq \bigwedge_{j=1}^{n-m} \bigwedge_{i=1}^{m} \mathbf{o}_{m+j}^T \, d\mathbf{o}_i \bigwedge_{1 \le i < j \le m} \mathbf{o}_j^T \, d\mathbf{o}_i. \tag{16.35}$$

It can be shown that

$$\int_{V_{m,n}} \omega_{m,n} = \frac{2^m \pi^{mn/2}}{\Gamma_m(n/2)} \doteq \mathrm{Vol}(V_{m,n}). \tag{16.36}$$

As special cases,

$$\int_{S^{n-1}} \omega_{1,n} = \frac{2\pi^{n/2}}{\Gamma(n/2)} = \mathrm{Vol}(S^{n-1})$$

and

$$\int_{O(n)} \omega_{n,n} = \frac{2^n \pi^{n^2/2}}{\Gamma_n(n/2)} = \mathrm{Vol}(O(n)) = 2 \cdot \mathrm{Vol}(SO(n)).$$

This provides the normalization factors required for the normalized integral over the full orthogonal group—namely

$$dO \doteq \frac{\Gamma_n(n/2)}{2^n \pi^{n^2/2}} \, |\omega_{n,n}| \implies \int_{O(n)} dO = 1. \tag{16.37}$$

In particular, from (16.81),

$$\Gamma_2(1) = \pi^{\frac{1}{2}} \prod_{i=1}^{2} \Gamma[1 - (i-1)/2] = \pi^{\frac{1}{2}} \Gamma[1] \cdot \Gamma[1/2] = \pi,$$

and so it follows that

$$\left. \frac{2^n \pi^{n^2/2}}{\Gamma_n(n/2)} \right|_{n=2} = \frac{4\pi^2}{\Gamma_2(1)} = 4\pi.$$

Similarly, since

$$\Gamma_3(3/2) = \pi^{3/2} \prod_{i=1}^{3} \Gamma[3/2 - (i-1)/2] = \pi^{3/2} \Gamma[3/2] \cdot \Gamma[1] \cdot \Gamma[1/2] = \frac{\pi^{5/2}}{2},$$

it follows that

$$\left. \frac{2^n \pi^{n^2/2}}{\Gamma_n(n/2)} \right|_{n=3} = \frac{8\pi^{9/2}}{\Gamma_3(3/2)} = 16\pi^2.$$

This makes sense since these numbers are twice the volumes calculated in Chapter 10 for $SO(2)$ and $SO(3)$, respectively. This is as it should be given that for every rotation in $SO(n)$, there is the corresponding rotation and a reflection in $O(n)$, making it twice the volume.

Similarly, the normalized integration measure for the Stiefel manifold $V_{m,n}$ is

$$dV \doteq \frac{\Gamma_m(n/2)}{2^m \pi^{mn/2}} \, |\omega_{m,n}| \implies \int_{V_{m,n}} dV = 1. \tag{16.38}$$

A few examples help illustrate that this makes sense. First, when $m = n$, $V_{n,n} = O(n)$ and this reduces to the normalization factor for $O(n)$, as it should. Second, consider the case $V_{1,d} = S^{d-1}$. Observe from (16.81) that $\Gamma_1(d/2) = \Gamma(d/2)$ gives

$$\left.\frac{2^m \pi^{mn/2}}{\Gamma_m(n/2)}\right|_{(m,n)=(1,d)} = \frac{2\pi^{d/2}}{\Gamma_1(d/2)} = \frac{2\pi^{d/2}}{\Gamma(d/2)},$$

which is the same as $\mathrm{Vol}(S^{d-1})$ given in (2.35). As a final example, consider $V_{2,3}$, which consists of the 3×2 matrix with two orthonormal column vectors. These can be parameterized by Euler angles, and in fact we can write any element as $V = [\mathbf{o}_1, \mathbf{o}_2] = [R(\alpha,\beta,\gamma)\mathbf{e}_1, R(\alpha,\beta,\gamma)\mathbf{e}_2]$, where $R \in SO(3)$. Then (16.35) becomes

$$\begin{aligned}\omega_{2,3} &= \bigwedge_{i=1}^{2} \mathbf{o}_3^T d\mathbf{o}_i \bigwedge_{1\le i<j\le 2} \mathbf{o}_j^T d\mathbf{o}_i \\ &= (\mathbf{o}_3^T d\mathbf{o}_1) \wedge (\mathbf{o}_3^T d\mathbf{o}_2) \wedge (\mathbf{o}_2^T d\mathbf{o}_1) \\ &= (\mathbf{e}_3^T R^T dR\,\mathbf{e}_1) \wedge (\mathbf{e}_3^T R^T dR\,\mathbf{e}_2) \wedge (\mathbf{e}_2^T R^T dR\,\mathbf{e}_1).\end{aligned}$$

Then substituting

$$dR = \frac{\partial R}{\partial \alpha} d\alpha + \frac{\partial R}{\partial \beta} d\beta + \frac{\partial R}{\partial \gamma} d\gamma$$

and performing some laborious computations gives

$$\omega_{2,3} = \sin\beta \, d\alpha \wedge d\beta \wedge d\gamma.$$

Since this is exactly the same integration measure as for $SO(3)$ with exactly the same range of angles, it follows that its integral should give the volume of $SO(3)$, which is $8\pi^2$. On the other hand, from (16.36), the volume of $V_{2,3}$ should be

$$\left.\frac{2^m \pi^{mn/2}}{\Gamma_m(n/2)}\right|_{(m,n)=(2,3)} = \frac{4\pi^3}{\Gamma_2(3/2)} = 8\pi^2.$$

16.6 The Wishart Distribution: A Probabilistic View and Geometric Derivation

The Wishart distribution [107, 108] is a pdf on the space of symmetric positive-definite matrices. It arises in answer to the question of how sample covariance matrices are distributed when the covariance matrices describe vector samples that are drawn from a multivariate Gaussian distribution with zero mean. Two related distributions are the inverse Wishart distribution [2], which describes how the set of inverse covariance matrices are distributed, and the noncentral Wishart distribution [4, 53], which describes the case when samples are drawn from a Gaussian with nonzero mean.

16.6.1 Relationship to Gaussian Likelihood Computations

Suppose that $\mathbf{x}_i \in \mathbb{R}^n$ for $i = 1, \ldots, m$. Given the pdf $\rho(\mathbf{x}_i; \boldsymbol{\mu}_i, \Sigma_i)$, the composite vector $\mathbf{x} = [\mathbf{x}_1^T, \mathbf{x}_2^T, \ldots, \mathbf{x}_m^T]^T \in \mathbb{R}^{n\cdot m}$ will have a density $\rho(\mathbf{x}; \bigoplus_{i=1}^{m} \boldsymbol{\mu}_i, \bigoplus_{i=1}^{m} \Sigma_i)$, where

$$\overset{m}{\underset{i=1}{\oplus}} \boldsymbol{\mu} \doteq [\boldsymbol{\mu}_1^T, \boldsymbol{\mu}_2^T, \ldots, \boldsymbol{\mu}_m^T]^T \quad \text{and} \quad \overset{m}{\underset{i=1}{\oplus}} \Sigma_i \doteq \sum_{i=1}^{m} \bigoplus \Sigma_i.$$

The matrix variable $X = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_m] \in \mathbb{R}^{n \times m}$ is completely equivalent to $\mathbf{x}$ through the $\vee$ operation—$X^\vee = \mathbf{x}$—and the integration measure $dX = d\mathbf{x}_1\, d\mathbf{x}_2 \cdots d\mathbf{x}_m$, where each $d\mathbf{x}_i$ is the Lebesgue measure for a copy of $\mathbb{R}^n$ containing $\mathbf{x}_i$. Below, the case when $\Sigma_1 = \Sigma_2 = \cdots = \Sigma_m = \Sigma$ is considered.

In terms of X, we can write

$$\begin{aligned} \rho\left(\mathbf{x}; \overset{m}{\underset{i=1}{\oplus}} \boldsymbol{\mu}_i, \overset{m}{\underset{i=1}{\oplus}} \Sigma\right) &= \prod_{i=1}^{m} \rho(\mathbf{x}_i; \boldsymbol{\mu}_i, \Sigma) \\ &= \frac{1}{(2\pi)^{mn/2} |\Sigma|^{\frac{m}{2}}} e^{-\frac{1}{2}\mathrm{tr}\left\{\Sigma^{-1}\left[\sum_{i=1}^{m}(\mathbf{x}_i - \boldsymbol{\mu}_i)(\mathbf{x}_i - \boldsymbol{\mu}_i)^T\right]\right\}} \\ &= \frac{1}{(2\pi)^{mn/2} |\Sigma|^{\frac{m}{2}}} e^{-\frac{1}{2}\mathrm{tr}\left\{\Sigma^{-1}(X-M)(X-M)^T\right\}} \qquad (16.39) \\ &\doteq f'(X; M, \Sigma, m), \qquad (16.40) \end{aligned}$$

where $M \doteq [\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \ldots, \boldsymbol{\mu}_m]$. For fixed M, Σ, and m, the function $f'(X; M, \Sigma, m)$ is a pdf on $\mathbb{R}^{n \times m}$ with respect to Lebesgue measure $d'X$; that is,

$$\int_{\mathbb{R}^{n \times m}} f'(X; M, \Sigma, m)\, d'X = \int_{\mathbb{R}^{n \times m}} f'(X - M; \mathbb{O}, \Sigma, m)\, d'X = 1.$$

Define a mapping $\Phi_1 : \mathbb{R}^{n \times m} \to \mathbb{R}^{n \times n}$ as

$$S = \Phi_1(X) \doteq (X - M)(X - M)^T. \qquad (16.41)$$

How will S be distributed? Half of this question is answered by the form of (16.39), since we must have a distribution for S of the form $\rho'(S; \Sigma, m) \doteq f'(X - M; \mathbb{O}, \Sigma, m)$ that looks like

$$\rho'(S; \Sigma, m) = \frac{1}{(2\pi)^{mn/2} |\Sigma|^{\frac{m}{2}}} e^{-\frac{1}{2}\mathrm{tr}\left\{\Sigma^{-1} S\right\}}. \qquad (16.42)$$

However, this is a pdf relative to the measure $d'X$. The other half of the problem boils down to finding an appropriate measure of the form $w(S)\, d'S$, where $w(S)$ is a weighting function that can be computed from the mapping $\Phi_1(X)$ using differential geometric methods.

Eaton [29] computes

$$\int_{\mathbb{S}_n^+} |S|^{(m-n-1)/2} \exp\left[-\frac{1}{2}\mathrm{tr}S\right] d'S = 2^{mn/2} \cdot \Gamma_n(m/2),$$

indicating that when $\Sigma = \mathbb{I}_n$,

$$w(S) = \frac{|S|^{(m-n-1)/2}}{\Gamma_n(m/2)}$$

will suffice.

More generally, from (16.33) with $a = m/2$,

$$\int_{\mathbb{S}_n^+} |S|^{(m-n-1)/2} \exp\left[-\frac{1}{2}\mathrm{tr}(\Sigma^{-1} S)\right] d'S = 2^{mn/2} \cdot \Gamma_n(m/2) \cdot |\Sigma|^{m/2}.$$

Thus,

$$\int_{\mathbb{S}_n^+} \rho'(S)\, w(S)\, d'S = 1. \tag{16.43}$$

Since constants and powers of $|S|$ can be regrouped, the weighting function $w(S)$ can be absorbed into appropriate definitions of $\rho(S)$ and dS such that

$$\int_{\mathbb{S}_n^+} \rho(S)\, dS = 1.$$

There are an infinite number of ways to do this since part of $w(S)$ can be absorbed into $\rho(S)$ and the remaining part can be absorbed into dS. In the literature, two of the standard choices are described below. The first choice sets $w(s) = 1$ and keeps the integration measure as the Lebesgue measure $d'S$. The second choice uses the invariant integration measure for $\mathbb{S}_n^+$ viewed as the homogeneous space $GL(n, \mathbb{R})/O(n)$. This amounts to splitting up $w(S)$ into two parts—one that gets incorporated into ρ and the other into dS. We take the latter approach and define $dS \doteq |S|^{(n-1)/2} d'S$. The remaining part of $w(S)$ is absorbed into the definition of the pdf.

16.6.2 Description When Using Lebesgue Versus Invariant Integration Measure

From the discussion above, it becomes possible to write the following pdf on $\mathbb{S}_n^+$ with respect to the measure $d'S$:

$$\boxed{W_n'(S; \Sigma, m) = \frac{1}{2^{n \cdot m/2} |\Sigma|^{m/2} \Gamma_n(m/2)} e^{-\frac{1}{2}\operatorname{tr}\left(\Sigma^{-1} S\right)} |S|^{(m-n-1)/2}.} \tag{16.44}$$

$W_n'(S; \Sigma, m)$ is called the *Wishart distribution* (relative to measure $d'S$). Note that $W_n'(S; \Sigma, m) = \rho'(\Sigma^{-1} S) w(S)$ from the previous section.

In the same way that a Gaussian distribution can be written with mean and covariance as subscripts or as parameters after the semicolon, we can write

$$W_n'(S; \Sigma, m) = W'(S; \Sigma, m, n) = W_{\Sigma, m, n}'(S),$$

moving quantities of interest back and forth between subscripts and locations after the semicolon, depending on which is most convenient.

The significance of this distribution will be explored shortly. However, first we examine the equivalent distribution $W(S; \Sigma, m)$ with respect to the measure dS obtained from group theory. The details of the derivation are given in the following sections.

The result is that the "natural" measure on $\mathbb{S}_n^+$ is

$$\boxed{dS = |S|^{-(n+1)/2}\, d'S.} \tag{16.45}$$

This measure has the nice properties that for well-behaved functions $f : \mathbb{S}_n^+ \to \mathbb{R}$ and any $A \in GL(n, \mathbb{R})$,

$$\int_{\mathbb{S}_n^+} f(S^{-1})\, dS = \int_{\mathbb{S}_n^+} f(S)\, dS,$$

which follows from (16.28), and

$$\int_{\mathbb{S}_n^+} f(S)\, dS = \int_{\mathbb{S}_n^+} f(ASA^T)\, dS,$$

which follows from (16.29). See [29] for details and proof.

The Wishart distribution $W_n(S; \Sigma, m)$ defined relative to this measure is the one that describes exactly the same probability as that in (16.44), which means that

$$W_n(S; \Sigma, m)\, dS = W_n'(S; \Sigma, m)\, d'S,$$

or

$$\boxed{W_n(S; \Sigma, m) = \frac{1}{2^{n \cdot m/2} |\Sigma|^{m/2} \Gamma_n(m/2)} e^{-\frac{1}{2}\mathrm{tr}\left(\Sigma^{-1} S\right)} |S|^{m/2} = W_n(\Sigma^{-\frac{1}{2}} S \Sigma^{-\frac{1}{2}}; \mathbb{I}_n, m).}$$

(16.46)

In the following section the derivation of dS (or equivalently, $w(S) = |S|^{-(n+1)/2}$) is given. There are two cases—$m = n$ and $m > n$, each of which is discussed separately below.

16.7 Invariant Integration on $\mathbb{S}_n^+$

This section fills in some of the details regarding properties that were stated and used in the previous section. First, a general theorem is stated and then it is illustrated in the context of differential forms.

Theorem 16.1 *(Wishart)***.** *Let $X \in \mathbb{R}^{n \times m}$ with $m \geq n$ and let $f : \mathbb{S}_n^+ \to \mathbb{R}_{\geq 0}$. If $f(XX^T)$ is a pdf with respect to the measure $dX \doteq |XX^T|^{-m/2} d'X$ and $S = XX^T$, then $2^{-n} \cdot \mathrm{Vol}(V_{n,m}) \cdot f(S)$ is a pdf with respect to the measure $dS \doteq |S|^{-(n+1)/2} d'S$. In other words,*

$$\int_{\mathbb{R}^{n \times m}} f(XX^T)\, dX = 2^{-n} \cdot \mathrm{Vol}(V_{n,m}) \cdot \int_{\mathbb{S}_n^+} f(S)\, dS = 1, \tag{16.47}$$

or, equivalently, if $f'(S) \doteq f(S)|S|^{-m/2}$, then

$$\int_{\mathbb{R}^{n \times m}} f'(XX^T)\, d'X = 2^{-n} \cdot \mathrm{Vol}(V_{n,m}) \cdot \int_{\mathbb{S}_n^+} f'(S) |S|^{(m-n-1)/2}\, d'S = 1. \tag{16.48}$$

For the proof, see [29, pp. 220–224], combined with (16.36).

From a Lie-group perspective, the measure $dX = |XX^T|^{-m/2}\, d'X$ is invariant under actions of the direct product group $GL(n, \mathbb{R}) \times O(m)$ of the form $(A, O) \cdot X = AXO^T$, where (A, O) is a typical element of $GL(n, \mathbb{R}) \times O(m)$. That this is a valid action is verified as follows:

$$\begin{aligned} ((A_1, O_1) \circ (A_2, O_2)) \cdot X &= (A_1 A_2, O_1 O_2) \cdot X = (A_1 A_2) X (O_1 O_2)^T \\ &= A_1 (A_2 X O_2^T) O_1^T = (A_1, O_1) \cdot ((A_2, O_2) \cdot X). \end{aligned}$$

Using (16.24), the invariance of this measure is observed as

$$\begin{aligned} |(AXO)(AXO)^T|^{-m/2}\, d'(AXO) &= |AXOO^T X^T A^T|^{-m/2} |A|^m |O|^n\, d'X \\ &= |AA^T|^{-m/2} |XX^T|^{-m/2} |A|^m |O|^n\, d'X \\ &= |XX^T|^{-m/2}\, d'X. \end{aligned}$$

In the subsections that follow, the equivalence of the measures dX and $2^{-n} \cdot \mathrm{Vol}(V_{n,m}) \cdot dS$ are viewed from the perspective of differential forms, demonstrated with low-dimensional examples.

16.7.1 Jacobians for Matrix Decompositions Related to $\mathbb{S}_n^+$

A connection between multivariate analysis and the theory of integration on Lie groups and homogeneous spaces in Chapter 12 is that $SO(n)\backslash GL^+(n,\mathbb{R}) \cong \mathbb{S}_n^+ \cong GL^+(n,\mathbb{R})/SO(n)$. Thus, integration on $\mathbb{S}_n^+$ can be viewed as integration on a homogeneous space. However, it is not necessarily the case that the Haar measure for $GL^+(n,\mathbb{R})$ will decompose into a product of the Haar measure for $SO(n)$ and the $GL^+(n,\mathbb{R})$-invariant measure for $\mathbb{S}_n^+$. Additionally, there are many measures on $\mathbb{S}_n^+$ that are $SO(n)$ invariant. This point will be illustrated with examples in this section, together with the mechanics of computing Jacobian trasformations related to $\mathbb{S}_n^+$, such as the Cholesky and spectral (eigenvector–eigenvalue) decompositions.

As a first example, consider the two-dimensional polar decomposition. Let

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}, \quad P = \begin{pmatrix} p_{11} & p_{12} \\ p_{12} & p_{22} \end{pmatrix}, \quad S = \begin{pmatrix} s_{11} & s_{12} \\ s_{12} & s_{22} \end{pmatrix}, \quad O = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

be related as follows:

$$X = PO \quad \text{and} \quad S = P^2.$$

Here, $X \in GL^+(2,\mathbb{R})$, $O \in SO(2)$, and $P, S \in \mathbb{S}_2^+$. If X had been taken to be in $GL(2,\mathbb{R})$, then O would be taken to be in $O(2)$.

A straightforward calculation then gives

$$ds_{11} \wedge ds_{12} \wedge ds_{22} = 4\,|P|\,\mathrm{tr}(P)\,dp_{11} \wedge dp_{12} \wedge dp_{22} \implies d'S = 4\,|P|\,\mathrm{tr}(P)\,d'P$$

and

$$dx_{11}\wedge dx_{12}\wedge dx_{21}\wedge dx_{22} = \mathrm{tr}(P)\,d\theta \wedge dp_{11}\wedge dp_{12}\wedge dp_{22} \implies d'X = \mathrm{tr}(P)\,d\theta\,d'P. \quad (16.49)$$

Using the fact that $S = P^2$, and therefore $|P| = |S|^{\frac{1}{2}}$, these can be combined to give

$$d'X = \frac{1}{4|S|^{\frac{1}{2}}}\,d\theta\,d'S = \frac{4\pi}{2^2}\,|S|^{-\frac{1}{2}}\,dO\,d'S, \quad (16.50)$$

where 4π is the volume of $O(2)$ and $dO = d\theta/4\pi$ is its normalized Haar measure. The reason for writing (16.50) without canceling the factor of 4 will be explained in Section 16.7.2.

This same result could have been obtained without using differential forms by computing the product $S = PO$ and stacking the nonredundant entries in these matrices as

$$\begin{pmatrix} s_{11} \\ s_{12} \\ s_{22} \end{pmatrix} = \begin{pmatrix} p_{11}^2 + p_{12}^2 \\ p_{11}p_{12} + p_{12}p_{22} \\ p_{12}^2 + p_{22}^2 \end{pmatrix}$$

and then

$$d'S = |J|\,d'P,$$

where

$$|J| = \begin{vmatrix} \frac{\partial s_{11}}{\partial p_{11}} & \frac{\partial s_{11}}{\partial p_{12}} & \frac{\partial s_{11}}{\partial p_{22}} \\ \frac{\partial s_{12}}{\partial p_{11}} & \frac{\partial s_{12}}{\partial p_{12}} & \frac{\partial s_{12}}{\partial p_{22}} \\ \frac{\partial s_{22}}{\partial p_{11}} & \frac{\partial s_{22}}{\partial p_{12}} & \frac{\partial s_{22}}{\partial p_{22}} \end{vmatrix} = 4 \cdot \begin{vmatrix} p_{11} & p_{12} & 0 \\ p_{12} & p_{11} + p_{22} & p_{12} \\ 0 & p_{12} & p_{22} \end{vmatrix} = 4 \cdot |P| \cdot \mathrm{tr}(P).$$

It is interesting to note in passing that in the three-dimensional case when $P, S \in \mathbb{S}_3^+$, the computation is much more formidable and the result becomes $d'S = 8 \cdot |P| \cdot |\mathrm{tr}(P)\mathbb{I}_3 - P|\, d'P$

Returning to (16.49) and dividing both sides by $|X|^2 = |P|^2$ gives

$$dX = |X|^{-2}\, d'X = 4\,\mathrm{tr}(P)|P|^{-2}\, d\theta\, d'P = 4\,\mathrm{tr}(P)|P|^{-\frac{1}{2}}\, d\theta\, dP \tag{16.51}$$

since $dP = |P|^{-\frac{3}{2}}\, d'P$. Note that the factor $\mathrm{tr}(P)|P|^{-\frac{1}{2}}$ is a function of the matrix invariants of P, and hence invariant under the action of $SO(2)$ on $\mathbb{S}_2^+$ of the form $P \to OPO^T$. What (16.51) shows is that the Haar measure for $GL^+(2,\mathbb{R})$ *does not* neatly decompose into a product of the Haar measure for $SO(2) < GL^+(2,\mathbb{R})$ and the homogeneous space $\mathbb{S}_2^+ \cong GL^+(2,\mathbb{R})/SO(2)$.

However, as (16.50) illustrates, when $X = S^{\frac{1}{2}}O$, and so $X^2 = S$,

$$dX = |X|^{-2}\, d'X = \frac{4\pi}{2^2}|S|^{-\frac{3}{2}}\, dO\, d'S = \frac{4\pi}{2^2}\, dO\, dS; \tag{16.52}$$

thus, *in this parameterization* it is possible to decompose the Haar measure for $GL^+(2,\mathbb{R})$ into the product of Haar measure for $SO(2)$ and the $GL^+(2,\mathbb{R})$-invariant measure for $\mathbb{S}_2^+$. The lesson learned is that parameterizations matter. For this reason, Jacobians for some of the most important parametrizations of $\mathbb{S}_n^+$ are discussed below and are illustrated in the 2×2 case.

Jacobian for the Cholesky Decomposition

Recall from the Appendix of Volume 1 that the Cholesky decomposition of a symmetric positive-definite matrix, $S \in \mathbb{S}_n^+$, is of the form $S = T^T T$, where T is an upper triangular $n \times n$ matrix with positive entries on the diagonal.[6] For example, in the case when $n = 2$,

$$\begin{pmatrix} s_{11} & s_{12} \\ s_{12} & s_{22} \end{pmatrix} = \begin{pmatrix} t_{11} & 0 \\ t_{12} & t_{22} \end{pmatrix} \begin{pmatrix} t_{11} & t_{12} \\ 0 & t_{22} \end{pmatrix}.$$

Arranging the nonredundant entries on each side into the form of a vector gives

$$\begin{pmatrix} s_{11} \\ s_{12} \\ s_{22} \end{pmatrix} = \begin{pmatrix} t_{11}^2 \\ t_{11}t_{12} \\ t_{12}^2 + t_{22}^2 \end{pmatrix}.$$

Computing the Jacobian determinant is then straightforward and

$$d'S = ds_{11}\, ds_{12}\, ds_{22} = 4\, t_{11}^2\, t_{22}\, dt_{11}\, dt_{12}\, dt_{22} \;=\; 4\, t_{11}^2\, t_{22}\, d'T.$$

The $GL^+(2,\mathbb{R})$-invariant measure for $\mathbb{S}_2^+$ in this parameterization is then

$$dS = \frac{4t_{11}^2 t_{22}}{t_{11}^3 t_{22}^3}\, d'T = \frac{4}{t_{11}t_{22}^2}\, d'T.$$

These generalize in the n-dimensional case as [31, 47]

$$d'S = 2^n \prod_{k=1}^{n} (t_{kk})^{n+1-k}\, d'T \qquad \text{and} \qquad dS = 2^n \prod_{k=1}^{n} (t_{kk})^{-k}\, d'T. \tag{16.53}$$

[6] These upper triangular matrices form a Lie group under the operation of matrix multiplication, but this fact will not be used here.

Jacobian for the Spectral Decomposition

Recall from Volume 1 that the spectral decomposition of a symmetric positive-definite matrix $S \in \mathbb{S}_n^+$ is of the form $S = Q\Lambda Q^T$, where Q is the orthogonal matrix consisting of the normalized eigenvectors of S and Λ is the diagonal matrix with the eigenvalues of S (which are all real) ordered on the diagonal. It does not matter if this ordering is from least to greatest or vice versa.

For example, in the case when $n = 2$,

$$\begin{pmatrix} s_{11} & s_{12} \\ s_{12} & s_{22} \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Then

$$\begin{pmatrix} s_{11} \\ s_{12} \\ s_{22} \end{pmatrix} = \begin{pmatrix} \lambda_1 \cos^2\theta + \lambda_2 \sin^2\theta \\ (\lambda_1 - \lambda_2)\cos\theta \sin\theta \\ \lambda_1 \sin^2\theta + \lambda_2 \cos^2\theta \end{pmatrix}$$

and

$$d'S = |\lambda_1 - \lambda_2| \, d\lambda_1 \, d\lambda_2 \, d\theta \implies dS = \frac{|\lambda_1 - \lambda_2|}{(\lambda_1\lambda_2)^{\frac{3}{2}}} \, d\lambda_1 \, d\lambda_2 \, d\theta.$$

The absolute value sign is introduced to kill any sign dependence due to the ordering chosen for the eigenvalues along the diagonal of Λ.

The above formula generalizes to the n-dimensional case as [31, 68, 101]

$$d'S = \mathrm{Vol}(SO(n)) \cdot \prod_{i<j} |\lambda_i - \lambda_j| \, d'\Lambda \, dQ \quad \text{and}$$

$$dS = \mathrm{Vol}(SO(n)) \cdot \frac{\prod_{i<j} |\lambda_i - \lambda_j|}{\prod_{k=1}^n \lambda_k^{\frac{n+1}{2}}} \, d'\Lambda \, dQ, \tag{16.54}$$

where dQ is the normalized Haar measure for $SO(n)$ and $d'\Lambda \doteq \prod_{k=1}^n d\lambda_k = d\boldsymbol{\lambda}$.

Decompositions Similar to the Weyl Integration Formula

Using the results referenced previously, integrals over spaces of $n \times n$ symmetric real matrices $\mathbb{S}_n$ and Hermitian matrices $\mathbb{H}_n$ can be decomposed in a manner analogous to the Weyl integration formula, which was discussed in Section 12.4.3 in the context of integrals over compact Lie groups. In particular, Faraut [35] gave

$$\int_{\mathbb{S}_n} f(S) \, d'S = \frac{\pi^{n(n+1)/4}}{n! \prod_{k=1}^n \Gamma(k/2)} \int_{Q \in O(n)} \left[\int_{\boldsymbol{\lambda} \in \mathbb{R}^n} f(Q\Lambda Q^T) \prod_{i<j} |\lambda_i - \lambda_j| \, d\boldsymbol{\lambda} \right] dQ,$$

where $\int_{O(n)} dQ = 1$, and

$$\int_{\mathbb{H}_n} f(H) \, d'H = \frac{\pi^{n(n-1)/2}}{\prod_{k=1}^n k!} \cdot \int_{U(n)} \left[\int_{\mathbb{R}^n} f(V\Lambda V^*) \cdot \prod_{i<j} (\lambda_i - \lambda_j)^2 \, d\lambda \right] dV,$$

where $\int_{U(n)} dV = 1$ and

$$d'H = \prod_{i=1}^n dh_{ii} \prod_{i<j} d(\mathrm{Re}(h_{ij})) \, d(\mathrm{Im}(h_{ij})).$$

Note that although these integrals are similar to the Weyl integration formula for compact Lie groups, the spaces $\mathbb{S}_n$ and $\mathbb{H}_n$ are neither compact nor are they Lie groups. Such integrals appear in random matrix theory in the analysis of distributions of eigenvalues as n becomes large.

The following subsections address a decomposition that is of particular importance in multivariate statistical analysis.

16.7.2 The Polar Decomposition When $m = n$

Given the pdf $f(X; \Sigma, \mathbb{O}, m)$ with respect to the measure dX, we would like to obtain the pdf for S with respect to an appropriate measure dS.

Since we are starting with $S = \Phi_1(X)$ in (16.41) and a pdf in X and we seek the corresponding pdf in S, an inverse transformation of the form $X = \Psi_1(S)$ would be convenient. However, since S has $n(n+1)/2$ independent parameters and X has n^2 independent parameters, the mapping Φ_1 is necessarily many-to-one and, hence, not invertible. However, if we view Φ_1 as only half of a larger picture in which X is parameterized by S and an orthogonal matrix, A, via the polar decomposition $X = S^{\frac{1}{2}}O$, then a complementary mapping $O = \Phi_2(X) = (XX^T)^{-\frac{1}{2}}X$, where $O \in O(n)$, can be defined. Therefore, a combined mapping $\Phi = (\Phi_1, \Phi_2)$ can be defined where $\Phi : \mathbb{R}^{n\times n} \to \mathbb{S}_n^+ \times O(n)$ and $(\Phi_1, \Phi_2)(X) = ((XX^T)^{\frac{1}{2}}, (XX^T)^{-\frac{1}{2}}X)$. This is bijective, and the inverse mapping is $\Psi = (\Psi_1, \Psi_2)(S, O) = S^{\frac{1}{2}}O = X$.

Viewing $d'X$ as an n^2-form (with sign killed) and letting dO be the normalized Haar measure in (16.37) (viewed as an $n(n-1)/2$-form with sign killed) on $O(n)$, the corresponding pull-back form of the map Ψ is

$$d'X = d'(S^{\frac{1}{2}}O) = |\omega_{n,n}|\, d'(S^{\frac{1}{2}}) = \frac{\mathrm{Vol}(O(n))}{2^n}\, |S|^{-\frac{1}{2}}\, dO\, d'S. \tag{16.55}$$

The factor of $\mathrm{Vol}(O(n))$ comes from the relationship between the unnormalized volume form $\omega_{n,n}$ and the normalized dO in (16.37), and the factor of 2^n comes from the fact that S is $n \times n$ and it appears as a half-power in the polar decomposition of X.

The result in (16.55) can be written in terms of invariant forms as

$$dX = |XX^T|^{-n/2}\, d'X = \frac{\mathrm{Vol}(O(n))}{2^n}\, |S|^{-(n+1)/2}\, dO\, d'S = \frac{\mathrm{Vol}(O(n))}{2^n}\, dO\, dS. \tag{16.56}$$

Note that this generalizes (16.51).

Given any function $f : \mathbb{S}_n^+ \to \mathbb{R}$ (f need not be a pdf) measurable with respect to $|S|^{-\frac{1}{2}}\, d'S$,

$$\begin{aligned}\int_{\mathbb{R}^{n\times n}} f'(XX^T)\, d'X &= \int_{(S,A)\in\mathbb{S}_n^+\times O(n)} f'(S)\, d'(S^{\frac{1}{2}}O) \\ &= 2^{-n}\cdot \mathrm{Vol}(O(n))\cdot \int_{\mathbb{S}_n^+}\int_{O(n)} f'(S)\, |S|^{-\frac{1}{2}}\, dO\, d'S \\ &= 2^{-n}\cdot \mathrm{Vol}(O(n))\cdot \int_{\mathbb{S}_n^+} f'(S)\, |S|^{-\frac{1}{2}}\, d'S.\end{aligned}$$

In the case when $f(S) \doteq f'(S)|S|^{n/2}$ is a pdf with respect to dS, then *Wishart's theorem* can then be stated in the $m = n$ case as

$$\int_{\mathbb{R}^{n\times n}} f(XX^T)\, dX = 2^{-n}\cdot \mathrm{Vol}(O(n))\cdot \int_{\mathbb{S}_n^+} f(S)\, dS = 1. \tag{16.57}$$

16.7.3 The Polar Decomposition When $m > n$

The same sort of derivation that was used in the case when $m = n$ can be used with minor adjustments when $X \in \mathbb{R}^{n \times m}$ with $m > n$. In particular, the polar decomposition $X = (XX^T)^{\frac{1}{2}} \cdot (XX^T)^{-\frac{1}{2}} X$ (here, $\cdot$ is just matrix multiplication) can still be performed. Since $m > n$, XX^T is nonsingular and so $(XX^T)^{-\frac{1}{2}}$ is meaningful. The difference between this case and the $n = m$ case is that whereas $(XX^T)^{\frac{1}{2}} \doteq S \in \mathbb{S}_n^+$, $(XX^T)^{-\frac{1}{2}} X \doteq V^T \in \mathbb{R}^{n \times m}$ is no longer an orthogonal matrix, since it is not square. However, $V^T V = \mathbb{I}_n$, indicating that $V \in V_{n,m}$. Note that here the roles of n and m are reversed relative to how they were used in Section 16.5.4.

Counting dimensions, there are $n \cdot m$ degrees of freedom in X. There are $n(n+1)/2$ degrees of freedom in S and there are $m{\cdot}n{-}n(n{+}1)/2$ degrees of freedom in V. Therefore, the degrees of freedom in S and in V add up to those in X, and the decomposition $X = S^{\frac{1}{2}} V^T$ can be used in analogy with the way the decomposition $S^{\frac{1}{2}} A$ was used when $n = m$.

In parallel with the discussion in Section 16.7.2, viewing $d'X$ as an $(n \cdot m)$-form with sign killed,

$$d'X = d'(S^{\frac{1}{2}} V^T) = |\omega_{n,m}| \, d'(S^{\frac{1}{2}}) = 2^{-n} \mathrm{Vol}(V_{n,m}) |S|^{(m-n-1)/2} \, dV \, d'S,$$

or

$$dX = |XX^T|^{-m/2} \, d'X = 2^{-n} \mathrm{Vol}(V_{n,m}) |S|^{-(n+1)/2} \, dV d'S = 2^{-n} \mathrm{Vol}(V_{n,m}) \, dV \, dS.$$

Given any function $f' : \mathbb{S}_n^+ \to \mathbb{R}$ measurable with respect to $|S|^{(m-n-1)/2} \, d'S$, it follows that

$$\begin{aligned}
\int_{\mathbb{R}^{n \times m}} f'(XX^T) \, d'X &= \int_{(S,V) \in \mathbb{S}_n^+ \times V_{n,m}} f'(S) \, d'(S^{\frac{1}{2}} V^T) \\
&= 2^{-n} \cdot \mathrm{Vol}(V_{n,m}) \cdot \int_{\mathbb{S}_n^+} \int_{V_{n,m}} f'(S) \, |S|^{(m-n-1)/2} \, dV \, d'S \\
&= 2^{-n} \cdot \mathrm{Vol}(V_{n,m}) \cdot \int_{\mathbb{S}_n^+} f'(S) \, |S|^{(m-n-1)/2} \, d'S.
\end{aligned}$$

Here, dV is the normalized integration measure for the Stiefel manifold in (16.38) with the roles of m and n reversed.

As a sanity check, consider the case when $n = 1$ and $m = 2$ and

$$X = [x, y] = r \cdot [\cos\theta, \sin\theta] = PO.$$

Then $s = r^2$, and so $2r \, dr = ds$. Therefore

$$dx \wedge dy = r \, dr \wedge d\theta = r \frac{ds}{2r} \wedge d\theta = \frac{1}{2} ds \wedge d\theta$$

can be written with sign killed as

$$d'X \, = \, dx \, dy = \frac{1}{2} \, d\theta \, ds = \frac{4\pi}{2} \, dO \, d'S.$$

Integrating over $O(2)$ then removes $d\theta$ and replaces it with 4π, giving the measure $2\pi \, ds$.

16.8 Wishart Distributions: Applications in Multivariate Statistics

The previous section treated the Wishart distribution from the perspectives of probability and geometry. This section examines applications of the Wishart distribution in multivariate statistical analysis. In doing so, two related probability densities on $\mathbb{S}_n^+$ arise: the noncentral Wishart distribution and the inverse (or inverted) Wishart distribution.

16.8.1 The Wishart Distribution

Although the main purpose of the discussion of the Wishart distribution in the previous chapter was to illustrate how geometric and group-theoretic ideas can related to problems in probability, as a practical matter the Wishart distribution is used extensively by applied statisticians.

Given a set of samples $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_m \in \mathbb{R}^n$ with $m \geq n$, it was discussed in Section 16.2 how the sample mean and sample covariance are computed. Furthermore, if the samples are drawn from a Gaussian distribution, the expected value of the sample mean will be the mean of the Gaussian and the covariance of the sample mean will be proportional to the covariance of the Gaussian from which the samples are drawn and will be inversely proportional to the number of samples. Additionally, we also know that the sample covariance will approximate the covariance of the underlying Gaussian well when there is a large number of samples. However, what about the "covariance of the sample covariance"? In other words, what amount of dispersion or deviation should we expect around this covariance value if we perform many draws?

Actually, the answer is that $S = \sum_i (\mathbf{X}_i - \boldsymbol{\mu})(\mathbf{X}_i - \boldsymbol{\mu})^T$ is distributed according to the Wishart distribution. Unlike results pertaining to the sample mean, the distribution of the sample covariance is a parametric result; that is, it depends on the samples being drawn from a Gaussian. This should not be too surprising since the Wishart distribution originated by manipulating a Gaussian in (16.40).

It is common in the multivariate statistics literature to write $W_n'(S; \Sigma, m)$ from (16.44) in the form

$$W'(S; \Sigma, m, n) = \frac{1}{c(\Sigma, n, p)} \cdot |S|^{\frac{1}{2}(m-n-1)} \exp\left(-\frac{1}{2}\,\mathrm{tr}\Sigma^{-1}S\right), \tag{16.58}$$

where

$$c(\Sigma, m, n) = 2^{mn/2}\pi^{n(n-1)/4}|\Sigma|^{m/2}\prod_{i=1}^{n}\Gamma[(m+1-i)/2)].$$

Here, the classical Gamma function is used instead of the multivariate Gamma function using the result from (16.81).

16.8.2 The Noncentral Wishart Distribution

Given $X = [\mathbf{x}_1, \ldots, \mathbf{x}_m] \in \mathbb{R}^{n\times m}$, each column of which is a Gaussian governed by the pdf $\rho(\mathbf{x}_i; \boldsymbol{\mu}_i, \Sigma)$, the noncentral Wishart distribution characterizes the variable $Z = XX^T \in \mathbb{S}_n^+$ rather than $S = (X - M)(X - M)^T \in \mathbb{S}_n^+$, where $M = [\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \ldots, \boldsymbol{\mu}_m]$. In other words, Z describes the distribution from the origin, $\mathbb{O} \in \mathbb{R}^{n\times n}$, which is a perspective offset from the mean, or "center," M. The noncentral Wishart distribution is derived starting from the same point as the regular Wishart distribution. If we let $X = Z^{\frac{1}{2}}V$, where $V \in V_{n,m}$, then

$$\begin{aligned}\operatorname{tr}\left[\Sigma^{-1}(X-M)(X-M)^T\right] &= \operatorname{tr}\left[\Sigma^{-1}(Z^{\frac{1}{2}}V - M)(Z^{\frac{1}{2}}V - M)^T\right]\\ &= \operatorname{tr}\left[\Sigma^{-1}(Z - Z^{\frac{1}{2}}VM^T - M^TV^TZ^{\frac{1}{2}} + MM^T)\right]\\ &= \operatorname{tr}\left[\Sigma^{-1}(Z + MM^T)\right] - 2\operatorname{tr}\left[\Sigma^{-1}(Z^{\frac{1}{2}}VM^T)\right].\end{aligned}$$

Since this trace originated from inside of an exponential, it should come as no surprise that returning to that exponential and integrating out the dependence on V gives

$$\begin{aligned}&W'_{nc}(Z;\Sigma,M,m,n)\\ &\quad = c'(\Sigma,M,m,n)\exp\left\{-\frac{1}{2}\operatorname{tr}\left[\Sigma^{-1}(Z+MM^T)\right]\right\}\cdot\int_{V_{n,m}} e^{\operatorname{tr}\left[\Sigma^{-1}(Z^{\frac{1}{2}}VM^T)\right]}\,dV.\end{aligned} \tag{16.59}$$

The noncentral Wishart distribution has a long history in multivariate statistics. See, for example, James [52] and Anderson [4] (see discussion in [36] for more references). We will not be concerned with computing the constant $c'(\Sigma,M,m,n)$. However, view (16.59) as an application of integrals over groups and coset spaces. In particular, the integral over the Stiefel manifold can be viewed as one over the orthogonal group $O(m)$, using the result of Exercise 16.13 as

$$\int_{V_{n,m}} e^{\operatorname{tr}\left[\Sigma^{-1}(Z^{\frac{1}{2}}VM^T)\right]}d'V = \frac{2^n\pi^{mn/2}}{\Gamma_n(m/2)}\int_{O(m)} e^{\operatorname{tr}\left[\Sigma^{-1}(Z^{\frac{1}{2}}V(O)M^T)\right]}\,d'O,$$

where $d'V = \omega_{n,m}$ and $d'O = \omega_{m,m}$ are unnormalized measures and $V(O) = [\mathbf{o}_1,\dots,\mathbf{o}_n] \in V_{n,m}$.

16.8.3 The Inverse Wishart Distribution

If $S \in \mathbb{S}_p^+$ is distributed according to the pdf $W'_n(S;\Sigma,m)$ with respect to measure $d'S$, then $B = S^{-1}$ is distributed as [2]

$$W'^{-1}_n(B;\Psi,m) = \frac{|\Psi|^{m/2}\,e^{-\frac{1}{2}\operatorname{tr}(\Psi B^{-1})}}{2^{mn/2}\Gamma_n(m/2)|B|^{(m+n+1)/2}} \tag{16.60}$$

with respect to measure $d'B$, where $\Psi = \Sigma^{-1}$ is called the *precision matrix*. If Σ is thought of in terms of how spread out a distribution is, then Ψ describes how concentrated a distribution is. The so-called inverse Wishart distribution $W'^{-1}_n(\cdot)$ in (16.60) is obtained from $W'_n(\cdot)$ and the Jacobian for the mapping $inv : \mathbb{S}_n^+ \to \mathbb{S}_n^+$ defined by $inv(S) = S^{-1}$.

When written in terms of the measure dB, this becomes

$$W_n^{-1}(B;\Psi,m) = \frac{|\Psi|^{m/2}\,e^{-\frac{1}{2}\operatorname{tr}(\Psi B^{-1})}}{2^{mn/2}\Gamma_n(m/2)|B|^{m/2}}. \tag{16.61}$$

This can be useful because in some applications, it is the inverse of the covariance matrix that arises rather than the covariance matrix itself. For example, in the analysis of biomolecular stiffness matrices in Chapter 14, the stiffness matrices were the inverse of the covariance matrices.

16.9 Non-Gaussian Multivariate Statistics

Although the emphasis of this chapter has been on multivariate Gaussian statistics, obviously not all multivariate problems fall within this framework. As an example of a non-Gaussian multivariate distribution's the generalized Student t-distribution is discussed briefly here. See [47, 63] for more details.

Given any function $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$, a pdf on $\mathbb{R}^p$ can be defined as $\rho_f(\mathbf{x}; \mathbf{0}, \mathbb{I}) \doteq f(\mathbf{x}^T\mathbf{x}) / \int_{\mathbb{R}^p} f(\mathbf{x}^T\mathbf{x})\, d\mathbf{x}$, where the normalization ensures that $\int_{\mathbb{R}^p} \rho_f(\mathbf{x})\, d\mathbf{x} = 1$. The normalization can be incorporated into the definition of $f(\cdot)$, and so without loss of generality, it can be assumed that $\int_{\mathbb{R}^p} f(\mathbf{x}^T\mathbf{x})\, d\mathbf{x} = 1$.

The distribution $\rho_f(\mathbf{x}; \mathbf{0}, \mathbb{I})$ will be spherically symmetric about the origin. The application of an affine transformation together with appropriate scaling will give rise to a new pdf of the form

$$\rho_f(\mathbf{x}; \mathbf{m}, C) \doteq |C|^{-\frac{1}{2}} f((\mathbf{x} - \mathbf{m})^T C^{-1} (\mathbf{x} - \mathbf{m})). \tag{16.62}$$

The contours of equal probability density will be hyper-ellipsoids. As a concrete example, if $f(y) = (2\pi)^{-n/2} e^{-y/2}$, then $\rho_f(\mathbf{x}; \boldsymbol{\mu}, \Sigma)$ will be the usual multivariate Gaussian distribution, $\rho(\mathbf{x}; \boldsymbol{\mu}, \Sigma)$. However, for other choices of $f(\cdot)$, Σ need not be equal to C and $\rho_f(\cdot)$ need not be Gaussian.

As another example, when

$$f_{m,n}(y) = t(y; m, n) \doteq \frac{\Gamma((m+n)/2)}{(\pi m)^{n/2} \Gamma(m/2)} \left(1 + \frac{y}{m}\right)^{-(m+n)/2},$$

then

$$t(\mathbf{x}; \boldsymbol{\mu}, \Sigma, m, n) \doteq t((\mathbf{x} - \boldsymbol{\mu})^T C^{-1} (\mathbf{x} - \boldsymbol{\mu}); m, n) \tag{16.63}$$

is called the *multivariate Student's t-distribution* with m degrees of freedom on $\mathbb{R}^n$.

Given $\mathbf{x} \in \mathbb{R}^n$ and the parameters $\boldsymbol{\mu} \in \mathbb{R}^n$, $R \in \mathbb{S}_+^n$, and $k \in \mathbb{Z}_{>0}$ (called the degree of freedom), the multivariate t-distribution is defined as

$$t(\mathbf{x}; \mu, R, k) \doteq \frac{\Gamma((k+n)/2)}{(\pi k)^{n/2} \Gamma(k/2) |R|^{\frac{1}{2}}} \left[1 + \frac{1}{k} (\mathbf{x} - \boldsymbol{\mu})^T R^{-1} (\mathbf{x} - \boldsymbol{\mu})\right]^{-(k+n)/2}. \tag{16.64}$$

Here, the *correlation matrix*, $R = [r_{ij}]$, is related to the covariance matrix, $\Sigma = [\sigma_{ij}]$, by the definition[7]

$$r_{ij} = \frac{\sigma_{ij}}{(\sigma_{ii}\sigma_{jj})^{\frac{1}{2}}}. \tag{16.65}$$

Given N such variables $\mathbf{x}_i \in \mathbb{R}^n$ for $i = 1, \ldots, N$ that are each independently distributed, the resulting joint pdf on the matrix $X = [\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_N] \in \mathbb{R}^{n \times N}$ will be distributed as $T(X; \mu, R, k) \doteq \prod_{i=1}^{N} t(\mathbf{x}_i; \mu, R, k)$. A distribution related to (but not identical with) this is the *multivariate t model* [54]

[7] Often in the literature the notation $\mathrm{Corr}(X_i, X_j)$ is used for the matrix entries R_{ij} and $\mathrm{Cov}(X_i, X_j)$ is used for σ_{ij}, where X_i is the random variable corresponding to the coordinate x_i. The difficulty with using that notation here is that it would become confusing when discussing statistics on Lie groups where X_i is standard terminology

$$
\begin{aligned}
&T'(X;\mu,R,k)\\
&\quad\doteq \frac{\Gamma((k+n)/2)}{(\pi^N k)^{n/2}\Gamma(k/2)|R|^{\frac{N}{2}}}\left[1+\frac{1}{k}\sum_{i=1}^{N}(\mathbf{x}_i-\boldsymbol{\mu})^T R^{-1}(\mathbf{x}_i-\boldsymbol{\mu})\right]^{-(k+n\cdot N)/2}\\
&\quad= \frac{\Gamma((k+n)/2)}{(\pi^N k)^{n/2}\Gamma(k/2)|R|^{\frac{N}{2}}}\left[1+\frac{1}{k}\operatorname{tr}\left(R^{-1}\sum_{i=1}^{N}(\mathbf{x}_i-\boldsymbol{\mu})(\mathbf{x}_i-\boldsymbol{\mu})^T\right)\right]^{-(k+n\cdot N)/2}\\
&\quad= \frac{\Gamma((k+n)/2)}{(\pi^N k)^{n/2}\Gamma(k/2)|R|^{\frac{N}{2}}}\left[1+\frac{1}{k}\operatorname{tr}\big(R^{-1}(X-M)(X-M)^T\big)\right]^{-(k+n\cdot N)/2},
\end{aligned}
$$

where $M=[\boldsymbol{\mu},\boldsymbol{\mu},\dots,\boldsymbol{\mu}]$.

This model can be written as a continuous Gaussian mixture model as [55]

$$
\begin{aligned}
&T'(X;\mu,R,k)\\
&\quad=(2\pi)^{-nN/2}\int_0^\infty |\tau^2R|^{-N/2}\exp\left[-\frac{1}{2}\operatorname{tr}\big((\tau^2R)^{-1}(X-M)(X-M)^T\big)\right]h(\tau)\,d\tau,
\end{aligned}
$$

where

$$
h(\tau)=\frac{2\tau^{-(1+k)}}{(2/k)^{k/2}\Gamma(k/2)}\exp(-k/2\tau^2)
$$

is the so-called inverted Gamma distribution.

Corresponding to this distribution of X is a distribution of $S=(X-M)(X-M)^T\in\mathbb{S}_+^n$, which serves as an analog of the Wishart distribution. This distribution has the form [63]

$$
M'(S;R,k)=\frac{\Gamma((k+n)/2)}{k^{n/2}\Gamma(k/2)\Gamma_n(N/2)}\frac{[k+\operatorname{tr}(R^{-1}S)]^{-(k+n(N-1))/2}}{|R|^{(N-1)/2}|S|^{(N-n-2)/2}}.
$$

It follows from the representation of $T'(X;\mu,R,k)$ as a Gaussian mixture model that the above distribution of S will be a mixture of Wishart distributions.

From this example it should be clear that all of the geometry that went into defining integration measures on Stiefel manifolds, $\mathbb{S}_+^n$, and $GL(n,\mathbb{R})$ are useful regardless of whether the statistical problem is Gaussian or not. Additionally, knowledge of Gaussians and Wishart distributions can be used as a starting point for discussions of a wide variety of other multivariate distributions.

16.10 Random Facts About Random Matrices

A rich theory has developed over the past century that makes connections between invariant integration on the unitary group $U(n)$, the distribution of eigenvalues of random $n\times n$ Hermitian matrices, and the classical Gaussian distribution. In this section some of these relationships are summarized, and pointers to the literature are provided. Recent books on random matrix theory and applications include [1, 7, 8, 97].

Three very different kinds of problems associated with random matrices are reviewed here: (1) defining matrices by filling their entries with random samples drawn from a specified distribution (such as a univariate Gaussian on the real line or bi-variate Gaussian on the complex plane) and examining the asymptotic behavior of these matrices as their dimensions become infinite; (2) considering whole matrices as samples drawn from pdfs on spaces of matrices (e.g, random symmetric matrices drawn from a Wishart distribution, or unitary matrices drawn from the Haar measure for a compact matrix Lie group); and (3) the behavior of products of random matrices, and the relationship between such problems and random walks and convolutions on groups. Although this list is not complete and does not address the physical significance of these problems, sufficient pointers to the literature are given in order that the reader will be able to begin navigating this immense literature. The three subsections that follow flesh out each of the three broad areas listed above.

16.10.1 Random Matrices Defined at the Component Level

In this subsection random matrices are defined by filling real matrix entries by sampling randomly from a fixed univariate distribution, and the resulting properties of such matrices are discussed. The complex case follows in a similar way, with entries drawn at random from an isotropic bivariate distribution centered at the origin in the complex plane. A topic *not* discussed here is that of random matrices with correlations between adjacent entries, as can be the case when noisy image data is obtained from experimental techniques such as electron microscopy [74].

Simple Limiting Behaviors as Dimensions Become Infinite

To begin, let $M_n = [m_{kl}]$ denote an $n \times n$ matrix with real entries and let $\mathcal{M}(N) \doteq \{M_n^{(1)}, M_n^{(2)}, \ldots, M_n^{(N)}\}$ denote a set of such matrices. Can anything special be said about the structure of M_n if each m_{kl} is defined by independently sampling each of these entries from a univariate Gaussian distribution with zero mean and unit variance? Can anything special be said about the ensemble behavior of the collection $\mathcal{M}(N)$?

Let us address this second question first. Let $F : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$ be some matrix function, and for fixed n and N, define

$$\langle F(M_n)\rangle_{\mathcal{M}(N)} \doteq \frac{1}{N}\sum_{k=1}^{N} F(M_n^{(k)}). \qquad (16.66)$$

Clearly, in the case when $F_1(M_n) = M_n$ and $F_2(M_n) = (M_n)^2$, (16.66) becomes

$$\lim_{N\to\infty} \langle M_n\rangle_{\mathcal{M}(N)} = \mathbb{O}_n \quad \text{and} \quad \lim_{N\to\infty} \langle (M_n)^2\rangle_{\mathcal{M}(N)} = \mathbb{I}_n, \qquad (16.67)$$

respectively.

The first limit follows from the fact that each entry has zero mean, and the second follows from the independence of the entries (which is why nondiagonal entries go to 0) and the unit variance of the distribution from which entries are drawn (which gives values of unity on the diagonal). Note that the equalities in (16.67) do not depend on the entries being Gaussian, but only on the fact that they are zero mean, unit variance, and independent and identically distributed (iid).

Two other limiting behaviors can also be reasoned quite easily:

$$\lim_{N\to\infty} \left\langle \frac{1}{n} M_n M_n^T \right\rangle_{\mathcal{M}(N)} = \mathbb{I}_n \quad \text{and} \quad \lim_{n\to\infty} \frac{1}{n} M_n M_n^T = \mathbb{I}_n. \qquad (16.68)$$

The first of these is a statement about averages taken over an infinite ensemble consisting of matrices with fixed finite dimension n, and the second is a statement about the behavior of individual matrices with iid entries drawn from a univariate zero-meanunit-variance distribution in the case when the dimensions of the matrix become infinite. In particular, the second equality says that $\frac{1}{\sqrt{n}}M_n$ becomes *orthogonal* as $n \to \infty$.

If instead of sampling from a univariate distribution, the entries m_{kl} are defined to be complex numbers drawn from a bivariate distribution of the form $F(x,y) = f(x)f(y)$ on the complex $x - y$ plane with $\mu_f = 0$ and $\sigma_f^2 = 1/2$, then statements analogous to (16.67) and (16.68) can be made with the transpose being replaced by the Hermitian conjugate and orthogonality being replaced by unitarity.

Wigner's Semi-circle Law

In the above discussion, no structure was given to the matrices other than the way that individual entries were sampled at random. One simple way to add additional structure is the following. Construct a large Hermitian matrix W_n with entries $w_{kl} = x_{kl} + iy_{kl}$ with $k \leq l$, where x_{kl} and y_{kl} are drawn independently and at random from a univariate distribution with zero mean and variance σ^2. Then fill in the remaining values as $w_{lk} = \overline{w_{kl}}$. Alternatively, one could start with a complex random matrix M_n with no structure such as those discussed above and define $W_n = \frac{1}{2}(M_n + M_n^*)$.

How will the eigenvalues of the matrix $\frac{1}{n}W_n$ be distributed as $n \to \infty$? This is a problem proposed by Wigner. In the real case ($y_{kl} = 0$), the resulting distribution of eigenvalues is of the form

$$\boxed{p(\lambda) = f_W(\lambda; 2\sigma), \quad \text{where } f_W(x; R) \doteq \frac{2}{\pi R^2}\sqrt{R^2 - x^2}.} \tag{16.69}$$

The distribution $f_W(x; R)$ is called *Wigner's semi-circle distribution*, which is a pdf in the variable x for any $x \in [-R, R]$. The fact that $p(\lambda)$ in (16.69) follows Wigner's semi-circle distribution is called *Wigner's semi-circle law*. This law is considered by many to be the starting point of the field of random matrices. Such matrices have applications in physics and in the theory of communications. Classic references include the works of Wigner [101–103], Dyson [27, 28], and Mehta [67, 68] from physics and a number of mathematicians [15, 38, 66]. Connections between random matrix theory and communications/information theory include [9, 64, 95].

In the following subsection, concepts of random matrices in which whole matrices are considered as samples from a distribution of matrices are reviewed. This is a very different way to construct random matrices than the component-based approach discussed above and ties in to the discussion of multivariate statistical analysis from earlier in this chapter.

16.10.2 Random Matrices Defined by Sampling from Distributions on Lie Groups and Their Homogeneous Spaces

Previously in this section, random Hermitian and unitary matrices defined at the component level were discussed. Another kind of random Hermitian matrices would be those that are drawn at random from a complex version of the Wishart distribution. In that context, since Hermitian matrices are always unitarily diagonalizable, it makes sense to expect that relationships for the eigenvalues that result can be obtained by marginalizing over $U(n)$ the distributions from which the matrices are drawn. Other questions can be asked about the ensemble behavior and covariances of distributions of eigenvalues of unitary or orthogonal matrices drawn from pdfs on compact matrix Lie groups such as $U(n)$, $SU(n)$, or $SO(n)$. In particular, if the pdfs from which such matrices are drawn at random are class functions, then statements about eigenvalues are obtained easily from the Weyl integration formula.

Random Versus Deterministic Sampling of Orthogonal Matrices

In many practical applications such as robot motion planning or protein–protein docking, it is important to sample the rotation group. This sampling can be deterministic or random, but the desire is that the histogram of the resulting samples gets "close to" the uniform distribution as the number of samples is increased. Moreover, it is desirable for the speed of convergence to the uniform distribution to be fast so that, practically speaking, the number of samples can be smaller than would be the case otherwise. Deterministic almost-uniform sampling on $SO(n)$ [70] (and $SO(3)$ in particular [109]) have been developed recently. Generating random orthogonal matrices is discussed in [3, 49, 89, 105] and in [29, 30]. Random sampling from general compact Lie groups is discussed in [69]. Given a parametrization of a Lie group and a pdf $f(g)$, it is always possible possible to sample randomly as discussed at the beginning of this chapter. This is not restricted to the compact case.

Closed-Form Integrals over the Full Orthogonal Group

Recall that the full orthogonal group $O(n)$ can be described as two components and therefore is equivalent as a manifold to $\{-1,+1\} \times SO(n)$. Integration over $O(n)$ is therefore equivalent to integration over both components, each of which is like $SO(n)$. When n is odd, the mapping $O \to -O$ takes O from one component to the other, whereas in the even-dimensional case, multiplication by $-1 \oplus \mathbb{I}_{n-1}$ will serve. Therefore, integration over $O(n)$ can be thought of as integration over two copies of $SO(n)$.

Using the fact that integration over the $n \times n$ orthogonal matrices can be computed as [41]

$$\int_{O(n)} O_{ij} O_{lk} \, dO = \frac{1}{n} \delta_{il} \delta_{jk}, \quad \text{where} \quad \int_{O(n)} dO = 1, \tag{16.70}$$

Giri [41] lists the following:

$$\int_{O(n)} \operatorname{tr}(AOBO^T) \, dO = \frac{(\operatorname{tr} A)(\operatorname{tr} B)}{n}, \tag{16.71}$$

$$\int_{O(n)} [\operatorname{tr}(AOBO^T)]^2 \, dO = \frac{(\operatorname{tr} A^2)(\operatorname{tr} B^2)}{n(n+1)}, \tag{16.72}$$

$$\int_{O(n)} \operatorname{tr}(AO) \operatorname{tr}(BO) \, dO = \frac{\operatorname{tr}(AB^T)}{n}. \tag{16.73}$$

These integrals, as well as ones over $GL(n, \mathbb{R})$, arise in some problems in multivariate statistical hypothesis testing

Properties of Random Positive-Definite Matrices

If $S \in \mathbb{S}_n^+$, $f(S)$ is a pdf on $\mathbb{S}_n^+$ with respect to the measure dS, $S = O\Lambda O^T$, where $O \in O(n)$, and

$$\Lambda = \operatorname{diag}[\lambda_1, \lambda_2, \ldots, \lambda_n] \quad \text{and} \quad \lambda_1 > \lambda_2 > \cdots > \lambda_n > 0,$$

then the function [71]

$$\rho_f(\lambda_1, \lambda_2, \ldots, \lambda_n) \doteq \frac{\pi^{n^2/2}}{\Gamma_n(n/2)} \prod_{1 \le i < j \le n} (\lambda_i - \lambda_j) \int_{O(n)} f(O\Lambda O^T)\, dO \tag{16.74}$$

is a pdf on $(\mathbb{R}_{>0})^n$ with respect to $d\lambda_1 \wedge d\lambda_2 \wedge \cdots \wedge d\lambda_n$. Additionally, in the special case when $f(S) = W(S; m, \sigma^2 \mathbb{I}_n)$ with $m \ge n$, then

$$\rho_{W(m,\sigma^2\mathbb{I}_n)}(\lambda_1, \lambda_2, \ldots, \lambda_n) = \frac{\pi^{n^2/2}}{(2\sigma^2)^{mn/2}\Gamma_n(n/2)\Gamma_n(m/2)} \exp\left(-\frac{1}{2\sigma^2}\sum_{i=1}^n \lambda_i\right) \prod_{k=1}^n \lambda_k^{(m-n-1)/2} \prod_{1 \le i < j \le n} (\lambda_i - \lambda_j).$$

This is illustrates one of many possible connections between integration on Lie groups and random matrix theory which results from being able to perform integrals of the form

$$I = \int_{O(n)} f(O\Lambda O^T)\, dO$$

in closed form.

Closed-Form Integrals on $U(n)$

Let $\mathbb{C}$ denote the complex plane and let $z = x + iy$ denote an arbitrary complex number where $x, y \in \mathbb{R}$. Any function $\phi : \mathbb{C} \to \mathbb{C}$ can be integrated with respect to the Gaussian distribution according to the definition

$$\int_{\mathbb{C}} \phi(z)\, d\mu(z) \doteq \frac{1}{\pi} \int_{\mathbb{R}^2} \phi(x+iy)\, e^{-(x^2+y^2)} dx \wedge dy.$$

As it turns out, this same value can be obtained by integrating on $U(n)$; that is [16],

$$\int_{U(n)} \phi(\mathrm{tr}(W))\, dW = \int_{\mathbb{C}} \phi(z)\, d\mu(z), \tag{16.75}$$

where $\phi(z)$ is any polynomial in z and $\overline{z}$ of degree less than or equal to $2n$. Specifically,

$$\int_{U(n)} [\mathrm{tr}(W)]^k\, \overline{[\mathrm{tr}(W)]^l}\, dW = c_{k,n}\delta_{kl}, \quad \text{where} \quad c_{k,n} \le k!$$

for $k \le n$ and $c_{n,n} = n!$. In addition [16],

$$\int_{U(n)} \prod_{p=1}^r |\mathrm{tr}(W^p)|^{2k_p}\, dW = \prod_{p=1}^r p^{k_p} k_p!, \quad \text{where} \sum_{p=1}^r p k_p = n, \tag{16.76}$$

and the above statement will also be true if both equal signs are replaced with inequalities, <. The equality in (16.76) follows in part from the fact that [16, 26]

$$\int_{\mathbb{R}^{2r}} \prod_{p=1}^r \frac{\pi}{p} |x_p + iy_p|^{2k_p} e^{-\pi(x_p^2+y_p^2)/p}\, dx_p \wedge dy_p = \prod_{p=1}^r p^{k_p} k_p!.$$

The full proof involves the representation theory of the symmetric group and is beyond the scope of the current presentation.

16.10.3 Relationships Among Random Matrices, Random Walks, and Convolutions on Groups

Let G be a unimodular matrix group. It can be either a finite or countably infinite discrete group, a compact Lie group, or even a noncompact unimodular Lie group such as $SE(n)$, $GL(n)$, or $H(n)$. Since G is a matrix group, elements $g_i \in G$ drawn at random from some probability distribution $f(g)$ can be considered as random matrices with structure defined by the fact that they belong to a group. Unlike the discussion in Section 16.10.1 in which the matrices had no specific structure and could therefore be added, the operation of addition of two group elements usually does not make sense. However, adding or averaging IURs $U(g_i, \lambda)$ is perfectly acceptable as long as we do not expect the result to be unitary. For example, if g_i are drawn independently at random from a well-behaved pdf $f(g)$, then

$$\lim_{N\to\infty} \frac{1}{N}\sum_{k=1}^{N} U^*(g_k,\lambda) = \lim_{N\to\infty} \int_G \left(\frac{1}{N}\sum_{k=1}^{N} \delta(g_k^{-1}\circ g)\right) U(g^{-1},\lambda)\, dg \tag{16.77}$$

$$= \int_G f(g) U(g^{-1},\lambda)\, dg = \hat{f}(\lambda). \tag{16.78}$$

In the particular case when $f(g) = 1$ is uniform with respect to the normalized Haar measure of a compact Lie group, $\hat{f}(\lambda) = \mathbb{O}_{d(\lambda)}$ (a zero matrix of appropriate size $d(\lambda) > 1$) for all values of $\lambda \in \hat{G}$ except the first one, λ_0 for which $d(\lambda_0) = 1$, $U(g, \lambda_0) = 1$, and $\hat{f}(\lambda_0) = 1$.

Constructing products of group elements of the form $g_1 \circ g_2 \circ \cdots \circ g_N$ defines a discrete-time random walk on G. If many such walks are constructed, one would expect the distribution of this product to be captured by the n-fold convolution $(f * f * \cdots * f)(g)$. Even more than that, with an appropriate concept of mean and covariance, one would expect that this distribution converges to some kind of analogue of the Gaussian distribution. Indeed, this is the topic of Chapter 20.

16.11 Chapter Summary

This chapter has provided a brief introduction to multivariate statistical analysis from the point of view of the theory of Lie groups. It began with an introduction to sampling and resampling methods. In recent years, particle filtering/sequential Monte Carlo sampling has become quite popular. Unfortunately, space limitations prevent a detailed discussion of these, and excellent treatments already exist.

The space of all sample covariance matrices can be identified with the homogeneous space $\mathbb{S}_n^+ = GL^+(n,\mathbb{R})/SO(n)$, and therefore computing the probability that a sample matrix is close to the covariance of an assumed underlying Gaussian distribution is performed using integration measures derived from Lie theory. Integrals over orthogonal groups enter naturally in this field. Similarly, in the statistical analysis of the distribution of eigenvalues in a random Hermitian matrix, integrals over unitary groups are computed. Therefore, even for data in Euclidean space, geometric and Lie-theoretic ideas are applicable. In the chapters that follow, it will be shown how various applications fit within the framework of probability and statistics on group manifolds.

Although we jumped right in to multivariate statistics and bypassed discussions of univariate statistics, it can be useful to realize that the Wishart distribution can be viewed as the multi-dimensional generalization of the χ^2-distribution (pronounced chi square or chi squared where chi = "kai"), and likewise the noncentral Wishart distribution is a generalization of the noncentral χ^2-distribution. Many excellent books exist on univariate statistics. The emphasis here has been on the multivariate case because that is where geometric and Lie-theoretic issues arise.

In the limited space available to survey the extensive literature on multivariate analysis and random matrix theory it was not possible to go into depth. The presentation provided here is most similar to those in [29, 30, 71]. For other treatments dedicated to differential-geometric and group-theoretic treatments of multivariate statistics, see [10, 11, 18, 36, 45, 47, 51, 104]. For the standard references in the field, which is now almost 100 years old, see [2, 56, 77, 106]. For detailed Jacobian computations associated with transformation groups see [19, 23, 73]. Random matrix theory, which is now 50 years old, has attracted substantial recent interest. These new developments were for the most part not integrated into this presentation. The interested reader can consult [12, 44, 50]. Classic references include the works of Wigner [100–103], Dyson [27, 28], and Mehta [67, 68] from the physics community, and a number of contributions from mathematicians [15, 38, 66]. Connections between random matrix theory and communications/information theory include [9, 64, 95].

The rate of convergence to the semi-circle law as the number of samples increases has been studied extensively [5, 6, 44] as has other ensembles of random matrices [15, 24]. Random matrices have been connected to problems in information theory for many years [9], and most recently connections between random matrices and communication in wireless networks has become a topic of interest [7, 64, 95]. Investigations of distributions of eigenvalues and invariants of ensembles of random matrices include [26, 31, 39, 42, 66, 75, 76, 80, 82–88, 90–93, 110]. Various properties of products of random matrices have been studied in [20, 38, 96–99, 111] Applications of random matrices in nuclear and particle physics have been investigated [27, 28, 67, 68]. For other aspects and recent work on random matrix theory, see [12, 17, 21, 24, 32, 37, 43, 46, 50, 57–62, 79, 80, 112].

The next chapter reviews the basics of Shannon's theory of communication and makes connections between problems in communication and the theory of Lie groups, which we have already seen is related to random matrix theory. In subsequent chapters the connection between pdfs on Lie groups, sampling methods using stochastic differential equations, and information-theoretic identities will be tied together in the context of applications.

16.12 Exercises

16.1. Generate random samples for the pdf $\frac{1}{2}\sin\theta$ on the interval $[0,\pi]$ using the methods in Section 16.1: (a) the ITM method, (b) the transformation method, and (c) by sampling inside the box $[0,1]^3$ in $\mathbb{R}^3$, accepting those samples that lie inside the unit sphere, projecting them onto the unit sphere, converting to spherical coordinates, and marginalizing over ϕ.

16.2. Use the classical inverse function theorem (16.3) together with the definitions of Hodge star operator and pull-back from Chapter 6 to prove (16.4).

16.3. Fill in the details that lead to (16.39) from the preceding line; that is, given $\mathbf{x}_1,\ldots,\mathbf{x}_m$ where $\mathbf{x}_i=\sum_{j=1}^{n}x_{ji}\mathbf{e}_j$, show that

$$\sum_{i=1}^{m} \mathbf{x}_i^T A \mathbf{x}_i = \operatorname{tr}(AXX^T), \tag{16.79}$$

where $X = [x_{ij}]$.

16.4. Calculate the mean and covariance of pdfs of the form in (16.62). Does the correlation matrix defined in (16.65) depend on $f(\cdot)$?

16.5. For the case when $p = 2$ and $p = 3$, verify (16.70) and (16.71)–(16.73).

16.6. Verify (16.24) using (a) the properties of differential forms and (b) the Kronecker product and conversion of the matrix equation $Y = AXB$ to a vector equation $\mathbf{y} = (B^T \hat{\otimes} A)\mathbf{x}$.

16.7. Show that in $\mathbb{R}^n$, the volume n-form $\bigwedge_{i=1}^{n} dx_i$ is expressed in spherical coordinates

$$\begin{aligned}
x_1 &= r \sin\theta_1 \sin\theta_2 \cdots \sin\theta_{n-2} \sin\theta_{n-1}, \\
x_2 &= r \sin\theta_1 \sin\theta_2 \cdots \sin\theta_{n-2} \cos\theta_{n-1}, \\
x_3 &= r \sin\theta_1 \sin\theta_2 \cdots \cos\theta_{n-2}, \\
&\vdots \qquad \vdots \\
x_{n-2} &= r \sin\theta_1 \sin\theta_2 \cos\theta_3, \\
x_{n-1} &= r \sin\theta_1 \cos\theta_2, \\
x_n &= r \cos\theta_1
\end{aligned}$$

as [71]

$$\bigwedge_{i=1}^{n} dx_i = r^{n-1} \cdot \left(\prod_{k=1}^{n-2} \sin^{n-k-1}\theta_k \right) \cdot \left(\bigwedge_{i=1}^{n-1} d\theta_i \right) \wedge dr \tag{16.80}$$

and verify that

$$|G(r,\boldsymbol{\theta})|^{\frac{1}{2}} = r^{n-1} \sin^{n-2}\theta_1 \sin^{n-3}\theta_2 \cdots \sin\theta_{n-2} = r^{n-1} \prod_{k=1}^{n-2} \sin^{n-k-1}\theta_k.$$

16.8. Let $S \in \mathbb{S}_n^+$ and use the Cholesky decomposition $S = T^T T$. Prove (16.53) where T is an upper triangular matrix and $d'T$ is computed in the same way for T as $d'S$ is for symmetric S.

16.9. Show that the multivariate Gamma function defined in (16.32) is related to the usual one as

$$\Gamma_n(a) = \pi^{n(n-1)/4} \prod_{i=1}^{n} \Gamma[a - (i-1)/2], \quad \text{where } a - (i-1)/2 \in \mathbb{R}_{>0}. \tag{16.81}$$

Hint: Use the result of the Exercise 16.8.

16.10. Prove that the Stiefel manifold $V_{m,n}$ can be identified with a subset of the sphere of radius $\sqrt{m}$ in mn-dimensional space, $S_{\sqrt{m}}^{mn-1}$, by stacking columns and for each $V \in V_{m,n}$ to define $V^\vee \in \mathbb{R}^{n \cdot m}$.

16.11. If G is a compact Lie group, $U(g,\lambda)$ is an IUR of G, and $H = H^*$ is a constant Hermitian matrix, what will be the relationship between H and

$$M = \lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} U^*(g_k,\lambda) H U(g_k,\lambda)$$

if g_k are independent random samples drawn from the Haar measure of G?

16.12. Which of the following binary operations (if any) convert $\mathbb{S}^n_+$ into a Lie group?

$$\begin{aligned}
(\Sigma_1,\Sigma_2) &\longrightarrow \frac{1}{2}\left(\Sigma_1\Sigma_2 + \Sigma_2\Sigma_1\right), \\
(\Sigma_1,\Sigma_2) &\longrightarrow \frac{1}{4}\left(\Sigma_1^{\frac{1}{2}}\Sigma_2^{\frac{1}{2}} + \Sigma_2^{\frac{1}{2}}\Sigma_1^{\frac{1}{2}}\right)^2, \\
(\Sigma_1,\Sigma_2) &\longrightarrow \Sigma_1^{\frac{1}{2}}\Sigma_2\Sigma_1^{\frac{1}{2}}, \\
(\Sigma_1,\Sigma_2) &\longrightarrow (\Sigma_1\Sigma_2^2\Sigma_1)^{\frac{1}{2}}.
\end{aligned}$$

16.13. The Stiefel manifold $V_{m,n}$ can be viewed as the coset space $O(n)/O(n-m)$. Therefore, when using the unnormalized Haar measures for $O(n)$ and $O(n-m)$, how should $\mathrm{Vol}(V_{m,n})$ in (16.36) be related to $\mathrm{Vol}(O(n))$ and $\mathrm{Vol}(O(n-m))$?

Hint: What is the Lie-group version of Lagrange's theorem?

16.14. The Group $O(m)$ acts on $V_{m,n}$ from the right as $V \to VO$, where $O \in O(m)$ and $V \in V_{m,n}$. The resulting quotient space $V_{m,n}/O(m)$ is called the *Grassmann manifold* and is denoted as $G_{m,n-m}$. What are $\mathrm{Vol}(G_{m,n-m})$ and $\dim(G_{m,n-m})$?

References

1. Anderson, G.W., Guionnet, A., Zeitouni, O., *An Introduction to Random Matrices*, Cambridge Studies in Advanced Mathematics Vol. 118, Cambridge University Press, Cambridge, 2010.
2. Anderson, T.W., *An Introduction to Multivariate Statistical Analysis*, 3rd ed., Wiley Series in Probability and Statistics, John Wiley and Sons, New York, 2003.
3. Anderson, T.W., Olkin, I., Underhill, L.G., "Generation of random orthogonal matrices," *SIAM J. Sci. Statist. Comp.* 8, pp. 625–629, 1987.
4. Anderson, T.W., "The noncentral Wishart distribution and certain problems of multivariate statistics," *Ann. Math. Statist.*, 17, pp. 409–431, 1946.
5. Bai, Z. D., Yin, Y. Q., "Convergence to the semicircle law," *Ann. Probab.*, 16(2), pp. 863–875, 1988.
6. Bai, Z. D., "The circle law," *Ann. Probab.*, 25, pp. 494–529, 1997.
7. Bai, Z. D., Chen, Y., Liang, Y.-C., eds., *Random Matrix Theory and Its Applications: Multivariate Statistics and Wireless Communications*, World Scientific, Singapore, 2009.
8. Bai, Z., Silverstein, J.W., *Spectral Analysis of Large Dimensional Random Matrices*, 2nd ed., Springer, New York, 2009.
9. Balian, R., "Random matrices in information theory," *Il Nuovo Cimento*, 57(1), pp. 183–193, 1968.
10. Barndorff-Nielsen, O.E., Blæsild, P., Eriksen, P.S., *Decompostion and Invariance of Measures, and Statistical Transformation Models*, Lecture Notes in Statistics Vol. 58, Springer-Verlag, New York, 1989.
11. Beran, R.J., "Testing for uniformity on a compact homogeneous space," *J. Appl. Probab.*, 5, pp. 177–195, 1968.

12. Bleher, P., Its, A., eds., *Random Matrix Models and Their Applications*, Cambridge University Press, Cambridge, 2001.
13. Blower, G., *Random Matrices: High Dimensional Phenomena*, London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 2009.
14. Box, G.E.P., Muller, M.E., "A note on the generation of random normal deviates," *Ann. Math. Statist.*, 29(2), pp. 610–611 (1958).
15. Bronk, B., "Exponential ensembles for random matrices," *J. Math. Phys.*, 6, pp. 228–237, 1965.
16. Bump, D., *Lie Groups*, Springer, New York, 2004.
17. Carmeli, M., *Statistical Theory and Random Matrices*, Marcel Dekker, New York, 1983.
18. Chikuse, Y., *Statistics on Special Manifolds*, Springer, New York, 2003.
19. Chirikjian, G.S., Kyatkin, A.B., *Engineering Applications of Noncommutative Harmonic Analysis*, CRC Press, Boca Raton, FL, 2001.
20. Cohen, J.E., Newman, C.M., "The stability of large random matrices and their products," *Ann. Probab.* 12, pp. 283–310, 1984.
21. Cohen, J.E., Kesten, H., Newman, C.M., eds., *Random Matrices and Their Applications*, Contemporary Mathematics Vol. 50, American Mathematical Society, Providence, RI, 1984.
22. Davison, A.C., Hinkley, D.V., *Bootstrap Methods and their Applications*, Cambridge Series in Statistical and Probabilistic Mathematics, Cambridge University Press, Cambridge, 1997.
23. Deemer, W.L., Olkin, I., "The Jacobians of certain matrix transformations useful in multivariate analysis," *Biometrica*, 38, pp. 345–367, 1951.
24. Deift, P., Gioev, D., *Random Matrix Theory: Invariant Ensembles and Universality*, Courant Lecture Notes in Mathematics Vol. 18, American Mathematical Society, Providence, RI, 2009.
25. Devroye, L., *Non-Uniform Random Variate Generation*, Springer-Verlag, New York, 1986.
26. Diaconis, P., Shahshahani, M., "On the eigenvalues of random matrices," *J. Appl. Probab.*, 31, pp. 49–62, 1994.
27. Dyson, F., "Statistical theory of the energy levels of complex systems," *J. Math. Phys.*, 3, pp. 140–175, 1962.
28. Dyson, F., "A class of matrix ensembles," *J. Math. Phys.*, 13, p. 90, 1972.
29. Eaton, M.L., *Multivariate Statistics: A Vector Space Approach*, John Wiley and Sons, New York, 1983.
30. Eaton, M.L., *Group Invariance Applications in Statistics*, Regional Conference Series in Probability and Statistics Vol 1, Institute of Mathematical Statistics, Hayward, CA, 1989.
31. Edelman, A., *Eigenvalues and Condition Numbers of Random Matrices*, Ph.D. dissertation, MIT, Cambridge, MA, 1989. Available at www-math.mit.edu/∼edelman/thesis/thesis.ps
32. Edelman, A., Rao, N.R., "Random matrix theory," *Acta Numer.* 14, pp. 233–297 (2005).
33. Efron, B., "Bootstrap methods: Another look at the jackknife," *Ann. Statist.*, 7, pp. 1–26, 1979.
34. Efron, B., *The Jackknife, the Bootstrap, and Other Resampling Plans*, SIAM, Philadelphia, 1982.
35. Faraut, J., *Analysis on Lie Groups: An Introduction*, Cambridge Studies in Advanced Mathematics Vol. 110, Cambridge University Press, Cambridge, 2008.
36. Farrell, R.H., *Multivariate Calculation: Use of the Continuous Groups*, Springer-Verlag, New York, 1985.
37. Forrester, P.J., *Log-Gases and Random Matrices*, London Mathematical Society Monographs Vol. 34, Princeton University Press, Princeton, NJ, 2010.
38. Furstenberg, H., Kesten, H., "Products of random matrices," *Ann. Math. Statist.*, 31(2), pp. 457–469, 1960.
39. Geman, S., "A limit theorem for the norm of random matrices," *Ann. Probab.* 8, pp. 252–261, 1980.

40. Gentle, J.E., *Random Number Generation and Monte Carlo Methods*, 2nd ed., Springer, New York, 2004.
41. Giri, N.C., *Multivariate Statistical Analysis*, 2nd ed., Marcel Dekker, New York, 2004.
42. Girko, V.L., *Theory of Random Determinants*, Kluwer Academic, Dordrecht, 1990.
43. Götze, F., Tikhomirov, A. “Rate of convergence to the semi-circular law,” *Probab. Theory Related Fields*, 127, pp. 228–276, 2003.
44. Götze, F., Tikhomirov, A. N., “Rate of convergence to the semicircular law for the Gaussian unitary ensemble,” *Theory Probab. Appl.*, 47(2), pp. 323–330, 2003.
45. Graczyk, P., Letac, G., Massam, H., “The complex Wishart distribution and the symmetric group,” *Ann. Statist.*, 31(1), pp. 287–309, 2003.
46. Grenander, U., Silverstein, J.W., “Spectral analysis of networks with random topologies,” *SIAM J. Appl. Math.*, 32, pp. 499–519, 1977.
47. Gupta, A.K., Nagar, D.K., *Matrix Variate Distributions*, Chapman & Hall/CRC, Boca Raton, FL, 2000.
48. Hartigan, J.A., “Using subsample values as typical value,” *J. Am. Statist. Assoc.*, 64, pp. 1303–1317, 1969.
49. Heiberger, R. M., “Algorithm AS127. Generation of random orthogonal matrices,” *Appl. Statist.* 27, pp. 199–206 (1978).
50. Hiai, F., Petz, D., *The Semicircle Law, Free Random Variables and Entropy*, American Mathematical Society, Providence, RI, 2000.
51. Hotelling, H., “Tubes and spheres in n-space and a class if statistical problems,” *Am. J. Math.*, 61, pp. 440–460, 1939.
52. James, A.T., “Normal multivariate analysis and the orthogonal group,” *Ann. Math. Statist.*, 25, pp. 40–75, 1954.
53. James, A.T., “The noncentral Wishart distribution,” *Proc. R. Soc. London A*, 229, pp. 364–366, 1955.
54. Joarder, A.H., Ahmed, S.E., “Estimation of the characteristic roots of the scale matrix,” *Metrika*, 44, pp. 259–267 (1996).
55. Joarder, A.H., Ali, M.M., “Estimation of the scale matrix of a multivariate t-model under entropy loss,” *Metrika*, 46, pp. 21–32 (1997).
56. Johnson, R.A., Wichern, D.W., *Applied Multivariate Statistical Analysis*, Prentice-Hall, Englewood Cliffs, NJ, 1982.
57. Johansson, K., “On fluctuations of eigenvalues of random Hermitian matrices,” *Duke Math. J.*, 91, pp. 151–204, 1998.
58. Jonsson, D., “Some limit theorems for the eigenvalues of a sample covariance matrix,” *J. Multivariate Anal.*, 12, pp. 1–38, 1982.
59. Kabe, D.G., “Decomposition of Wishart distribution,” *Biometrica*, 51, p. 267, 1964.
60. Katz, N.M., Sarnak P., *Random matrices, Frobenius eigenvalues, and Monodromy*, American Mathematical Society Colloquium Publications Vol. 45. American Mathematical Society, Providence, RI, 1999.
61. Khatri, C.G., “Some results on the non-central multivariate beta distribution and moments of trace of two matrices,” *Ann. Math. Statist.*, 36(5), pp. 1511–1520, 1965.
62. Khatri, C.G., “On certain distribution problems based on positive definite quadratic functions in normal vectors,” *Ann. Math. Statist.*, 37, pp. 467–479, 1966.
63. Kotz, S., Nadarajah, S., *Multivariate t Distributions and Their Applications*, Cambridge University Press, Cambridge, 2004.
64. Mallik, R.K., “The pseudo-Wishart distribution and its application to MIMO systems,” *IEEE Trans. Inform. Theory*, 49, pp. 2761–2769, 2003.
65. Marsaglia, G., MacLaren, M.D., Bray, T.A., “A fast procedure for generating normal random variables,” *Commun. ACM*, 7(1), pp. 4–10, 1964.
66. Marčenko, V.A., Pastur, L.A., “Distributions of eigenvalues for some sets of random matrices,” *Math. USSR-Sbornik*, 1, pp. 457–483, 1967.
67. Mehta, M.L., Dyson, F., “Statistical theory of the energy levels of complex systems,” *J. Math. Phys.*, 4, pp. 713–719, 1963.

68. Mehta, M.L., *Random Matrices*, 2nd ed., Academic Press, New york, 1990.
69. Mezzadri, F., "How to generate random matrices from the classical compact groups," *Notices AMS*, 54, pp. 592–604, 2007. arXiv:math-ph/0609050v2
70. Mitchell, J.C., "Sampling rotation groups by successive orthogonal images," *SIAM J. Sci. Comput.*, 30(1), pp. 525–547, 2007.
71. Muirhead, R.J., *Aspects of Multivariate Statistical Theory*, John Wiley and Sons, New York, 1982.
72. Naiman, D., "Volumes of tubular neighborhoods of spherical polyhedra and statistical inference," *Ann. Statist.*, 18(2), pp. 685–716, 1990.
73. Olkin, I., "Note on the Jacobians of certain matrix transformations useful in multivariate analysis," *Biometrika*, 40, pp. 43–46, 1952.
74. Park, W., Midgett, C.R., Madden, D.R., Chirikjian, G.S., "A stochastic kinematic model of class averaging in single-particle electron microscopy," *Int. J. Robot. Res.*, 30(6), pp. 730–754, 2011.
75. Pastur, L.A., "Eigenvalue distribution of random matrices: some recent results," *Ann. Inst. Henri Poincaré*, 64, pp. 325–337, 1996.
76. Pastur, L.A., Shcherbina, M., "Universality of the local eigenvalue statistics for a class of unitary invariant ensembles," *J. Statist. Phys.*, 86, pp. 109–147, 1997.
77. Press, S.J., *Applied Multivariate Analysis*, 2nd ed., Dover, New York, 2005.
78. Quenouille, M., "Approximation tests of correlation in time series," *J. R. Statist. Soc. B*, 11, pp. 18–84, 1949.
79. Ratnarajah, T., Vaillancourt, R., Alvo, M., "Complex random matrices and applications," *Math. Rep. Acad. Sci. R. Soc. Canada*, 25, pp. 114–120, 2003.
80. Rosenthal, J.S., "Random rotations: characters and random-walks on SO(N)," *Ann. Probab.*, 22(1), pp. 398–423, 1994.
81. Shao, J., Tu, D., *The Jackknife and Bootstrap*, Springer Series in Statistics, Springer, New York, 1995.
82. Shcherbina, M., "On universality for orthogonal ensembles of random matrices." Available at http://arxiv.org/abs/math-ph/0701046.
83. Shen, J., "On the singular values of Gaussian random matrices," *Linear Algebra Applic.*, 326(1–3), p. 114, 2001.
84. Silverstein, J.W., "On the eigenvectors of large dimensional sample covariance matrices," *J. Multivariate Anal.*, 30, p. 116, 1989.
85. Silverstein, J.W., "Strong convergence of the empirical distribution of eigenvalues of large dimensional random matrices," *J. Multivariate Anal.*, 55, pp. 331–339, 1995.
86. Silverstein, J.W., Bai, Z.D., "On the empirical distribution of eigenvalues of a class of large dimensional random matrices," *J. Multivariate Anal.*, 54, pp. 175–192, 1995.
87. Silverstein, J.W., "The smallest eigenvalue of a large dimensional Wishart matrix," *Ann. Probab.* 13(4), pp. 1364–1368, 1985.
88. Silverstein, J.W., "Describing the behavior of eigenvectors of random matrices using sequences of measures on orthogonal groups," *SIAM J. Math. Anal.*, 12(2), pp. 274–281, 1981.
89. Stewart, G.W., "The efficient generation of random orthogonal matrices with an application to condition estimators," *SIAM J. Numer. Anal.*, 17, pp. 403–409, 1980.
90. Sugiyama, T., "On the distribution of the largest latent root of the covariance matrix," *Ann. Math. Statist.*, 38, pp. 1148–1151, 1967.
91. Sverdrup, E., "Derivation of the Wishart distribution of the second order sample moments by straightforward integration of a multiple integral," *Skand. Akturaietidskr.*, 30, pp. 151–166, 1947.
92. Tracy, C.A., Widom, H., "Correlation functions, cluster functions, and spacing distributions for random matrices," *J. Statist. Phys.*, 92, pp. 809–835, 1998.
93. Trotter, H.F., "Eigenvalue distributions of large Hermitian matrices; Wigner's semi-circle law and a theorem of Kac, Murdock, and Szegö," *Adv. Math.*, 54, pp. 67–82, 1984.
94. Tukey, J., "Bias and confidence in not quite large samples," *Ann. Math. Statist.*, 29, p. 614, 1958.

95. Tulino, A.M., Verdú, S., *Random Matrix Theory and Wireless Communications*, Now Publishers, Boston, 2004.
96. Tutubalin, V.N., "On limit theorems for a product of random matrices," *Theoret. Probab. Appl.*, 10(1), pp. 25–27, 1965.
97. Verbaarschot, J., *Topics In Random Matrix Theory*. Available at http://tonic.physics.sunysb.edu/∼verbaarschot/lecture/
98. Virtzer, A.D., "On the product of random matrices and operators," *Theoret. Probab. Appl.* 24, pp. 367–377, 1979.
99. Voiculescu, D., "Multiplication of certain non-commuting random variables," *J. Operator Theory*, 18, pp. 223–235, 1987.
100. Wigner, E.P., "Random matrices in physics," *SIAM Rev.*, 9, pp. 1–23, 1967.
101. Wigner, E., "Statistical properties of real symmetric matrices with many dimensions," *Proceedings of the 4th Canadian Mathematics Congress*, pp. 174–176, 1959.
102. Wigner, E., "Distribution laws for the roots of a random Hermitian matrix," in *Statistical Theories of Spectra: Fluctuations*, C.E. Porter, ed., Academic, New York, 1965.
103. Wigner, E., "Random matrices in physics," *SIAM Rev.*, 9, pp. 11–23, 1967.
104. Wijsman, R.A., *Invariant Measures on Groups and their Use in Statistics*, Lecture Notes-Monograph Series Vol. 14, Institute of Mathematical Statistics Hayward, CA, 1990.
105. Wijsman, R.A., "Random orthogonal transformations and their use in some classical distribution problems in multivariate analysis," *Ann. Math. Statist.*, 28, pp. 415–423, 1957.
106. Wilks, S.S., "Certain generalizations in the analysis of variance," *Biometrika*, 24, pp. 471–494, 1932.
107. Wishart, J., "The generalized product moment distribution in samples from a normal multivariate population," *Biometrika*, 20A, pp. 32–52, 1928.
108. Wishart, J., "Proof of the distribution law of the second order moment statistics," *Biometrika*, 35, pp. 55–57, 1948.
109. Yershova, A., Jain, S., LaValle, S., Mitchell, J.C., "Generating uniform incremental grids on SO(3) using the Hopf fibration," *Int. J. Robot. Res.*, 29(7), pp. 801–812, 2010.
110. Yin, Y.Q., Krishnaiah, P.R., "Limit theorem for the eigenvalues of the sample covariance matrix when the underlying distribution is isotropic," *Theoret. Probab. Appl.*, 30, pp. 861–867, 1985.
111. Yin, Y.Q., Krishnaiah, P.R., "A limit theorem for the eigenvalues of product of two random matrices," *J. Multivariate Anal.*, 13, pp. 489–507, 1983.
112. Zyczkowski, K., Kus, M., "Random unitary matrices," *J. Phys. A: Math. Gen.* 27, pp. 4235–4245, 1994.

17

Information, Communication, and Group Theory

Information theory, as it is known today, resulted from the confluence of two very different roots that had their origins in the first half of the 20th century. On the one hand, information theory originated from electrical engineers such as Hartley, Nyquist, and Shannon [49, 86, 104], who worked on the analysis of systems and strategies to communicate messages from one location to another. On the other hand, mathematicians such as de Bruijn, Cramér, Fisher, Kullbach, and Rao were inventing ideas in probability and statistics that have direct relevance to the study of information transmission. In this chapter the "communications" aspect of information theory is emphasized, whereas in Chapter 3 the "probability and statistics" side was reviewed. In recent years, the theory of finite groups has been connected with equalities in information theory. Lie groups enter as symmetry operations associated with continuous physical models of information transmission such as the linear telegraph equation and nonlinear soliton equations. Lie groups also appear as a domain in which stochastic trajectories evolve in the analysis of noise in optical communication systems that transmit information over fiber optic cables. In addition, some of the basic concepts and definitions in the theory of communication have interesting properties that are enriched by merging them with concepts from group theory. Some of this recent work will be explored here.

The important points to take away from this chapter are as follows:

- Quantitative measures of the information content in a message exist, and these measures can be used together with characteristics of the medium over which a message is to be sent to assess the rate at which the message can be sent.
- Information to be sent over a noisy channel can be coded so as to make reconstruction of the message on the receiving end possible even if parts of the message are corrupted by noise.
- Group theory (as it applies to both finite and Lie groups) can play several roles in this field, including defining new information inequalities and analyzing the characteristics of physical communication systems;

In Section 17.1 a review of the basic ideas in the mathematical theory of communication are addressed, including the definition of the information content in a message, channel capacity, and Shannon entropy. Section 17.1 also reviews alternative measures of information, including Rényi entropy, f-divergence, and Tsallis entropy. Section 17.2 provides concrete examples of channels and codes including brief reviews of Morse code, ASCII, and so forth and reviews Shannon's theorems for discrete channels. Section 17.3 examines areas of overlap between the information theory of discrete channels and the theory of finite groups. Section 17.4 provides a detailed treatment of the linear telegraph

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_8,

equation, and shows how Lie group analysis is applicable to describe the symmetries of this equation. Section 17.5 reviews work in which the the problem of transmission of information through noisy media has been modeled as random walks in the hyperbolic plane. Section 17.6 reviews how some problems in optical communications can be formulated using methods from the theory of Lie groups. Section 17.7 provides an introduction to nonlinear traveling wave problems (i.e., solitons) that arise in modes of communication ranging from smoke signals to fiber optic systems. These sections are not intended to exhaustively cover the vast literature on information theory, but rather to illustrate connections between selected topics in information theory and group theory. The chapter concludes with discussions of more connections between information theory, Lie groups, and random matrix theory, and exercises are provided.

17.1 What Is Communication?

Communication is the transmission of information from one point to another. "Information" can be thought of as a continuous or discrete pattern that is articulated at a source point.[1] The intent of communication is to reproduce this pattern at the receiver/sink. Discrete patterns include sequences of dots and dashes in Morse code, sentences in a natural language, digital images or image sequences, and the DNA sequence of a living being. Continuous patterns include AM/FM radio waves, the chirps of crickets, the vocalization of spoken human language, and the dance of a ballerina.

Examples of communication include when Alexander Graham Bell spoke into the first telephone and Thomas A. Watson heard through the receiver in the room where he was waiting "Mr Watson – Come here – I want to see you." Communication could be the transmission of dots, dashes, and spaces using Morse code and a telegraph or the transmission of a television program through the airwaves. It could be ground control sending radio signals to a space probe or one person winking at another across a smoke-filled room. Communication need not be the transmission of information from one place to another. Other examples of communication include experimental observation of physical phenomena (as mentioned in Chapter 14, Brillouin was a proponent of this view) and a robot sensing its environment. Communication also can be the transmission of information from one time to another (i.e., the process of storing a message (such as the text of this book, or a song or video on a digital storage medium)). Retrieving a stored message (such as a person reading a book 100 years after it is written) is also communication.

Continuous patterns can either be communicated directly (e.g., the image of the ballerina stimulates the retinas of viewers in a live audience) or they can be discretized (e.g., the motion of the ballerina is recorded with a digital image capture device). As such, two versions of information theory exist: continuous (also called "differential") and discrete. It should come as no surprise that Lie groups, being continuous objects, are more applicable to problems involving the transmission of information in the continuous mode. However, the distinction between discrete and continuous can be blurred. Phenomena in the macroscopic world can often be described from the continuum perspective (as reviewed in Chapter 1). However, at a more detailed level one can view the physical world as being composed of the discrete nuclei and electons of atoms with

[1] The word "data" can be used in place of "pattern," but the former has connotations of being discrete and organized in that it specifies the values of variables, whereas the latter is perhaps more general. Likewise, the words "arrangement" and "formation" could be used in place of "pattern," but they too have connotations that detract from the concept of information.

specific positions and velocities, in which case the world is viewed in a discrete way. Then in the quantum mechanical and statistical mechanical views, the world becomes continuous again, with probabilities replacing discrete locations, but these have discrete properties (the quantum states). The point is that in practice any continuous system can be discretized and any discrete system can be smoothed when viewed from the proper perspective.

Inherent in communication between humans is the goal of conveying meaning, understanding, and, in some cases, wisdom. The mathematical theory of communication is not focused on any of these things. Rather, the focus is on the reliable reproduction of data that has an origin or "source" at another point called the "sink." This is depicted in Figure 17.1, where, on a coarse scale, there is the message to be sent, the channel over which it is to be sent, and the message to be received. Complicating matters is that noise is injected in the channel. For example, lightning strikes or solar flares can add noise to telephone communications, a rain storm can affect digital satellite broadcasts, and background noise can interfere with a conversation. Noise both has the potential to corrupt messages that are sent and to slow the transfer of information.

At a finer scale, the channel, sender, and receiver can be broken down into finer elements. The actual hardware that is used to transmit and receive coded messages can be considered to be part of the "information channel" that also includes the physical channel, or medium, through which the coded message travels. One reason for grouping things this way is that hardware devices used to transmit and receive information can themselves be subject to noise. The actual coding and decoding of messages (e.g., turning music into a sequence of binary numbers and vice versa) is considered here to be a very reliable process, and so it is grouped together with the source/sink of the message.

This model is the basic one initiated by Shannon in his seminal work, first reported in 1948 and repeated in [104]. A number of important variations can be built on this basic model. For example, if the noise has known characteristics, then analytical models can be built and the message on the receiving end can be "cleaned up" as best as possible using this knowledge of the noise. This is important both in communication and sensing and is often referred to as "filtering." Norbert Wiener, whose work has been referred to throughout these two books, is credited with making major contributions to filtering theory.

Another variation on the basic model is whether the system has memory or not. Consider the sentence consisting of 22 letters and 4 spaces grouped into 5 words separated by 4 spaces, where 9 out of the 22 + 4 of the received symbols are corrupted by noise: "T - e q- - - n vacu - m - d t - - r - g." With no prior knowledge (i.e., no memory) of the English language, it would be impossible to fill in the missing blanks. However,

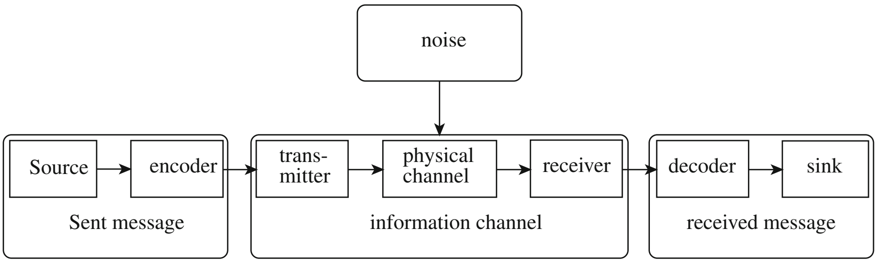


Fig. 17.1. Layout of a Generic Communications System

equipped with the knowledge that the word "the" is one of the most common words and that whenever a "q" starts a word that "u" is very likely to follow, then some of the missing information is replaced as "The qu- - n vacu - m - d the r - g." From here, searching through a dictionary for possible fits and evaluating the rules of grammar and searching for possible meanings, it should be possible to fill in the remainder as "The queen vacuumed the rug."

The following subsections address the basics of Shannon's mathematical theory of communication, including the concept of entropy for discrete and continuous channels both with and without noise and the concept of mutual information. This requires some basic knowledge of concepts from probability theory, which are also reviewed.

17.1.1 Message Probabilities

For now, consider a message to be a collection of discrete symbols/characters arranged as a linear sequence called a string. Each character is drawn from a finite alphabet. For example, in the English languages, there are 26 letters in the alphabet plus spaces between words, punctuation, and Arabic numerals. Our discussion here will illustrate the basics of information theory with the simplified case of 27 symbols: the 26 letters in the alphabet plus spaces. This is not too bad, since, in principle, the name of any numeral or punctuation mark could be expressed in longhand using these 27 symbols, or we could simply choose to ignore them.

If one were to pour over a major dictionary or encyclopedia written in the English language and count how many times each symbol appears in relation to the total number of symbols, then each symbol would have a frequency of occurrence that more or less reflects the number of times that a given symbol should appear in any message as a fraction of the total number of symbols. Let $p(A), p(B), \ldots, p(Z), p(\_)$ denote these relative frequencies of occurrence. If #(text), denotes all of the symbols in the dictionary (or other large body of text), then, for example, $p(A) = \#(A)/\#(\text{text})$, where $\#(A)$ is the number of times the letter A appears.

These are probabilities, and so, by definition, their sum must be equal to 1. Let $\mathcal{A} = \{A, B, \ldots, Z, \_\}$ be the whole alphabet (including the empty space symbol) and let a generic symbol be denoted as $\alpha \in \mathcal{A}$. In other words, α could be A, B, or any of the 27 symbols. Sometimes it is convenient to rename the symbols so that they are indexed by numbers. In this case, $\alpha_1 = A$, $\alpha_2 = B, \ldots, \alpha_{26} = Z$, $\alpha_{27} = \_$. Using these notations,

$$\sum_{\alpha \in \mathcal{A}} p(\alpha) = \frac{1}{\#(\text{text})} \sum_{\alpha \in \mathcal{A}} \#(\alpha) = 1. \tag{17.1}$$

This sum could also be written using indices as $\sum_{i=1}^{27} p(\alpha_i) = 1$. The notation in (17.1) has the benefit of being general (and therefore applicable to any alphabet), whereas the index notation has the benefit of being concrete. Note that $0 \leq p(\alpha) \leq 1$. In both cases, the symbol α is a dummy variable; it can be replaced with any other character that has no special meaning. For consistency here, other lowercase Greek characters will be used.

Suppose that we construct a two-symbol string (which need not be a real English word) by randomly sampling a symbol from the alphabet, placing it in the first place, and then randomly sampling another symbol independently of the first and placing it in the second place. There are 27 × 27 possible outcomes in this random experiment corresponding to any possible symbol in the first place, and likewise for the second place. Let E_1 be the *event* that the letter A is sampled for the first place and let E_2

be the event that the letter M appears in the second place.[2] The events E_1 and E_2 are subsets of the set of all possible outcomes with $E_1 = \{AA, AB, \ldots, AZ, A\_\}$ and $E_2 = \{AM, BM, \ldots, ZM, \_M\}$. The probability of E_1 is defined to be the sum of probabilities of all elements of E_1, and so $p(E_1) = \sum_{\alpha\in\mathcal{A}} p(A)p(\alpha) = p(A)$ and $p(E_2) = \sum_{\beta\in\mathcal{A}} p(\beta)p(M) = p(M)$. Here, (17.1) has been used.

Probabilities of Intersections and Unions of Events

In the previous example, the probability of the string AM actually occurring from this random process can then be thought of as[3]

$$p(E_1 \cap E_2) = p(E_1) \cdot p(E_2). \tag{17.2}$$

This is the probability that E_1 and E_2 both happen. Stated another way, $p(E_1 \cap E_2)$ is the probability that E_1 happens *and* E_2 happens. This assumes that if a symbol is picked for the first place, then it is still available to be picked again for the second spot. Such "sampling with replacement" has different statistical properties than sampling without replacement, such as in drawing straws, games like Bingo, or lotteries, where the selection of a symbol for use in one slot precludes its use in another. The probability $p(E_1 \cap E_2)$ in this example would be the product $p(A) \cdot p(M)$ if these symbols were chosen at random based on their frequencies in the dictionary.

The probability $p(E_1 \cup E_2)$ also can be computed. This is the probability that E_1 happens *or* E_2 happens, or both happen. In this particular example,

$$p(E_1 \cup E_2) = p(A) + p(M) - p(A) \cdot p(M).$$

The reason for this is that the two-letter word "AM" appears both in E_1 and in E_2, and to not subtract off its probability would mean that its effect would be double counted. This argument holds in very general contexts as

$$\boxed{p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2).} \tag{17.3}$$

This is the same equality as the definition of a valuation (additive measure) discussed in Chapters 1 and 15. Since each probability is a non-negative quantity, this means that

$$p(E_1 \cup E_2) \leq p(E_1) + p(E_2).$$

This inequality can be iterated so that $p(E_1 \cup E_2 \cup \cdots \cup E_n) \leq p(E_1) + p(E_2) + \cdots + p(E_n)$.

Now, consider a different scenario. Suppose that the two symbols in the string might *not* be selected independently and suppose that one of them has already been specified. This leads to the concept of a *conditional probability.* The notation for this is $p(E_1 \mid E_2)$, which is the probability that event E_1 will happen given that the event E_2 has already happened. If the events E_1 and E_2 are not independent (e.g., because placing an M in the second place severely restricts the number of possible symbols that can go in the first place to form part of a valid English word), then (17.2) no longer holds.

[2] Here, E_i has absolutely nothing to do with basis elements of Lie algebras!

[3] The notation $p(E_1 \cap E_2)$ can be thought of as the joint distribution $p(E_1, E_2)$ on the Cartesian product of the space of events with itself. Here, the use of set-theoretic notation following [65] will afford the compact expression of other statements such as $p(E_1 \cup E_2)$ that are more difficult to express otherwise.

The Role of Conditional Probabilities

Suppose that in addition to recording the frequency of occurrence of all individual symbols in a large text, all two-symbol strings in a dictionary are also recorded. Therefore, $p(E_1)$, $p(E_2)$, and $p(E_1 \cap E_2)$ would all be known. In principle, $p(E_1 \mid E_2)$ could also be calculated by running over all two-symbol sequences ending in M and computing the ratio of the number of such sequences that have an "A" in the first place, $\#(AM)$, compared to the total number, $\sum_{\alpha \in \mathcal{A}} \#(\alpha\, M)$. By rearranging terms, it becomes clear that

$$p(E_1 \mid E_2) \doteq \frac{\#(AM)}{\sum_{\alpha \in \mathcal{A}} \#(\alpha\, M)} = \frac{\#(AM)}{\#(\text{all pairs})} \cdot \frac{\#(\text{all pairs})}{\sum_{\alpha \in \mathcal{A}} \#(\alpha\, M)} = p(E_1 \cap E_2) \cdot \frac{1}{p(E_2)}.$$

which leads to

$$\boxed{p(E_1 \mid E_2) = \frac{p(E_1 \cap E_2)}{p(E_2)}.} \tag{17.4}$$

In the evaluation of $\#(\text{all pairs})$ above, if it is assumed that a window that selects two adjacent symbols at a time runs over the whole text, wrapping back around to the beginning, then this number will be equal to the total number of characters in the text. However, if it does not wrap around, then $\#(\text{all pairs})$ will be less than the total number of symbols by 1.

Equipped with this concept of conditional probability, a conditional version of (17.3) can be derived. Following [65] and respectively substituting $E_1 \cap E_3$ and $E_2 \cap E_3$ for E_1 and E_2 in (17.3) gives

$$p((E_1 \cap E_3) \cup (E_2 \cap E_3)) = p(E_1 \cap E_3) + p(E_2 \cap E_3) - p(E_1 \cap E_3 \cap E_2 \cap E_3).$$

However, in set theory, $(E_1 \cap E_3) \cup (E_2 \cap E_3) = (E_1 \cup E_2) \cap E_3$ and $E_1 \cap E_3 \cap E_1 \cap E_3 = E_1 \cap E_2 \cap E_3$. (No parentheses are needed for that last expression.) Substituting these facts in the above equation and dividing by $p(E_3)$ gives

$$\frac{p(E_1 \cup E_2 \cap E_3)}{p(E_3)} = \frac{p(E_1 \cap E_3)}{p(E_3)} + \frac{p(E_2 \cap E_3)}{p(E_3)} - \frac{p(E_1 \cap E_2 \cap E_3)}{p(E_3)}.$$

However, this is exactly

$$\boxed{p(E_1 \cup E_2 \mid E_3) = p(E_1 \mid E_3) + p(E_2 \mid E_3) - p(E_1 \cap E_2 \mid E_3).} \tag{17.5}$$

Stated in words, this says that conditioning does not affect the equality in (17.3). Depending on which conditional probabilities are available, $p(E_1 \cap E_2 \mid E_3) = p(E_1 \cap E_2 \cap E_3)/p(E_3)$ can be computed in several different ways. For example, using the definition in (17.4) twice, it follows that [65]

$$p(E_1 \mid E_2 \cup E_3) = \frac{p(E_1 \cap E_2 \cap E_3)}{p(E_2 \cap E_3)} = \frac{p(E_1 \cap E_2 \cap E_3)}{p(E_2 \mid E_3)p(E_3)},$$

which can be rewritten as

$$p(E_1 \cap E_2 \cap E_3) = p(E_1 \mid E_2 \cap E_3)p(E_2 \mid E_3)p(E_3). \tag{17.6}$$

17.1.2 Entropy, Information, and Discrete Alphabets

Let $C = \{E_1, E_2, \ldots, E_n\}$ be a finite collection of events in which $p_i \doteq p(E_i) \geq 0$ and $\sum_{i=1}^{n} p_i = 1$. The *self-information* of the event E_i is defined as

$$\mathcal{I}(E_i) \doteq -\log p(E_i). \tag{17.7}$$

If the base of the logarithm is 2, then $\mathcal{I}(E_i)$ is said to be measured in "bits," whereas if the base of the logarithm is e or 10, then $\mathcal{I}(E_i)$ is said to be measured in "nats" or "decs," respectively. This concept of information goes back to Hartley [49] and no doubt motivated the definition of measure-theoretic information in ergodic theory that was discussed in Chapter 14. $\mathcal{I}(E_i)$ reflects the fact that if a binary message is sent over m parallel wires, then specifying the binary values on each wire produces $N = 2^m$ possible outcomes at each instant in discrete time. Therefore, the probability of selecting any particular message will be $p = 1/2^m$ and so $I = -\log_2 p = m$ reflects the amount of freedom to choose a particular message from all of the possibilities.

Entropy and Conditional Entropy

The *entropy* of the collection C is defined to be the average self-information of all events[4] in C,

$$H(C) \doteq \sum_{i=1}^{n} p(E_i)\mathcal{I}(E_i) = -\sum_{i=1}^{n} p(E_i) \log p(E_i). \tag{17.8}$$

Given two systems of events $C_1 = \{E_1, \ldots, E_n\}$ and $C_2 = \{E_1', \ldots, E_m'\}$ with associated probabilities $0 \leq p(E_i) \leq 1$, $0 \leq p(E_j') \leq 1$, and $0 \leq p(E_i \cap E_j') \leq 1$ for $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, m\}$, the following constraints apply:

$$\sum_{i=1}^{n} p(E_i) = \sum_{j=1}^{m} p(E_j') = \sum_{i=1}^{n}\sum_{j=1}^{m} p(E_i \cap E_j') = 1$$

and

$$\sum_{i=1}^{n} p(E_i \cap E_j') = p(E_j') \qquad \text{and} \qquad \sum_{j=1}^{m} p(E_i \cap E_j') = p(E_i).$$

The *conditional self-information* of E_i given E_j' is defined as

$$\mathcal{I}(E_i \mid E_j') \doteq -\log p(E_i \mid E_j') = -\log \frac{p(E_i \cap E_j')}{p(E_j')}. \tag{17.9}$$

The *conditional entropy* is defined as[5]

$$H(C_1 \mid C_2) \doteq \sum_{i=1}^{n}\sum_{j=1}^{m} p(E_i \cap E_j')\mathcal{I}(E_i \mid E_j') = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(E_i \cap E_j') \log \frac{p(E_i \cap E_j')}{p(E_j')}. \tag{17.10}$$

[4] In some contexts (such as in Chapters 3 and 19), it is more convenient to define the entropy as a functional of the probability function, $S(p)$ where $p : C \to \mathbb{R}_{\geq 0}$ returns the value $p(E_i)$ for each $E_i \in C$, rather than as a function on the collection of events, $H(C)$. Thus either one of the interchangeable notations $S(p)$ and $H(C)$ can be used based on which is more convenient in a given context.

[5] In the notation of Chapter 3, this would be written in terms of probabilities as $S\left(p(E_i \cap E_j')/p(E_j')\,;\, p(E_i \cap E_j')\right)$.

If $p(E_i \cap E'_j) = 0$ for any pair (i, j), then this is omitted from the sum. Additionally, since by the constraints listed above, $p(E'_j) = 0$ implies that $p(E_i \cap E'_j) = 0$, division by 0 cannot occur in the sum.

Mutual Information

The *mutual information between two events* is defined as

$$\mathcal{I}(E_i, E'_j) \doteq \log \frac{p(E_i \cap E'_j)}{p(E_i)\, p(E'_j)}. \tag{17.11}$$

In contrast, the *mutual information between two collections of events* is defined as[6]

$$\mathcal{I}(C_1; C_2) \doteq \sum_{i=1}^{n} \sum_{j=1}^{m} p(E_i \cap E'_j)\, \mathcal{I}(E_i, E'_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} p(E_i \cap E'_j) \, \log \frac{p(E_i \cap E'_j)}{p(E_i)\, p(E'_j)}. \tag{17.12}$$

Finally, the *joint entropy* of two collections of events is defined as

$$H(C_1 \cap C_2) \doteq - \sum_{i=1}^{n} \sum_{j=1}^{m} p(E_i \cap E'_j) \, \log p(E_i \cap E'_j). \tag{17.13}$$

Note that $H(C_1 \cap C_2) = H(C_2 \cap C_1)$, $\mathcal{I}(C_1; C_2) = \mathcal{I}(C_2; C_1)$, and $\mathcal{I}(E_i, E'_j) = \mathcal{I}(E'_j, E_i)$. However, in general, $\mathcal{I}(E_i \mid E'_j) \neq \mathcal{I}(E'_j \mid E_i)$, $\mathcal{I}(C_1 \,|\, C_2) \neq \mathcal{I}(C_2 \,|\, C_1)$ and $H(C_1 \,|\, C_2) \neq H(C_2 \,|\, C_1)$.

From the above definitions and properties of the logarithm function, it follows that

$$\begin{gathered} \mathcal{I}(E_i, E'_j) = \mathcal{I}(E_i) - \mathcal{I}(E_i \mid E'_j); \quad H(C_1 \cap C_2) = H(C_1 \,|\, C_2) + H(C_2); \\ \mathcal{I}(C_1; C_2) = H(C_2) - H(C_2 \,|\, C_1); \quad \mathcal{I}(C_1; C_2) = H(C_1) + H(C_2) - H(C_1 \cap C_2). \end{gathered} \tag{17.14}$$

Since $H(C_1 \cap C_2) \geq 0$, it follows from the last of these equalities that

$$\mathcal{I}(C_1; C_2) \leq H(C_1) + H(C_2),$$

with equality holding when $C_1 \cap C_2 = \emptyset$.

Using the above definitions and inequalities, together with the fact that $\log x \leq x - 1$, it can be shown that

$$\boxed{H(C_1 \mid C_2) \leq H(C_1) \quad \text{and} \quad \mathcal{I}(C_1; C_2) \geq 0.} \tag{17.15}$$

This is important because it says that conditioning cannot increase entropy. Equality in (17.15) results only if C_1 and C_2 are independent.

Given three collections of events $C_1 = \{E_1, \ldots, E_n\}$, $C_2 = \{E'_1, \ldots, E'_m\}$, and $C_3 = \{E''_1, \ldots, E''_l\}$ with $0 \leq p(E_i \cap E'_j \cap E''_k) \leq 1$ and

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{k=1}^{l} p(E_i \cap E'_j \cap E''_k) = 1,$$

[6] The similar symbols $\mathcal{I}(\cdot\,, \cdot)$ and $\mathcal{I}(\cdot\,; \cdot)$ are used for the mutual information between individual events and systems of events, respectively. These are two very different functions, and there should be no confusion about which is being discussed since they are specified by their arguments. In the notation of Chapter 3, $\mathcal{I}(C_1; C_2)$ would be written in terms of probabilities as $I(p(E_i), p(E'_j); p(E_i \cap E'_j))$.

all of the probabilities discussed earlier can be obtained by appropriate marginalizations. Additionally, other information-theoretic definitions can be made. For example,

$$\mathcal{I}(E_i \cap E'_j, E''_k) \doteq \log \frac{p(E_i \cap E'_j \cap E''_k)}{p(E_i \cap E'_j)p(E''_k)}$$

and

$$\begin{aligned}\mathcal{I}(C_1 \cap C_2; C_3) &\doteq \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(E_i \cap E'_j \cap E''_k)\mathcal{I}(E_i \cap E'_j, E''_k)\\ &= \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(E_i \cap E'_j \cap E''_k) \log \frac{p(E_i \cap E'_j \cap E''_k)}{p(E_i \cap E'_j)p(E''_k)}.\end{aligned}$$

The *mutual information between E_i and E'_j conditioned on E''_k* is defined as

$$\mathcal{I}(E_i, E'_j \mid E''_k) \doteq \log \frac{p(E_i \cap E'_j \mid E''_k)}{p(E_i \mid E''_k)p(E'_j \mid E''_k)}$$

and *mutual information between C_1 and C_2 conditioned on C_3* is defined as

$$\begin{aligned}\mathcal{I}(C_1; C_2 \mid C_3) &\doteq \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(E_i \cap E'_j \cap E''_k)\mathcal{I}(E_i, E'_j \mid E''_k)\\ &= \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(E_i \cap E'_j \cap E''_k) \log \frac{p(E_i \cap E'_j \mid E''_k)}{p(E_i \mid E''_k)p(E'_j \mid E''_k)}.\end{aligned}$$

Note that $\mathcal{I}(C_1; C_2 \mid C_3) = \mathcal{I}(C_2; C_1 \mid C_3)$ and that

$$\mathcal{I}(C_1; C_2) = \mathcal{I}(C_1; C_3) + \mathcal{I}(C_1; C_2 \mid C_3) - \mathcal{I}(C_1; C_3 \mid C_2). \tag{17.16}$$

It can be shown that

$$\boxed{\mathcal{I}(C_1; C_2 \mid C_3) \geq 0,} \tag{17.17}$$

with equality holding only when the condition $p(E_i \cap E'_j \mid E''_k) = p(E_i \mid E''_k)p(E'_j \mid E''_k)$ is observed. If this holds for all i, j, and k for which $p(E''_k) \neq 0$, then C_1 and C_2 are referred to as being *statistical independent when conditioned on C_3*. Several inequalities are associated with the concept of statistical independence. For example, if C_1 and C_2 are statistical independent when conditioned on C_3, then

$$\mathcal{I}(C_1; C_2) \leq \min\{\mathcal{I}(C_1; C_3), \mathcal{I}(C_2; C_3)\} \quad \text{and} \quad \mathcal{I}(C_1; C_3) \geq \mathcal{I}(C_1; C_3 \mid C_2). \tag{17.18}$$

The first of these is a version of the *data processing inequality*, and the second is called the *convexity theorem* [65].

Another inequality that is sometimes called the *information processing inequality* is stated as

$$D_{KL}(p \,\|\, q) \geq D_{KL}(Q(p) \,\|\, Q(q)), \quad \text{where } Q(p)_i = \sum_j Q_{ij}\, p_j, \tag{17.19}$$

where Q_{ij} is a *stochastic matrix* (i.e., the set of numbers Q_{ij} for $i = 1, \dots, n$ forms a partition of unity for each fixed value of j).[7]

A special case of this in the context of finite groups in which $p_j = p(g_j)$, $q_j = q(g_j)$, and $Q_{ij} = f(g_i \circ g_j^{-1})$, where $f(g)$, $p(g)$, and $q(g)$ are all probability distribution functions on a finite group Γ, is

$$D_{KL}(p \,\|\, q) \geq D_{KL}(f * p \,\|\, f * q), \tag{17.20}$$

where $*$ denotes convolution of functions on Γ. Generalizations of (17.20) in the context of convolution on Lie groups are discussed in Chapter 19. In this context, Q_{ij} is doubly stochastic. If Γ is commutative, this will become a *circulant matrix*.

17.1.3 Alternative Measures of Information

Although the Boltzmann–Shannon form of entropy and associated information measures are the standard, it is worth mentioning that there are several alternative concepts that have been proposed in the literature over the past half-century. This is the topic of a recent review [77]. In the discussion that follows, definitions are given in the discrete case.

Rényi Entropy

The *Rényi entropy* is defined as [97]

$$S_R(p; s) \doteq (1-s)^{-1} \log\left(\sum_{i=1}^{n} p_i^s\right).$$

As $s \to 1$, $S_R(p; s) \to S(p)$. The case when $s = 2$ is another popular choice. The *relative Rényi entropy* of two discrete probability distributions $\{p_1, \dots, p_n\}$ and $\{q_1, \dots, q_n\}$ is defined as

$$D_R(p \,\|\, q; s) \doteq (s-1)^{-1} \log\left(\sum_{i=1}^{n} p_i^s \, q_i^{1-s}\right).$$

In the limit as $s \to 1$, $D_R(p \,\|\, q; s) \to D_{KL}(p \,\|\, q)$. The relative Rényi entropy is also related to the Kullback–Leibler divergence in that

$$\frac{\partial}{\partial s}[(s-1) D_R(p \,\|\, q; s)]\bigg|_{s=0} = -D_{KL}(q \,\|\, p)$$

and

$$\frac{\partial}{\partial s}[(s-1) D_R(p \,\|\, q; s)]\bigg|_{s=1} = D_{KL}(p \,\|\, q).$$

The *f*-Divergence

In the mid-1960s, Ali and Silvey [2] and Csiszár [23] independently introduced another way to compare probability distributions. It is commonly referred to as the *f-divergence*

[7] Conventions vary in different books. Sometimes the entries of Q are denoted as Q_i^j and sometimes instead of the $Q\mathbf{p}$ notation, the $\mathbf{p}^T Q$ notation is used, in which case the roles of rows and columns in the stochastic matrix will be reversed.

and is defined relative to any convex function, $f(x)$, as

$$D_f(p\|q) \doteq \sum_{i=1}^{n} p_i f\left(\frac{q_i}{p_i}\right).$$

Other conventions exist, but in the one chosen here, $D_f(p\|q)$ becomes $D_{KL}(p\|q)$ when $f(x) = -\log x$. Additionally, it becomes the *Hellinger distance* when $f(x) = 1 - \sqrt{x}$.

Some authors refer to $D_f(p\|q)$ as the *f-relative entropy*. It can be shown (using Jensen's inequality) that it has the same information processing property as in (17.19) and (17.20) [54].

Tsallis Entropy

A relatively new entropy measure (introduced by Tsallis in 1988) is defined as [115]

$$S_T(p; s) \doteq (s-1)^{-1}\left(1 - \sum_{i=1}^{n} p_i^s\right)$$

in the discrete case and in an analogous way in the continuous case.

Other Concepts of Divergence and Information

Other concepts of divergence exist. For example, the symmetrized (or Jeffreys) divergence [21] of two discrete probability distributions $p = \{p_1, \ldots, p_n\}$ and $q = \{q_1, \ldots, q_n\}$ is

$$D_J(p\|q) \doteq D_{KL}(p\|q) + D_{KL}(q\|p). \tag{17.21}$$

The *Jensen–Shannon divergence* is defined using the Kullback–Leibler divergence as[8]

$$D_{JS}(p\|q) \doteq \frac{1}{2}\left[D_{KL}(p\|(p+q)/2) + D_{KL}(q\|(p+q)/2)\right], \tag{17.22}$$

where $p + q = \{p_1 + q_1, \ldots, p_n + q_n\}$. Clearly, this is symmetric, and although it is not a metric (since it does not satisfy the triangle inequality), it has been proven that $\sqrt{D_{JS}(p\|q)}$ is a metric [27, 89]. The following inequalities also have been proven [21]:

$$D_{JS}(p\|q) \leq \log\left[\frac{2}{1 + \exp\left(-\frac{1}{2}D_J(p\|q)\right)}\right] \leq \frac{1}{4}D_J(p\|q). \tag{17.23}$$

Finally, *Chernoff information* is defined as

$$C(p,q) \doteq -\min_{0\leq\lambda\leq 1} \log\left(\sum_{j=1}^{n} p_j^{\lambda}\, q_j^{1-\lambda}\right),$$

and the *Bhattacharyya distance* is defined by setting $\lambda = 1/2$ rather than performing the above minimization.

[8] The fact that $D_{JS}(p\|q)$ is defined here with a factor of 1/2 and $D_J(p\|q)$ is not is for consistency with the literature, even though it makes them inconsistent with each other.

17.1.4 Applications in Imaging and Sensor Networks

Without knowing anything about information theory other than the measures presented in the previous section and the properties that result from the discussions in Chapter 3, it nevertheless is possible to discuss some applications. In particular, if $p_i(\mathbf{x})$ is the discrete probability distribution describing an image that has been normalized appropriately and if X_i is the corresponding random variable, then [125]

$$\rho(X_1, X_2, \ldots, X_m) \doteq \sum_{i=1}^{m} H(X_i | X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_m)$$

can be used as a cost function to align the images under some Lie group, G, such as the group of translations, rigid-body motions, or affine deformations. Explicitly, what is sought is $(g_1^*, g_2^*, \ldots, g_{m-1}^*) \in G \times G \times \cdots \times G$ such that

$$(g_1^*, g_2^*, \ldots, g_{m-1}^*) = \underset{(g_1, g_2, \ldots, g_{m-1})}{\arg\min} \ \rho(X_1, g_1 \cdot X_2, \ldots, g_{m-1} \cdot X_m).$$

Similar pairwise matchings can be done both for images using other information metrics [28].

Another area in which information measures are used is in distributed sensor networks. A fundamental problem in that field is how to spread out sensors in an optimal way under the constraint of limited information. Additionally, if the sensors are attached to mobile robots, how should the robots move relative to each other so as to maximize coverage without global knowledge and with limited and possibly noisy communication among local neighbors? This is an emerging area of research that naturally combines Lie theory and information gathering, as described in [96, 114]. The concept of Chernoff information discussed in the previous section was used in [29] in the context of scalable optimization of sensor networks.

17.2 Channels and Codes

In the classical discrete models of communications theory, a stream of individual *characters/symbols/letters* is organized into larger *words/messages/text*. It is assumed that the distribution of these characters in a large text is *stationary* and *ergodic*. In other words, the discrete probability, p_i, obtained by recording the frequency of occurrence of letters for any large section of text is the same as that of any other large section of text. The section of text can be taken as a sequential string or cut out as an arbitrary large rectangle from random places in the text, and the statistics should be the same. The first two columns of Table 17.1 respectively list the Roman letters (and the empty space used to break up words) and their frequency of occurrence in English text. The frequency of the empty space is approximately 1/6, meaning that, on average, words have five letters followed by one space. The third column renormalizes the frequency of occurrence of the letters only, without spaces. If $\overline{word}$ denotes the average length of a word, then $p(\_) = (\overline{word} + 1)^{-1}$. The other columns provide the representations of these characters in Morse code and in even-parity ASCII.

Morse code is a collection of dots, dashes, and empty spaces. It was used heavily by telegraph operators to transmit information over long distances by wire before the advent of the telephone. In the event that radio communication is not possible, Morse code still can be used at sea or between aircraft to communicate optically by flashing lights in

Table 17.1. Roman Letters, Their Frequency of Occurrence in English, and Representation in Morse Code and Even-Parity ASCII (with the First Bit Serving as the Parity Bit)

Symbol	p_i	p'_i	Morse Code	Binary Morse	Length (l_i)	EP ASCII
A	0.0642	0.08167	·_−_	101110	$6+3$	01000001
B	0.0127	0.01492	−_·_·_·_	1110101010	$10+3$	01000010
C	0.0218	0.02782	−_·_−_·_	111010111010	$12+3$	11000011
D	0.0317	0.04253	−_·_·_	11101010	$8+3$	01000100
E	0.1031	0.12702	·_	10	$2+3$	11000101
F	0.0208	0.02228	·_·_−_·_	1010111010	$10+3$	11000110
G	0.0152	0.02015	−_−_·_	1110111010	$10+3$	01000111
H	0.0467	0.06094	·_·_·_·_	10101010	$8+3$	01001000
I	0.0575	0.06966	·_·_	1010	$4+3$	11001001
J	0.0008	0.00153	·_−_−_−_	10111011101110	$14+3$	11001010
K	0.0049	0.00772	−_·_−_	1110101110	$10+3$	01001011
L	0.0321	0.04025	·_−_·_·_	1011101010	$10+3$	11001100
M	0.0198	0.02406	−_−_	11101110	$8+3$	01001101
N	0.0574	0.06749	−_·_	111010	$6+3$	01001110
O	0.0632	0.07507	−_−_−_	111011101110	$12+3$	11001111
P	0.0152	0.01929	·_−_−_·_	101110111010	$12+3$	01010000
Q	0.0008	0.00095	−_−_·_−_	11101110101110	$14+3$	11010001
R	0.0484	0.05987	·_−_·_	10111010	$8+3$	11010010
S	0.0514	0.06327	·_·_·_	101010	$6+3$	01010011
T	0.0796	0.09056	−_	1110	$4+3$	11010100
U	0.0228	0.02758	·_·_−_	10101110	$8+3$	01010101
V	0.0083	0.00978	·_·_·_−_	1010101110	$10+3$	01010110
W	0.0175	0.02360	·_−_−_	1011101110	$10+3$	11010111
X	0.0013	0.00150	−_·_·_−_	111010101110	$12+3$	11011000
Y	0.0164	0.01974	−_·_−_−_	11101011101110	$14+3$	01011001
Z	0.0005	0.00074	−_−_·_·_	111011101010	$12+3$	01011010
_	0.1859	N/A	___	000000	$3+3$	01011111

short and long pulses separated by pauses. Regardless of the physical implementation, a "dot" is implemented by a short pulse, followed by an empty space for the same period of time. A "dash" is implemented as a pulse with three times the duration of a dot, followed by an empty space of one time period. In Table 17.1, the code for each individual letter is given. Morse code has additional rules regarding how to put letters together into words and how to put words together into a larger message. In particular, whenever two letters are juxtaposed, a letter space consisting of an additional pause of three time units is added. In addition, the end of a word is marked by two such letter spaces (i.e., a pause of six time units). Therefore, when the Morse codes for the Roman characters and space symbol in the table are used in a message, their length increases by three units to "glue" them together into a message. The number l_i in Table 17.1 reflects this.

Something that has been added to the table is a "Binary Morse" code in which each pulse is represented as a "1" and each empty space is represented as a "0." For example, sending the message "SOS_" would be implemented as

·_·_·__−_−_−__·_·_·___

which in the binary representation can be written as

101010000111011101110000101010000000.

Based on the numbers reported in Table 17.1, the entropy of this alphabet and average length (measured in terms of the number of bits) for each symbol are respectively

$$H \doteq -\sum_{i=1}^{27} p_i \log_2 p_i = 4.03 \text{ bits/symbol} \quad \text{and} \quad L \doteq \sum_{i=1}^{27} p_i l_i = 9.296 \text{ bits/symbol.}$$

Here, H is the *source entropy* (i.e., the entropy of the set of symbols used to construct any long English message). l_i is the number of bits used to encode each symbol in a long message (including the space between each letter).

Suppose that we want to send a message down a noiseless channel and that channel can accept a rate of b bits/second. Then the rate (on average) that symbols can be transmitted in Morse code will be b/L, which is measured in symbols/second. Furthermore, if the transmitter is sending symbols according to the statistics of large messages, then we can say that it has an *entropy rate* (measured in bits per second) of[9]

$$\dot{H} \doteq H \cdot b/L\,.$$

This concept will be used later in the statement of Shannon's theorem for noisy channels. First, the noisless case is considered.

17.2.1 Shannon's Theorem for Discrete Noiseless Channels

The concept of the bit rate, b, at which that the channel allows information to flow from transmitter to receiver can be generalized. This generalized concept is called the *channel capacity* and is defined as

$$C \doteq \lim_{T\to\infty} \frac{\log_2 M(T)}{T}, \tag{17.24}$$

where $M(T)$ is the number of all possible messages of duration T that can be transmitted in the channel. So, for example, if b bits/second can be transmitted over a channel for a duration of T seconds, then any one of the 2^{bT} possible messages can be sent during that time interval and

$$C = \lim_{T\to\infty} \frac{\log_2 2^{bT}}{T} = \lim_{T\to\infty} \frac{bT}{T} = b. \tag{17.25}$$

The reason for defining the channel capacity as in (17.24) rather than simply saying that it is b is that C is a more general concept that extends to the case when the set of messages has structure (such as in the case when they are drawn from a known language which has pre-defined grammar and spelling rules) and to continuous signals as well.

Note that $H < L$ for both Morse code and ASCII. The reason for this will be revisited in Chapter 18. Shannon's theorem for discrete memoryless channels without noise generalizes this result to all possible codes and all possible alphabets and languages. This is an idealization that is useful in understanding the central role that information-theoretic entropy plays in the theory of communications. Clearly, the addition of noise to a channel, which is addressed later, will not make the rate of transmission of information increase.

[9] This is Shannon's "entropy per second" [104], not the "entropy rate of a stochastic process" discussed in Chapter 4 of Cover and Thomas [20]. Moreover, $\dot{H}$ is not the time derivative of H. This notation is used here to emphasize that it is entropy "per time" instead of "per symbol".

Theorem 17.1 *(Shannon's Fundamental Theorem for Discrete Noiseless Channels [104]). Given an ergodic message source with entropy H (measured in bits per symbol), then the average rate, R, at which information can be transmitted (measured in symbols/second) over a discrete noiseless channel is bounded from above as $R < C/H$ (where C is measured in bits per second), and it is possible to encode the output of the source in such a way that R comes arbitrarily close to C/H.*

Suppose that the message being sent through an information channel is a 0 or a 1. It is possible that in the process of sending a 0 that an error of the form $0 \to 1$ occurs. Likewise, when attempting to send a 1, an error of the form $1 \to 0$ can occur. Let $\epsilon_{0\to1}$ and $\epsilon_{1\to0}$ denote the probabilities of these two events. If

$$\epsilon_{0\to1} = \epsilon_{1\to0} = e,$$

then the information channel is called symmetric. Here, $0 < e < 1$ describes how likely it is for a binary digit to be flipped during the communication process. If there is no prior knowledge about the contents or special structure[10] in the message, then the channel is called memoryless.

A *memoryless binary channel* is a simple, yet very instructive, model. The *channel capacity* for this model is

$$C(e) = 1 + e\log_2 e + (1-e)\log_2(1-e).$$

It is a measure of the effect of noise on the speed with which information can be transmitted through the channel. If $e = 0.5$, then no information at all can be transmitted because the received message would be completely random. In other words, regardless of whether a 0 or 1 was transmitted, the expected result would be the same as flipping a coin with the numbers 0 and 1 painted on either side. In all other cases, some amount of information is transmitted. If $e = 0$, a pristine copy of the original message is received. If $e = 1$, an exactly inverted message is received with all bit values flipped. Running this message through an inverter then recovers the original message easily. In all other cases, some degree of degradation of the message occurs. This can be overcome in a variety of ways. For example, two-way communication back and forth between sender and receiver can be performed to verify that the intended message was received; or the sender could send the message many times, and if e is small, then, with high probability, errors in random locations would not likely occur a large fraction of the time. Or, embedded in the message can be checks that alert the receiver that an error has occurred and possibly even identify its location.

17.2.2 Shannon's Theorem for Discrete Noisy Channels

Regardless of the strategy used to overcome errors in communication, one thing is certain: When there is noise in the information channel (and in a real channel, there always is!), the rate at which information can be transmitted becomes slower than if there were no noise. Additionally, as the probability of flipping a binary digit approaches 50%, the rate at which information can be transmitted approaches 0.

If a message x is sent through the channel, it may or may not reach the other end in its original form. Call the received message y. If the properties of the channel are completely characterized, then for all possible sent and received messages, the probabilities $p(x)$,

[10] Such special structure would exist if statistical correlations among characters and between words were precomputed and the rules of proper spelling and grammar in a given language were invoked on both the sending and receiving ends.

$p(y)$, and $p(x, y)$ will be known. In the language of Section 17.1.1, an "event" is a particular message, x, and a "collection" is the set of all possible messages, X. Therefore, $p(x \mid y)$ can be computed, and the discrete entropies $H(X)$, $H(Y)$, $H(X, Y)$, and $H(X \mid Y)$ can be computed from these probabilities. Shannon referred to the conditional entropy $H(X \mid Y)$ as the *equivocation.* This is a good name because if the intended message is actually received, $p(x \mid y) = \delta_{x,y}$ and $H(X \mid Y) = 0$, meaning that there is no ambiguity/confusion as to the relationship between the received and sent messages. On the other hand, if $p(x \mid y)$ is more spread out over the set of symbols than this Kronecker delta, then it is not possible to say unequivocally that the received message is the intended one.

The *capacity of a noisy channel*, C, is defined to be the supremum (which for a finite set is the same as the maximum) over all possible information sources of the mutual information of the source and sink:

$$C \doteq \sup_{p(x)} \mathcal{I}(X; Y).$$

If the channel is noiseless, the equivocation is 0, $H(X \mid Y) = 0$, and $\mathcal{I}(X; Y) = H(X)$. In this case, the $p(x)$ that maximizes $H(X)$ is the uniform distribution, and so if there are $N = 2^b$ possible symbols transmitted per second, this reduces to

$$C = \sup_{p(x)} \sum_{i=1}^{N} (1/N) \log_2 N = b \, \frac{\text{bits}}{\text{second}},$$

which is the same as in (17.25).

Since real channels have noise, the following theorem, which indicates that it is possible to drive this level of confusion down at the expense of a reduced rate of information transmission, is very useful in practice.

Theorem 17.2 *(Shannon's Fundamental Theorem for Discrete Noisy Channels [104]). For a discrete noisy channel with a capacity of C and a source entropy rate of $\dot{H}(X)$, there exists a coding system such that when $\dot{H}(X) \leq C$, the output of the source can be transmitted over the channel in such a way that $H(X \mid Y)$ approaches (but never reaches) zero by use of an appropriate coding method. And when $\dot{H}(X) > C$ the best possible code will have an error that approaches (but never reaches) $\dot{H}(X) - C$.*

The implication of this theorem is that when information is transmitted at a rate less than the capacity of a noisy channel, it can be done so almost always without error by using an "appropriate coding technique." Moreover, if an attempt is made to send more information through the channel than its capacity allows, then errors will undoubtedly result, although the frequency of these errors can be reduced by packaging (encoding) the message by taking into account knowledge of the channel. The theorem does not provide a means for constructing an "appropriate coding technique." Rather, it establishes bounds on what is possible and what is not.

Classical coding theory (as discussed in the next chapter) generally does not produce rates that approach this bound [1], but more modern coding methods do come quite close [6] at the expense of more computations on the encoding and decoding ends of the communication process. However, as computers become ever faster and less expensive, greater levels of computation become acceptable.

17.2.3 Continuous Channels with Gaussian Noise

In continuous channels, where messages are transmitted as continuous functions of time, $s(t)$ (called signals, rather than sequences of symbols), analogous theorems relating the rate of information transmission to the amount of noise in the channel are known. In particular, the *Shannon–Hartley* theorem relates the capacity of a channel to carry continuous information to the ratio of the power (or amplitude) of the signal and that of additive Gaussian white noise that corrupts the signal. Wiener filtering is a method for the recovery of signals corrupted by noise. The concepts of continuous entropy reviewed in Chapter 3 play a role in the analysis of continuous information transmission, and the channel can be modeled using the sorts of SDEs discussed in Chapter 4. The topic of continuous channels with Gaussian noise is treated in detail in [49, 105]. Our discussions of this topic and classical "rate-distortion theory" is postponed until Chapter 21, where this theory is generalized to the context of Lie groups and associated principal (fiber) bundles.

The remainder of this chapter explores various connections between information theory and group theory.

17.3 Groups and Information

Finite-group theory and information theory interacted in the context of the design of error-correcting codes. There are several other ways that properties of finite groups and information can be combined. Some of these are discussed in the subsections of this section. In contrast, the next section illustrates a connection between Lie groups and a problem in communications.

17.3.1 Convexity and Convolution

Recall from Chapter 3 that a *convex function* $\Phi : \mathbb{R} \to \mathbb{R}$ is one which satisfies the property

$$\Phi(\beta x + (1-\beta)y) \leq \beta\Phi(x) + (1-\beta)\Phi(y).$$

For example, a function with a positive derivative and second derivative will satisfy this property, but these are not necessary conditions for convexity. Differentiability (or even continuity) are not required for a function to be convex. Two important examples of convex functions are $\Phi(x) = -\log x$ and $\Phi(x) = +x\log x$. The negative of a convex function is called a *concave function.*

Convexity is unaffected by "external" affine transformations of the form $\Phi(x) \to E_{(a,b)}(\Phi(x)) \doteq a \cdot \Phi(x) + b$, where $a \in \mathbb{R}^{+}$ and $b \in \mathbb{R}$. Convexity is also unaffected by "internal" affine transformations of the form $\Phi(x) \to I_{(a,b)}(\Phi(x)) \doteq \Phi((x-b)/a)$. Successive internal or external affine transformations add up according to the group law for the affine group:

$$I_{(a_1,b_1)}(I_{(a_2,b_2)}(\Phi(x))) = I_{(a_1,b_1)\circ(a_2,b_2)}(\Phi(x))$$

and

$$E_{(a_1,b_1)}(E_{(a_2,b_2)}(\Phi(x))) = E_{(a_1,b_1)\circ(a_2,b_2)}(\Phi(x)),$$

where

$$(a_1,b_1)\circ(a_2,b_2) = (a_1a_2, a_1b_2+b_1).$$

This operation can be thought of as the matrix multiplication

$$\begin{pmatrix} a_1 & b_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2+b_1 \\ 0 & 1 \end{pmatrix}.$$

Given probabilities $\{p_1, \dots, p_n\}$ (defined by a probability function $p(x_i) = p_i$) that sum to 1 and any positive numbers $\{\alpha_1, \dots, \alpha_n\}$, it follows from the definition of a convex function that

$$\Phi\left(\frac{\sum_{i=1}^n \alpha_i p_i}{\sum_{i=1}^n \alpha_i}\right) \leq \frac{\sum_{i=1}^n \alpha_i \Phi(p_i)}{\sum_{i=1}^n \alpha_i}.$$

If entropy is viewed as a functional of the probability function p,

$$S(p) = -\sum_{i=1}^{n} p(x_i) \log p(x_i),$$

then the fact that $-p \log p$ is a concave function leads to the inequality

$$\boxed{S\left(\frac{\sum_{i=1}^n \alpha_i p_i}{\sum_{i=1}^n \alpha_i}\right) \geq \frac{\sum_{i=1}^n \alpha_i S(p_i)}{\sum_{i=1}^n \alpha_i}.} \tag{17.26}$$

Given a group G that acts on a set $X = \{x_1, \dots, x_n)$, a kind of convolution can be defined as

$$(\alpha * p)(x_i) = \sum_{g \in G} \alpha(g) p(g^{-1} \cdot x_i), \quad \text{where} \sum_{g \in G} \alpha(g) = 1 \quad \text{and} \quad \sum_{i=1}^{n} p(x_i) = 1.$$

For example, G might cyclically shift or otherwise permutate a set of characters, X. Although the sum here is over G rather than the elements of X, essentially the same reasoning as that behind (17.26) results in

$$\boxed{S(\alpha * p) \geq S(p).} \tag{17.27}$$

In other words, entropy never decreases as a result of convolution. This is related to (17.20). The next subsection addresses the case when the set X and G are the same set (denoted as Γ) and iterated convolutions are performed.

17.3.2 Groups and Information Inequalities

Earlier in this chapter a number of inequalities were presented. Information theory is full of inequalities that relate mutual information, entropy, marginalization, and so forth. In recent work, a number of researchers in information theory have observed a parallel between inequalities in information theory and inequalities in group theory. Part of this work is reviewed here.

To begin, let H and K be subgroups of a finite group G that has operation $\circ$. It can be shown (see the exercises and [59, 80]) that $H \cap K$ will always be a *subgroup* of G and

$$HK \doteq \{h \circ k \mid h \in H, k \in K\}$$

always will be a *subset* of G. It will be a subgroup of G if and only if $HK = KH$. One way in which this identity will hold is if G is commutative. Regardless of whether or not this condition holds, it can be shown that the number of entries in the set HK will be [59, p. 45]:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} \leq |G|. \tag{17.28}$$

This equality will be useful in the sequel.

Counting Formulas

Chan and Yeung [17, 18] have used this fact in the context of a family of subgroups of G to obtain information-theoretic inequalities. Let $\{G_1, G_2, \ldots, G_n\}$ denote a family of subgroups of G and let $G_{ij} \doteq G_i \cap G_j$ and, by extension, $G_{i_1,i_2,\ldots,i_m} \doteq G_{i_1} \cap G_{i_2} \cap \cdots \cap G_{i_m}$, which must all be a subgroups of G. Then using (17.28), it follows that

$$|G_{ij}G_{jk}| = \frac{|G_{ij}| \cdot |G_{jk}|}{|G_{ij} \cap G_{jk}|} = \frac{|G_{ij}| \cdot |G_{jk}|}{|G_{ijk}|}.$$

Without loss of generality, let $i = 1$, $j = 3$, and $k = 2$.

As is pointed out in [17], it follows from (17.28) that $|G_{13}| \cdot |G_{23}|/|G_{123}| \leq |G_3|$. Dividing both sides by $|G_{13}| \cdot |G_{23}| \cdot |G_3|$ and multiplying by $|G|$ gives

$$\frac{|G|}{|G_{123}| \cdot |G_3|} \leq \frac{|G|}{|G_{13}| \cdot |G_{23}|}.$$

Taking the logarithm of both sides gives

$$\log\frac{|G|}{|G_{13}|} + \log\frac{|G|}{|G_{23}|} \geq \log\frac{|G|}{|G_3|} + \log\frac{|G|}{|G_{123}|}.$$

Due to the analogy between group theory and information theory established in [17], this equality can be viewed as a derivation of the inequality

$$H(C_1 \cap C_2) + H(C_2 \cap C_3) \geq H(C_3) + H(C_1 \cap C_2 \cap C_3) \quad \text{or} \quad \mathcal{I}(C_1, C_2|C_3) \geq 0,$$

which was stated without reference to group theory in (17.17).

These analogies go both ways. For example, as pointed out in [17], the information inequality by Zhang and Yueng [128],

$$\begin{aligned} &H(C_1) + H(C_2) + 2H(C_1 \cap C_2) + 4H(C_3) + 4H(C_4) + 5H(C_1 \cap C_3 \cap C_4) \\ &\quad + 5H(C_2 \cap C_3 \cap C_4) \\ &\qquad \leq 6H(C_3 \cap C_4) + 4H(C_1 \cap C_3) + 4H(C_1 \cap C_4) + 4H(C_2 \cap C_3) + 4H(C_2 \cap C_4), \end{aligned}$$

can be used to write the corresponding group inequality

$$\begin{aligned} &\log\frac{|G|}{|G_1|} + \log\frac{|G|}{|G_2|} + 2\log\frac{|G|}{|G_{12}|} + 4\log\frac{|G|}{|G_3|} + 4\log\frac{|G|}{|G_4|} + 5\log\frac{|G|}{|G_{134}|} + 5\log\frac{|G|}{|G_{234}|} \\ &\quad \leq 6\log\frac{|G|}{|G_{34}|} + 4\log\frac{|G|}{|G_{13}|} + 4\log\frac{|G|}{|G_{14}|} + 4\log\frac{|G|}{|G_{23}|} + 4\log\frac{|G|}{|G_{24}|}. \end{aligned}$$

Exponentiation of both sides and some rearrangement of terms gives the group inequality

$$|G_{34}|^6 \cdot |G_{13}|^4 \cdot |G_{14}|^4 \cdot |G_{23}|^4 \cdot |G_{24}|^4 \leq |G_1| \cdot |G_2| \cdot |G_3|^4 \cdot |G_4|^4 \cdot |G_{12}|^2 \cdot |G_{134}|^5 \cdot |G_{234}|^5.$$

Ingleton Inequality and Homomorphisms

In very recent work, Li and Chong [75, 76] and Chan [18] have addressed the relationship between group homomorphisms and information inequalities using the Ingleton inequality [62]. This work is reviewed here in notation consistent with the rest of this chapter, which is somewhat different than their notation.

Let G be a finite group with elements $g_i \in G$ with $i = 1, \dots, |G|$. Let ϕ_1, ϕ_2, ϕ_3, and ϕ_4 be homomorphisms from G into other groups, G_1', G_2', G_3', and G_4'; that is, $\phi_j : G \to G_j'$. Let $p : G \to \mathbb{R}$ be any pdf on G. A probability density on G_j' can be defined by combining $p(\cdot)$ and $\phi_j(g_i)$ in an appropriate way. In particular, for any $g' \in G_j'$,

$$p_j'(g') \doteq \begin{cases} \sum_{g \in \phi_j^{-1}(G_j')} p(g) & \text{if } g' \in \phi_j(G) \\ 0 & \text{if } g' \notin \phi_j(G). \end{cases} \tag{17.29}$$

Let $p_0(g_i) = 1/|G|$ for all $i = 1, \dots, |G|$ denote the uniform probability distribution on G. Now, if G and G_j' are isomorphic to each other, the uniformity of $p_0(\cdot)$ will be preserved by the isomorphism. In contrast, if the homomorphism is injective (one-to-one) but not surjective, then the value $1/|G|$ can be assigned to all elements in $\phi_i(G)$ and a value of 0 can be assigned to all remaining elements, $G_i' - \phi_i(G)$. If the homomorphism is not injective, then multiple elements of G will be mapped to each element of $\phi_i(G)$. The number of elements from G that are mapped to each element in $\phi_i(G)$ will be exactly the same as the number of elements from G that map to the identity element of $\phi_i(G)$, and so

$$\sum_{g \in \phi_j^{-1}(G_j')} p_0(g) = \frac{|Ker\,\phi_j|}{|G|}.$$

In other words, the uniformity of the probability on G will be preserved on $\phi_i(G)$, although its magnitude will be scaled.

Entropies and mutual information can be defined on finite groups in the same way as on any finite set. Whereas it is common in classical probability and information theory to denote a deterministic variable as a lowercase letter and a random variable as the corresponding uppercase letter (e.g., x and X), when addressing information theory on groups this would lead to a notational problem because g and G already have well-established meanings. Therefore, g will be used to describe both deterministic and stochastic group elements, and the context will specify which is being considered at any particular instance.

Given homomorphisms from G into the direct products of the form $G_i' \times G_j'$ constructed simply as $(\phi_i, \phi_j) : G \to (\phi_i(G), \phi_j(G))$, it is possible to define probability distributions on $G_i' \times G_j'$ from $p(g)$ using a construction similar to that in (17.29). This can be extended to a many-fold product. It then makes sense to discuss joint entropy, mutual information, conditional mutual information, and so forth. Using this construction, Li and Chong [75] computed

$$H(\phi_1(G), \phi_2(G)) = \log |G| - \log |Ker\,\phi_1 \cap Ker\,\phi_2|,$$

$$\mathcal{I}(\phi_1(G); \phi_2(G)) = \log |G| - \log \frac{|Ker\,\phi_1| \cdot |Ker\,\phi_2|}{|Ker\,\phi_1 \cap Ker\,\phi_2|},$$

$$\mathcal{I}(\phi_1(G); \phi_2(G)|\phi_3(G)) = \log \frac{|Ker\,\phi_1 \cap Ker\,\phi_2 \cap Ker\,\phi_3| \cdot |Ker\,\phi_3|}{|Ker\,\phi_1 \cap Ker\,\phi_3| \cdot |Ker\,\phi_2 \cap Ker\,\phi_3|}.$$

They then used rules of group theory and information inequalities from [47] to prove Ingleton's inequality in this context:

$$\boxed{\begin{gathered} \mathcal{I}(\phi_1(G); \phi_2(G)|\phi_3(G)) + \mathcal{I}(\phi_1(G); \phi_2(G)|\phi_4(G)) + \mathcal{I}(\phi_3(G); \phi_4(G)) \\ \geq \mathcal{I}(\phi_1(G); \phi_2(G)). \end{gathered}} \tag{17.30}$$

The discussion in this section has focused on the relationship between finite groups and discrete information inequalities. In contrast, Lie groups enter into the theory of communication in several ways, as is explained in the following section.

17.4 The Telegraph Equation

The physical transmission of information can take place in many different ways. One of the first modes of communication in the modern era was the telegraph. The way that the amplitude of a signal in, for example, Morse code gets distorted as it traverses a telegraph line is governed by the so-called telegraph equation. This equation is of the form

$$\frac{\partial^2 u}{\partial t^2} + (\alpha+\beta)\frac{\partial u}{\partial t} + \alpha\beta u - c^2\frac{\partial^2 u}{\partial x^2} = 0, \tag{17.31}$$

where $c^2 = 1/LC$, $\alpha = G/C$, and $\beta = R/L$, where L is the inductance, R is the resistance, C is the capacitance, and G is the conductance of the cable. $u(x,t)$ is the voltage in the cable at position x and time t.

Given initial conditions, it is possible to solve for $u(x,t)$ using classical Fourier analysis, as reviewed in [19]. The goal in this section is not to solve (17.31) but rather to examine Lie symmetries of the equation itself. This can serve as a paradigm for the Lie-theoretic analysis of other equations governing the physical transmission of information. These include acoustic transmission in three dimensions. Here, (17.31) is used to demonstrate the simplest example (not because of any expected resurgence in the use of telegraphic information transmission!).

17.4.1 Standard Form

To begin, it will be convenient to convert (17.31) into a standard form. Suppose that we introduce three real parameters: $T > 0$, a time scale, $X > 0$, a length scale, and $\lambda > 0$, a decay constant. Let $x = X\xi$ and $t = T\tau$. Then it is possible to substitute $u(x,t) = e^{-\lambda\tau}v(X\xi, T\tau)$ into (17.31). Since

$$\frac{\partial u}{\partial t} = e^{-\lambda\tau}\frac{\partial v}{\partial \tau}\frac{\partial \tau}{\partial t} - \lambda e^{-\lambda\tau}\frac{\partial \tau}{\partial t}v = \frac{e^{-\lambda\tau}}{T}\left(\frac{\partial v}{\partial \tau} - \lambda v\right)$$

and

$$\frac{\partial u}{\partial x} = e^{-\lambda\tau}\frac{\partial v}{\partial \xi}\frac{\partial \xi}{\partial x} = \frac{e^{-\lambda\tau}}{X}\frac{\partial v}{\partial \xi},$$

it follows that repeated application of these rules gives

$$\frac{\partial^2 u}{\partial t^2} = \frac{e^{-\lambda\tau}}{T^2}\left[\frac{\partial^2 v}{\partial \tau^2} - 2\lambda\frac{\partial v}{\partial \tau} + \lambda^2 v\right]$$

and

$$\frac{\partial^2 u}{\partial x^2} = \frac{e^{-\lambda\tau}}{X^2}\frac{\partial^2 v}{\partial \xi^2}.$$

Therefore, substitution in (17.31) and division by $e^{-\lambda\tau}$ gives the "standard form"

$$\frac{\partial^2 v}{\partial \tau^2} + v - \frac{\partial^2 v}{\partial \xi^2} \doteq Qv = 0 \tag{17.32}$$

for the choice

$$T = 1 \pm \frac{\alpha - \beta}{\alpha + \beta}, \quad \lambda = \frac{1}{2}(\alpha + \beta)T, \quad X = cT.$$

It is not necessary to convert from (17.31) to (17.32) in order to perform a symmetry analysis, but the removal of parameters and elimination of the single derivative term reduces the complexity of the calculations somewhat. Hence, the remainder of this discussion is restricted to (17.32).

17.4.2 Symmetry Operators

Following the same procedure as with the heat equation in Chapter 2, we seek a first-order linear operator of the form[11]

$$L = T(\xi, \tau)\frac{\partial}{\partial \tau} + X(\xi, \tau)\frac{\partial}{\partial \xi} + Z(\xi, \tau)$$

such that

$$[L, Q]v = RQv$$

for some $R(\xi, \tau)$. A direct calculation similar to that for the heat equation in Chapter 2 then yields the conditions

$$\frac{\partial^2 Z}{\partial \tau^2} - \frac{\partial^2 Z}{\partial \xi^2} = -R, \tag{17.33}$$

$$\frac{\partial^2 T}{\partial \tau^2} - \frac{\partial^2 T}{\partial \xi^2} + 2\frac{\partial Z}{\partial \tau} = 0, \tag{17.34}$$

$$2\frac{\partial T}{\partial \tau} = -R, \tag{17.35}$$

$$\frac{\partial^2 X}{\partial \tau^2} - \frac{\partial^2 X}{\partial \xi^2} - 2\frac{\partial Z}{\partial \xi} = 0, \tag{17.36}$$

$$\frac{\partial X}{\partial \tau} - \frac{\partial T}{\partial \xi} = 0, \tag{17.37}$$

$$2\frac{\partial X}{\partial \xi} = -R. \tag{17.38}$$

Combining (17.35) and (17.38) gives

$$\frac{\partial X}{\partial \xi} = \frac{\partial T}{\partial \tau}, \tag{17.39}$$

which together with (17.37) leads to

$$\frac{\partial^2 X}{\partial \xi^2} = \frac{\partial^2 X}{\partial \tau^2} \quad \text{and} \quad \frac{\partial^2 T}{\partial \xi^2} = \frac{\partial^2 T}{\partial \tau^2}.$$

Substituting this into (17.34) and (17.36) gives

$$\frac{\partial Z}{\partial \xi} = \frac{\partial Z}{\partial \tau} = 0 \implies Z = const.$$

[11] $T(\xi, \tau)$ and $X(\xi, \tau)$ are unrelated to the length scales T and X used above, which will not appear in the rest of this analysis.

This, in turn, implies from (17.33) that $R = 0$, which together with (17.38) gives that $X = X(\tau)$ and (17.35) gives $T = T(\xi)$. From (17.39), the condition $X'(\tau) = T'(\xi)$ follows, and revisiting (17.34) and (17.36) gives $X''(\tau) = T''(\xi) = 0$. Putting all of this together,

$$L = (l_3\xi + l_1)\frac{\partial}{\partial \tau} + (l_3\tau + l_2)\frac{\partial}{\partial \xi} + l_0,$$

where $l_0, \ldots, l_3$ are free constants. Neglecting l_0 by setting it equal to 0 (since it corresponds to the trivial identity operator), the resulting operator is spanned by basis elements of the form

$$L_1 = \frac{\partial}{\partial \tau}, \quad L_2 = \frac{\partial}{\partial \xi}, \quad L_3 = \xi\frac{\partial}{\partial \tau} + \tau\frac{\partial}{\partial \xi}. \tag{17.40}$$

These operators form a Lie algebra with commutation relations

$$[L_1, L_2] = 0, \quad [L_1, L_3] = L_2, \quad [L_2, L_3] = L_1.$$

Note that these commutation relations are the same as those for the Lie algebra of the motion group of the Lobachevsky plane in Section 10.6.4 with $L_1 \leftrightarrow -X_1$, $L_2 \leftrightarrow X_2$, and $L_3 \leftrightarrow X_3$.

Of course, in the modern era, the value of understanding the telegraph equation is not in order to improve communication via telegraphy. Rather, this equation is a model for various communication problems, including the transmission of nerve impulses in biological systems and dispersive wave phenomena more generally. Moreover, the continuous symmetries of equations governing the transmission of information via the telegraph equation are but one application of Lie theory. Treatments of Lie symmetries of other equations describing wave propagation can be found in numerous papers and books, including [13–15, 31, 64, 73, 84, 88, 92, 102].

17.5 Communications and Random Walks in the Hyperbolic Plane

The hyperbolic plane (also called the Lobachevsky plane) is a mathematical object that was linked to the theory of communication half a century ago [43, 44, 66, 117, 118]. In those modeling and analysis efforts, it was shown how noise due to random inhomogeneities in waveguides can be related to how a communication signal gets corrupted and how this is related to stochastic processes in the hyperbolic plane. After those efforts, a number of famous theorems about the properties of random walks on groups and homogenous spaces, including those due to Furstenberg [39, 40], were published. Interest in these topics has continued to the present day [3, 4, 46, 61, 85, 110].

In this section the mathematical modeling tools necessary to derive SDEs and the corresponding Fokker–Planck equation on the hyperbolic plane are developed. Two models of the hyperbolic plane are common: the Poincaré disk model and the Poincaré half-plane model. These two models are related by a conformal mapping, as is explained below. Since different groups of transformations act on the disk and on the half-plane models, the conformal mapping between the models defines mappings between the groups acting on these models.

What is presented here in two dimensions extends naturally to higher dimensions with the open ball in $\mathbb{R}^n$ replacing the open disk and the open half-space $\mathbb{R}^{n-1} \times \mathbb{R}_{>0}$

replacing the open half-plane. Although these objects, together with their metrics, are model examples of spaces of negative curvature, the emphasis here is only the two-dimensional case.

17.5.1 The Group $SU(1,1)$ and the Poincaré Disk Model

The group $SU(1,1)$ consists of all 2×2 complex matrices of the form

$$A = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix}, \quad \text{where } \alpha\overline{\alpha} - \beta\overline{\beta} = 1 \text{ and } \alpha, \beta \in \mathbb{C}, \tag{17.41}$$

such that the quadratic form

$$A^* \mathbb{J}_2 A = \mathbb{J}_2, \quad \text{where } \mathbb{J}_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{17.42}$$

is preserved. An action of this group on the open unit disk in the complex plane, $D \doteq \{w \in \mathbb{C} \,|\, |w| < 1\}$, can be defined as [56]

$$A \cdot w \doteq \frac{\alpha w + \beta}{\overline{\beta} w + \overline{\alpha}}.$$

By observing that

$$SO(2) \cong \{A(\theta) \mid \theta \in [0, 2\pi)\} < SU(1,1), \quad \text{where } A(\theta) = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix},$$

D itself can be viewed as the homogeneous space

$$D = SU(1,1)/SO(2).$$

If $w = x_1 + ix_2$ are the coordinates for D, then its metric tensor can be expressed as [56]

$$g_{ij} = \frac{\delta_{ij}}{(1 - x_1^2 - x_2^2)^2}. \tag{17.43}$$

The unit open disk, D, in the complex plane together with this metric is called the *hyperbolic plane.*

With the above information, we have everything we need to simulate random walks and Fokker–Planck equations in the hyperbolic plane. In particular, the volume element and Laplace–Beltrami operator are

$$dz = \frac{dx_1 dx_2}{(1 - x_1^2 - x_2^2)^2} \quad \text{and} \quad \nabla^2 = (1 - x_1^2 - x_2^2)^2 \left(\frac{\partial^2}{\partial x_1^2} + \frac{\partial^2}{\partial x_2^2} \right). \tag{17.44}$$

There is a very intuitive geometric way to view the above equations. As explained in [74], a mapping can be defined between D and one sheet of a hyperboloid of two sheets. Recall from high school geometry that a hyperboloid of two sheets embedded in $\mathbb{R}^3$ is of the form

$$\frac{z^2}{c^2} - \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \implies z = \pm c \sqrt{1 + \frac{x^2}{a^2} + \frac{y^2}{b^2}}. \tag{17.45}$$

The + branch in the above equation corresponds to the "upper" sheet. We are interested in the case when $a = b$, so that it is symmetric around the z axis. The two points on the two sheets that are closest to each other are $(0, 0, \pm c)$, and as $x^2 + y^2$ increases, the hyperboloid asymptotes to a cone. An invertible mapping between a disk in the $x - y$ plane centered at the origin and the upper sheet can be defined by stereographic projection from $(0, 0, -c)$ through the disk and intersecting the upper sheet. By adjusting the values of a and c, it can be ensured that this is a unit disk. It is left as an exercise to compare the metric in (17.43) with the metric for the hyperboloid of one sheet induced from its embedding in $\mathbb{R}^3$.

17.5.2 The Groups $SL(2, \mathbb{R})$ and $PSL(2, \mathbb{R})$ and the Poincaré Half-Plane Model

The group $SL(2, \mathbb{R})$ was reviewed earlier. It consists of all 2×2 matrices with real entries and determinant of $+1$. Note that since this is an even-dimensional matrix, both $\mathbb{I}_2$ and $-\mathbb{I}_2$ have a determinant of $+1$. The two matrices $\mathbb{I}_2$ and $-\mathbb{I}_2$ form a finite subgroup of $SL(2, \mathbb{R})$ with two elements. This subgroup $\{\mathbb{I}_2, -\mathbb{I}_2\} \cong \mathbb{Z}_2$. The group $PSL(2, \mathbb{R})$ is defined as the quotient $SL(2, \mathbb{R})/\{\mathbb{I}_2, -\mathbb{I}_2\}$. In other words, there is a two-to-one mapping from $SL(2, \mathbb{R})$ onto $PSL(2, \mathbb{R})$.

An action of $PSL(2, \mathbb{R})$ on the upper half of the complex plane $\mathbb{H} \doteq \{z \in \mathbb{C} \,|\mathrm{Im}(z) > 0\}$, $PSL(2, \mathbb{R}) : \mathbb{H} \to \mathbb{H}$, can be defined as

$$A \cdot z \doteq \frac{az + b}{cz + d} = -A \cdot z, \quad \text{where } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{R}).$$

This is an example of a *Möbius transformation* (also called a *linear fractional transformation*). This sort of transformation received considerable attention on "Youtube" recently [6]

The set $\mathbb{H}$, together with the metric in (17.43), which is called the *Poincaré half-plane model*, can be thought of as the homogeneous space

$$\mathbb{H} = PSL(2, \mathbb{R})/SO(2).$$

The disk and the half-plane models are related by any *conformal mapping* of the form [82, 108]

$$w = e^{i\theta_0} \left(\frac{z - z_0}{z - \overline{z_0}} \right), \tag{17.46}$$

where $z_0 = r_0 e^{i\theta_0} \in \mathbb{H}$ is arbitrary; that is, each choice of z_0 defines a different mapping from $\mathbb{H}$ to D. For the applications of these concepts to the analysis of waveguides with random inhomogeneities, see [43, 44, 66, 90, 117, 118], and for more reading about the hyperbolic plane, see [109].

17.6 Optical Communications and Lie Groups

Optical communication is an important subject in any discussion of communications. Two kinds of optical communication systems exist: direct detection systems and coherent detection systems. In direct detection systems, the optical signal is converted directly into a demodulated electrical output. In coherent detection systems, light is added to the modulated signal as part of the detection process. Coherent detection systems have several advantages over direct detection systems, including increased sensitivity and increased frequency selectivity. However, this comes at the cost of increased complexity, and a problem called *laser phase noise* is a large barrier preventing their applications. It is therefore important to analyze the effects of phase noise on the performance of various coherent receivers.

17.6.1 Coherent Optical Systems

In optical communications, the work “coherent” describes any receiver that adds a local oscillator (LO) lightwave to the incoming wave, even if subsequent processing and demodulation ignore the phase and frequency, as is the case of envelope detectors [67]. This is because adding the LO to the weak conventional intensity modulation increases sensitivity of the system. This is what is called a “weakly coherent system.” This contrasts with the meaning of coherent systems in the classical communications literature, which requires the recovery and use of the phase and frequency of the carrier to perform the demodulation and detection.

The basic coherent optical system works as follows. Laser light possessing a sufficiently stable frequency (quasi-monochromatic signal) is used as the carrier wave and modulated (in amplitude, frequency, phase, or polarization) by the information signal. At the receiver site, a LO lightwave is added to the received signal, and the combined lightwave is directed toward a photodetector. The resulting photocurrent is bandpass filtered to select the modulated intermediate frequency (IF) carrier. The IF is equal to the difference between the LO and carrier frequencies, usually in the microwave (GHz) range. If the LO and the carrier have the same frequency, the electrical currents at the output of the photodiodes are at baseband, and the receiver is called *homodyne*. On the other hand, if they do not have the same frequency, the electrical currents are frequency translated at IF. In this case, the receiver is called *heterodyne*.

Coherent optical systems have two major advantages. The first is the high sensitivity which results in an expansion of the repeater spacing. The second is the high-frequency selectivity which results in a contraction of the frequency spacing between multiplexed channels. In contrast to direct detection systems, coherent detection systems have the capability to detect the phase, frequency, amplitude, and polarization of the incident light signal. Therefore, information can be transmitted via phase, frequency, amplitude, or polarization modulation. By applying FDM (frequency division multiplexing) of a large number of densely spaced channels in the transmitter, the bandwidth inherent in conventional single-mode fibers can be effectively exploited [25], and each receiver is able to select one of the FDM channels carried by the fiber by simply tuning its own local oscillator.

Of all the obstacles preventing coherent techniques from making a smooth transition into the optical domain, laser phase noise is one of the largest, and therein lies an application of the theory of Lie groups.

17.6.2 Laser Phase Noise

The phase of the light emitted from a semiconductor laser exhibits random fluctuations due to spontaneous emissions in the laser cavity [58]. This phenomenon is commonly referred to as phase noise. Because there are only about 10^4 photons in the active region of a semiconductor laser, the phase of the light is significantly perturbed by just one spontaneous photon [78]. If there is no spontaneous emission, the output light spectrum consists of delta functions (each delta function $\delta(\omega - \omega_i)$ corresponding to one longitudinal mode at frequency ω_i). When there are random spontaneous emissions, the spectrum is no longer a sum of delta functions. Instead, the spectrum is broadened and has a finite nonzero linewidth around each ω_i. The amount of phase noise is directly related to its so-called linewidth—the 3-dB linewidth of its power spectrum density. The spectral width of a modern microwave oscillator is less than 1 Hz and that of a distributed feedback (DFB) laser is 1 MHz. The best of today's GaAsInp DFB lasers based on superstructure, hand-selected from bulk production, have a linewidth less than 1 kHz [112, 126].

Phase noise has two important adverse effects on the performance of coherent optical communications. One effect is the broadening of the linewidth of a light source output. It results in inefficient use of the available bandwidth and causes interchannel interference and thus necessitates wider channel spacing. This is especially dominant at low data rates where channels occupy a small bandwidth. Additionally, a large linewidth results in a larger propagating dispersion in optical fibers. The second effect is that phase noise directly corrupts the phase or frequency of a modulated carrier. It makes the correct retrieval of the transmitted data bits more difficult for the receiver. The system sensitivity is degraded, as measured by the BER (bit error rate) [12]. For a fixed BER, this necessitates an increase in received signal power compared to the ideal situation (power penalty). In some cases, the presence of phase noise creates a lower limit on the probability of a bit error (BER floor) below which the system cannot operate.

Some methods to alleviate the influence of phase noise have been proposed in [8, 34]. They involve receiver structures and signaling mechanisms that are relatively insensitive to phase uncertainty (e.g. amplitude shift keying and frequency shift keying). Envelope detector structures with widened filter bandwidths are used in conjunction with these modulation formats to reduce the performance degradation. Reference transmission schemes that provide a reference signal at the receiver that has the same phase structure as the received signal may cancel phase noise.

The Three-Dimensional Phase–Noise Fokker–Planck Equation

As was pointed out in [35, 42, 120], to evaluate the phase noise effects on coherent optical systems, the main issue is to find the statistical characterization of the output of the IF filter. Unfortunately, this is a difficult problem even in the simple but significant case in which a finite-time integrator (integrate-and-dump filter) is used. Analytical models that describe the relationship between phase noise and the filtered signal are found in [16, 35, 36, 42]. In particular, the Fokker–Planck approach represents the most rigorous description of phase noise effects [41, 42, 127]. To better apply this approach to system design and optimization, an efficient and powerful computational tool is necessary. In this chapter, we introduce one such tool for use in lightwave communications.

The Fokker–Planck approach has been described in [16, 35, 127] in which the derivation for a specific IF filter, the finite-time integrator, is outlined. Here, we derive it for any IF filter with a bounded impulse response.

In the field of fiber optic communication systems, a limitation on the amount of information that can be transmitted when using particular architectural paradigms is imposed by laser phase noise. This noise results when random photons in the laser cavity are spontaneously emitted. The resulting noise in the phase of transmitted laser pulses, $\phi(t)$, is usually modeled as a Brownian motion process [67] as

$$\phi(t) \doteq \sqrt{D}\int_0^t dw \quad \text{or} \quad d\phi = \sqrt{D}dw. \tag{17.47}$$

The parameter D is related to the laser linewidth Δv by $D = 2\pi\Delta v$.

Using the equivalent baseband representation and normalizing it to unit amplitude, the corresponding random part of a signal being sent by the laser can be written as [42][12]

$$s(t) \doteq e^{j\phi(t)}.$$

If $h(t)$ is the impulse response of the IF filter, then the (complex) random variable $z(t)$ (the output of the IF filter) describes how the filter and noise interact:

$$z(t) \doteq (h * s)(t) = \int_0^t h(\tau)\, e^{j\phi(t-\tau)} d\tau. \tag{17.48}$$

Here, $s(t)$ is the input signal to the IF filter which is corrupted by phase noise.

Since phase noise $\phi(t)$ is a stationary random process, the reversal of the time direction in $\phi(t)$ does not affect the statistics of $z(t)$. Moreover, $\phi(t-\tau)$ can be replaced by $\phi(\tau)$. Then (17.48) can be rewritten as

$$z(t) = \int_0^t h(\tau)\, e^{j\phi(\tau)} d\tau. \tag{17.49}$$

Equation (17.49) is not a Markov process. There are two ways to construct Markov processes with the same statistical characteristics as (17.49). One way is to adopt a vector process which is Markov. This will give a three-dimensional Fokker–Planck equation. The other way is to use an auxiliary variable by a slight modification of (17.49). This way will give a two-dimensional Fokker–Planck equation. In the following, we will derive the corresponding stochastic differential equations first. Then we show their Fokker–Planck equations.

Let us expand $z(t)$ into its real and imaginary parts as

$$z(t) = x(t) + jy(t) = r(t)e^{j\theta t}.$$

From (17.49), we can easily get

$$x(t) = \int_0^t h(\tau) \cos\phi(\tau)\, d\tau, \tag{17.50}$$

$$y(t) = \int_0^t h(\tau) \sin\phi(\tau)\, d\tau. \tag{17.51}$$

Although $z(t)$, $x(t)$, and $y(t)$ are not Markov processes, the three-component vector process $[\phi(t), x(t), y(t)]^T$ and $[\phi(t), r(t), \theta(t)]^T$ are Markov vector processes. From (17.47), (17.50), and (17.51), we can derive the stochastic differential equations as

$$\begin{bmatrix} d\phi(t) \\ dx(t) \\ dy(t) \end{bmatrix} = \begin{bmatrix} 0 \\ h(t)\cos\phi(t) \\ h(t)\sin\phi(t) \end{bmatrix} dt + \begin{bmatrix} \sqrt{D} \\ 0 \\ 0 \end{bmatrix} dw(t) \tag{17.52}$$

with initial conditions $\phi(0) = 0, x(0) = 0$, and $y(0) = 0$. Since D is a constant, it does not matter if (17.52) us viewed as being Itôor Stratonovich.

Comparing (17.52) with a standard SDE, we see that the drift vector and diffusion matrix are respectively

$$\mathbf{a} = \begin{bmatrix} 0 \\ h(t)\cos\phi(t) \\ h(t)\sin\phi(t) \end{bmatrix} \quad \text{and} \quad H = \begin{bmatrix} \sqrt{D} \\ 0 \\ 0 \end{bmatrix}.$$

[12] In electrical engineering, it is common to use $j = \sqrt{-1}$ rather than i, and so to be consistent with the literature, we use j in this section.

Using the methods of Chapter 4, we can derive the three-dimensional Fokker–Planck equation for (17.52) as

$$\boxed{\frac{\partial f}{\partial t} = -h(t)\cos\phi\frac{\partial f}{\partial x} - h(t)\sin\phi\frac{\partial f}{\partial y} + \frac{D}{2}\frac{\partial^2 f}{\partial \phi^2}} \tag{17.53}$$

with initial condition $f(x,y,\phi;0) = \delta(x)\delta(y)\delta(\phi)$, δ being the Dirac delta function. When the IF filter is a finite-time integrator, the three-dimensional Fokker–Planck equation can be simplified as

$$\frac{\partial f}{\partial t} = -\cos\phi\frac{\partial f}{\partial x} - \sin\phi\frac{\partial f}{\partial y} + \frac{D}{2}\frac{\partial^2 f}{\partial \phi^2}. \tag{17.54}$$

This equation is similar to the equation describing the evolution of the stochastic robot in Chapter 1. It is evolving on the group of rigid-body motions of the plane, $SE(2)$, with elements of the form $g(x,y,\phi)$.

The Two-Dimensional Phase Noise Equation

Corresponding to the three-dimensional Fokker–Planck equation defined earlier is a two-dimensional equation that describes the evolution of marginal densities. This two-dimensional equation is derived here.

Since increments of Wiener processes are invariant under shifts, the following substitutions can be made:

$$\phi(t-\tau) \Longleftrightarrow \phi(t) - \phi(\tau) \quad \text{and} \quad \phi(t) \Longleftrightarrow -\phi(t). \tag{17.55}$$

Using the first of these,

$$z(t) \doteq (h * s)(t) = e^{j\phi(t)} \cdot \int_0^t h(\tau)\, e^{-j\phi(\tau)} d\tau. \tag{17.56}$$

Since this is a physical process, this integral should be interpreted in the Stratonovich sense when computing increments. This means that the usual calculus can be used to obtain

$$dz(t) = e^{j\phi(t)} \cdot \left(h(\tau)\, e^{-j\phi(\tau)}\right)\Big|_{\tau=t} dt + j\, d\phi(t) \circledS e^{j\phi(t)} \cdot \int_0^t h(\tau)\, e^{-j\phi(\tau)}\, d\tau, \tag{17.57}$$

which can be written as

$$dz(t) = h(t)\, dt + j\sqrt{D}\, z(t) \circledS dw(t). \tag{17.58}$$

If we use the second expression in (17.55), then the plus sign will become a minus. This sign is irrelevant. The $\circledS$ crept in because we used the usual calculus on a stochastic system, which is consistent with the Stratonovich interpretation.

If instead of using the Stratonovich calculus, we can apply Itô's rule to evaluate dz. Itô's product rule is $d(x(t)y(t)) = x(t)\, dy(t) + y(t)\, dx(t) + dx(t)\, dy(t)$. Applying this to

(17.56) gives

$$dz(t) = de^{j\phi(t)} \cdot \int_0^t h(\tau)\, e^{-j\phi(\tau)} d\tau + e^{j\phi(t)} \cdot d\int_0^t h(\tau)\, e^{-j\phi(\tau)} d\tau + de^{j\phi(t)} \cdot d\int_0^t h(\tau)\, e^{-j\phi(\tau)} d\tau. \tag{17.59}$$

Here,

$$de^{j\phi(t)} = e^{j\phi(t)}\left[j\, d\phi(t) - \frac{1}{2}(d\phi(t))^2\right] = e^{j\phi(t)}\left[j\sqrt{D}\, dw - \frac{1}{2}D\, dt\right].$$

The first equality can be obtained by expanding out using Euler's formula, $e^{i\phi} = \cos\phi + j\sin\phi$, and using Itô's rule for the real and imaginary parts and recombining. This result has been used in, for example, [33]. The second equality is because $d\phi(t) = \sqrt{D}\, dw$ and so $(d\phi(t))^2 = D(dw(t))^2 = Dt$.

Recognizing that, in general, $dz(t) = z(t + dt) - z(t)$, the increment of the integral term becomes

$$d\int_0^t h(\tau)\, e^{-j\phi(\tau)} d\tau = \int_0^{t+dt} h(\tau)\, e^{-j\phi(\tau)} d\tau - \int_0^t h(\tau)\, e^{-j\phi(\tau)} d\tau = h(t)\, e^{-j\phi(t)} dt.$$

Therefore, the last term in (17.59) vanishes, since it is of higher order (i.e., smaller) than dt.

Making all of the above substitutions into (17.59), the following Itô SDE results:

$$dz(t) = \left[h(t) - \frac{1}{2}Dz(t)\right] dt + j\sqrt{D}z(t)\, dw(t). \tag{17.60}$$

If $z(t) = x(t) + jy(t)$, then this becomes

$$dx = (h - Dx/2)\, dt - \sqrt{D}y\, dw \quad \text{and} \quad dy = (-Dy/2)\, dt + \sqrt{D}x\, dw. \tag{17.61}$$

In the Stratonovich case, Jacobsen [63] wrote that

$$dx = h(t)\, dt + \sqrt{D}\, y ⓢ dw \quad \text{and} \quad dy = -\sqrt{D}\, x ⓢ dw. \tag{17.62}$$

If $x = x_1$ and $y = x_2$, then the corresponding Fokker–Planck equation is

$$\frac{\partial f}{\partial t} = -\sum_{i=1}^{d} \frac{\partial}{\partial x_i}(h_i^s f) + \frac{1}{2}\sum_{i,j=1}^{d} \frac{\partial}{\partial x_i}\left[\sum_{k=1}^{m} H_{ik}^s \frac{\partial}{\partial x_j}(H_{jk}^s f)\right], \tag{17.63}$$

where

$$\mathbf{h}^s = \begin{pmatrix} h \\ 0 \end{pmatrix}$$

and

$$H^s = \begin{pmatrix} H_{11}^s \\ H_{12}^s \end{pmatrix} = \begin{pmatrix} -\sqrt{D}x_2 \\ \sqrt{D}x_1 \end{pmatrix}.$$

As in Chapter 4, the relationship between the Itô and Stratonovich forms can be equated by observing that

$$H_{ij} = H_{ij}^s \quad \text{and} \quad h_i = h_i^s + \frac{1}{2}\sum_{k=1}^{d}\sum_{j=1}^{m}\frac{\partial H_{ij}}{\partial x_k}H_{kj}. \tag{17.64}$$

Therefore, we can drop the superscript s on H_{ij} (but not on h_i^s!).

Both can only be true simultaneously if (17.64) reduces to $\mathbf{h}^s = \mathbf{h}$, which can happen in some special cases but does not usually. Is that the case here? In this case, $m = 1$, and from (17.64),

$$\begin{aligned}\frac{1}{2}\sum_{k=1}^{d}\sum_{j=1}^{m}\frac{\partial H_{ij}}{\partial x_k}H_{kj} &= \frac{1}{2}\sum_{k=1}^{2}\frac{\partial H_{i1}}{\partial x_k}H_{k1}\\ &= \frac{1}{2}\frac{\partial H_{i1}}{\partial x_1}H_{11} + \frac{1}{2}\frac{\partial H_{i1}}{\partial x_2}H_{21}.\end{aligned}$$

Thus,

$$\frac{1}{2}\frac{\partial H_{11}}{\partial x_1}H_{11} + \frac{1}{2}\frac{\partial H_{11}}{\partial x_2}H_{21} = \frac{1}{2}\cdot 0 + \frac{1}{2}(-\sqrt{D})\sqrt{D}x_1 = -\frac{1}{2}Dx_1.$$

$$\frac{1}{2}\frac{\partial H_{21}}{\partial x_1}H_{11} + \frac{1}{2}\frac{\partial H_{21}}{\partial x_2}H_{21} = \frac{1}{2}\sqrt{D}(-\sqrt{D}x_2) + \frac{1}{2}\cdot 0 = -\frac{1}{2}Dx_2.$$

What this means is that the Itô SDEs that correspond to our Stratonovich SDEs (17.62) are

$$dx_1 = (h - D\,x_1/2)\,dt - \sqrt{D}\,x_2\,dw \quad \text{and} \quad dx_2 = (-D\,x_2/2)\,dt + \sqrt{D}\,x_1\,dw. \tag{17.65}$$

The Itô and Stratonovich SDEs are not the same in Cartesian coordinates, and one would not expect them to be the same in polar coordinates either. Below we investigate the polar coordinate version.

Stratonovich SDEs transform easily under changes of coordinates. In particular, if we want to represent (17.62) in polar coordinates, then we can simply differentiate the expressions $x = r\cos\theta$ and $y = r\sin\theta$ and substitute into (17.62) to give

$$dr\,\cos\theta - r\,d\theta\,\sin\theta = h\,dt - \sqrt{D}\,x_2 \circledS\, dw, \tag{17.66}$$

$$dr\,\sin\theta + r\,d\theta\,\cos\theta = \sqrt{D}\,x_1 \circledS\, dw. \tag{17.67}$$

Isolating dr and $d\theta$ then gives the SDE

$$\begin{bmatrix} dr \\ d\theta \end{bmatrix} = \begin{bmatrix} h\cos\theta \\ -\dfrac{h\sin\theta}{r} \end{bmatrix} dt - \begin{bmatrix} 0 \\ \sqrt{D} \end{bmatrix} \circledS\, dw. \tag{17.68}$$

Note that if the negative sign in front of the noise term is flipped to a positive sign, then the Fokker–Planck equation will be exactly the same. Additionally, note that since in polar coordinates, the factor multiplying the noise is independent of r and θ and that $|G|^{\frac{1}{2}} = r$ is not a function of θ (and therefore in the Fokker–Planck equation, r only multiplies terms inside of $\partial^2/\partial\phi^2$), the Itô and Stratonovich forms of the Fokker–Planck equation will be exactly the same in polar coordinates.

Substituting this into the general Stratonovich form of the Fokker–Planck equation with $|G| = r$ gives

$$\boxed{\frac{\partial \tilde{f}}{\partial t} = -h(t)\cos\phi \frac{\partial \tilde{f}}{\partial r} + h(t)\frac{\sin\phi}{r}\frac{\partial \tilde{f}}{\partial \phi} + \frac{D}{2}\frac{\partial^2 \tilde{f}}{\partial \phi^2}.} \tag{17.69}$$

Alternatively, substituting (17.62) into the Stratonovich form of the Fokker–Planck equation in (17.63) (or equivalently, (17.65) into the Itô form of the Fokker–Planck equation) gives

$$\frac{\partial f}{\partial t} = -h(t)\frac{\partial f}{\partial x} + \frac{D}{2}\left[x_2^2\frac{\partial^2 f}{\partial x_1^2} + x_1^2\frac{\partial^2 f}{\partial x_2^2} - x_2\frac{\partial}{\partial x_1}\left(x_1\frac{\partial f}{\partial x_2}\right) - x_1\frac{\partial}{\partial x_2}\left(x_2\frac{\partial f}{\partial x_1}\right)\right]. \tag{17.70}$$

This can be simplified as

$$\boxed{\frac{\partial f}{\partial t} = -h(t)\frac{\partial f}{\partial x} + \frac{D}{2}\left(y\frac{\partial}{\partial x} - x\frac{\partial}{\partial y}\right)^2 f.} \tag{17.71}$$

If we want to convert to polar coordinates $x = r\cos\phi$ and $y = r\sin\phi$, $f(x,y;t) = \tilde{f}(r,\phi;t)$, then

$$\frac{\partial f}{\partial x} = \cos\phi\frac{\partial \tilde{f}}{\partial r} - \frac{\sin\phi}{r}\frac{\partial \tilde{f}}{\partial \phi} \quad \text{and} \quad \frac{\partial f}{\partial y} = \sin\phi\frac{\partial \tilde{f}}{\partial r} + \frac{\cos\phi}{r}\frac{\partial \tilde{f}}{\partial \phi}.$$

Therefore,

$$\left(y\frac{\partial}{\partial x} - x\frac{\partial}{\partial y}\right) f = -\frac{\partial \tilde{f}}{\partial \phi} \quad \text{and} \quad \left(y\frac{\partial}{\partial x} - x\frac{\partial}{\partial y}\right)^2 f = \frac{\partial^2 \tilde{f}}{\partial \phi^2}.$$

We conclude that (17.71) can be written as (17.69). In [121], the author and collaborators presented a group-Fourier-transform method for solving (17.53), (17.69), and (17.71) numerically. This is because these equations can be written in an invariant way in terms of the differential operators $\tilde{E}_i^r$ for $SE(2)$, and the corresponding operational properties can be applied. The equations derived here will be revisited in Chapter 20 in the context of more general stochastic flows on Lie groups.

The next section addresses a very different set of problems in the transmission of information via wave motion that also draw on the theory of Lie groups.

17.7 Soliton Geometry and the Mechanics of Communication

Given a function $f \in \mathcal{N}(\mathbb{R})$, traveling waves are of the form $f(x-ct)$, where $c \in \mathbb{R}$ is the wave speed. These traveling waves can be viewed as solutions to *linear* wave equations (which are similar to the telegraph equation without diffusion/attenuation terms). In contrast, solitons are self-reinforcing traveling waves that are governed by *nonlinear* PDEs. Examples include waves that propagate in shallow water and smoke rings. The soliton phenomenon was first described by a naval engineer named John Scott Russell, who observed such waves in the Union Canal in Scotland in 1834. The name "soliton" was introduced by Zabusky and Kruskal in the context of plasmas in 1965 [129].

Unlike solutions to the (linear) telegraph equation, in which an initial pulse attenuates, solitons can exhibit persistence in wave shape and constancy of wave speed over significant distances and times. Perhaps this is why smoke signals were used from ancient times until the 1800s to visually relay information over long distances. In modern times, the use of solitons implemented as pulses of light traveling in fiber optic communication systems have been investigated. This technology, although not currently in use in commercial systems, may have applications in the future.

This section begins with a brief review of the most common nonlinear equations that give rise to solitons. Then the relationship between Lie groups and the sorts of solitons observed in optical fibers is explored. A connection between differential geometry of curves in $\mathbb{R}^3$ and vortex filaments (such as smoke rings) that are governed by the same nonlinear pde as solitons in fiber optic cables is then reviewed. Finally, additional connections between solitons and the differential geometry of surfaces are reviewed.

17.7.1 Traveling Wave Solutions of Some Nonlinear PDEs

A famous nonlinear PDE that admits traveling wave solutions (soliton) is the *Korteweg–deVries (or KdV) equation*[13]

$$\frac{\partial u}{\partial t} + 6u\frac{\partial u}{\partial x} + \frac{\partial^3 u}{\partial x^3} = 0. \tag{17.72}$$

It has solutions of the form[14]

$$u(x,t) = \frac{c}{2}\operatorname{sech}^2\left[\frac{\sqrt{c}}{2}(x-ct)\right], \quad \text{where } \operatorname{sech} z = \frac{2}{e^z + e^{-z}}.$$

The graph of the hyperbolic secant function, $\operatorname{sech} z = (\cosh z)^{-1}$, looks somewhat like a Gaussian distribution. The KdV equation can be derived from first principles of fluid mechanics, as is done in [72].

Another famous equation is the *sine–Gordon equation.*[15] In the literature, this is written in two equivalent forms:

$$\frac{\partial^2 u}{\partial x^2} - \frac{\partial^2 u}{\partial t^2} = \sin u \qquad \text{and} \qquad \frac{\partial^2 u'}{\partial x' \partial t'} = \sin u' \tag{17.73}$$

where $u(x,t) = u'(x',t')$ and

$$x' = \frac{1}{2}(x+t) \qquad \text{and} \qquad t' = \frac{1}{2}(x-t). \tag{17.74}$$

Solitons of the form

$$u(x,t) = 4\tan^{-1}\left[a\,\exp\!\left(\frac{x-ct}{\sqrt{1-c^2}}\right)\right]$$

exist for appropriate choices of a and c [72].

[13] Replacing the number 6 with the number 1 in this equation changes $c/2$ to $3c$ in the solution that is given here.

[14] It is left as an exercise to check what values of $c \in \mathbb{R}_{>0}$ will work.

[15] The name “Sine-Gordon” is a play on words resulting from the fact that this equation has a similar appearance to the (linear) “Klein–Gordon” equation in which the right-hand side would be u rather than $\sin u$.

17.7.2 Lie-Group Invariance and Optical Solitons

Solitons in optical fibers are governed by the nonlinear Schrödinger equation [50, 81]

$$-i\frac{\partial u}{\partial x} = \frac{1}{2}\frac{\partial^2 u}{\partial t^2} + |u|^2 u. \tag{17.75}$$

This equation can be derived from Maxwell's laws as in [50].[16] A fundamental solution to this equation is of the form [81]

$$u_f(x,t) = e^{ix/2}\operatorname{sech} t.$$

Starting with this fundamental solution, it becomes clear immediately that given constants κ, σ, η, and t_0, each of the following four transformations also produces a solution:

$$\begin{gathered}(T_1(t_0)u_f)(x,t) = u_f(x, t-t_0),\\ (T_2(\sigma)u_f)(x,t) = u_f(x-2\sigma, t) = e^{-i\sigma}u_f(x,t),\\ (T_3(\kappa)u_f)(x,t) = u_f([1-\kappa^2]x - 2\kappa t, t+\kappa x) = \exp\left[-i(\kappa t + \frac{1}{2}\kappa^2 x)\right] u_f(x, t+\kappa x),\\ (T_4(\eta)u_f)(x,t) = \eta\, u_f(\eta^2 x, \eta t).\end{gathered}$$

Each transformation above can be iterated to yield $(T_i(\alpha)T_i(\alpha')u_f)(x,t) = (T_i(\alpha\circ\alpha')u_f)(x,t)$, and so each forms a one-dimensional (and hence Abelian) group. These groups are respectively $G_1 = (\mathbb{R}, +)$, $G_2 = SO(2)$, $G_3 = (\mathbb{R}, +)$, and $G_4 = (\mathbb{R}_{>0}, \cdot)$. Combining these transformations results in a four-parameter family of new solutions of (17.75) of the form [50]

$$\begin{aligned}(T(\kappa,\sigma,\eta,t_0)u_f)(x,t) &\doteq \eta\, u_f([\eta^2-\kappa^2]x - 2[\kappa t+\sigma], \eta[t+\kappa x - t_0])\\ &= \eta \exp\left[-i\kappa t + \frac{i}{2}(\eta^2-\kappa^2)x - i\sigma\right]\operatorname{sech}\,[\eta(t+\kappa x - t_0)].\end{aligned} \tag{17.76}$$

Clearly, $T_1(t_0) = T(0,0,1,t_0)$, $T_2(\sigma) = T(0,\sigma,1,0)$, $T_3(t_0) = T(\kappa,0,1,0)$, and $T_4(t_0) = T(0,0,\eta,0)$. Moreover, concatenating $T(\kappa,\sigma,\eta,t_0)$ and $T(\kappa',\sigma',\eta',t_0')$ defines a binary operation for this four-parameter set of transformations. Due to the separability of $u_f(x,t)$ and the fact that the x dependence is unimodular, this means that $|(T(\kappa,\sigma,\eta,t_0)u_f)(x,t)|$ has the form of a traveling wave.

17.7.3 Vortex Filaments and the Nonlinear Schrödinger equation

The nonlinear Schrödinger equation that appeared above in the context of solitons in optical fiber communications also appears in the study of vortex filaments in fluid mechanics. Indeed, the fluids scenario in which these equations arise came first (see, e.g., [24]). A vortex filament is a curve around which fluid circulates, such as the centerline of a tornado or the moving circle around which a smoke ring rolls). In addition to moving rigidly, this curve can change shape over time. This shape change results from self-induced changes in vorticity (i.e., if the filament is curved, the circulations around the tangents at two different values of arc length will interact). This is governed by the law of Biot-Savart [72].

[16] The appearance of this equation is somewhat similar to the (linear) Schrödinger equation of quantum mechanics, although (17.75) has purely classical origins.

If $\mathbf{x}(s,t)$ denotes this time-evolving arc-length-parameterized curve describing a time-evolving vortex filament, certain kinematic conditions apply and can be described using the Frenet–Serret apparatus discussed in Chapter 5—namely it can be shown that [99]

$$\frac{\partial \mathbf{x}}{\partial s} = \mathbf{u} \quad \text{and} \quad \frac{\partial \mathbf{x}}{\partial t} = \kappa \mathbf{n}_2,$$
$$\frac{\partial \kappa}{\partial t} = -2\tau \frac{\partial \kappa}{\partial s} - \kappa \frac{\partial \tau}{\partial s},$$
$$\frac{\partial \tau}{\partial t} = \frac{\partial}{\partial s}\left(-\tau^2 + \frac{1}{\kappa}\frac{\partial^2 \kappa}{\partial s^2} + \frac{1}{2}\kappa^2\right).$$

The above equations were derived and used by Hasimoto [51] together with the transformations

$$q(s,t) = \kappa(s,t)\,\exp\left[i\int_{s_0}^{s} \tau(s',t)\,ds'\right]$$

and

$$u(s,t') = q(s,t')\,\exp\left[i\int_{0}^{t'} \left(-\tau^2 + \frac{1}{\kappa}\frac{\partial^2 \kappa}{\partial s^2} + \frac{1}{2}\kappa^2\right)\Bigg|_{s=s_0} dt\right]$$

to yield a version of (17.75) with rescaled arguments. When $\frac{\partial \tau}{\partial t}\big|_{s=s_0} = 0$, $u(s,t) = q(s,t)$. Since curvature and torsion completely specify the shape of a space curve and since these can be recovered from $q(s,t)$ as

$$\kappa(s,t) = |q(s,t)| \quad \text{and} \quad \tau(s,t) = \frac{\partial}{\partial s}[\mathrm{Atan2}(\mathrm{Re}(q(s,t)), \mathrm{Im}(q(s,t))],$$

it follows that the time-evolving shape of a vortex filament can be determined by solving (17.75). The explicit form of the resulting $\mathbf{x}(s,t)$ is given in [99] together with plots under different conditions.

17.7.4 Bäcklund Transformations

As seen previously in this section, differential-geometric tools play an important role in the analysis of the nonlinear PDEs that admit solitons as solutions. A number of works employ Bäcklund (also called Lie–Bäcklund) transformations to study such equations. A Bäcklund transformation is a change of coordinates of a parametric surface that produces a new surface with some conserved geometric quantity (such as mean or Gaussian curvature). For example, the change of coordinates in (17.74) in the context of the sine–Gordon equation is a kind of Bäcklund transformation that makes it easier to identify solitions. The study of transformations of surfaces (and, more recently, transformations of manifolds) has roots that are more than a century old, with mathematicians such as Bianchi and Darboux having made seminal contributions. Since books such as [5, 99] discuss Bäcklund transformations and their applications to solitons in detail and other books such as [60] use properties of exterior algebras (wedge products, etc.) to study these nonlinear pdes, there is no need to do so here. However, it is worth mentioning that the relevance of these geometric tools to communication lies in the properties of solitions to persist in shape and speed in contexts where linear modes of information transfer may have difficulties. For example, it has been hypothesized that crickets chirping is a form of vortex-ring communication [55].

The topics discussed in this section are only a few of the many possible connections between soliton geometry and the mechanics of communication. Classic references on solitons include [26, 71, 111], and these may provide insights into future research at the interface of geometry, transformation groups, and information theory.

17.8 Chapter Summary

This chapter has served as an introduction to the engineering side of information theory (i.e., the mathematical theory of communication and coding). The concept of discrete entropy and its relationship to Shannon's theorems on the rate of information that can be transmitted through a noisy channel were reviewed. Recent work on connections between information inequalities and the structure of finite groups was reviewed. Natural connections between the theory of communication and SDEs exist [93]. Moreover, references to classical continuous channels with Gaussian noise and the associated rate-distortion theory were provided, but a detailed discussion is postponed until Chapter 21, where this theory is generalized to the geometric setting of Lie groups and principal bundles. This chapter also illustrated Lie groups enter in some applications (e.g., the telegraph and soliton equations) as symmetry operators that define the physical properties of continuous communication channels. Lie groups also can serve as the continuous domains over which the the communicated signal and noise propagate (e.g., the case of laser phase noise). Laser phase noise and solitons are examples of information theory interacting with the geometric/physical world. Additionally, Lie groups arise in these contexts in very natural ways. This chapter also provided pointers to the literature such as [43, 66], in which the transmission of messages through waveguides with random inhomogeneities is related to Brownian motion in the Lobachevsky plane, which is a homogeneous space.

Therefore, this chapter can be viewed as a bridge between the stochastic processes in continuous space studied in Volume 1 (which had very little to do with group theory) and the discrete-group-theoretic problems that arise in classical coding and communications theory. The sorts of problems that will be addressed later in this volume, which are almost exclusively focused on physical/geometric problems involving continuous information theory and Lie groups, will draw heavily on this chapter.

A popular area of modern information theory is concerned with issues in wireless communications. References to this literature include [1, 37, 40, 94]. And random matrix theory has been shown to be a useful tool in the context of wireless communication networks in [38, 52, 53, 95, 103, 106, 119].

For further reading on various aspects of classical and modern information theory, see [7, 10, 30, 32, 45, 48, 68–70, 79, 87, 91, 98, 101, 116, 122].

For connections between information theory (including quantum information theory) and geometry see [9, 11, 57, 83, 100, 107]. Other topics that bring together methods from group theory, geometry, and information theory include different aspects of modern imaging [123, 124].

17.9 Exercises

17.1. Given sets E_1, E_2, and E_3, which of the following are true?

$$\begin{aligned}(E_1 \cap E_2) \cup (E_2 \cap E_3) &= (E_1 \cup E_2) \cap E_3,\\ E_1 \cup (E_2 \cup E_3) &= (E_1 \cup E_2) \cup E_3,\\ E_1 \cap (E_2 \cap E_3) &= (E_1 \cap E_2) \cap E_3,\\ E_1 \cup (E_2 \cap E_3) &= (E_1 \cup E_2) \cap E_3,\\ (E_1 \cap E_2) \cup (E_2 \cap E_3) &= E_1 \cap (E_2 \cup E_3) \cap E_3.\end{aligned}$$

17.2. Use the same reasoning as in the derivation of (17.6) to prove that

$$p(E_1 \cap E_2 \cap E_3 \cap E_4) = p(E_1 \mid E_2 \cap E_3 \cap E_4)\, p(E_2 \mid E_3 \cap E_4)\, p(E_3 \mid E_4)\, p(E_4).$$

17.3. Prove the inequalities in (17.14).

17.4. Prove the equality in (17.16).

17.5. Prove the inequality in (17.17).

17.6. Prove the inequalities in (17.18).

17.7. If $\Phi_i : \mathbb{R} \to \mathbb{R}$ for $i = 1, 2$ are convex functions, will the composed function $\Phi_1 \circ \Phi_2$ be convex also?

17.8. If H and K are subgroups of G, prove that $H \cap K$ is also a subgroup of G.

17.9. If H and K are subgroups of G, prove that HK is a subgroup of G if and only if $HK = KH$.

17.10. Is the mapping defined in (17.46) invertible?

17.11. Show that $D_{JS}(p\|q)$ defined in (17.22) can be computed as

$$D_{JS}(p\|q) = S((p+q)/2) - \frac{1}{2}S(p) - \frac{1}{2}S(q),$$

where $S(p)$ is the Shannon entropy of $p = \{p_1, \ldots, p_n\}$.

17.12. (a) Show that the function $\psi(x) \doteq \log[2/(1+e^{-x/2})]$ is concave and $\psi(x) \leq x/4$. (b) Using these facts, prove (17.23) (as in [21]). (c) Split the Jensen–Shannon divergence into two parts as was done in [113] and prove that [21]

$$D_{KL}(p\|(p+q)/2) \leq \log\left[\frac{2}{1+\exp(-D_{KL}(p\|q))}\right].$$

17.13. Is

$$d(X,Y) \doteq H(X|Y) + H(Y|X)$$

a metric?

Hint: See [22].

17.14. Verify (17.42).

17.15. Parameterize the group $SU(1,1)$ with elements defined in (17.41) and compute Jacobian matrices and the volume element. Is this a unimodular Lie group?

17.16. Work out the details of the stereographic projection that maps the upper sheet of the hyperboloid of two sheets in (17.45) to the unit disk. Using the methods of Chapter 5, compute the metric tensor for the hyperboloid of two sheet embedded in $\mathbb{R}^3$ defined in (17.45) using the coordinates (x, y). How does this compare with (17.43)? How are (x, y) and (x_1, x_2) related?

References

1. Alamouti, S.M., “A simple transmit diversity technique for wireless communications,” *IEEE J. Select Areas Commun.*, 16(8), p. 1451, 1998.

2. Ali, S.M., Silvey, S.D.,“A general class of coefficients of divergence of one distribution from another,” *J. R. Statist. Soc. B*, 28(1), pp. 131–140, 1966.
3. Ambroladze, A., Wallin, H., “Random iteration of Möbius transformations and Furstenberg’s theorem,” *Ergodic Theory Dynam. Syst.*, 20(4), pp. 953–962, 2000.
4. Anderson, J.W., *Hyperbolic Geometry*, 2nd ed., Springer, New York, 2005
5. Anderson, R.L., Ibragimov, N.H., *Lie-Bäcklund Transformations in Applications*, SIAM, Philadelphia, 1987.
6. Arnold, D.N., Rogness, J., “Möbius transformations revealed,” *Notices AMS*, 55(10), pp. 1226–1231, 2008.
7. Ash, R.B., *Information Theory*, John Wiley and Sons, New York, 1965 (Dover edition, 1990).
8. Azizoglu, M., Humblet, P.A., “Envelope detection of orthogonal signals with phase noise,” *J. Lightwave Technol.*, 9, pp. 1398–1410, 1991.
9. Bachoc, C., Ben-Haim, Y., Litsyn, S., “Bounds for codes in products of spaces, Grassmann and Stiefel manifolds,” *IEEE Trans. Inform. Theory*, 54(3), pp. 1024–1035, 2008.
10. Balakrishnan, A.V., *Communication Theory*, McGraw-Hill Book Company, New York, 1968.
11. Barg, A., Nogin, D.Yu., “Bounds on packings of spheres in the Grassmann manifold,” *IEEE Trans. Inform. Theory*, 48(9), pp. 2450–2454, 2002.
12. Barry, J.R., Lee, E.A., “Performance of coherent optical receivers”, *Proc. IEEE*, 78(8), pp. 1369–1394, 1990.
13. Bluman, G.W., Temuerchaolu, Sahadevan, R., “Local and nonlocal symmetries for nonlinear telegraph equation,” *J. Math. Phys.*, 46, 023505, 2005.
14. Bluman, G., Temeuerchaolu, “Conservation laws for nonlinear telegraph equations,” *J. Math. Anal. Appl.*, 310, pp. 459–476, 2005.
15. Bluman, G., Temuerchaolu, “Comparing symmetries and conservation laws of nonlinear telegraph equations,” *J. Math. Phys.*, 46, 073513, 2005.
16. Bond, D.J., “The statistical properties of phase noise,” *Br. Telecom. Technol. J.*, 7(4), pp. 12–17, 1989.
17. Chan, T.H., Yeung, R.W., “On a relation between information inequalities and group Theory,” *IEEE Trans. Inform. Theory*, 48(7), JULY 2002, pp. 1992–1995.
18. Chan, T.H., “Group characterizable entropy functions,” *ISIT2007*, Nice, France, June 24–29, 2007, pp. 506–510.
19. Chirikjian, G.S., Kyatkin, A.B., *Engineering Applications of Noncommutative Harmonic Analysis*, CRC Press, Boca Raton, FL, 2001.
20. Cover, T.M., Thomas, J.A., *Elements of Information Theory*, John Wiley and Sons, New York, 2006.
21. Crooks, G.E., “Inequalities between the Jenson–Shannon and Jeffreys divergences,” http://threeplusone.com/pubs/technote/CrooksTechNote004.pdf.
22. Crutchfield, J., “Information and its metric,” in *Nonlinear Structures in Physical Systems—Pattern Formation, Chaos and Waves*, L. Lam, and H. Morris, eds., pp. 119–130. Springer-Verlag, New York, 1990.
23. Csiszár, I., “Information-type measures of difference of probability distributions and indirect observation,” *Studia Sci. Math. Hungary.*, 2, pp. 229–318, 1967.
24. Da Rios, L.S., “Sul moto d’un liquido indefinito con un filetto vorticoso,” *Rend. Circ. Mat. Palermo*, 22, pp. 117–135, 1906.
25. De Marchis, G., “Coherent communications,” *Fiber Integrated Optics*, 11, pp. 277–317, 1992.
26. Drazin, P.G., Johnson, R.S., *Solitons: An Introduction*, 2nd ed., Cambridge University Press, Cambridge, 1989.
27. Endres, D.M., Schindelin, J.E., “A new metric for probability distributions,” *IEEE Trans. Inform. Theory*, 49(7), pp. 1858–1860, 2003.
28. Escolano, F., Suau, P., Bonev, B., *Information Theory in Computer Vision and Pattern Recognition*, Springer, New York, 2009.

29. Fabeck, G., Mathar, R., "Chernoff information-based optimization of sensor networks for distributed detection," in *Proceedings of the IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, pp. 606–611, December 14–17, 2009.
30. Fano, R.M., *Transmission of information: a statistical theory of communications*, MIT Press, Cambridge, MA, 1961.
31. Farlow, S.J., *Partial Differential Equations for Scientists and Engineers*, Dover, New York, 1993.
32. Feinstein, A., "A new basic theorem of information theory," *IEEE Trans. Inform. Theory*, 4(4), pp. 2–22, 1954.
33. Field, T.R., Tough, R.J.A., "Diffusion processes in electromagnetic scattering generating K-distributed noise," *Proc. R. Soc. London A*, 459, pp. 2169–2193, 2003.
34. Foschini, G.J., Greenstein, L.J., Vannucci, G., "Noncoherent detection of coherent lightwave signals corrupted by phase noise," *IEEE Trans. Commun.*, 36, pp. 306–314, 1988.
35. Foschini, G.J., Vannucci, G.,"Characterizing filtered light waves corrupted by phase noise," *IEEE Trans. Inform. Theory*, 34(6), pp. 1437–1448, 1988.
36. Foschini, G.J., Vannucci, G., Greenstein, L.J., "Envelope statistics for filtered optical signals corrupted by phase noise," *IEEE Trans. Commun.*, 37(12), pp. 1293–1302, 1989.
37. Foschini, G., Gans, M., "On limits of wireless communications in fading environment when using multiple antennas," *Wireless Personal Commun.*, 6(6), pp. 315–335, 1998.
38. Franceschetti, M., Meester, R., *Random Networks for Communication: From Statistical Physics to Information Systems*, Cambridge University Press, Cambridge, 2007.
39. Furstenberg, H., *Random Walks and Discrete Subgroups of Lie Groups*, Advances in Probability and Related Topics Vol. 1, Marcel Dekker, New York, 1971, pp. 1–63.
40. Furstenberg, H., "Boundary theory and stochastic processes on homogeneous spaces," in *Harmonic Analysis on Homogeneous Spaces*, Proc. Symp. Pure. Math. Vol. XXVI, Williams College, pp. 193–229, American Mathematical Soc. Providence, RI, 1973.
41. Garrett, I., Jacobsen, G., "Phase noise in weakly coherent systems," *IEEE Proc.*, 136, Pt. J, pp. 159–165, 1989.
42. Garrett, I., Bond, D.J., Waite, J.B., Lettis, D.S.L., Jacobsen, G., "Impact of phase noise in weakly coherent systems: a new and accurate approach," *J. Lightwave Technol.*, 8(3), pp. 329–337, 1990.
43. Gertsenshtein, M.E., Vasil'ev, V.B., "Waveguides with random inhomogeneities and Brownian motion in the Lobachevsky plane," *Theory Prob. Appl.*, 4(4), pp. 391–398, 1959.
44. Gertsenshtein, M.E., Vasilev, V.B., "Diffusion equations for statistically inhomogeneous waveguides," *Radiotekhn. Electron., IV*, 4, p. 611, 1959. (English translation, Radio Engineering and Electronics).
45. Gray, R.M., *Entropy and Information Theory*, 2nd ed., Springer-Verlag, New York, 2011.
46. Gromov, M., *Hyperbolic Groups: Essays in Group Theory*, pp. 75–263, Springer, New York, 1987.
47. Hammer, D., Romashchenko, A., Shen, A., Vereshchagin, N., "Inequalities for Shannon entropy and Kolmogorov complexity," *J. Comput. Syst. Sci.*, 60, pp. 442–464, 2000.
48. Hamming, R.W., *Coding and Information Theory*, 2nd ed., Prentice-Hall, Englewood Cliffs, NJ, 1986.
49. Hartley, R., "Transmission of information," *Bell Syst. Tech. J.*, pp. 535–563, 1928.
50. Hasegawa, A., Matsumoto, M., *Optical Solitons in Fibers*, 3rd ed., Springer, New York, 2003.
51. Hasimoto, H., "A soliton on a vortex filament," *J. Fluid Mech.*, 51, pp. 477–485, 1972.
52. Hassibi, B., Marzetta, T.L., "Multiple-antennas and isotropically-random unitary inputs: The received signal density in closed-form," *IEEE Trans. Inform. Theory*, 48(6), pp. 1473–1484, 2002.
53. Hassibi, B., "Random Matrices, Integrals and Space-time Systems," *DIMACS Workshop on Algebraic Coding and Information Theory*, December 15–18, 2003.
54. Hayashi, M., *Quantum Information: An Introduction*, Springer, Berlin, 2006.

55. Heinzel, H.-G., Dambach, M., "Travelling air vortex rings as potential communication signals in a cricket," *J. Comp. Physiol. A: Neuroethol., Sensory Neural Behav. Physiol.*, 160(1), pp. 79–88, 1987.
56. Helgason, S., *Groups and Geometric Analysis*, Mathematical Surveys and Monographs Vol. 83, American Mathematical Society, Providence, RI, 1984.
57. Hendricks, H., "A Cramér–Rao type lower bound for estimators with values in a manifold," *J. Multivariate Anal.*, 38, pp. 245–261, 1991.
58. Henry, C.H., "Theory of linewidth of semiconductor lasers," *IEEE J. Quantum Electron.*, pp. 259–264, 1982.
59. Herstein, I.N., *Topics in Algebra*, John Wiley and Sons, New York, 1975.
60. Hirota, R., *The Direct Method in Soliton Theory*, Cambridge University Press, Cambridge, 2004.
61. Ikeda, N., Matsumoto, H., "Brownian motion on the hyperbolic plane and Selberg trace formula," *J. Funct. Analy.*, 163(1), pp. 63–110, 1999.
62. Ingleton, A.W., "Representation of matroids," in *Combinatorial mathematics and Its Applications*, D. Welsh, ed., pp. 149–167. Academic Press, London, 1971.
63. Jacobsen, G., *Noise in Digital Optical Transmission Systems*, Artech House, Boston, 1994.
64. Janssen, A., Siebert, E., "Convolution semigroups and generalized telegraph equations," *Math. Zeitschr.,* 177(4), pp. 519–532, 1981.
65. Jones, D.S., *Elementary Information Theory*, Clarendon Press, Oxford, England, 1979.
66. Karpelevich, F.I., Tutubalin, V.N. and Shur, M.G. "Limit theorems for the composition of distributions in the Lobachevsky plane and space," *Theory Probab. Appl.*, 4(4), pp. 399–401, 1959.
67. Kazovsky, L.G., Benedetto, S., Willner, A.E., *Optical Fiber Communication Systems*, Artech House, Boston, 1996.
68. Kolmogorov, A.N., "Logical basis for information theory and probability theory," *IEEE Trans. Inform. Theory*, 14(5), pp. 662–664, 1968.
69. Kolmogorov, A.N., "Three approaches to the definition of the concept quantity of information," *Probl. Peredachi Inf.*, 1(1), p. 3–11, 1965.
70. Kornreich, P., *Mathematical Models of Information and Stochastic Systems*, CRC Press/Taylor and Francis, Boca Raton, FL, 2008.
71. Lamb, G.L. Jr., "Solitons on moving space curves," *J. Math. Phys.*, 18, pp. 1654–1661, 1977.
72. Lamb, G.L. Jr., *Elements of Soliton Theory*, John Wiley and Sons, New York, 1980.
73. Leach, P.G.L., "Symmetry and singularity properties of a system of ordinary differential equations arising in the analysis of the nonlinear telegraph equations," *J. Math. Anal. Applic.*, 336(2), pp. 987–994, 2007.
74. Lee, J.M., *Riemannian Manifolds: An Introduction to Curvature*, Springer, New York, 1997.
75. Li, H., Chong, E.K.P., "On connections between group homomorphisms and the Ingleton inequality," *ISIT2007*, Nice, France, June 24–29, 2007, pp. 1996–1999.
76. Li, H., Chong, E.K.P., "On a connection between information and group lattices," *Entropy*, 13(3), pp. 683–708, 2011.
77. Liese, F., Vajda, I. "On divergences and informations in statistics and information theory," *IEEE Trans. Inform. Theory*, 52(10), pp. 4394–4412, 2006.
78. Linke, R.A., Henry, P.S., "Coherent optical detection: A thousand calls on one circuit," *IEEE Spetrum*, 24(2), pp. 52–57, 1987.
79. MacKay, D.J.C., *Information Theory, Inference, and Learning Algorithms*, Cambridge University Press, Cambridge, 2003.
80. Miller, G.A., "Groups which are the products of two permutable proper sub-groups," *PNAS*, 21, pp. 469–472, 1935.
81. Mollenauer, L.F., Gordon, J.P., *Solitons in Optical Fibers*, Elsevier Academic Press, Amsterdam, 2006.
82. Nehari, Z., *Conformal Mapping*, Dover Publications, New York, 1975 (original published by McGraw Hill, 1952).

83. Nielsen, M.A., Chuang, I.L., *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
84. Nordbrock, U., Kienzler, R., "Conservation laws—a simple application to the telegraph equation," *J. Comput. Electron.*, 7(2), pp. 47–41, 2008.
85. Nikulin, V.V., Shafarevich, I.R., *Geometries and Groups*, M. Reid, transl., Springer, New York, 2009.
86. Nyquist, H., "Certain factors affecting telegraph speed," *Bell Syst. Tech. J.*, 3, pp. 324–346, 1924
87. Nyquist, H., "Certain topics in telegraph transmission theory," *AIEE Trans.*, 47, pp. 617–644, 1928.
88. Ody, M.S., Common, A.K., Sobhy, M.I., "Continuous symmetries of the discrete nonlinear telegraph equation," *Eur. J. Appl. Math.*, 10(3), pp. 265–284, 1999.
89. Österreicher, F., Vajda, I., "A new class of metric divergences on probability spaces and its applicability in statistics," *Ann. Inst. Statist. Math.*, 55(3), pp. 639–653, 2003.
90. Papanicolaou, G.C., "Wave propagation in a one-dimensional random medium," *SIAM J. Appl. Math.*, 21, pp. 13–18, 1971.
91. Pierce, J.R., *An Introduction to Information Theory: Symbols, Signals and Noise*, 2nd ed., Dover Publications, New York, 1980.
92. Pinsky, M.A., *Introduction to Partial Differential Equations with Applications*, McGraw-Hill Book Company, New York, 1984.
93. Primak, S., Kontorovich, V., Lyandres, V., *Stochastic Methods and Their Applications to Communications*, John Wiley and Sons, New York, 2004.
94. Rappaport, T.S., *Wireless Communications Principles and Practice*, 2nd ed., Prentice Hall, Upper Saddle River, New Jersey, 2002.
95. Ratnarajah, T., Vaillancourt, R., Alvo, M., "Complex random matrices and Rayleigh channel capacity," *Commun. Inform. Syst.*, pp. 119–138, 2003.
96. Ren, W., Beard, R., Atkins, E., "Information consensus in multivehicle cooperative control," *IEEE Control Syst. Mag.*, pp. 71–82, 2007.
97. Rényi, A., "On measures of information and entropy," *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability 1960*, pp. 547–561, 1961.
98. Reza, F.M., *An Introduction to Information Theory*, Dover Publications, New York, 1994 (originally published by McGraw-Hill, 1961).
99. Rogers, C., Schief, W.K., *Bäcklund and Darboux Transformations: Geometry and Modern Applications in Soliton Theory*, Cambridge University Press, Cambridge, 2002.
100. Scharf, L.L., McWhorter, L.T., "Geometry of the Cramer–Rao bound," *Signal Process.* 31(3), pp. 1–11 (1993); reprinted in *Bayesian Bounds for Parameter Estimation and Nonlinear Filtering/Tracking*, H.L. Van Trees and K. Bell, eds., John Wiley and Sons, New York, 2007.
101. Scharf, L.L., *Statistical Signal Processing: Detection, Estimation, and Time Series Analysis*, Addison-Wesley, New York, 1990.
102. Seshadri, R., Na, T.Y., *Group Invariance in Engineering Boundary Value Problems*, Springer-Verlag, New York, 1985.
103. Sengupta, A.M., Mitra, P.P., "Capacity of multivariate channels with multiplicative noise: I. Random matrix techniques and large-N expansions for full transfer matrices," http://arxiv.org/abs/physics/0010081.
104. Shannon, C.E., Weaver, W., *The Mathematical Theory of Communication*, The University of Illinois Press, Urbana, 1949.
105. Shannon, C.E., "Communication in the presence of noise," *Proc. Inst. Radio Eng.*, 37(1), pp. 10–21, 1949.
106. Silverstein, J.W., Combettes, P.L., "Signal detection via spectral theory of large dimensional random matrices," *IEEE Trans. Signal Process.*, 40, pp. 2100–2105, 1992.
107. Smith, S.T., Scharf, L.L., McWhorter, L.T., "Intrinsic quadratic performance bounds on manifolds," *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2006)*, Toulouse, France, May 14–19, 2006, pp. V-1013–V-1016.

108. Spiegel, M.R., *Complex Variables*, Schaum's Outline Series in Mathematics, McGraw-Hill Book Company, New York, 1964.
109. Stahl, S., *A Gateway to Modern Geometry: The Poincaré Half-Plane*, 2nd ed., Jones & Bartlett Publishers, Subburg, MA, 2007.
110. Suzuki, N., Biyajima, M., "Analytic solution for Brownian motion in three dimensional hyperbolic space," http://arxiv.org/abs/math-ph/0406040.
111. Sym, A., "Soliton surfaces," *Lett. Nuovo Cimento* 33(12), pp. 394–400, 1982 (see also others in this series, including Sym, A., "Soliton surfaces V: Geometric theory of loop solitons," *Lett. Nuovo Cimento* 41(2), pp. 33–44, 1984.)
112. Tomkos, I., Roudas, I., Hesse, R., Antoniades, N., Boskovic, A., Vodhanel, R., "Extraction of laser rate equations parameters for representative simulations of metropolitan-area transmission systems and networks", *Optics Commun.*, 194(1–3), pp. 109–129, 2001.
113. Topsoe, F., "Some inequalities for information divergence and related measures of discrimination," *IEEE Trans. Inform. Theory*, 46(4), pp. 1602–1609, 2002.
114. Tron, R., Vidal, R., Terzis, A., "Distributed pose averaging in camera networks via consensus on $SE(3)$," *Proceedings of the Second ACM/IEEE International Conference on Distributed Smart Cameras, ICDSC 2008*, pp. 1–10, Stanford, CA, September 7–11, 2008.
115. Tsallis, C., "Possible generalization of Boltzmann–Gibbs statistics," *J. Statist. Phys.*, 52, pp. 479–487, 1988.
116. Tse, D., Viswanath, P., *Fundamentals of Wireless Communication*, Cambridge University Press, Cambridge, 2005.
117. Tutubalin, V.N., "On random walk in the Lobachevsky plane," *Theory Probab. Appl.*, 13, pp. 487–490, 1968.
118. Tutubalin, V.N., "On the limit behavior of compositions of measures in the plane and space of Lobachevsky," *Theory Probab. Applic.*, 7, pp. 189–196, 1962.
119. Tulino, A.M., Verdú, S., *Random Matrix Theory and Wireless Communications*, Now Publishers, Boston, 2004.
120. Waite, J.B., Lettis, D.S.L., "Calculation of the properties of phase noise in coherent optical receivers," *Br. Telecommun. Technol. J.*, 7(4), pp. 18–26, 1989.
121. Wang, Y., Zhou, Y., Maslen, D.K., Chirikjian, G.S., "Solving the phase-noise Fokker–Planck equation using the motion-group Fourier transform," *IEEE Trans. Commun.*, 54(5), pp. 868–877, 2006.
122. Wiener, N., *Cybernetics: or Control and Communication in the Animal and Machine*, MIT Press, Cambridge, MA, 1948 and 1961.
123. Yazici, B., "Stochastic deconvolution over groups," *IEEE Trans. Inform. Theory*, 50(3), pp. 494–510, 2004.
124. Younes, L., Qiu, A., Winslow, R.L., Miller, M.I., "Transport of relational structures in groups of diffeomorphisms," *J. Math. Imaging Vision*, 32, pp. 41–56, 2008.
125. Zhang, J., Rangarajan, A., "Affine image registration using a new information metric," *CVPR'04*, Vol. 1, pp. 848–855, Washington DC, 2004.
126. Zhang, W., Lai, Y.C., Williams, J.A.R., Lu, C., Zhang, L., Bennion, I., "A fibre grating DFB laser for generation of optical microwave signal," *Optics Laser Technol.*, 32(5), pp. 369–371, 2000.
127. Zhang, X., "Analytically solving the Fokker–Planck equation for the statistical characterization of the phase noise in envelope detection," *J. Lightwave Technol.*, 13(8), pp. 1787–1794, 1995.
128. Zhang, Z., Yeung, R.W., "On the characterization of entropy function via information inequalities," *IEEE Trans. Inform. Theory*, 44, pp. 1440–1452, 1998.
129. Zabusky, N.J., Kruskal, M.D., "Interaction of 'solitons' in a collisionless plasma and the recurrence of initial states," *Phys. Rev. Lett.*, 15(6), pp. 240–243, 1965.

18

Algebraic and Geometric Coding Theory

Coding theory is concerned with methods for "packaging" and "unpackaging" messages in order that the most information can be reliably send over a communication channel. In this chapter, a greater emphasis is given to the roles of geometry and group theory in communication problems than is usually the case in presentations of this subject. Geometry and group theory enter in problems of communication in a surprising number of different ways. These include the use of finite groups and sphere packings in high-dimensional spaces for the design of error-correcting codes (such as those due to Golay and Hamming). These codes facilitate the efficient and robust transmission of information. Additionally, Lie groups enter in certain decoding problems related to determining the state of various motion sensors.

The important points to take away from this chapter are as follows:

- Geometry and group theory play important roles in the design of codes and in decoding algorithms.
- Understanding the geometry and symmetry of sphere packing in high-dimensional Euclidean spaces leads to efficient codes.
- Problems in Robotics and Computer-Integrated Surgical Systems can be viewed from the perspective of encoding/decoding problems over the groups $SO(3)$, $SE(2)$, and $SE(3)$.
- Algebraic structures other than groups, such as rings and fields, are important in coding theory.

The remainder of this chapter is structured as follows. Section 18.1 provides a general introduction to classical coding theory. Section 18.2 reviews how algebra and coding are related. Section 18.3 addresses the associated geometric and group-theoretic issues. Section 18.4 describes the interplay between information theory and the measurement of rotational motion in the context of rotary and spherical encoder design. Section 18.5 continues along this theme by examining motion coding problems in medical image registration.

18.1 Classical Coding Theory

In this section two fundamental results of coding theory for discrete alphabets are reviewed: (1) the Kraft–McMillan inequality and (2) the source coding theorem. The brief presentation here is necessarily truncated given the overall goals of this book.

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_9,

For comprehensive introductions to coding theory, see the information theory references from Chapter 17 and [17, 20, 29, 31, 32], and references therein.

18.1.1 The Kraft–McMillan Inequality

Let $\mathcal{A} = \{\alpha_i\}$ be an alphabet consisting of $|\mathcal{A}|$ symbols and let $D = \{W_i\}$ be a dictionary consisting of $|D|$ words. Each of these words is constructed from symbols drawn from $\mathcal{A}$. The number of symbols used to construct W_i is denoted as $|W_i|$ and is called the length of the word. Some caution is necessary when interpreting this terminology. If the symbols α_i in the alphabet $\mathcal{A}$ are the fundamental elements of the code, such as 0s and 1s in a binary code like ASCII or dots and dashes in Morse code, then the "words" in the dictionary actually would be letters in, say, the Roman alphabet rather than actual words in the sense of a human language. This is consistent with the discussion in Section 17.3.

A fundamental result in coding theory is the *Kraft–McMillan inequality*, which was originally derived by Kraft for instantaneous/tree codes (such as Morse code)[1] and extended by McMillan to any uniquely decodable code (which includes ASCII).[2] This inequality places a constraint on the lengths of the words for given sizes of the alphabet and dictionary as follows:

$$\boxed{\sum_{i=1}^{|D|} |\mathcal{A}|^{-|W_i|} \leq 1\,.} \tag{18.1}$$

A proof of this theorem can be found in books on classical information theory.

18.1.2 The Source Coding Theorem

Starting with the same terminology and conditions as in the previous subsection, let p_i denote the probability of W_i occurring in a typical message. Denote the average word length as $L = \sum_{i=1}^{|D|} p_i\,|W_i|$. Then the *source coding theorem* states that[3]

$$\boxed{H(D) \leq L \cdot \log\,|\mathcal{A}|, \quad \text{where } H(D) \doteq -\sum_{i=1}^{|D|} p_i \log\,p_i\,.} \tag{18.2}$$

This theorem is easy to prove using the Kraft–McMillan inequality. Let $l_i = |W_i|$, $n = |D|$, and $r = |\mathcal{A}|$, and for the moment let us fix the base of the logarithm as e. Then the terms in (18.2) can be written as

$$H_e(D) - L \cdot \log_e\,r = -\sum_{i=1}^{n}\{p_i \log_e p_i\,+\,p_i\,l_i\,\log_e r\} = \sum_{i=1}^{n} p_i \log_e\left(\frac{1}{p_i\,r^{l_i}}\right).$$

[1] In such codes, no codeword appears at the beginning part (or prefix) of another codeword; hence, these are also called prefix codes. Words in such codes can be viewed as the leaves on a decision tree rooted on the first symbol in the word.

[2] The terminology "uniquely decodable" is highly technical and is defined precisely in books in classical information theory, but, in essence, it means that words in an encoded message can be parsed without any ambiguity.

[3] This inequality holds regardless of the base of the logarithm, which appears on both sides of the equation. It is a restatement of Shannon's theorem for noiseless channels.

Then since for any $x \in \mathbb{R}_{>0}$ the inequality $\log_e x \leq x - 1$ holds,

$$H_e(D) - L \cdot \log_e r \leq \sum_{i=1}^{n} p_i \left(\frac{1}{p_i \, r^{l_i}} - 1 \right) = \left(\sum_{i=1}^{n} r^{-l_i} \right) - 1 \leq 0,$$

where the last inequality is the Kraft–McMillan inequality.

The results presented in this section are generic and establish bounds on the performance of any uniquely decodable code. However, they are not constructive in providing guidelines as to how to design a code. This is where algebra and geometry come in to play.

18.2 Algebraic Coding Theory

This section focuses on elementary algebraic, rather than geometric, aspects of coding theory. First, a review of the algebraic structures known as *rings* and *fields* is provided. Fields are a kind of number system that can be used as the values of functions as well as the entries of vectors and matrices. Thus, it makes sense, for example, to talk about functions that take their values in a field ($\mathbb{R}$ and $\mathbb{C}$ are fields, but, more generally, a function can be defined on a set S as $f : S \rightarrow \mathbb{F}$, where $\mathbb{F}$ is some general field). When vectors and sets of invertible matrices have entries that take their values in a field, the result is a "vector space over a field" or a "matrix group over a field."

18.2.1 Rings and Fields

In modern algebra, the fundamental objects of study are groups, rings, fields, vector spaces, and algebras. The formal definition of vector spaces is given in Appendix A.1 of Volume 1 and is well known to engineers and physical scientists. A working definition of a group was given in Chapter 1 and was formalized in Chapter 10. Rings and fields are mathematical objects that have more structure (i.e., more defining rules) than groups but less than vector spaces. Fields have more structure than rings, and algebras have the most structure. As with the definition of a group and a vector space, the definitions of a ring and a field can be found in books on modern algebra. Basically, a *field* is a set, $\mathbb{F}$, together with two binary operations, $+$ (called addition) and $\cdot$ (called multiplication). The pair $(\mathbb{F}, +)$ is a commutative group and the identity element is denoted as 0. Let $\mathbb{F}^{\times} \doteq \mathbb{F} - 0$ (which should be read as $\mathbb{F}$ with 0 excluded). By definition, the pair $(\mathbb{F}^{\times}, \cdot)$ is also a commutative group with the identity element denoted as 1. The usual distributive laws $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for any $a, b, c \in \mathbb{F}$ completes the defining properties of the field $(\mathbb{F}, +, \cdot)$. As in the case of groups, $\mathbb{F}$ is sometimes used as shorthand for $(\mathbb{F}, +, \cdot)$ when it is understood from the context. A *ring* can be thought of as a weakened version of a field in the sense that the existence of a multiplicative inverse for each nonzero element (and all of the group rules that involve a multiplicative inverse) is not required.

As a concrete example of a field, consider the set $\{0, 1\}$ with addition and multiplication "modulo 2." In modular arithmetic, $1 + 1 \doteq 0$ rather than $1 + 1 = 2$, which gives closure to $(\{0, 1\}, +)$. In modular arithmetic, the result of the sum or product of two numbers from the set $\{0, 1, 2, \ldots, p - 1\}$ can be evaluated "$\bmod p$" by first computing it in the usual arithmetic and then adding or subtracting p until the result falls back in the set $\{0, 1, 2, \ldots, p - 1\}$.

In the particular case of $(\{0,1\},+,\cdot)$, the multiplication in modular arithmetic is the same as in usual arithmetic. The rules for this field can be summarized in the following tables:

+	0	1
0	0	1
1	1	0

and

·	0	1
0	0	0
1	0	1

(18.3)

This field is denoted as $\mathbb{F}_2$. The "+" and "·" operations can be thought of as the logical "exclusive or" and "and" operations, respectively.

Given any prime number p, modular arithmetic operations can be used to define a field $\mathbb{F}_p = (\{0,1,2,\ldots,p-1\},+,\cdot)$. For example, $\mathbb{F}_5$ is defined by

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

and

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(18.4)

Note that $(\mathbb{F}_5,+)$ is a commutative group,[4] but $(\mathbb{F}_5,\cdot)$ is not. The corresponding table defining multiplication for the commutative group $(\mathbb{F}_5^\times,\cdot)$ is

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(18.5)

As a counterexample, the set of quaternions $\mathbb{H}$ is *not* a field since it is not commutative under multiplication. It is called a *skew field* or *division algebra.*

Note that unlike a vector space which requires two sorts of objects (scalars and vectors), there is only one kind of object involved in a field (scalars). In the definition of a vector space, the scalars are drawn from a field. In the discussion of vector spaces in Appendix A.1.1 of Volume 1, the scalars were taken from the fields of real, $(\mathbb{R},+,\cdot)$, and complex, $(\mathbb{C},+,\cdot)$, numbers. However, a vector space can be defined "over" any field.

18.2.2 Groups over Fields

In the same way that a vector space can be defined over a field, groups with elements that are matrices can be defined over any field by populating the entries of those matrices with scalars drawn from a field. In general, given a field $\mathbb{F}$, the "general linear group over $\mathbb{F}$" is

$$GL(n,\mathbb{F}) \doteq \{A \in \mathbb{F}^{n\times n} \mid \det A \neq 0\}.$$

In other words, $GL(n,\mathbb{F})$ consists of $n \times n$ matrices with entries drawn from the field $\mathbb{F}$ under the constraint that the matrices are invertible. The group operation is matrix multiplication.[5]

[4] Actually, $(\mathbb{F}_p,+)$ for any $p \in \mathbb{Z}_{>0}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

[5] Although the quaternions are not a field, it is still possible to refer to a matrix group over the quaternions such as $GL(n,\mathbb{H})$.

For example, it can be shown that the group $GL(n, \mathbb{F}_2)$ consists of the following six matrices [2]:

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ; \; g_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} ; \; g_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} ;$$
$$g_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} ; \; g_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} ; \; g_5 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

(where all of the arithmetic operations involved in the multiplication of matrices is interpreted as mod 2). The corresponding group multiplication table with i, jth entry corresponding to $g_i \circ g_j$ is

$\circ$	e	g_1	g_2	g_3	g_4	g_5
e	e	g_1	g_2	g_3	g_4	g_5
g_1	g_1	e	g_3	g_2	g_5	g_4
g_2	g_2	g_5	e	g_4	g_3	g_1
g_3	g_3	g_4	g_1	g_5	g_2	e
g_4	g_4	g_3	g_5	g_1	e	g_2
g_5	g_5	g_2	g_4	e	g_1	g_3

(18.6)

Note that this is a noncommutative group, as can be observed by the lack of symmetry about the major diagonal of this table.

In contrast to the finite group $GL(n, \mathbb{F}_2)$, it is possible to define $GL(2, \mathbb{Z}) \doteq \{A \in \mathbb{Z}^{2\times 2} \mid \det A \in \{1, -1\}\}$. This is a discrete group consisting of an infinite number of elements. (Note: $\mathbb{Z}$ is a ring but not a field.) $GL(2, \mathbb{R})$ is a four-dimensional Lie group. (The restriction on the determinant ensures the existence of a multiplicative inverse for each matrix in $GL(2, \mathbb{R})$. Each of the four entries in the matrix is free except for the condition $\det A \neq 0$, which does not affect the dimensionality.) Similarly, $GL(2, \mathbb{C})$ is an eight-dimensional Lie group because each complex entry is defined by two real numbers. So the specification of the field over which a group is defined makes a huge difference.

In the next section the concept of a field is demonstrated in the context of coding theory.

18.2.3 The Hamming $(7, 4)$ Code

A binary code of length n consisting of r message bits and $n - r$ check bits is called an (n, r) code. For example, sending the same message s times is an $(r \cdot s, r)$ code. If the error probability, e, is small and s is large, then this is a reliable way to encode a message (since on the receiving end, the average of each corresponding bit can be computed and rounded to the nearest value), but this method can be slow.

The basic goal is to code information in such a way that optimizes the trade-off between *robustness* (i.e., to maximize the ability to recover the original message from a version corrupted by noise/random bit errors) and *efficiency* (i.e., to minimize the ration r/n). Actually, if all of the message bits are equally likely, the probability of any particular message being sent is $1/2^r$, and so

$$-\log_2(1/2^r)/n = r/n$$

is the "information rate" of the code. This is a measure of how much message gets through given the checking machinery that is carried along with it.

A bound established by Hamming for perfect codes is reviewed here. It is important as a guideline in designing error-correcting codes. Given the goal of designing an (n, r) code that is robust to single errors during transmission of the message, the goal is to minimize n for given r. However, in this scenario, the number of check bits, $n - r$, must be able to encode the n possible locations of a single error and also account for the possibility of no error. Therefore, $n - r$ must be large enough that $2^{n-r} \geq n + 1$, or

$$\boxed{\frac{2^n}{n+1} \geq 2^r.} \tag{18.7}$$

By exhaustive enumeration of the possibilities, Hamming provided the following table of values that satisfy (18.7):

n	r	$n-r$	r/n
1	0	1	0.000
2	0	2	0.000
3	1	2	0.333
4	1	3	0.250
5	2	3	0.400
6	3	3	0.500
7	4	3	0.571
8	4	4	0.500
9	5	4	0.555
10	6	4	0.600

The list goes on. Note, however, that the assumption that at most a single error occurs is the basis for (18.7). If the goal was to develop an error-correcting code that is robust up to two errors, then an inequality of the form $2^{n-r} \geq n(n-1)/2 + n + 1$ would need to be satisfied. As a sequence becomes longer, switching to such an equation would become important, and that would change the numbers in the table, decreasing the ratio r/n as n increases. Examining the small values of n, it becomes clear that the $(7, 4)$ case has a better ratio than its neighbors and therefore deserves greater attention. That is, a $(7, 4)$ code is equally effective in error-correction ability while carrying less baggage (i.e., it has a higher information rate) than its neighbors in the above table.

Hamming developed such a code in 1948, which was patented by Bell Labs. The intuition behind the development of this code is quite interesting and is described in [17]. Here, only the "nuts and bolts" of how it works are described. Suppose a 4-bit error-correcting message of the form $m_1m_2m_3m_4$ is to be transmitted, where $m_i \in \mathbb{F}_2$. Let $\mathbf{m} = [m_1, m_2, m_3, m_4]^T \in \mathbb{F}_2^4$ (the four-dimensional vector space over the field $\mathbb{F}_2$). Let

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 7} \quad \text{and} \quad \mathbf{c} = G\mathbf{m} \in \mathbb{F}_2^7. \tag{18.8}$$

The coded message $c_1c_2c_3c_4c_5c_6c_7$ is then sent through the channel. Let $v_1v_2v_3v_4v_5v_6v_7$ denote the received message and $\mathbf{v} = [v_1, v_2, v_3, v_4, v_5, v_6, v_7]^T$ be the corresponding vector. It could be that $\mathbf{v} = \mathbf{c}$, or $\|\mathbf{v} - \mathbf{c}\| = 1$.

On the receiving side, two matrices are applied. First,

$$\mathbf{b} = H\mathbf{v}, \quad \text{where } H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

The matrix H is actually the null-space projector matrix for G, meaning that

$$HG = \mathbb{O}_{3\times 4}. \tag{18.9}$$

Therefore, if $\mathbf{v} = \mathbf{c}$, then $\mathbf{b} = \mathbf{0}$, and this serves as verification that no error exists in the received message.

If an error does exist in $\mathbf{v}$, then computing $\mathbf{b} = H\mathbf{v}$ gives the column of H corresponding to the location of the error. For example, if the message $m_1m_2m_3m_4 = 1010$ is sent, then

$$\mathbf{c} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Clearly,

$$H\mathbf{c} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Remember that both of these matrix–vector multiplications are performed in modulo 2 arithmetic. If a single error is introduced during transmission, then the result might be something like

$$\mathbf{c} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

In this case,

$$H\mathbf{v} = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

However, this is the third column of H, indicating that the error has occurred in the third bit of the encoded message. Knowing were the error occurs is 99.999% of the problem, since correction just requires flipping the value of the bit at that location.

Once a correct (or corrected) coded message has been received, then it can be decoded by multiplying by another matrix to recover $\mathbf{m}$. Specifically, from (18.8) it is clear that

$$\mathbf{c} = [m_1, m_1 + m_2, m_2 + m_3, m_1 + m_3 + m_4, m_2 + m_4, m_3, m_4]^T,$$

and so,

$$\mathbf{m} = K\mathbf{c}, \quad \text{where } K = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

is one such matrix that will work since the first, third, and fourth rows pick off m_1, m_3 and m_4, respectively, and in modulo 2 arithmetic, $m_1 + m_1 + m_2 = m_2$, so the second row picks off m_2. Other valid K matrices would result if the second row were replaced with 0000101 (because $m_2 + m_4 + m_4 = m_2$) or 0010010 (because $m_2 + m_3 + m_3 = m_2$). Since all of the operations involved can be implemented as matrix–vector operations, this is said to be *linear code*. Note, however, that this is not the best way to implement encoding/decoding in hardware since the arithmetic operations involved in these matrix–vector multiplications involve many multiplications and addition by 0 that are unnecessary.

Additionally, the choice of G and H are not unique. For example, if

$$G' = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad H' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad K' = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

this defines another $(7,4)$ Hamming code. In this one, since the columns of H' are arranged in the order of the binary number from 1 to 7, the binary location of the position of the error can simply be read off of $H'\mathbf{v}'$. Here, the two versions of Hamming $(7,4)$ codes presented are related to each other by a permutation of columns of H; that is, $H' = H\pi$, where

$$\pi = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \Pi_7. \tag{18.10}$$

Imposing the condition (18.9) on both codes means that G' can be defined as a permutation of rows of G by π^{-1} since

$$H'G' = (H\pi)(\pi^{-1}G) = HG.$$

If $KG\mathbf{m} = \mathbf{m}$, then $K'G'\mathbf{m} = \mathbf{m}$ if $K'G' = (K\pi)(\pi^{-1}G)$, so $K' = K\pi$.

From this construction, it is clear that there are $|\Pi_7| = 7!$ equivalent Hamming $(7,4)$ codes with different G and H matrices. In addition, for each one, multiple K matrices exist. Thus, rather than referring to "the Hamming $(7,4)$ code," it makes sense to either refer to "a Hamming $(7,4)$ code" or "the equivalence class of Hamming $(7,4)$ codes."

Note also that any two messages encoded with the same Hamming $(7,4)$ code can be added as $\mathbf{c}^{(1)} + \mathbf{c}^{(2)}$. It follows from linearity that $H(\mathbf{c}^{(1)} + \mathbf{c}^{(2)}) = \mathbf{0}$, and so, $\mathbf{c}^{(1)} + \mathbf{c}^{(2)}$ is also a Hamming-$(7,4)$-coded message. In other words, the set of all coded messages produced by the same Hamming $(7,4)$ code form a commutative group under the operation of addition modulo 2. This makes them an example of a *group code*.

18.3 Codes and Geometry

When sending a message over a noisy channel, a natural question to ask is whether or not it is possible to know if the intended message was received. Of course, one way to do this would be to send the same message back and forth several times and match the message that was originally intended with its replicas. However, this would be quite time-consuming and would decrease the amount of possible information that can flow over a given channel. In contrast, a more efficient way of doing things is to prepackage the message in order to maximize its success of reaching the receiving end intact and, if the original message is not received, to be able to detect (and possibly even repair) any corruption of the original message. The trick is to do this without having to send the message back to the sender.

The problem with any verification scheme is that exactness in communication is never possible. For example, one can imagine a scenario in which a sequence of characters in an original message is sent and that one of the characters on the receiving end gets changed in the process. Even in the brute-force approach in which the received message is sent back to the sender for verification, it is possible (however, unlikely) that the character that was changed gets changed back to the original. Therefore, the sender would believe that the correct message was received when in fact it was not. Although this scenario illustrates that it is never possible to know if a sent message has been received without any corruption, it is possible to make probabilistic comments about how likely it is that the intended message has been received. Within this probabilistic framework, the theory of error detection and correction in received messages is based on the assumption that the error rate is low enough that multiple errors will not occur in a message of a given size. In this context, various codes exist to prepackage a message in a form that is robust to disturbances introduced by the noisy channel.

The following subsections address this kind of *channel coding* problem; that is, how to bundle up a message with additional information so as to maximize the probability that it can be recovered on the receiving end, given the model of noise described above: random bit inversions. It should be noted, however, that other sorts of errors can occur. For example, the omission or insertion of extraneous bits or the swapping of sequences of bits might be possible. Such things certainly happen in biology (e.g., DNA transcription errors or infection of a host cell's genome with retroviruses). In the old days when an analog Morse code signal was sent over long wires, the dots and dashes could end up spreading out and overlapping each other due to signal attenuation (described by the telegraph equation, as discussed in Chapter 17), which would also be a different kind of error. However, if the discussion is limited to communications engineering and the transfer of data inside or between computers, the model of individual bit flipping appears to be a reasonable model.

18.3.1 Error Detection Versus Error Correction

The theory of error detection and error-correcting codes has both geometric and algebraic aspects. In error detection, the goal is to determine (with high probability) whether or not errors exist between the received and sent messages. If the probability of an error occurring in any particular location in a message is very small and that probability is uniform over all locations, then a *parity check* over a small sequence is an effective way to detect an error. For example, if the probability of an error occurring in a message consisting of four binary numbers is 1 out of 1000 in each digit, then the probability of some kind of error occurring in the message is 4×0.001. The probability of a single error occurring is $4 \times (0.999)^3 \times (0.001)$ because the probability of any three digits being right is $(0.999)^3$, the probability of one being wrong is 0.001, and the error can be in one of four places. The probability of two errors occurring is $6 \times (0.999)^2 \times (0.001)^2$ because each independent error has a probability of 0.001, and two such errors can occur in any of the six digits (1,2), (1,3), (1,4), (2,3), (2,4), (3,4). The factor of $(0.999)^2$ is required because this is the probability that the other bits were transmitted correctly. Three errors of this kind have a probability of $4 \times (0.999) \times (0.001)^3$ because they can occur at the four locations (1,2,3), (1,2,4), (1,3,4), (2,3,4) and the probability of the remaining bit being correct is 0.999.

More generally, if the probability that any individual bit in a message will have an error is p, then the probability that no error occurs in a message of length n is $(1-p)^n$. The probability that one and only one error occurs is $np(1-p)^{n-1}$, and the probability that exactly two errors occur is $n(n-1)p^2(1-p)^{n-2}/2$. Indeed, the probability that exactly k errors occur in a message of length n will be given by the binomial theorem as

$$P(k) \doteq \binom{n}{k} p^k (1-p)^{n-k}.$$

The probability that some kind of error will occur is $n \times p$. The probability that either no error or a single error will occur is $(1-p)^n + np(1-p)^{n-1}$. The probability that k or more errors will occur is $\sum_{j=k}^{n} P(j)$.

When p is very small and n is not very large, it can be reasoned that the probability of either no errors or a single error will be greater than the probability of two or more errors. In this scenario, the addition of a parity bit to a binary message can be an effective way to detect an error. For example, consider the message 001010111. Summing up the bits gives 5. In modulo 2 arithmetic, $5 \cong 1 \bmod 2$. Therefore, appending a 1 to the message and modifying it as 0010101111 means that if 1 out of these 10 digits in this message is corrupted on the receiving end, it will be clear that the intended message was not received. For example, 0000101111 does not make sense because adding up the message bits gives $4 \cong 0 \bmod 2$, and $0 \neq 1$. If it happens to be that the parity bit is corrupted, 0000101110 would not make sense either. Of course, the assumption here is that the probability of errors is so low that multiple errors have not occurred, since any even number of errors will preserve the parity. Error detection in the presence of greater error probabilities (or longer message lengths) is possible by the inclusion of more parity bits. This is equivalent to chopping the message up into smaller parts, which is what is done in practice. For example, each character in the even-parity ASCII code used to represent alphabetical and numerical symbols has a parity bit built in, so any alphanumeric message is filled with parity bits.

It is important to have a sense of how noisy the information channel is a priori before selecting a strategy for robust communication because, on the one hand, the inclusion of too many parity bits reduces the rate at which information can be sent and, on the other hand, if the channel is noisier than expected, the inclusion of too few parity bits means that received messages will be corrupted too frequently without any way to trust their contents.

Once an error has been detected, a request from the receiver to the sender can be made to resend the message. This requires two-way communication. In some cases, this is not desirable. For example, communicating with a deep-space probe has significant time delays, and sending a message, sending back a request to resend, and then resending triples the amount of delay. Thus, it is desirable to develop codes that are robust to noise in the sense that when a message is received, not only can an assessment be made as to whether an error has occurred or not but also the location of the error can be pinpointed and therefore fixed (since in binary knowing that an error has occurred at a specific location means that the bit in that location should be flipped).

Geometric problems arise in the design of binary code words that are robust to single or multiple errors because some measure of distance is required to design codewords that are well separated from each other; that is, a received message that is corrupted by noise can be restored (or corrected) to the original sent message with high probability.

For example, in a two-letter alphabet $\{A, B\}$ if the letter "A" is encoded as the binary number 00000 and the letter "B" is encoded as 11111 and if the message "A B A" is sent but 01000 11101 00001 is received, it can be reasoned with high confidence that "A B A" was intended, and one bit error has occurred in each code word. This is because counting up the bit differences between the word for "A" and for "B" results in the number 5. However, 01000 and 00001 have a distance of 1 from "A" and 4 from "B."

Introducing concepts of distance between messages leads to geometry. The geometric aspects of code design has a long and rich history that will be reviewed in the following subsections.

18.3.2 Arrangement of Message Blocks as Spatial Arrays

In the previous subsection, an example was given of a message 000010111 | 1, where | 1 is the parity bit, which is written here as being separated from the rest, but in an actual transmitted message, there would be no such separation (and no empty spaces between the bits either). If we are not satisfied with single-bit error detection, but also want to correct single-bit errors without envoking two-way communication, there are several geometric ways to approach the problem. Imagine that we arrange the contents of the message (forget about the parity bit for now) as a 3×3 array of binary numbers. Then the parity bits of each row and each column can be computed and embedded as part of a message. Suppose that this message is sent and a bit is corrupted (as indicated below by the arrow and box, respectively).

$$\begin{array}{ccc|c} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & \end{array} = 000001011111101 \longrightarrow 00000\boxed{0}011111101 = \begin{array}{ccc|c} 0 & 0 & 0 & 0 \\ 0 & \boxed{0} & 0 & 1 \\ 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 1 & \end{array} .$$

Then on the receiving end it will be clear that something went wrong because the parity does not work in the row and column containing $\boxed{0}$. This not only detects the error but also provides Cartesian array coordinates indicating its location!

There is no reason to limit this to the two-dimensional case. A message with a length that can be factored into the product of three integers can be visualized as a three-dimensional array. Additionally, parity bits can be thought of as occupying locations on the edges of this three-dimensional box, much like coordinate axes in three-dimensional Cartesian coordinates. In this way, correction of single-bit errors in long messages can be attained with relatively fewer check bits because as the number of dimensions of the object increases, the volume grows exponentially and the number of axes grows linearly.

18.3.3 Hamming Spheres and Perfect Codes

Hamming introduced the concept of viewing a codeword of length n as a vertex on the unit hyper-cube in $\mathbb{R}^n$. For example, in $\mathbb{R}^2$, the 2^2 possible vertices of the unit square in the first quadrant are $(0,0)$, $(0,1)$, $(1,0)$, and $(1,1)$. In $\mathbb{R}^3$, the coordinates of the 2^3 possible vertices of the unit cube in the first octant are $(0,0,0)$, $(0,0,1)$, $(0,1,0)$, $(0,1,1)$, $(1,0,0)$, $(1,0,1)$, $(1,1,0)$, and $(1,1,1)$. A natural metric to use in this context is the l_1-norm of the difference of any two sets of coordinates on the same hyper-cube viewed as a vector. This is equivalent to the length of the shortest path connecting vertices in the graph formed from the edges and vertices of the hyper-cube. This is called the *Hamming distance* and is denoted here as $D(\cdot,\cdot)$. It satisfies the properties of a metric, or distance, function. For example,

$$D(00,11) = |0-1| + |0-1| = 1+1 = 2$$

and

$$D(010,110) = |0-1| + |1-1| + |0-0| = 1+0+0 = 1.$$

If $r \in \mathbb{Z}^+$, a *Hamming sphere* centered on a vertex v is the set of all vertices such that

$$S(v,r) \doteq D(v,r) \leq r. \tag{18.11}$$

Actually, from a strict mathematical perspective, this should not be called a sphere but rather a ball. However, since the name “Hamming sphere” is so well ingrained in the literature, that name will be used here as well rather than attempting to call it a “Hamming ball.” All points within a Hamming sphere of radius r around a message of length n (Hamming space of dimension n) correspond to alterations of the message in up to r of its bits. If a code is designed such that any two messages that would ever be sent are each at the center of nonintersecting Hamming spheres or radius r, then if at most r errors occur, the received messages will remain inside of their Hamming spheres on the receiving end. Additionally, since by design the spheres do not intersect, there will never be any ambiguity about what message was intended. However, if a code is designed satisfying this property but has a lot of empty vertices that do not belong to any Hamming sphere, then this means that the code is too conservative. Therefore, the following two properties are important:

$$\boxed{S(v_1,r) \cap S(v_2,r) = \emptyset \quad \text{and} \quad \bigcup_{i\in I} S(v_i,r) = B^n,} \tag{18.12}$$

where I is the index set that enumerates all possible messages in a code and B^n is the whole n-dimensional unit hyper-cube. If $s(v)$ is the version of the message v that is received and if it is known a priori that the communication channel will not introduce any more than r errors, then $D(v,s(v)) \leq r$. From the first condition in (18.12) and the triangle inequality, it follows that for any other message $w \neq v$, $D(v,w) > 2r$, and so $D(v,s(v)) + D(s(v),w) \geq D(v,w)$ or

$$D(s(v),w) \geq D(v,w) - D(v,s(v)) > r.$$

This means that under the assumed noise properties of the channel, there is no way to mistake $s(v)$ for any message, w, other than the intended message, v.

Any code that satisfies the conditions in (18.12) is called a *perfect code* because it affords the desired degree of error correction and is as efficient as possible in the sense of not leaving any wasted vertices.

18.3.4 Coding Theory, Sphere Packing, and Symmetry Groups

Given that a perfect error-correcting code can be defined geometrically as the packing of disjoint Hamming spheres that cover the full Hamming cube, there is a natural connection between coding theory and geometry. This led to a confluence of interests of mathematicians motivated by coding problems and those interested in the packing of congruent (equal-sized) spheres in $\mathbb{R}^n$ [41]. Of course, the difference is that spheres in $\mathbb{R}^n$ are defined by the Euclidean metric rather than the Hamming distance.

The packing of congruent circles in the plane so as to attain the highest density has a long history. Gauss proved that hexagonally close packing of congruent circles in a honeycomb lattice in which every circle has six neighbors contacting it provides the highest density of any regular packing. Elementary geometry can be used to show that this density is $\pi/\sqrt{12}$. However, it was not until 1940 that the Hungarian mathematician László Fejes Tóth proved that this density could not be exceeded by using an irregular packing.

Kepler conjectured in the early 1600s that the highest-density packing of congruent spheres in $\mathbb{R}^3$ is $\pi/\sqrt{18}$. The face-centered-cubic lattice, in which each central sphere is surrounded by other spheres of the same size placed at the corners and faces of a cube, attains this bound. Additionally, if a layer of spheres is placed in a plane and hexagonally close packed and then if two such planes are stacked in an offset way so as to pack as closely as possible, then this also attains this bound. Using these constructions, every sphere has 12 neighbors in contact. As with the case of regular planar packings, there is a relatively small number of regular spatial packings of congruent spheres, and it can be checked that the $\pi/\sqrt{18}$ bound holds for all of these regular packings. However, it was not proved that this bound also holds for irregular packings until 1998, when Thomas Hales proved it by exhaustive enumeration by computer.

In higher dimensions, the proof of the exact highest-density sphere packing becomes even harder, since the number of possible packings grows very rapidly with the dimension. Even enumerating the regular packings becomes very difficult. However, a relatively simple upper bound on the packing density in $\mathbb{R}^n$ can be obtained from the packing density of $n+1$ unit spheres with centers placed on a regular simplex[6] with sides of length 2. This bound, due to Rogers [33] is [34, 41]

$$r(n) = \frac{(n+1)^{\frac{1}{2}}(n!)^2\pi^{n/2}}{2^{3n/2}\Gamma(n/2+1)} f_n(n), \quad \text{where } f_n(x) = F_n(\text{arcsec}(x)/2),$$

and

$$F_{n+1}(\alpha) = \frac{2}{\pi}\int_{\text{arcsec}(n)/2}^{\alpha} F_{n-1}(\beta)\, d\theta, \quad \text{where } \sec 2\beta = \sec 2\theta - 2,$$

is a recursive definition of $F_n(\alpha)$ starting with $F_1(\alpha) = F_0(\alpha) = 1$.

It is an upper bound because in general $\mathbb{R}^n$ cannot be filled by close-packing copies of a simplex. Nevertheless, having such an upper bound gives a way to assess "how bad"

[6] A simplex is the multi-dimensional generalization of a triangle or tetrahedron.

a proposed backing is. Since there is no guarantee that this bound can be attained, even coming close means that the packing is pretty good.

An interesting connection between coding theory and geometry is that a $(23, 12)$ error-correcting code introduced by Golay [14] can be related to study regular packing of spheres in $\mathbb{R}^{24}$. In particular, Leech found a packing in $\mathbb{R}^{24}$ with a particularly high density [28]. This packing has a density of $\pi^{12}/12! \approx 0.0019296$, which is a high percentage of the Rogers bound in this case, which is approximately 0.002455. Leech's packing is regular and has an associated group of symmetry operations which were studied extensively.

Related areas of discrete geometry include the packing of noncongruent circles in irregular packings [39] and the optimal packing of congruent or noncongruent circles on the surface of the sphere [7, 8]. There are a very small number of regular packings of circles on the sphere; these correspond to the Platonic solids. Therefore, most work in this area has been on the optimal irregular packing of equal-sized circles. However, in the context of an application related to the design of a spherical motor, the author and his student explored the problem of regular circle packings on the sphere using circles of different sizes. Basically, the goal was to come up with two packings of circles on the sphere, each with a different symmetry group, and both of which had circles of approximately equal size [4]. The reason for these constraints was that the rotor (the ball that moves) and the stator (the cavity that houses the ball) each had to have poles (magnets/electromagnets) that could interact in a way that would induce motion. This is not the only kind of spherical motor design, but it is one that relates to the theme of circle/sphere packing. Nature also comes up with ways to approximate packings on the surface of the sphere in the context of spherical virus capsids, which are the protein shells that protect and encapsulate the genetic material of a spherical virus. This geometric problem is not unrelated to coding theory, because a virus must encode the geometry of the parts that form its capsid in its genetic material. For simplicity it is desirable that this genetic material encode as few different kinds of parts as possible.

The following section discusses how rotary and spherical motion can be encoded and decoded and explores one of the relationships between Lie groups and information theory.

18.4 Rotary and Spherical Encoders

An optical rotary encoder is a device used to detect the angle through which a shaft turns. They are often packaged together with a motor (e.g., in a robot arm) to provide feedback about the angular state of a shaft, such as the axis of the motor. The central part of a rotary encoder is a circular disk, usually made of transparent material, that is divided into n concentric annuli and 2^n sectors. An array of n light-emitting diodes (LEDs) are lined up on one side of the disk—one for each annulus. Corresponding to each LED is a sensor on the opposite side of the disk. The $n \cdot 2^n$ annular sections of the disk resulting from the intersections of sectors and annuli are either painted to block light or left transparent. Based on the bit pattern that is received by the light sensors (e.g., a "1" corresponding to sensed light and a "0" corresponding to no light), the angle of the shaft is resolved to within a discretization of shaft motions of one part out of 2^n.

One kind of code that is commonly used in the encoding of rotational motion around a fixed axis is a Gray code (named after Frank Gray [15], and not the color gray). Gray codes have the interesting property that as the shaft rotates, the bit pattern changes one bit at a time, all the way around the circle. This is explained more in the following subsection.

18.4.1 Gray Codes: Definition and Recursive Generation

Given the modest goal of resolving the orientation of a shaft to within a 180° rotation, we could simply paint one-half of the disk black and leave the other half clear. The resulting LED–sensor pair then provides one bit of information. In this case, the Gray code is simply

$$\begin{array}{c}0\\1\end{array}.$$

Actually, it does not matter if the "0" is given the meaning of the painted half and "1" the clear half of the disk, or vice versa. However, for the sake of argument let us take "1" to be painted and "0" clear. When this assignment is made, the bits received by the sensor will be inverted, since nothing will be received when the black paint stands between the LED and the sensor, and light will pass through the clear annular sections.

Now, suppose that we need to resolve the orientation to within 90° rather than 180°. Dividing the disk into four sectors and two annuli, the resulting sections can be painted according to the rule

$$\begin{array}{c}00\\01\\11\\10\end{array} = \begin{array}{c|c}0&0\\0&1\\\hline 1&1\\1&0\end{array}$$

Note that while it was trivial in the single-bit case to have the code "wrap around the circle" in a way in which one bit changes per change in sector, here the pattern of single bit changes is less trivial. Now, suppose that we want a resolution of 45°. A Gray code that does this is

$$\begin{array}{c}000\\001\\011\\010\\110\\111\\101\\100\end{array} = \begin{array}{c|cc}0&0&0\\0&0&1\\0&1&1\\0&1&0\\\hline 1&1&0\\1&1&1\\1&0&1\\1&0&0\end{array}$$

Again, this wraps around so that there is a single bit change between the first entry, 000, and the last, 100. This three-bit (or $n = 3$) Gray code corresponds to the encoder disk painted as in Figure 18.1(a), where the list starts at the positive x axis and traverses the disk counterclockwise.

Optical encoders can have very high resolution. If $n = 8$, then $2^8 = 256$ sectors means a resolution of approximately 1.4°. Some commercially available encoders list a value of $n = 12$, which provides a resolution of less than one-tenth of a degree (i.e., 360/4096). The above codes listed for the cases of $n = 1, 2$, and 3 can be extended to any value of n. There is a recursive procedure to do this. Starting with the Gray code for n, the Gray code for $n + 1$ is obtained using four simple steps. First, list the code of length n. Second, append to this list the code of length n listed in reverse order. Third, append a column of n zeros to the left side of the upper half of this list. Fourth, append a column of n ones to the left side of the lower half of this list.

18.4.2 Symmetries in Gray Codes

Clearly, by the construction described in the previous section, Gray codes have symmetries built in. Furthermore, if their only important feature is that one bit changes per

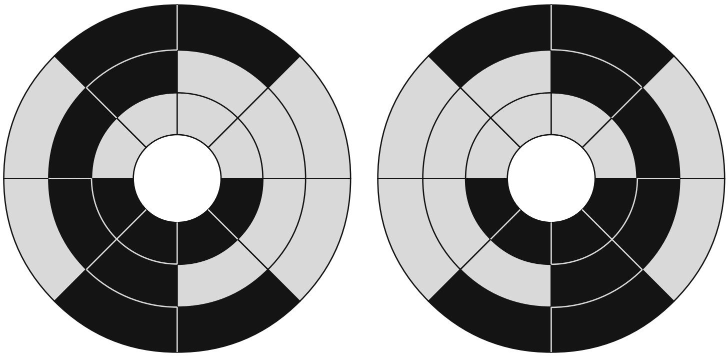


Fig. 18.1. A Gray Code: (a) Standard Case; (b) Flipped by 180° Around the Vertical Line

rotation from one sector into an adjacent one, then the codes listed cannot be unique. One way in which the code can be changed and still preserve this property is that the disk can be flipped 180° along the vertical before being inserting it into the encoder housing. Figure 18.1(a) shows an encoder painted in the standard way. Any planar rotation of this constitutes an equivalent painting. Figure 18.1(b) shows an encoder pattern that results from flipping it out of plane around the vertical line by 180°. Since these two patterns cannot be related to each other through an in-plane rotation, they represent two different Gray codes. It corresponds to a transformation of the form

$$\begin{array}{c} 000\\ 001\\ 011\\ 010\\ 110\\ 111\\ 101\\ 100 \end{array} \quad \Longrightarrow \quad \begin{array}{c} 010\\ 011\\ 001\\ 000\\ 100\\ 101\\ 111\\ 110 \end{array} \tag{18.13}$$

Another way to construct new Gray codes from existing ones is to invert the colors; that is, replace the annular sections that are painted with clear ones and vice versa. For the three-bit case, this is equivalent to making the following change:

$$\begin{array}{c} 000\\ 001\\ 011\\ 010\\ 110\\ 111\\ 101\\ 100 \end{array} \quad \Longrightarrow \quad \begin{array}{c} 111\\ 110\\ 100\\ 101\\ 001\\ 000\\ 010\\ 011 \end{array} \tag{18.14}$$

These two sequences are not cyclically reordered versions of each other. This transformation results in the Gray code in Figure 18.2(a). Applying both the 180° flipping and color inversion results in the encoder in Figure 18.2(b).

How else might an existing Gray code be modified while preserving the property that they change one bit per incremental rotation? It is not difficult to imagine that reflecting the painting through the center point or about any of the lines separating sectors. It would seem a priori that such operations could be used as a way to change a given Gray

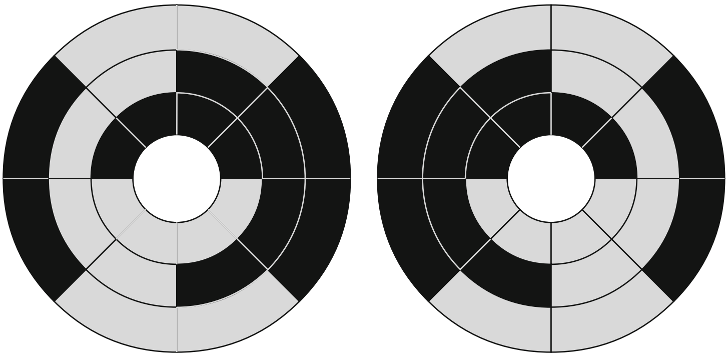


Fig. 18.2. Inverted Gray Code: (a) Inverted from Standard Case; (b) Inverted and Flipped by 180° Around the Vertical Line

code into another one that preserves the essential property of one bit per incremental rotation. However, it is easy to verify in the three-bit case that this produces, to within a planar rotation, exactly the same paintings as one of the four shown in Figures 18.1 and 18.2.

Another operation that can be performed on an existing Gray code that preserves this property is reversing the order of the paintings from the inner most annulus. This would be equivalent to making

$$\begin{array}{c} 000 \\ 001 \\ 011 \\ 010 \\ 110 \\ 111 \\ 101 \\ 100 \end{array} \Longrightarrow \begin{array}{c} 000 \\ 100 \\ 110 \\ 010 \\ 011 \\ 111 \\ 101 \\ 001 \end{array} \qquad (18.15)$$

Although this is a valid code mathematically, it is not as desirable as the others physically for use in optical disk encoders because the innermost bit must change more frequently than in the other codes. This means that on the encoder disk, there would be more opportunity for misreading the inner bit, since it would change state more frequently than with other codes. For this reason, it will be put aside for now.

Let the "flipping" transformation in (18.13) be labeled as "a" and the "color-inversion" transformation in ((18.14) is labeled as "b"). Then it makes sense to compose these operations and it can be verified that "flipping then inverting color" gives the same result as "inverting color followed by flipping." In other words, $a \circ b = b \circ a$. Let this result be called "c," and let the "do nothing" operation on a code be denoted as "e." Then the following group multiplication table can be constructed:

$$\begin{array}{c|cccc} \circ & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array} \qquad (18.16)$$

If the characters $\{e, a, b, c\}$ are identified with the numbers $\{0, 1, 2, 3\}$ and the composition operation $\circ$ is identified with addition modulo 4, then the group tables match up also. This is an example of a group isomorphism. In other words, if $\phi : \{e, a, b, c\} \rightarrow \{0, 1, 2, 3\}$ with $\phi(e) = 0$, $\phi(a) = 1$, $\phi(b) = 2$, and $\phi(c) = 3$, then this is an invertible function with the properties

$$\phi(a \circ b) = \phi(a) + \phi(b) \bmod 4 \quad \text{and} \quad \phi^{-1}(0) = e, \; \phi^{-1}(1) = a, \text{ etc.} \tag{18.17}$$

18.4.3 de Bruijn Sequences

The same Gray codes used in optical disk encoders could be implemented in a very different way physically. Specifically, instead of having sensor and LED on each side of a disk, it is possible to use two kinds of paint: one reflective (e.g., high-gloss white) and one absorbing (e.g., flat black) and having both the LED and sensor on the *same* side of the disk. Furthermore, encoding the orientation of a shaft by painting a disk that moves in the plane normal to the shaft is not the only strategy. By painting the sequence for each bit in reflective or absorbing colors at different heights on a cylinder and having the sensor and LED situated at the appropriate heights along the cylinder and pointing toward the inward normal of this cylinder, it is possible to implement a Gray-code-based encoder without any disk in the normal plane. This has the advantage that all of the bits have the same visibility from the perspective of the sensor, and so the code defined in (18.15) becomes equally viable as the other Gray codes.

If painting on the shaft (or a cylinder concentric with the shaft) is used as an alternative to an optical disk encoder, then other possible encoding schemes open up as well. One such scheme is the use of *de Bruijn sequences* painted on the shaft rather than Gray codes. An n-bit de Bruijn sequence in the characters “0” and “1” is a sequence of 2^n in which every possible sequence of length n is contained. For example, three-bit and four-bit de Bruijn sequences are respectively 00010111 and 0000111101100101. Recursive schemes for generating longer sequences exist. Note that unlike the Gray code painted on a cylinder, the sensors in the case of a de Bruijn code are spaced around one circle rather than parallel to the cylinder’s axis.

The history of the de Bruijn sequence in two characters, attributed to the general paper [11] which holds for such sequences in many characters, was actually worked out long before. Even today, there is research into new methods for rotary encoding. See, for example, [13].

18.4.4 A Binary Spherical-Motion Encoder

In a number of applications, it is desirable to have a ball-like motor that can rotate in any direction while keeping its center fixed. For such motors, the problem of encoding spherical motion becomes important. One solution to this problem is addressed in [35, 38]. Basically, LED–sensor pairs can be distributed within the socket in which the ball rotates. The distribution itself is not critical, as long as they are not closely clumped together. The ball is painted in flat black and glossy white regions. The shape of these regions is also not critical, but the painting should not possess rotational symmetry, otherwise ambiguities about the orientational state will result. Figure 18.3 shows the pattern of black and white triangles painted on the two hemispheres of the spherical encoder developed in the authors lab. The LED–sensor pairs were arranged to sit uniformly on circular rings (Figure 18.4(b)) that are inserted around each electromagnet in the stator assembly (Figure 18.4(a)) that forms the socket in which the ball rotates. A ring of ball bearings at the top of the hemisphere and ball bearings situated on posts around the stator cavity support the ball.

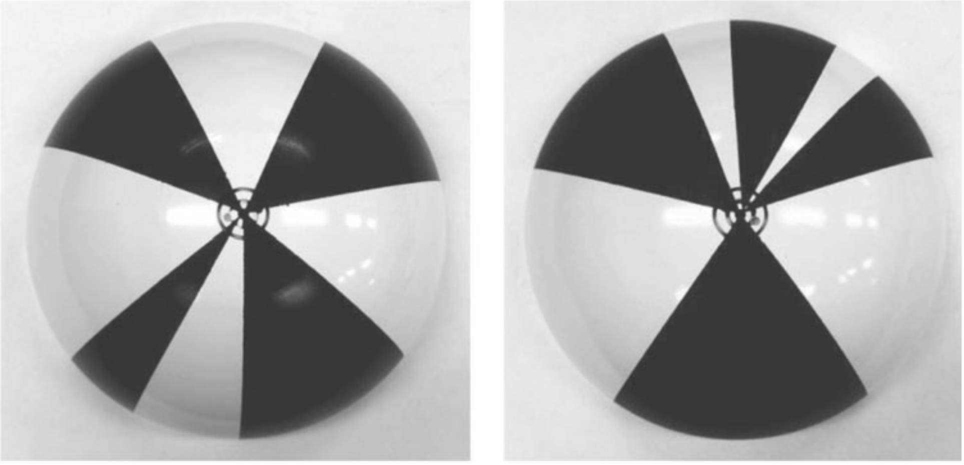


Fig. 18.3. The Rotor/Ball of a Spherical Encoder [35, 38]

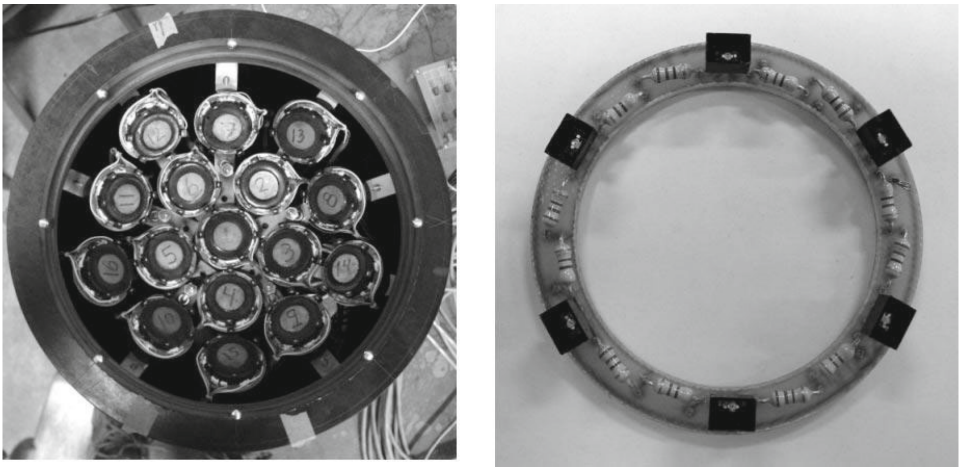


Fig. 18.4. (a) The Stator/Socket of a Spherical Motor; (b) Photosensor Ring Placed Around Each Stator Electromagnet [35, 38]

The orientational decoding problem then becomes one of determining what the orientation of the ball is, given a sequence of binary (black or white) measurements observed by the sensors. Mathematically, since the painting of the ball, $\pi : S^2 \to \{0,1\}$, and positions of the sensors, $\{\mathbf{c}_i \mid i = 1, \ldots, n\}$, are both known and since the corresponding sensor measurements $\{s_i \mid i = 1, \ldots, n\}$ are provided by the hardware, the decoding problem becomes that of finding the rotation matrix, $R \in SO(3)$, such that

$$f_p(R) = \left(\sum_{i=1}^{n} |\pi(R^T \mathbf{c}_i) - s_i|^p \right)^{\frac{1}{p}} \tag{18.18}$$

is minimized. Here, $p = 1$ or $p = 2$ would be the most common choices. Or, by normalizing as

$$s_i' = \frac{s_i}{\sum_{j=1}^{n} s_j} \quad \text{and} \quad \pi'(R^T \mathbf{c}_i) = \frac{\pi(R^T \mathbf{c}_i)}{\sum_{j=1}^{n} \pi(R^T \mathbf{c}_j} \, ,$$

an information-based divergence can be used as the cost function [5]:

$$f_{KL}(R) = \sum_{i=1}^{n'} s_i' \log\left(\frac{s_i'}{\pi'(R^T \mathbf{c}_i)}\right),$$

where the sum is taken over all values of s_i' and $\pi'(R^T \mathbf{c}_i)$ that are nonzero.

In any case, for any such cost function, $f(R)$, if the painting and sensor placements are both chosen so as to be compatible, then when $f(R) = 0$, the resulting $R \in SO(3)$ will be the orientation of the ball (to within the resolution of the spherical encoder). Thus, the problem of decoding spherical motion becomes one of minimization over the rotation group. Several approaches to solving this spherical decoding problem have been explored by the author and collaborators [38]. Similar problems can be formulated in relation to planting factory floors for the positional localization of mobile robots [36].

From a mechanical perspective, the design of the spherical motor is concerned with how the magnets/electromagnets should be placed in the rotor and stator so as to achieve good performance [4]. This is related to the topic of *spherical codes*, which is concerned with placing a finite set of points on the sphere as evenly as possible [12]. The related concept of *spherical designs* addresses sampling points on the sphere so as to develop quadrature rules to compute integrals of certain classes of functions on the sphere (e.g., bandlimited in terms of spherical harmonics) exactly as finite sums at the points in the design. These concepts relate to the design of efficient strategies in classical coding theory.

Related concepts are relevant to problems in quantum information theory in which it is desirable to replace computations of integrals over unitary groups with finite sums evaluated at special points. See, for example, [16] and references therein.

18.5 The Design of Medical Fiducials and the Language of Surgical Operations

In Section 5.2, a prototypical medical imaging problem (the three-dimensional–to–two-dimensional conical projection of a circle with arbitrary spatial position and orientation) was formulated using methods from parametric and implicit geometry. This can be viewed from the perspective of information theory, where the "sent message" is the position and orientation (modulo symmetry) of the circle, the "channel" is the X-ray projection process, and the "received message" is the resulting projection onto sensors embedded in a table. The goal is to recover the sent message as best as possible from the received one. Here, the "noise" is due to a combination of limited resolution of the photosensors in the table, the background clutter resulting from the projection of skeletal and other anatomical features,[7] and inhomogeneity of the X-ray source. This channel has memory, in the sense that we know what we are looking for in the projection.

In contrast to the problem of hip replacement discussed in Section 5.2 in which the size and shape of the circle is fixed in advance by mechanical performance constraints, we can ask similar questions related to the *design* of small three-dimensional patterns that can be attached to surgical instruments. Such patterns are called *fiducial markers.* They are used so that the three-dimensional position and orientation of these instruments can

[7] In the context of medical diagnosis problems such as reading a chest X-ray, this "clutter" actually is the message.

be tracked from their projections in X-ray images. An ideal design would be the one that is most robust under the ensemble of all possible poses of the tool (which can be described in terms of probability densities on $SE(3)$ based on the frequency of occurrence of poses recorded from prior medical procedures).

Let D denote the space of all feasible designs constructed from an “alphabet” of primitives, each “letter” of which is easy to manufacture (such as line segments, circles, and small solid spheres). These letters can be assembled into a more complex pattern. The resulting “word” in a sent message is then this pattern at a specific position and orientation in space. Since it is impractical to redesign a pattern for use at each different pose, the goal is to design the single pattern that is most robust given the distribution $\rho(g)$ of poses experienced in typical surgical procedures. In other words, we seek the specific fiducial pattern design $d^* \in D$ such that

$$C(d) = \max_{g \sim \rho(g)} \mathcal{I}(X(g \in G, d \in D); Y(m)), \tag{18.19}$$

where X is the sent message (that depends on both the pose g and the design d) and Y is the received message, which depends on the the method, m, of feature extraction in the projection image. The geometric design of such fiducials has been investigated in [21, 27] without using information-theoretic concepts.

A related problem, arises in the treatment of prostate cancer. One treatment method (called *brachytherapy*) involves the insertion of radioactive pellets (called seeds) into the prostate for direct ablation of the cancer and surrounding tissue. In brachytherapy, a cloud of on the order of 100 seeds is formed that is consistent with a surgical plan based on preoperative anatomical information.This plan is executed so as to deliver a desired dose profile. However, after the seeds are inserted, the prostate swells, and the seeds migrate. Therefore, the desired dose is not actually achieved. Follow-up involves taking X-ray projections from two or three different directions. From these projections, one can attempt to recover the full three-dimensional distribution of seeds [22]. This can be formulated as a communication/coding problem similar to the fiducial problem discussed earlier. Here, the intended seed cloud is the original message. The channel consists of the whole process of seed insertion and reconstruction of the seed cloud from projection information. Distortion arises because no insertion process is perfect, the effects of swelling cannot be modeled perfectly in advance, and seeds can occlude other seeds, making it impossible to uniquely recover the original distribution always.

All of the problems reviewed here have both a geometric and information-theoretic flavor that have not yet been fully exploited.

18.6 Chapter Summary

This chapter provided a concrete introduction to algebraic structures such as rings and fields and has demonstrated their relationship to certain kinds of groups and applications in error-correcting codes. Several connections among information theory, geometry and group theory have been illustrated. Many other such connections exist. For example, Golay developed a $(23, 11)$ code that has the ability to correct up to three errors. The relationship between this code and the densest known packing of congruent spheres in $\mathbb{R}^{24}$ (called the Leech lattice), and the symmetry group of this lattice, have been established. Another topic relating to group theory is that of error correction within digital devices, which has also been addressed using concepts from harmonic analysis on finite groups [25, 26]. For reading on further connections between lattices, codes, spherical designs, and geometry, see [31].

Very different from this sort of discrete geometry problem are the continuous information theory problems that result from encoding motion and transmitting information with physical devices in continuous space. Rotary/spherical encoders and the design of fiducial patterns for surgical applications are examples of coding theory interacting with the geometric/physical world. Lie groups arise in these contexts in very natural ways. Therefore, this chapter can be viewed as a bridge between the stochastic processes in continuous space studied earlier in this book (which had very little to do with group theory) and the discrete-group-theoretic problems that arise in classical coding and communications theory.

In recent years, information-theoretic problems involving the Grassmann and Stiefel manifolds discussed in Chapter 16 have arisen in the context of coding [9–11, 18, 42]. Unitary matrices have arisen in modulation problems [19]. Recent works use the symplectic group $Sp(2)$ [23] and the special unitary group $SU(3)$ [24] for coding in MIMO systems. Other connections between multi-antenna communications, geometry, and statistics are discussed in the references of Chapter 16 in the context of random matrix theory.

A major goal in coding theory is to construct and analyze codes that come as close as possible to the limits established by Shannon for classical communication problems [1, 6], as well as to establish codes for modern distributed communication problems, [40]. Keeping with the general theme of this book, this chapter has reviewed only those aspects of coding theory that have a group-theoretic or geometric flavor. Further reading on these topics can be found in [3, 20, 37, 41].

18.7 Exercises

18.1. Use the same reasoning as in the derivation of (17.6) to prove that

$$p(E_1 \cap E_2 \cap E_3 \cap E_4) = p(E_1 \mid E_2 \cap E_3 \cap E_4)\, p(E_2 \mid E_3 \cap E_4)\, p(E_3 \mid E_4)\, p(E_4).$$

18.2. Prove the inequalities in (17.14).

18.3. Prove the equality in (17.16).

18.4. Prove the equality in (17.17)

18.5. Prove the equality in (17.18)

18.6. If $\Phi_i : \mathbb{R} \to \mathbb{R}$ for $i = 1$ and 2 are convex functions, will the composed function $\Phi_1 \circ \Phi_2$ be convex also?

18.7. Since permutation matrices have zeros and ones and have determinants of ±1, it is clear that $\Pi_n \subseteq GL(n, \mathbb{F}_2)$. In the case of $n = 2$, we have seen that Π_2 has two elements and $GL(2, \mathbb{F}_2)$ has six. (a) Try to find an element of $GL(7, \mathbb{F}_2)$ that is not a permutation; (b) If in Subsection 18.2.3 the permutation π in (18.10) is replaced with the element of $GL(7, \mathbb{F}_2)$ that you have obtained, will the resulting $G', H'K'$ be valid $(7, 4)$ error-correcting codes? Explain.

18.8. If H and K are subgroups of G, prove that $H \cap K$ is also a subgroup of G.

18.9. If H and K are subgroups of G, prove that HK is a subgroup of G if and only if $HK = KH$.

18.10. The *quaternions* are a number system where each element is of the form $q = q_0 + iq_1 + jq_2 + kq_3$. They can be viewed as an extension of the field of complex numbers where instead of the sole rule $i^2 = -1$, the rules $i^2 = j^2 = k^2 = ijk = -1$ apply. (a) Show that from these properties it follows that $ij = k = -ji$, $jk = i = -kj$, and $ki = j = -ik$. The set of quaternions is often denoted as $\mathbb{H}$ (after their inventor, Sir Hamilton). The set of all quaternions together with the two operations of scalar addition and multiplication do not quite form a field (because multiplication is not commutative). They are sometimes called a *skew field* or *division algebra*. The subset of quaternions defined by the constraint $q_0^2 + q_1^2 + q_2^2 + q_3^2 = 1$ form a group under multiplication, and this group is useful for describing rotations in $\mathbb{R}^3$. (b) Is $GL(2, \mathbb{H})$ a valid definition of a group? Explain.

References

1. Ahlswede, R., "Group codes do not achieve Shannon's channel capacity for general discrete channels," *Ann. Math. Statist.*, 42(1), pp. 224–240, 1971.
2. Ash, A., Gross, R., *Fearless Symmetry: Exposing the Hidden Patterns of Numbers*, Princeton University Press, Princeton, NJ, 2006.
3. Berlekamp, E.R., *Algebraic Coding Theory*, Aegean Park Press, Laguna Hills, CA, 1984.
4. Chirikjian, G.S., Stein, D., "Kinematic design and commutation of a spherical stepper motor," *IEEE/ASME Trans. Mechatron.*, 4(4), pp. 342–353, 1999.
5. Chirikjian, G.S., Kim, P.T., Koo, J.Y., Lee, C.H., "Rotational matching problems," *Int. J. Comput. Intell. Applic.*, 4(4), pp. 401–416, 2004.
6. Chung, S.-Y., Forney, G.D., Jr., Richardson, T.J., Urbanke, R., "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," *IEEE Commun. Lett.*, 5, pp. 58–60, 2001.
7. Conway, J.H., Sloane, N.J.A., *Sphere Packings, Lattices and Groups*, 3rd ed., Springer, New York, 1999.
8. Coxeter, H.S.M., "The problem of packing a number of equal nonoverlapping circles on a sphere," *Trans. NY Acad. Sci.*, 24, pp. 320–331, 1962.
9. Dai, W., Liu, Y., Rider, B., "Volume growth and general rate quantization on Grassmann manifolds," *IEEE Global Telecommunications Conference (GLOBECOM)*, 2007.
10. Dai, W., Liu, Y., Rider, B., "Quantization bounds on Grassmann manifolds and applications to MIMO communications," *IEEE Trans. Inform. Theory*, 54(3), pp. 1108–1123, 2008.
11. de Bruijn, N.G. "A combinatorial problem," *Koninklijke Nederlandse Akademie Wetenschappen*, 49, pp. 758–764, 1946.
12. Delsarte, P., Goethals, J.M., Seidel, J.J., "Spherical codes and designs," *Geom. Dedicata*, 6, pp. 363–388, 1977.
13. Fuertes, J.M., Balle, B., Ventura, E., "Absolute-type shaft encoding using LFSR sequences with a prescribed length," *IEEE Trans. Instrum. Measur.*, 57(5), pp. 915–922, 2008.
14. Golay, M.J.E., "Notes on digital coding," *Proc. IRE*, 37, p. 657, 1949.
15. Gray, F., "Pulse code communication," US Patent 2632058, March 1958.
16. Gross, D., Audenaert, K., Eisert, J., "Evenly distributed unitaries: On the structure of unitary designs," *J. Math. Phys.*, 48, p. 052104, 2007.
17. Hamming, R.W., *Coding and Information Theory*, 2nd ed., Prentice-Hall, Englewood Cliffs, NJ, 1986.
18. Henkel, O., "Sphere-packing bounds in the Grassmann and Stiefel manifolds," *IEEE Trans. Inform. Theory*, 51(10), pp. 3445–3456, 2005.
19. Hochwald, B.M., Marzetta, T.L., "Unitary space-time modulation for multiple-antenna communication in Rayleigh flat-fading," *IEEE Trans. Inform. Theory*, 46, pp. 543–564, 2000.

20. Huffman, W.C., Pless, V., *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, 2003.
21. Jain, A.K., Mustafa, T., Zhou, Y., Burdette, C., Chirikjian, G.S., Fichtinger, G., "FTRAC—A robust fluoroscope tracking fiducial," *Med. Phys.*, 32(10), pp. 3185–3198, 2005.
22. Jain, A., Zhou, Y., Mustufa, T., Burdette, E.C., Chirikjian, G.S., Fichtinger, G., "Matching and reconstruction of brachytherapy seeds using the Hungarian algorithm (MARSHAL)," *Med. Phys.*, 32(11), pp. 3475–3492, 2005.
23. Jing, Y., Hassibi, B., "Design of fully-diverse multiple-antenna codes based on $Sp(2)$," *IEEE Trans. Inform. Theory*, 50(11), pp. 2639–2656, 2004.
24. Jing, Y., Hassibi, B., "Three-transmit-antenna space-time codes based on $SU(3)$," *IEEE Trans. Signal Process.*, 53(10), pp. 3688–3702, 2005.
25. Karpovsky, M.G., "Fast Fourier transforms on finite non-Abelian groups," *IEEE Trans. Computers*, 26(10), pp. 1028–1030, 1977.
26. Karpovsky, M.G., Stankovic, R.S., Astola, J.T., *Spectral Logic and Its Applications for the Design of Digital Devices*, Wiley-Interscience, New York, 2008.
27. Lee, S., Fichtinger, G., Chirikjian, G.S., "Novel algorithms for robust registration of fiducials in CT and MRI," *Med. Phys.*, 29(8), pp. 1881–1891, 2002.
28. Leech, J., "Some sphere packings in higher space," *Can. J. Math.*, 16, pp. 657–682, 1964.
29. Moon, T.K., *Error Correction Coding: Mathematical Methods and Algorithms*, John Wiley and Sons, New York, 2005.
30. Nebe, G., Rains, E.M., Sloane, N.J.A., *Self-Dual Codes and Invariant Theory*, Algorithms and Computation in Mathematics Vol. 17, Springer, New York, 2006.
31. Neutsch, W., *Coordinates*, Walter de Gruyter and Co., Berlin, 1996.
32. Pless, V., *Introduction to the Theory of Error-Correcting Codes*, 3rd ed., John Wiley and Sons, New York, 1998.
33. Rogers, C.A., "The packing of equal spheres," *Proc. London Math. Soc., Ser. 3*, 8, pp. 609–620, 1958.
34. Rogers, C.A., *Packing and Covering*, Cambridge University Press, Cambridge, 1964.
35. Scheinerman, E., Chirikjian, G.S., Stein, D., "Encoders for spherical motion using discrete sensors," in Algorithmic and Computational Robotics: New Directions 2000 WAFR (B. Donald, K. Lynch, D. Rus, eds.), A.K. Peters, Natick, Mass., 2001.
36. Scheinerman, E.R., "Determining planar location via complement-free de Brujin sequences using discrete optical sensors," *IEEE Trans. Robot. Autom.*, 17(6), pp. 883–889, 2001.
37. Sloane, N.J.A., *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, Elsevier, Amsterdam, 1977.
38. Stein, D., Scheinerman, E.R., Chirikjian, G.S., "Mathematical models of binary spherical-motion encoders," *IEEE-ASME Trans. Mechatron.*, 8(2), pp. 234–244, 2003.
39. Stephenson, K., *Introduction to Circle Packing, the Theory of Discrete Analytic Functions*, Cambridge University Press, Cambridge, 2005.
40. Tarokh, V., Seshadri, N., Calderbank, A.R., "Space-time codes for high data rate wireless communication: Performance criterion and code construction," *IEEE Trans. Inform. Theory*, 44(2), pp. 744–765, 1998.
41. Thompson, T.M., *From Error-Correcting Codes through Sphere Packings to Simple Groups*, The Carus Mathematical Monographs No. 21, Mathematical Association of America, Washington, DC, 1983.
42. Zheng, L., Tse, D.N.C., "Communication on the Grassmann manifold: A geometric approach to the noncoherent multiple-antenna channel," *IEEE Trans. Inform. Theory*, 48(2), pp. 359–383, 2002.

19

Information Theory on Lie Groups

Classical inequalities used in information theory such as those of de Bruijn, Fisher, Cramér, Rao, and Kullback carry over in a natural way from Euclidean space to unimodular Lie groups. The extension of core information-theoretic inequalities defined in the setting of Euclidean space to this broad class of Lie groups is potentially relevant to a number of problems relating to information-gathering in mobile robotics, satellite attitude control, tomographic image reconstruction, biomolecular structure determination, and quantum information theory. In this chapter, several definitions are extended from the Euclidean setting to that of Lie groups (including entropy and the Fisher information matrix), and inequalities analogous to those in classical information theory are derived and stated in the form of more than a dozen theorems. In all such inequalities, addition of random variables is replaced with the group product, and the appropriate generalization of convolution of probability densities is employed.

This chapter has several goals:

- To extend the inequalities of classical continuous (differential) information theory to the setting of probabilities on Lie groups;
- To illustrate how splitting integrals over groups such as subgroup-coset decomposition can lead to conditional probabilities and associated information-theoretic inequalities;
- To understand how the bi-invariance of the integration measure on unimodular Lie groups and the properties of Lie derivatives lead to interesting definitions and properties of Fisher information matrices.

This chapter consists of several sections. Section 19.1 reviews the related literature. Section 19.2 defines entropy and relative entropy for unimodular groups (both finite-dimensional Lie groups and discrete groups) and proves some of their properties under convolution and marginalization over subgroups and coset spaces. The concept of the Fisher information matrix for probability densities on unimodular Lie groups is defined in Section 19.3 and several elementary properties are proven regarding how these quantities behave under convolution of pdfs. This generalized concept of Fisher information is used in Section 19.4 to establish the de Bruijn inequality for unimodular Lie groups. These definitions and properties are combined with recent results by others on log-Sobolev inequalities in Section 19.5. Section 19.6 derives a version of the Cramér-Rao bound for concentrated pdfs on Lie groups. Section 19.7 discusses entropy powers. Section 19.8 summarizes the chapter and Section 19.9 provides exercises.

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_10,

19.1 Introduction and Literature Review

Shannon's brand of information theory is now more than six decades old, and some of the statistical methods developed by Fisher, Kullback, and so forth are even older. Similarly, the study of Lie groups is now more than a century old. Despite their relatively long and roughly parallel history, surprisingly few connections appear to have been made between these two vast fields. The only attempts to do so known to the author include those of Johnson and Suhov [22, 23] from an information-theoretic perspective and Maksimov [28] and Roy [30] from a probability perspective.

The goal of this chapter is therefore to present analytical foundations for "information theory on Lie groups." Unlike extensions of information theory to manifolds, the added structure inherent in Lie groups allow us to draw much stronger parallels with inequalities of classical information theory, such as those presented in [12, 15].

Johnson and Suhov [22, 23] use the concept and properties of information-theoretic entropy and the Kullback–Leibler divergence between pdfs on compact Lie groups to study the convergence to uniformity under iterated convolutions, in analogy with what was done by Linnik [27] and Barron [4] in the commutative case. The goal of the present chapter is complementary: Using some of the same tools, many of the main quantities and inequalities of (differential) information theory are extended from $\mathbb{R}^n$ to the context of unimodular Lie groups, which form a broader class of Lie groups than compact ones.

Several other research areas that would initially appear to be related to the present work have received intensive interest. Decades ago, Amari and Csiszár developed the concept of information geometry [1, 13] in which the Fisher information matrix is used to define a Riemannian metric tensor on spaces of probability distributions, thereby allowing those spaces to be viewed as Riemannian manifolds. This provides a connection between information theory and differential geometry. However, in information geometry, the probability distributions themselves (such as Gaussian distributions) are defined on a Euclidean space rather than on a Lie group. The presentation provided here opens up the possibility of defining information geometries on spaces of functions on Lie groups.

This chapter attempts to address this deficit with a two-pronged approach: (1) by collecting some known results from the functional analysis literature and reinterpreting them in information-theoretic terms (e.g. Gross' log-Sobolev inequality on Lie groups) and (2) by defining information-theoretic quantities such as entropy and Fisher information matrix and deriving inequalities involving these quantities that parallels those in classical information theory.

19.2 Properties of Entropy and Relative Entropy on Groups

The entropy of a pdf on a unimodular Lie group is defined as

$$S(f) = -\int_G f(g) \log f(g)\, dg.$$

For example, the entropy of a Gaussian distribution on $(G, \circ) = (\mathbb{R}^n, +)$ with covariance Σ is

$$S(\rho(g;t)) = \log\{(2\pi e)^{n/2} |\Sigma(t)|^{\frac{1}{2}}\}, \tag{19.1}$$

where $\log = \log_e$.

The Kullback–Leibler divergence between the pdfs $f_1(g)$ and $f_2(g)$ on a Lie group G naturally generalizes from its form in $\mathbb{R}^n$ as

$$D_{KL}(f_1(g)\|f_2(g)) = \int_G f_1(g)\log\left(\frac{f_1(g)}{f_2(g)}\right)\,dg. \tag{19.2}$$

As with the case of pdfs in $\mathbb{R}^n$, $D_{KL}(f_1\|f_2) \geq 0$. Equality holds in this expression if (but not only if) $f_1 = f_2$. More precisely, if $D_{KL}(f_1\|f_2) = 0$, then $f_1(g) = f_2(g)$ at "almost all" values of $g \in G$ (or, in probability terminology, "$f_1(g) = f_2(g)$ almost surely"); that is, they must be the same up to a set of measure zero.

If the set G can be decomposed into a product space $G = D_1 \times D_2$ (such as if G is a direct or semi-direct product or if integrals over G can be decomposed into separate integrals over G/H and H when $H < G$), then if $g = (h_1, h_2) \in D_1 \times D_2$, we can write

$$D_{KL}(f_1(g)\|f_2(g)) = D_{KL}(f_1(h_1,h_2)\|f_2(h_1,h_2)).$$

Furthermore, if $f_i(h_1|h_2) \doteq f_i(h_1,h_2)/f_i(h_2)$ is a conditional density (which is a pdf in the first argument), then the fact that

$$D_{KL}(f_1(h_1|h_2)\|f_2(h_1|h_2)) = \int_{D_1} f_1(h_1|h_2)\log\left(\frac{f_1(h_1|h_2)}{f_2(h_1|h_2)}\right)\,dh_1 \geq 0$$

immediately gives

$$D_{KL}(f_1(g)\|f_2(g)) \geq D_{KL}(f_1(h_2)\|f_2(h_2)). \tag{19.3}$$

This inequality will be used extensively later.

Something that is not true in $\mathbb{R}^n$ that holds for a compact Lie group is that the maximum-entropy distribution is constant that is equal to unity relative to the normalized Haar measure. Such a distribution can be considered the limiting distribution of the diffusion process in (20.14) as time goes to infinity. If $f_2(g) = 1$ is this sort of limiting distribution, then $D_{KL}(f_1\|1) = -S(f_1)$.

19.2.1 Entropy Inequalities from Jensen's Inequality

Jensen's inequality is a fundamental tool that is often used in deriving information-theoretic inequalities as well as inequalities in the field of convex geometry. In the context of unimodular Lie groups, Jensen's inequality can be written as

$$\Phi\left(\int_G \phi(g)\rho(g)\,dg\right) \leq \int_G \Phi(\phi(g))\rho(g)\,dg, \tag{19.4}$$

where $\Phi : \mathbb{R}_{\geq 0} \to \mathbb{R}$ is a convex function on the half infinite line, $\rho(g)$ is a pdf, and $\phi(g)$ is another non-negative measurable function on G.

Two important examples of $\Phi(x)$ are $\Phi_1(x) = -\log x$ and $\Phi_2(x) = +x\log x$. Using Jensen's inequality with Φ_2 gives the following result.

Theorem 19.1. *Given pdfs $f_1(g)$ and $f_2(g)$ on the unimodular Lie group G,*

$$S(f_1 * f_2) \geq \max\{S(f_1), S(f_2)\} \tag{19.5}$$

and

$$D_{KL}(f_1 \,\|\, f_2) \geq \max\left\{D_{KL}(f_1 * \phi \,\|\, f_2 * \phi), D_{KL}(\phi * f_1 \,\|\, \phi * f_2)\right\}. \tag{19.6}$$

Proof.

$$\begin{aligned}
-S(f_1 * f_2) &= \int_G \Phi_2((f_1 * f_2)(g))\, dg = \int_G \Phi_2\left(\int_G f_2(h^{-1} \circ g) f_1(h)\, dh\right) dg \\
&\leq \int_G \int_G \Phi_2(f_2(h^{-1} \circ g)) f_1(h)\, dh\, dg = \int_G \left(\int_G \Phi_2(f_2(h^{-1} \circ g))\, dg\right) f_1(h)\, dh \\
&= \int_G \left(\int_G \Phi_2(f_2(g))\, dg\right) f_1(h)\, dh = \left(\int_G \Phi_2(f_2(g))\, dg\right)\left(\int_G f_1(h)\, dh\right) \\
&= -S(f_2).
\end{aligned}$$

If, on the other hand, we were to use the version of convolution in the second equality in (12.28) and analogous manipulations as above, we would get $-S(f_1 * f_2) \leq -S(f_1)$, which completes the proof of (19.5).

The proof of (19.6) (which is the Lie-group version of the *data processing inequality*) follows from (19.3). Replace G with the direct product $G \times G$, and $D_1 = D_2 = G$. Then if $f_i(g)$ and $\phi(g)$ are pdfs on G, $f_i'(h,g) \doteq f_i(h)\phi(h^{-1} \circ g)$ will be a pdf on $G \times G$. The marginal of $f_i'(h,g)$ over g is simply $f_i(h)$. The marginal of $f_i'(h,g)$ over h is $(f_i * \phi)(g)$. Therefore, from (19.3),

$$D_{KL}(f_1 * \phi \| f_2 * \phi) \leq \int_G \int_G f_1(h)\phi(h^{-1} \circ g) \log\left(\frac{f_1(h)\phi(h^{-1} \circ g)}{f_2(h)\phi(h^{-1} \circ g)}\right) dh\, dg = D_{KL}(f_1 \| f_2).$$

A similar inequality results by performing convolutions in the reverse order.

If G is compact, any constant function on G is measurable. Letting $\phi(g) = 1$ and $\Phi(x) = \Phi_2(x)$ then gives $0 \leq -S(f)$ for a pdf $f(g)$. In contrast, for any unimodular Lie group, letting $\rho(g) = f(g)$, $\phi(g) = [f(g)]^\alpha$ and $\Phi(x) = \Phi_1(x)$ gives

$$-\log\left(\int_G [f(g)]^{1+\alpha} dg\right) \leq \alpha S(f). \tag{19.7}$$

This leads to the following theorem.

Theorem 19.2. *Let $\|\hat{f}(\lambda)\|$ denote the Frobenius norm and let $\|\hat{f}(\lambda)\|_2$ denote the induced 2-norm of the Fourier transform of $f(g)$ and define*

$$\begin{aligned}
D_2(f) &\doteq -\int_{\hat{G}} \log \|\hat{f}(\lambda)\|_2^2\, d(\lambda); \\
D(f) &\doteq -\int_{\hat{G}} \log \|\hat{f}(\lambda)\|^2\, d(\lambda); \\
\tilde{D}(f) &\doteq -\log \int_{\hat{G}} \|\hat{f}(\lambda)\|^2\, d(\lambda).
\end{aligned} \tag{19.8}$$

Then

$$S(f) \geq \tilde{D}(f) \quad \textit{and} \quad D(f) \leq D_2(f) \tag{19.9}$$

and

$$\begin{aligned} D_2(f_1 * f_2) &\geq D_2(f_1) + D_2(f_2), \\ D(f_1 * f_2) &\geq D(f_1) + D(f_2). \end{aligned} \tag{19.10}$$

Furthermore, denote the unit Heaviside step function on the real line as $u(x)$ *and let*

$$B = \int_{\hat{G}} u\left(\|\hat{f}(\lambda)\|\right) d(\lambda).$$

Then

$$\tilde{D}(f) + \log B \leq D(f)/B. \tag{19.11}$$

Proof. Substituting $\alpha = 1$ into (19.7) and using the Plancherel formula (12.70) yields

$$S(f) \geq -\log\left(\int_G [f(g)]^2 dg\right) = -\log\left(\int_{\hat{G}} \|\hat{f}(\lambda)\|^2 d(\lambda)\right) = \tilde{D}(f).$$

The fact that $-\log x$ is a decreasing function and $\|A\|_2 \leq \|A\|$ for all $A \in \mathbb{C}^{n\times n}$ gives the second inequality in (19.9).

The convolution theorem together with the facts that both norms are submultiplicative, $-\log(x)$ is a decreasing function, and the log of the product is the sum of the logs gives

$$\begin{aligned} D(f_1 * f_2) &= -\int_{\hat{G}} \log \|\widehat{f_1 * f_2}(\lambda)\|^2 d(\lambda) = -\int_{\hat{G}} \log \|\hat{f}_1(\lambda)\hat{f}_2(\lambda)\|^2 d(\lambda) \\ &\geq D(f_1) + D(f_2). \end{aligned}$$

An identical calculation follows for D_2. The statement in (19.11) follows from the Plancherel formula (12.70) and using Jensen's inequality (19.4) in the dual space $\hat{G}$ rather than on G:

$$\Phi\left(\int_{\hat{G}} \|\hat{\phi}(\lambda)\|\rho(\lambda)\, d(\lambda)\right) \leq \int_{\hat{G}} \Phi(\|\hat{\phi}(\lambda)\|)\rho(\lambda)\, d(\lambda), \tag{19.12}$$

where

$$\int_{\hat{G}} \rho(\lambda)\, d(\lambda) = 1 \quad \text{and} \quad \rho(\lambda) \geq 0.$$

Recognizing that when B is finite $\rho(\lambda) = u(\|\hat{f}(\lambda)\|)/B$ becomes a probability measure on this dual space, it follows that

$$\begin{aligned} \tilde{D}(f) &= -\log\left(\int_{\hat{G}} \|\hat{f}(\lambda)\|^2 d(\lambda)\right) = -\log\left(B\int_{\hat{G}} \|\hat{f}(\lambda)\|^2 \rho(\lambda)\, d(\lambda)\right) \\ &\leq -\log B - \int_{\hat{G}} \log\left(\|\hat{f}(\lambda)\|^2\right) \rho(\lambda)\, d(\lambda) = -\log B + D(f)/B. \end{aligned}$$

This completes the proof.

By definition, bandlimited expansions have B finite in these expressions. Properties of dispersion measures similar to $D(f)$ and $D_2(f)$ were studied in [18], but no connections to entropy were provided.

19.2.2 Entropy and Decompositions

Aside from the ability to sustain the concept of convolution, one of the fundamental ways that groups resemble Euclidean space is the way in which they can be decomposed. In analogy with the way that an integral over a vector-valued function with argument $\mathbf{x} \in \mathbb{R}^n$ can be decomposed into integrals over each coordinate, integrals over Lie groups can also be decomposed in natural ways. This has implications with regard to inequalities involving the entropy of pdfs on Lie groups. Analogous expressions hold for finite groups, with volume replaced by the number of group elements.

Theorem 19.3. *The entropy of a pdf on a unimodular Lie group is no greater than the sum of the marginal entropies on a subgroup and the corresponding coset space:*

$$S(f_G) \leq S(f_{G/H}) + S(f_H). \tag{19.13}$$

Proof. This inequality follows immediately from the non-negativity of the Kullback–Leibler divergence

$$D_{KL}(f_G \,\|\, f_{G/H} \cdot f_H) \geq 0.$$

For example, if $G = SE(n)$ is a Euclidean motion group and $H = SO(n)$ is the subgroup of pure rotations in n-dimensional Euclidean space, then $G/H \cong \mathbb{R}^n$, and an arbitrary element of $SE(n)$ is written as a pair $(R, \mathbf{t}) \in SO(n) \times \mathbb{R}^n$, then we can write

$$\begin{aligned}\int_{SE(n)} f(g)\, d(g) &= \int_{\mathbb{R}^n} \int_{SO(n)} f(R, \mathbf{t})\, dR\, d\mathbf{t} \\ &= \int_{SE(n)/SO(n)} \left(\int_{SO(n)} f((\mathbb{I}, \mathbf{t}) \circ (R, \mathbf{0}))\, dR \right) d\mathbf{t},\end{aligned}$$

and the marginal entropies on the right-hand side of (19.13) are those computed for pure rotations and pure translations.

Theorem 19.4. *The entropy of a pdf on a group is no greater than the sum of marginal entropies over any two subgroups and the corresponding double-coset space:*

$$S(f_G) \leq S(f_K) + S(f_{K\backslash G/H}) + S(f_H). \tag{19.14}$$

Proof. Let

$$\begin{aligned}f_K(k) &= \int_{K\backslash G/H} \int_H f_G(k \circ c_{K\backslash G/H}(KgH) \circ h)\, dh\, d(KgH), \\ f_H(h) &= \int_{K\backslash G/H} \int_K f_G(k \circ c_{K\backslash G/H}(KgH) \circ h)\, dk\, d(KgH),\end{aligned}$$

and

$$f_{K\backslash G/H}(KgH) = \int_K \int_H f_G(k \circ c_{K\backslash G/H}(KgH) \circ h)\, dh\, dk;$$

then again using the non-negativity of the Kullback–Leibler divergence

$$D_{KL}(f_G \,\|\, f_K \cdot f_{K\backslash G/H} \cdot f_H) \geq 0$$

gives (19.14).

Theorem 19.5. *The entropy of a pdf is no greater than the sum of entropies of its marginals over coset spaces defined by nested subgroups $H < K < G$:*

$$S(f_G) \leq S(f_{G/K}) + S(f_{K/H}) + S(f_H). \tag{19.15}$$

Proof. Given a subgroup K of H, which is itself a subgroup of G (i.e., $H < K < G$), apply (19.13) twice. Then $S(f_G) \leq S(f_{G/K}) + S(f_K)$ and $S(f_K) \leq S(f_{K/H}) + S(f_H)$, resulting in (19.15). Explicitly, $g = c_{G/K}(gK) \circ c_{K/H}(kH) \circ h$, and so, $f_G(g) = f_G(c_{G/K}(gK) \circ c_{K/H}(kH) \circ h)$. Therefore,

$$f_{G/K}(gK) = \int_{K/H} \int_H f_G(c_{G/K}(gK) \circ c_{K/H}(kH) \circ h)\, dh\, d(kH),$$

$$f_{K/H}(kH) = \int_{G/K} \int_H f_G(c_{G/K}(gK) \circ c_{K/H}(kH) \circ h)\, dh\, d(gK),$$

and

$$f_H(h) = \int_{G/K} \int_{K/H} f_G(c_{G/K}(gK) \circ c_{K/H}(kH) \circ h)\, d(kH)\, d(gK).$$

19.2.3 When Inequivalent Convolutions Produce Equal Entropy

In general, $(\rho_1 * \rho_2)(g) \neq (\rho_2 * \rho_1)(g)$. Even so, it can be the case that $S(\rho_1 * \rho_2)(g) = S(\rho_2 * \rho_1)(g)$. This section addresses several special cases when this equality holds.

Let G denote a unimodular Lie group, and for arbitrary $g, g_1 \in G$, define $\rho^{\#}(g) = \rho(g^{-1})$, $L_{g_1}\rho(g) = \rho(g_1^{-1} \circ g)$, $R_{g_1}\rho(g) = \rho(g \circ g_1)$, and $C_{g_1}\rho(g) = \rho(g_1^{-1} \circ g \circ g_1)$. Then if $\rho(g)$ is a pdf, it follows immediately that $\rho^{\#}(g)$, $L_{g_1}\rho(g)$, $R_{g_1}\rho(g)$, and $C_{g_1}\rho(g)$ are all pdfs. A function for which $\rho^{\#}(g) = \rho(g)$ is called symmetric, whereas a function for which $C_{g_1}\rho(g) = \rho(g)$ for all $g_i \in G$ is a class function (i.e., it is constant on conjugacy classes).

Theorem 19.6. *For arbitrary pdfs on a unimodular Lie group G and arbitrary g_1, $g_2 \in G$,*

$$\rho_1 * \rho_2 \neq \rho_2^{\#} * \rho_1^{\#} \neq L_{g_1}\rho_1 * R_{g_2}\rho_2 \neq C_{g_1}\rho_1 * C_{g_1}\rho_2;$$

however, entropy satisfies the equalities

$$S(\rho_1 * \rho_2) = S(\rho_2^{\#} * \rho_1^{\#}) = S(L_{g_1}\rho_1 * R_{g_2}\rho_2) = S(C_{g_1}\rho_1 * C_{g_1}\rho_2). \tag{19.16}$$

Proof. Each equality is proven by changing variables and using the unimodularity of the group.

$$\begin{aligned}(\rho_2^{\#} * \rho_1^{\#})(g) &= \int_G \rho_2^{\#}(h)\rho_1^{\#}(h^{-1} \circ g)\, dh = \int_G \rho_2(h^{-1})\rho_1(g^{-1} \circ h)\, dh \\ &= \int_G \rho_1(g^{-1} \circ k^{-1})\rho_2(k)\, dk = (\rho_1 * \rho_2)(g^{-1}) = (\rho_1 * \rho_2)^{\#}(g).\end{aligned}$$

Let $F[\rho] = -\rho \log \rho$. Then the integral over G of $F[\rho(g^{-1})]$ must be the same as $F[\rho(g)]$, proving the first equality in (19.16). The second equality follows from the fact that $(L_{g_1}\rho_1 * R_{g_2}\rho_2)(g) = (\rho_1 * \rho_2)(g_1 \circ g \circ g_2)$ and the integral of $F[\rho(g_1 \circ g \circ g_2)]$ must be the same as $F[\rho(g)]$. The final equality follows in a similar way from the fact that $(C_{g_1}\rho_1 * C_{g_1}\rho_2)(g) = (\rho_1 * \rho_2)(g_1^{-1} \circ g \circ g_1)$.

Note that the equalities in (19.16) can be combined. For example,

$$S(\rho_1 * \rho_2) = S(L_{g_1}\rho_2^{\#} * R_{g_2}\rho_1^{\#}) = S(C_{g_1}\rho_2^{\#} * C_{g_1}\rho_1^{\#}).$$

Theorem 19.7. *The equality $S(\rho_1 * \rho_2) = S(\rho_2 * \rho_1)$ holds for pdfs $\rho_1(g)$ and $\rho_2(g)$ on a unimodular Lie group G in the following cases: (a) $\rho_i(g)$ for $i = 1$ or $i = 2$ is a class function and (b) $\rho_i(g)$ for $i = 1, 2$ are both symmetric functions.*

Proof. Statement (a) follows from the fact that if either ρ_1 or ρ_2 is a class function, then convolutions commute. Statement (b) follows from the first equality in (19.16) and the definition of a symmetric function.

Theorem 19.8. *Given class functions $\chi_1(g)$ and $\chi_2(g)$ that are pdfs, then for general $g_1, g_2 \in G$,*

$$(\chi_1 * \chi_2)(g) \neq (L_{g_1}\chi_1 * L_{g_2}\chi_2)(g) \neq (R_{g_1}\chi_1 * R_{g_2}\chi_2)(g) \neq (R_{g_1}\chi_1 * L_{g_2}\chi_2)(g)$$

and yet

$$S(\chi_1 * \chi_2) = S(L_{g_1}\chi_1 * L_{g_2}\chi_2) = S(R_{g_1}\chi_1 * R_{g_2}\chi_2) = S(R_{g_1}\chi_1 * L_{g_2}\chi_2). \qquad (19.17)$$

Proof. Here, the first and final equalities will be proven. The middle one follows in the same way.

$$\begin{aligned}(L_{g_1}\chi_1 * L_{g_2}\chi_2)(g) &= \int_G (L_{g_1}\chi_1)(h) * (L_{g_2}\chi_2)(h^{-1} \circ g)\, dh \\ &= \int_G \chi_1(g_1^{-1} \circ h)\chi_2(g_2^{-1} \circ h^{-1} \circ g)\, dh \\ &= \int_G \chi_1(k)\chi_2(g_2^{-1} \circ k^{-1} \circ g_1^{-1} \circ g)\, dk \\ &= \int_G \chi_1(k)\chi_2(k^{-1} \circ g_1^{-1} \circ g \circ g_2^{-1})\, dk \\ &= (\chi_1 * \chi_2)(g_1^{-1} \circ g \circ g_2^{-1}).\end{aligned}$$

Similarly,

$$\begin{aligned}(R_{g_1}\chi_1 * L_{g_2}\chi_2)(g) &= \int_G (R_{g_1}\chi_1)(h) * (L_{g_2}\chi_2)(h^{-1} \circ g)\, dh \\ &= \int_G \chi_1(h \circ g_1)\chi_2(g_2^{-1} \circ h^{-1} \circ g)\, dh \\ &= \int_G \chi_1(k) * \chi_2(g_2^{-1} \circ g_1 \circ k^{-1} \circ g)\, dk \\ &= \int_G \chi_1(k) * \chi_2(k^{-1} \circ g \circ g_2^{-1} \circ g_1)\, dk \\ &= (\chi_1 * \chi_2)(g \circ g_2^{-1} \circ g_1).\end{aligned}$$

Then since the entropy integral on a unimodular Lie group is invariant under shifts, the equalities in (19.17) follow.

19.3 Fisher Information and Diffusions on Lie Groups

Let $\{X_i\}$ be an arbitrary orthonormal basis for the Lie algebra $\mathcal{G}$ corresponding to the Lie group G. The natural extension of the Fisher information matrix for the case when $f(g;\boldsymbol{\theta})$ is a parametric distribution on a Lie group is

$$F_{ij}(f,\boldsymbol{\theta}) = \int_G \frac{1}{f}\frac{\partial f}{\partial \theta_i}\frac{\partial f}{\partial \theta_j}\,dg. \tag{19.18}$$

In the case when $\boldsymbol{\theta}$ parameterizes G as $g(\boldsymbol{\theta}) = \exp(\sum_i \theta_i X_i)$ and $f(g,\boldsymbol{\theta}) = f(g \circ \exp(\sum_i \theta_i X_i))$, then

$$\left.\frac{\partial f}{\partial \theta_i}\right|_{\boldsymbol{\theta}=\mathbf{0}} = \tilde{X}_i^r f$$

and $F_{ij}(f,\mathbf{0})$ becomes

$$F_{ij}^r(f) = \int_G \frac{1}{f}(\tilde{X}_i^r f)(\tilde{X}_j^r f)\,dg. \tag{19.19}$$

In a similar way, we can define

$$F_{ij}^l(f) = \int_G \frac{1}{f}(\tilde{X}_i^l f)(\tilde{X}_j^l f)\,dg. \tag{19.20}$$

Theorem 19.9. *The matrices with elements defined in (19.19) and (19.20) have the properties*

$$F_{ij}^r(L(h)f) = F_{ij}^r(f) \quad \textit{and} \quad F_{ij}^l(R(h)f) = F_{ij}^l(f) \tag{19.21}$$

and

$$F_{ij}^r(I(f)) = F_{ij}^l(f) \quad \textit{and} \quad F_{ij}^l(I(f)) = F_{ij}^r(f), \tag{19.22}$$

where $(L(h)f)(g) = f(h^{-1} \circ g)$, $(R(h)f)(g) = f(g \circ h)$, and $I(f)(g) = f(g^{-1})$.

Proof. The operators $\tilde{X}_i^l$ and $R(h)$ commute, and likewise $\tilde{X}_i^r$ and $L(h)$ commute. This together with the invariance of integration under shifts proves (19.21). From the definitions of $\tilde{X}_i^l$ and $\tilde{X}_i^r$ in Chapter 11, it follows that

$$\begin{aligned}
\tilde{X}_i^r(I(f))(g) &= \left.\left(\frac{d}{dt} f([g \circ \exp(tX_i)]^{-1})\right)\right|_{t=0} \\
&= \left.\left(\frac{d}{dt} f(\exp(-tX_i) \circ g^{-1})\right)\right|_{t=0} \\
&= (\tilde{X}_i^l f)(g^{-1}).
\end{aligned}$$

Using the invariance of integration under shifts then gives (19.22).

As a special case, when $f(g)$ is a symmetric function, the left and right Fisher information matrices will be the same.

Note that the entries of Fisher matrices $F_{ij}^r(f)$ and $F_{ij}^l(f)$ implicitly depend on the choice of orthonormal Lie algebra basis $\{X_i\}$, and so it would be more descriptive to use the notation $F_{ij}^r(f,X)$ and $F_{ij}^l(f,X)$. Henceforth, a Fisher information matrix without a basis explicitly specified is one for which the natural basis $\{E_i\}$ is used.

If a different orthonormal basis $\{Y_i\}$ is used, such that $X_i = \sum_k a_{ik} Y_k$, then the orthonormality of both $\{X_i\}$ and $\{Y_i\}$ forces $A = [a_{ij}]$ to be an orthogonal matrix.

Furthermore, the linearity of the Lie derivative,

$$\tilde{X}^r f = \sum_i x_i \tilde{X}_i^r f, \quad \text{where } X = \sum_i x_i X_i,$$

means that

$$F_{ij}^r(f,X) = \int_G \frac{1}{f}\left(\sum_k a_{ik}\tilde{Y}_k^r f\right)\left(\sum_l a_{jl}\tilde{Y}_l^r f\right) dg = \sum_{k,l} a_{ik}a_{jl}F_{kl}^r(f,Y).$$

The same holds for F_{ij}^l. Summarizing these results in matrix form,

$$F^r(f,X) = AF^r(f,Y)A^T \quad \text{and} \quad F^l(f,X) = AF^l(f,Y)A^T. \tag{19.23}$$

This means that the eigenvalues of the Fisher information matrix (and therefore its trace) are invariant under change of orthonormal basis. Henceforth the orthonormal basis $\{E_i\}$ will be used.

Note that it follows immediately from (19.22) that the left and right Fisher information matrices are equal for class functions (i.e., functions satisfying the condition $f(g \circ h) = f(h \circ g)$ for all $h, g \in G$) and for symmetric functions (i.e., functions satisfying the condition $f(g) = f(g^{-1})$ for all $g \in G$). However, in general, the left and right Fisher information matrices are not equal. Even the traces of the left and right Fisher information matrices for arbitrary pdfs on a unimodular Lie group will be different from each other in the general case.

19.3.1 Fisher Information and Convolution on Groups

The decrease of Fisher information as a result of convolution can be studied in much the same way as for pdfs on Euclidean space. Two approaches are taken here. First, a straightforward application of the Cauchy–Bunyakovsky-Schwarz (CBS) inequality is used together with the bi-invariance of the integral over a unimodular Lie group to produce a bound on the Fisher information of the convolution of two probability densities. Then a tighter bound is obtained using the concept of conditional expectation in the special case when the pdfs commute under convolution. Other information/entropy inequalities involving finite groups can be found in [2].

Theorem 19.10. *The following inequalities hold for the diagonal entries of the left and right Fisher information matrices:*

$$F_{ii}^r(f_1 * f_2) \leq \min\{F_{ii}^r(f_1), F_{ii}^r(f_2)\} \quad \textit{and} \quad F_{ii}^l(f_1 * f_2) \leq \min\{F_{ii}^l(f_1), F_{ii}^l(f_2)\}. \tag{19.24}$$

Proof. The CBS inequality holds for groups:

$$\left(\int_G a(g)b(g)\, dg\right)^2 \leq \int_G a^2(g)\, dg \int_G b^2(g)\, dg.$$

If $a(g) \geq 0$ for all values of g, then it is possible to define $j(g) = [a(g)]^{\frac{1}{2}}$ and $k(g) = [a(g)]^{\frac{1}{2}}b(g)$, and since $j(g)k(g) = a(g)b(g)$,

$$\left(\int_G a(g)b(g)\, dg\right)^2 \leq \left(\int_G j^2(g)\, dg\right)\left(\int_G k^2(t)\, dg\right) = \left(\int_G a(g)\, dg\right)\left(\int_G a(g)[b(g)]^2\, dg\right). \tag{19.25}$$

Using this version of the CBS inequality and letting $b(g) = \tilde{E}_i^r f_2(h^{-1} \circ g)/[f_2(h^{-1} \circ g)]$ and $a(g) = f_1(h) f_2(h^{-1} \circ g)$, essentially the same manipulations as in [8] can be used, with the roles of f_1 and f_2 interchanged due to the fact that, in general, for convolution on a Lie group $(f_1 * f_2)(g) \neq (f_2 * f_1)(g)$:

$$\begin{aligned}
&F_{ii}^r(f_1 * f_2)\\
&= \int_G \frac{\left(\int_G [\tilde{E}_i^r f_2(h^{-1} \circ g)/f_2(h^{-1} \circ g)] \cdot [f_2(h^{-1} \circ g) f_1(h)]\, dh\right)^2}{(f_1 * f_2)(g)}\, dg\\
&\leq \int_G \frac{\left(\int_G [\tilde{E}_i^r f_2(h^{-1} \circ g)/f_2(h^{-1} \circ g)]^2 [f_2(h^{-1} \circ g) f_1(h)] dh\right)\left(\int_G f_2(h^{-1} \circ g) f_1(h)\, dh\right)}{(f_1 * f_2)(g)}\, dg\\
&= \int_G \left(\int_G \{[\tilde{E}_i^r f_2(h^{-1} \circ g)]^2 / f_2(h^{-1} \circ g)\} f_1(h)\, dh\right) dg\\
&= \int_G \left(\int_G \{[\tilde{E}_i^r f_2(h^{-1} \circ g)]^2 / f_2(h^{-1} \circ g)\}\, dg\right) f_1(h)\, dh\\
&= F_{ii}^r(f_2) \int_G f_1(h)\, dh\\
&= F_{ii}^r(f_2).
\end{aligned}$$

Since for a unimodular Lie group it is possible to perform changes of variables and inversion of the variable of integration without affecting the value of an integral, the convolution can be written in the following equivalent ways:

$$(f_1 * f_2)(g) = \int_G f_1(h) f_2(h^{-1} \circ g)\, dh \tag{19.26}$$

$$= \int_G f_1(g \circ h^{-1}) f_2(h)\, dh \tag{19.27}$$

$$= \int_G f_1(g \circ h) f_2(h^{-1})\, dh \tag{19.28}$$

$$= \int_G f_1(h^{-1}) f_2(h \circ g)\, dh. \tag{19.29}$$

It then follows that using (19.27) and the bi-invariance of integration (19.24) holds.

Note that inequalities similar to (19.24) have been derived for $(\mathbb{Z}_n, +)$ in [17] and for more general finite groups in [16], where essentially finite differences are used in place of left or right derivatives.

19.3.2 Bounds Using Conditional Expectation and Commuting pdfs

In this subsection a better inequality is derived.

Theorem 19.11. *The following inequality holds for the right and left Fisher information matrices:*

$$\mathrm{tr}[F^r(\rho_1 * \rho_2)P] \leq \mathrm{tr}[F^r(\rho_2)P] \quad \textit{and} \quad \mathrm{tr}[F^l(\rho_1 * \rho_2)P] \leq \mathrm{tr}[F^l(\rho_1)P], \tag{19.30}$$

where $i = 1, 2$ and P is an arbitrary symmetric positive definite matrix with the same dimensions as F.

Proof. Let

$$f_{12}(h,g) = \rho_1(h)\,\rho_2(h^{-1} \circ g).$$

Then $f_{12}(h,g)$ is a pdf on $G \times G$ with marginal densities

$$f_1(h) = \int_G f_{12}(h,g)\,dg = \rho_1(h) \quad \text{and} \quad f_2(g) = \int_G f_{12}(h,g)\,dh = (\rho_1 * \rho_2)(g).$$

It follows that

$$(\tilde{E}_i^r f_2)(g) = \int_G \rho_1(h)\tilde{E}_i^r\,\rho_2(h^{-1} \circ g)\,dh.$$

Then by the change of variables $k = h^{-1} \circ g$,

$$(\tilde{E}_i^r f_2)(g) = \int_G \rho_1(g \circ k^{-1})\,\tilde{E}_i^r \rho_2(k)\,dk.$$

This means that

$$\frac{(\tilde{E}_i^r f_2)(g)}{f_2(g)} = \int_G \frac{(\tilde{E}_i^r \rho_2)(k)}{\rho_2(k)}\,\frac{\rho_1(g \circ k^{-1})\rho_2(k)}{f_2(g)}\,dk = \left\langle \left.\frac{(\tilde{E}_i^r \rho_2)(k)}{\rho_2(k)}\right| g \right\rangle, \tag{19.31}$$

where $\langle \cdot | g \rangle$ denotes conditional expectation. This notation, which is standard in the literature, includes the functional dependence of whatever is in the place of "·" even though this is integrated out and no longer exists [10, 23].

Therefore, using this notation,

$$\begin{aligned} F_{ii}^r(f_2) &= \left\langle \left(\frac{(\tilde{E}_i^r \rho_2)(g)}{f_2(g)} \right)^2 \right\rangle = \left\langle \left\langle \left.\frac{(\tilde{E}_i^r \rho_2)(k)}{\rho_2(k)}\right| g \right\rangle^2 \right\rangle \\ &\leq \left\langle \left\langle \left.\left(\frac{(\tilde{E}_i^r \rho_2)(k)}{\rho_2(k)} \right)^2 \right| g \right\rangle \right\rangle = \left\langle \left(\frac{(\tilde{E}_i^r \rho_2)(k)}{\rho_2(k)} \right)^2 \right\rangle \\ &= F_{ii}^r(\rho_2). \end{aligned}$$

An analogous argument using $f_{12}(h,g) = \rho_1(g \circ h^{-1})\rho_2(h)$ and $f_2(g) = (\rho_1 * \rho_2)(g)$ shows that

$$\frac{(\tilde{E}_i^l f_2)(g)}{f_2(g)} = \left\langle \left.\frac{(\tilde{E}_i^l \rho_1)(k)}{\rho_1(k)}\right| g \right\rangle \tag{19.32}$$

and

$$F_{ii}^l(f_2) \leq F_{ii}^l(\rho_1).$$

The above results can be written concisely by introducing an arbitrary positive-definite diagonal matrix Λ as follows:

$$\mathrm{tr}[F^r(\rho_1 * \rho_2)\Lambda] \leq \mathrm{tr}[F^r(\rho_2)\Lambda] \quad \text{and} \quad \mathrm{tr}[F^l(\rho_1 * \rho_2)\Lambda] \leq \mathrm{tr}[F^l(\rho_1)\Lambda].$$

If this is true in one basis, then using (19.23), the more general statement in (19.30) must follow in another basis where $P = P^T > 0$. Since the initial choice of basis is arbitrary, (19.30) must hold in every basis for an arbitrary positive definite matrix P. This completes the proof.

In some instances, even though the group is not commutative, the functions ρ_1 and ρ_2 will commute. For example, if $\rho(g \circ h) = \rho(h \circ g)$ for all $h, g \in G$, then $(\rho * \rho_i)(g) = (\rho_i * \rho)(g)$ for any reasonable choice of $\rho_i(g)$. Or if $\rho_2 = \rho_1 * \rho_1 * \cdots \rho_1$, it will clearly be the case that $\rho_1 * \rho_2 = \rho_2 * \rho_1$. If, for whatever reason, $\rho_1 * \rho_2 = \rho_2 * \rho_1$, then (19.30) can be rewritten in the following form:

$$\mathrm{tr}[F^r(\rho_1 * \rho_2)P] \leq \min\{\mathrm{tr}[F^r(\rho_1)P], \mathrm{tr}[F^r(\rho_2)P]\}$$

and (19.33)

$$\mathrm{tr}[F^l(\rho_1 * \rho_2)P] \leq \min\{\mathrm{tr}[F^l(\rho_1)P], \mathrm{tr}[F^l(\rho_2)P]\}.$$

Theorem 19.12. *When $\rho_1 * \rho_2 = \rho_2 * \rho_1$, the following equality holds:*

$$\frac{2}{\mathrm{tr}[F^r(\rho_1 * \rho_2)P]} \geq \frac{1}{\mathrm{tr}[F^r(\rho_1)P]} + \frac{1}{\mathrm{tr}[F^r(\rho_2)P]} \quad \textit{for any } P = P^T > 0, \tag{19.34}$$

and likewise for F^l.

Proof. Returning to (19.31) and (19.32), in the case when $\rho_1 * \rho_2 = \rho_2 * \rho_1$, it is possible to write

$$\frac{(\tilde{E}_i^r f_2)(g)}{f_2(g)} = \left\langle \frac{(\tilde{E}_i^r \rho_2)(k)}{\rho_2(k)} \middle| g \right\rangle = \left\langle \frac{(\tilde{E}_i^r \rho_1)(k)}{\rho_1(k)} \middle| g \right\rangle \tag{19.35}$$

and

$$\frac{(\tilde{E}_i^l f_2)(g)}{f_2(g)} = \left\langle \frac{(\tilde{E}_i^l \rho_1)(k)}{\rho_1(k)} \middle| g \right\rangle = \left\langle \frac{(\tilde{E}_i^l \rho_2)(k')}{\rho_2(k')} \middle| g \right\rangle.$$

Since the following calculation works the same way for both the "l" and "r" cases, consider only the "r" case for now. Multiplying the first equality in (19.35) by $1-\beta$ and the second by β and adding together gives[1]

$$\frac{(\tilde{E}_i^r f_2)(g)}{f_2(g)} = \beta \left\langle \frac{(\tilde{E}_i^r \rho_1)(k)}{\rho_1(k)} \middle| g \right\rangle + (1-\beta) \left\langle \frac{(\tilde{E}_i^r \rho_2)(k')}{\rho_2(k')} \middle| g \right\rangle$$

for arbitrary value of β.

Now, squaring both sides gives

$$\left[\frac{(\tilde{E}_i^r f_2)(g)}{f_2(g)}\right]^2 = \left[\beta \left\langle \frac{(\tilde{E}_i^r \rho_1)(k)}{\rho_1(k)} \middle| g \right\rangle + (1-\beta) \left\langle \frac{(\tilde{E}_i^r \rho_2)(k')}{\rho_2(k')} \middle| g \right\rangle\right]^2.$$

Taking the (unconditional) expectation and using Jensen's inequality yields

$$\begin{aligned}\left\langle \left(\frac{(\tilde{E}_i^r f_2)(g)}{f_2(g)}\right)^2 \right\rangle &= \left\langle \left[\beta \left\langle \frac{(\tilde{E}_i^r \rho_1)(k)}{\rho_1(k)} \middle| g \right\rangle + (1-\beta) \left\langle \frac{(\tilde{E}_i^r \rho_2)(k')}{\rho_2(k')} \middle| g \right\rangle\right]^2 \right\rangle \\ &\leq \beta^2 \left\langle \left(\frac{(\tilde{E}_i^r \rho_1)(k)}{\rho_1(k)}\right)^2 \right\rangle + (1-\beta)^2 \left\langle \left(\frac{(\tilde{E}_i^r \rho_2)(k')}{\rho_2(k')}\right)^2 \right\rangle \\ &\quad + 2\beta(1-\beta) \left\langle \left\langle \frac{(\tilde{E}_i^r \rho_1)(k)}{\rho_1(k)} \middle| g \right\rangle \cdot \left\langle \frac{(\tilde{E}_i^r \rho_2)(k')}{\rho_2(k')} \middle| g \right\rangle \right\rangle.\end{aligned} \tag{19.36}$$

[1] The names of the dummy variables k and k' are unimportant. However, at this stage it is important that the names be different in order to emphasize their statistical independence.

However, observing (19.35), moving the rightmost term to the left, and writing $1-2\beta(1-\beta)$ as $(1-\beta)^2+\beta^2$ reduces (19.36) to

$$[(1-\beta)^2+\beta^2]F^r_{ii}(\rho_1 * \rho_2) \leq \beta^2\, F^r_{ii}(\rho_1) + (1-\beta)^2\, F^r_{ii}(\rho_2). \tag{19.37}$$

Dividing both sides by $[(1-\beta)^2+\beta^2]$, multiplying by $\lambda_i \geq 0$, and summing over i gives

$$\mathrm{tr}[\Lambda F^r(\rho_1 * \rho_2)] \leq \frac{\beta^2}{[(1-\beta)^2+\beta^2]}\,\mathrm{tr}[\Lambda F^r(\rho_1)] + \frac{(1-\beta)^2}{[(1-\beta)^2+\beta^2]}\,\mathrm{tr}[\Lambda F^r(\rho_2)], \tag{19.38}$$

where $\Lambda = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$.

Clearly,

$$0 \leq \frac{\beta^2}{[(1-\beta)^2+\beta^2]}, \frac{(1-\beta)^2}{[(1-\beta)^2+\beta^2]} \leq 1.$$

Choosing

$$\frac{\beta^2}{[(1-\beta)^2+\beta^2]} = \frac{\mathrm{tr}[\Lambda F^r(\rho_2)]}{\mathrm{tr}[\Lambda F^r(\rho_1)] + \mathrm{tr}[\Lambda F^r(\rho_2)]}$$

and

$$\frac{(1-\beta)^2}{[(1-\beta)^2+\beta^2]} = \frac{\mathrm{tr}[\Lambda F^r(\rho_1)]}{\mathrm{tr}[\Lambda F^r(\rho_1)] + \mathrm{tr}[\Lambda F^r(\rho_2)]}$$

then gives

$$\mathrm{tr}[\Lambda F^r(\rho_1 * \rho_2)] \leq \frac{2\mathrm{tr}[\Lambda F^r(\rho_1)]\mathrm{tr}[\Lambda F^r(\rho_2)]}{\mathrm{tr}[\Lambda F^r(\rho_1)] + \mathrm{tr}[\Lambda F^r(\rho_2)]}.$$

This can be written as

$$\frac{1}{\mathrm{tr}[\Lambda F^r(\rho_1)]} + \frac{1}{\mathrm{tr}[\Lambda F^r(\rho_2)]} \leq \frac{2}{\mathrm{tr}[\Lambda F^r(\rho_1 * \rho_2)]}. \tag{19.39}$$

Again, since the basis is arbitrary, Λ can be replaced with P, resulting in (19.34).

Note that in the classical (Abelian) version of this equality, it is possible to get the stronger condition without the factor of 2 in (19.34).

19.3.3 A Special Case: $SO(3)$

Consider the group of 3×3 orthogonal matrices with determinant $+1$. Let $\{E_i\}$ be the standard orthonormal basis used in (10.82) and define $\tilde{\mathbf{E}}^{\mathbf{r}} \doteq [\tilde{E}^r_1, \tilde{E}^r_2, \tilde{E}^r_3]^T$ and $\tilde{\mathbf{E}}^{\mathbf{l}} \doteq [\tilde{E}^l_1, \tilde{E}^l_2, \tilde{E}^l_3]^T$, where $\tilde{E}^r_i$ and $\tilde{E}^l_i$ are defined in Section 11.1.2. These two gradient vectors are related to each other by an adjoint matrix, which for this group is a rotation matrix. Therefore, in the case when $G = SO(3)$,

$$\|\tilde{\mathbf{E}}^{\mathbf{r}} f\|^2 = \|\tilde{\mathbf{E}}^{\mathbf{l}} f\|^2 \quad \Longrightarrow \quad \mathrm{tr}[F^r(f)] = \mathrm{tr}[F^l(f)].$$

Therefore, the inequalities in (19.33) will hold for pdfs on $SO(3)$ regardless of whether or not the functions commute under convolution, but restricted to the condition $P = \mathbb{I}$.

19.4 Generalizing the de Bruijn Identity to Lie Groups

This section generalizes the de Bruijn identity, in which entropy rates are related to Fisher information.

Theorem 19.13. *Let $f_{D,\mathbf{h},t}(g) = f(g,t;D,\mathbf{h})$ denote the solution of the diffusion equation (19.41) with constant* $\mathbf{h}$ *subject to the initial condition $f(g,0;D,\mathbf{h}) = \delta(g)$. Then for any well-behaved pdf $\alpha(g)$,*

$$\frac{d}{dt}S(\alpha * f_{D,\mathbf{h},t}) = \frac{1}{2}\mathrm{tr}[DF^r(\alpha * f_{D,\mathbf{h},t})]. \tag{19.40}$$

Proof. It is easy to see that the solution of the diffusion equation

$$\frac{\partial \rho}{\partial t} = \frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\tilde{E}_i^r \tilde{E}_j^r \rho - \sum_{k=1}^{n} h_k \tilde{E}_k^r \rho \tag{19.41}$$

subject to the initial conditions $\rho(g,0) = \alpha(g)$ is simply $\rho(g,t) = (\alpha * f_{D,\mathbf{h},t)}(g)$. This follows because all derivatives "pass through" the convolution integral for $\rho(g,t)$ and act on $f_{D,\mathbf{h},t}(g)$.

Taking the time derivative of $S(\rho(g,t))$, we get

$$\frac{d}{dt}S(\rho) = -\frac{d}{dt}\int_G \rho(g,t)\log\rho(g,t)\,dg = -\int_G \left\{\frac{\partial \rho}{\partial t}\log\rho + \frac{\partial \rho}{\partial t}\right\} dg. \tag{19.42}$$

Using (19.41), the partial with respect to time can be replaced with Lie derivatives. However,

$$\int_G \tilde{E}_k^r \rho\, dg = \int_G \tilde{E}_i^r \tilde{E}_j^r \rho\, dg = 0,$$

so the second term on the right-hand side of (19.42) completely disappears. Using the integration-by-parts formula[2]

$$\int_G f_1\, \tilde{E}_k^r f_2\, dg = -\int_G f_2\, \tilde{E}_k^r f_1\, dg,$$

with $f_1 = \log\rho$ and $f_2 = \rho$, then gives

$$\begin{aligned}\frac{d}{dt}S(\alpha * f_{D,\mathbf{h},t}) &= \frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\int_G \frac{1}{\alpha * f_{D,\mathbf{h},t}}\tilde{E}_j^r(\alpha * f_{D,\mathbf{h},t})\tilde{E}_i^r(\alpha * f_{D,\mathbf{h},t})\,dg \\ &= \frac{1}{2}\sum_{i,j=1}^{n} D_{ij}F_{ij}^r(\alpha * f_{D,\mathbf{h},t}) \;=\; \frac{1}{2}\mathrm{tr}\left[D\,F^r(\alpha * f_{D,\mathbf{h},t})\right].\end{aligned}$$

The implication of this is that

$$S(\alpha * f_{D,\mathbf{h},t_2}) - S(\alpha * f_{D,\mathbf{h},t_1}) = \frac{1}{2}\int_{t_1}^{t_2} \mathrm{tr}\left[DF^r(\alpha * f_{D,\mathbf{h},t})\right] dt.$$

[2] There are no surface terms because, like the circle and real line, each coordinate in the integral either wraps around or goes to infinity.

19.5 Information-Theoretic Inequalities from log-Sobolev Inequalities

In this section, information-theoretic identities are derived from log-Sobolev inequalities. Section 19.5.1 provides a brief review of log-Sobolev inequalities. Section 19.5.2 then uses these to write information-theoretic inequalities.

19.5.1 Log-Sobolev Inequalities in $\mathbb{R}^n$ and on Lie Groups

The log-Sobolev inequality can be stated as [5, 6, 26]

$$\int_{\mathbb{R}^n} |\psi(\mathbf{x})|^2 \log |\psi(\mathbf{x})|^2 \, d\mathbf{x} \leq \frac{n}{2} \log\left[\frac{2}{\pi e n} \int_{\mathbb{R}^n} \|\nabla\psi\|^2 \, d\mathbf{x}\right], \tag{19.43}$$

where

$$\nabla\psi = \left[\frac{\partial\psi}{\partial x_1}, \ldots, \frac{\partial\psi}{\partial x_n}\right]^T \quad \text{and} \quad \int_{\mathbb{R}^n} |\psi(\mathbf{x})|^2 \, d\mathbf{x} = 1.$$

Here, $\log = \log_e$. Actually, there is a whole family of log-Sobolev inequalities, and (19.43) represents the tightest of these. The original form of the log-Sobolev inequality as introduced by Gross [19] is

$$\frac{1}{2}\int_{\mathbb{R}^n} |\phi(\mathbf{x})|^2 \log |\phi(\mathbf{x})|^2 \rho(\mathbf{x}) \, d\mathbf{x} \leq \int_{\mathbb{R}^n} \|\nabla\phi(\mathbf{x})\|^2 \rho(\mathbf{x}) \, d\mathbf{x} + \|\phi\|^2_{L^2(\mathbb{R}^n,\rho)} \log \|\phi\|^2_{L^2(\mathbb{R}^n,\rho)}, \tag{19.44}$$

where

$$\|\phi\|^2_{L^2(\mathbb{R}^n,\rho)} = \int_{\mathbb{R}^n} |\phi(\mathbf{x})|^2 \rho(\mathbf{x}) \, d\mathbf{x},$$

Here, $\rho(\mathbf{x}) = \rho(\mathbf{x}, 0) = (2\pi)^{-n/2} \exp(-\|\mathbf{x}\|^2/2)$ is the solution of the heat equation on $\mathbb{R}^n$ evaluated at $t = 1$.

Several different variations exist. For example, by rescaling, it is possible to rewrite (19.44) with $\rho(\mathbf{x}, t)$ in place of $\rho(\mathbf{x})$ by introducing a multiplicative factor of t in the first term on the right-hand side of the equation. Or, by letting $\phi(\mathbf{x}) = \rho^{-\frac{1}{2}}(\mathbf{x})\psi(\mathbf{x}/a)$ for some scaling factor $a > 0$, substituting into (19.44), and integrating by parts then gives [26]

$$\int_{\mathbb{R}^n} |\psi(\mathbf{x})|^2 \log \frac{|\psi(\mathbf{x})|^2}{\|\psi\|_2^2} \, d\mathbf{x} + n(1 + \log a)\|\psi\|_2^2 \leq \frac{a^2}{\pi} \int_{\mathbb{R}^n} \|\nabla\psi(\mathbf{x})\|^2 \, d\mathbf{x},$$

where

$$\|\psi\|_2^2 = \int_{\mathbb{R}^n} |\psi(\mathbf{x})|^2 \, d\mathbf{x} \quad \text{and} \quad \|\nabla\psi(\mathbf{x})\|^2 = \nabla\psi(\mathbf{x}) \cdot \nabla\psi(\mathbf{x}).$$

This, together with an optimization over a, gives (19.43).

Gross [20] subsequently extended (19.44) to Lie groups as

$$\frac{1}{2}\int_G \left\{|\phi(g)|^2 \log |\phi(g)|^2\right\} \rho(g, t) \, dg \leq c_G(t) \int_G \|(\tilde{\mathbf{E}}^r \phi)(g)\|^2 \rho(g, t) \, dg + \|\phi\|^2_{L^2(G,\rho_t)} \log \|\phi\|^2_{L^2(G,\rho_t)}, \tag{19.45}$$

where $\rho(g,t)$ is the solution of the diffusion equation in (19.41) with $h_i = 0$, $D_{ij} = \delta_{ij}$, initial condition $\rho(g,0) = \delta(g)$, and

$$\tilde{\mathbf{E}}^r \phi = [\tilde{E}_1^r \phi, \ldots, \tilde{E}_n^r \phi]^T \qquad \text{and} \qquad \|\phi\|^2_{L^2(G,\rho_t)} = \int_G |\phi(g)|^2 \rho(g,t)\, dg.$$

In (19.45) the scalar function $c_G(t)$ depends on the particular group. For $G = (\mathbb{R}^n, +)$, we have $c_{\mathbb{R}^n}(t) = t$, and likewise $c_{SO(n)}(t) = t$.

In analogy with the way that (19.43) evolved from (19.44), a descendent of (19.45) for noncompact unimodular Lie groups is [3, 5, 6][3]

$$\int_G |\psi(g)|^2 \log |\psi(g)|^2 \, dg \leq \frac{n}{2} \log \left[\frac{2C_G}{\pi e n} \int_G \|\tilde{\mathbf{E}}\psi\|^2 \, dg \right]. \tag{19.46}$$

The only difference is that, to the author's knowledge, the sharp factor C_G in this expression is not known for most Lie groups. The information-theoretic interpretation of these inequalities is provided in the following subsection.

19.5.2 Information-Theoretic Inequalities

For our purposes, (19.43) and (19.46) will be most useful. It is interesting to note in passing that Beckner has extended this inequality to the case where the domain, rather than being $\mathbb{R}^n$, is the hyperbolic space $\mathbb{H}^2 \cong SL(2,\mathbb{R})/SO(2)$ and the Heisenberg groups $H(n)$, including $H(1)$ [5, 6]. Our goal here is to provide an information-theoretic interpretation of the inequalities from the previous section.

Theorem 19.14. *Entropy powers and Fisher information are related as*

$$[N(f)]^{-1} \leq \frac{1}{n} \operatorname{tr}(F), \quad \textit{where } N(f) = \frac{C_G}{2\pi e} \exp\left[\frac{2}{n} S(f)\right]. \tag{19.47}$$

Proof. We begin by proving (19.47) for $G = (\mathbb{R}^n, +)$. Making the simple substitution $f(\mathbf{x}) = |\psi(\mathbf{x})|^2$ into (19.43) and requiring that $f(\mathbf{x})$ be a pdf gives

$$\int_{\mathbb{R}^n} f(\mathbf{x}) \log f(\mathbf{x}) \, d\mathbf{x} \leq \frac{n}{2} \log \left[\frac{1}{2\pi e n} \int_{\mathbb{R}^n} \frac{1}{f} \|\nabla f\|^2 \, d\mathbf{x} \right],$$

or

$$-S(f) \leq \frac{n}{2} \log \frac{\operatorname{tr}(F)}{2\pi e n} \quad \Longrightarrow \quad \exp\left[-\frac{2}{n} S(f)\right] \leq \frac{\operatorname{tr}(F)}{2\pi e n} \quad \Longrightarrow \quad [N(f)]^{-1} \leq \frac{1}{n} \operatorname{tr}(F). \tag{19.48}$$

Here, $S(f)$ is the Boltzmann–Shannon entropy of f and F is the Fisher information matrix. As is customary in information theory, the entropy power can be defined as $N(f)$ in (19.47) with $C_G = 1$. Then the log-Sobolev inequality in the form in (19.48) is written as (19.47).

For the more general case, starting with (19.46) and letting $f(g) = |\psi(g)|^2$ gives

$$\int_G f(g) \log f(g) \, dg \leq \frac{n}{2} \log \left[\frac{C_G}{2\pi e n} \int_G \frac{1}{f} \|\tilde{\mathbf{E}} f\|^2 \right] dg \Longrightarrow -S \leq \frac{n}{2} \log \left[\frac{C_G}{2\pi e n} \operatorname{tr}(F) \right]. \tag{19.49}$$

The rest is the same as for the case of $\mathbb{R}^n$.

[3] Here $\tilde{\mathbf{E}}$ is written without a superscript r or l because either the norm $\|\cdot\|$ can be chosen to be Ad^*-invariant, or, if not, different constants C_G can be defined in the l and r cases.

Starting with Gross' original form of log-Sobolev inequalities involving the heat kernel, the following information-theoretic inequality results.

Theorem 19.15. *The Kullback–Leibler divergence and Fisher information distance of any arbitrary pdf and the heat kernel are related as*

$$D_{KL}(f \,\|\, \rho_t) \leq \frac{c_G(t)}{2} D_{FI}(f \,\|\, \rho_t), \tag{19.50}$$

where, in general, given $f_1(g)$ and $f_2(g)$,

$$D_{FI}(f_1 \,\|\, f_2) \doteq \int_G \left\| \frac{1}{f_1}\tilde{\mathbf{E}} f_1 - \frac{1}{f_2}\tilde{\mathbf{E}} f_2 \right\|^2 f_1 \, dg. \tag{19.51}$$

Proof. Starting with (19.45), let $\phi(g,t) = [\rho(g,t)]^{-\frac{1}{2}}[f(g)]^{\frac{1}{2}}$, where $f(g)$ is a pdf. Then

$$\int_G |\phi(g,t)|^2 \rho(g,t)\, dg = \int_G f(g)\, dg = 1,$$

and so, $\log \|\phi\|^2_{L^2(G,\rho_t)} = 0$, and we have

$$\frac{1}{2}\int_G f(g) \log \frac{f(g)}{\rho(g,t)}\, dg \leq c_G(t) \int_G \|\tilde{\mathbf{E}}([\rho(g,t)]^{-\frac{1}{2}}[f(g)]^{\frac{1}{2}})\|^2 \rho(g,t)\, dg.$$

By using the chain rule and product rule for differentiation,

$$\rho_t^{\frac{1}{2}} \cdot \tilde{\mathbf{E}}(\rho_t^{-\frac{1}{2}} f^{\frac{1}{2}}) = \frac{1}{2} f^{-\frac{1}{2}} \tilde{\mathbf{E}} f - \frac{1}{2} f^{\frac{1}{2}} \rho_t^{-1} \tilde{\mathbf{E}} \rho_t,$$

where $\rho_t = \rho(g,t)$ and $f = f(g)$. Substitution into the right-hand side of (19.45) then gives (19.50).

In the functional analysis community, several connections between log-Sobolev inequalities on $\mathbb{R}^n$ and information theory have emerged. For example, Carlen [9] addressed Theorem 19.13 for the case of $G = \mathbb{R}^n$. Ledoux [24, 25], Dembo [14], Talagrand [33], and Otto and Villani [29] addressed the connection between entropy and gradients of pdfs in the context of so-called "concentration of measure" phenomena related to logarithmic Sobolev inequalities. However, these studies are not usually concerned with the Lie-group setting. Moreover, the author has not found analogs of (19.48) in the context of Lie groups in the literature.

19.6 Covariance, the Weak Cramér–Rao Bound, and Maximum-Entropy Distributions on Unimodular Lie Groups

Given a pdf $f \in \mathcal{N}(G)$ that is in addition unimodal and decays rapidly from its mode (in the precise sense described in [32]), its *mean* is defined here as the point $\mu \in G$ such that [34]

$$\int_G (\log g)^\vee f(\mu \circ g)\, dg = \mathbf{0}. \tag{19.52}$$

Unlike in $\mathbb{R}^n$, in which a mean can be computed for any pdf, in the Lie-group setting it is important to restrict the class of pdfs for the concept of mean to make sense. If not for such restrictions, the usefulness of the concept of the mean would diminish. For example, for the uniform distribution on $SO(3)$, every point could be called a mean.

The covariance of a concentrated probability density centered around μ can be defined as [34]

$$\Sigma = \int_G (\log g)^\vee [(\log g)^\vee]^T f(\mu \circ g)\, dg. \tag{19.53}$$

This matrix will have finite values when $f(g)$ is rapidly decreasing. Note that this concept of covariance differs from those presented in [18, 21], which are more akin to the dispersion defined in Theorem 19.2. The definitions in (19.52) and (19.53) are used in the following theorem.

19.6.1 The Weak Cramér–Rao Bound

The following theorem is referred to here as the "weak" Cramér–Rao bound for unimodular Lie groups, because unlike the classical Cramér–Rao bound in $\mathbb{R}^n$, the proof only holds when the Lie-theoretic covariance is small. Indeed, even the very concept of this covariance breaks down for distributions that become too spread out.

Theorem 19.16. *Let $\rho(g) \in \mathcal{N}(G)$ be a pdf with the additional symmetry condition $\rho(g) = \rho(g^{-1})$ and set $f(g;\mu) = \rho(\mu^{-1} \circ g)$. Given an unbiased estimator of μ, then the Cramér–Rao bound*

$$\Sigma \geq F^{-1} \tag{19.54}$$

holds for sufficiently small $\|\Sigma\|$, where Σ and F are defined in (19.53) and (19.18) and the above matrix inequality is interpreted as each eigenvalue of $\Sigma - F^{-1}$ being non-negative.

Proof. For a symmetric pdf $\rho(g) = \rho(g^{-1})$, the mean is at the identity, and so,

$$\int_G (\log g)^\vee \rho(g)\, dg = \mathbf{0}. \tag{19.55}$$

The invariance of integration under shifts then gives

$$\phi(\mu) = \int_G (\log(\mu^{-1} \circ g))^\vee \rho(\mu^{-1} \circ g)\, dg = \mathbf{0}. \tag{19.56}$$

Applying the derivatives $\tilde{E}_i^r$ to $\phi(\mu)$ gives an expression for $\tilde{E}_i^r \phi(\mu) = 0$ that can be expanded under the integral using the product rule $\tilde{E}_i^r(a \cdot b) = (\tilde{E}_i^r a) \cdot b + a \cdot (\tilde{E}_i^r b)$, where in the present case, $a = (\log(\mu^{-1} \circ g))^\vee$ and $b = \rho(\mu^{-1} \circ g)$. Note that when $\rho(\cdot)$ is highly concentrated, the only values of g that significantly contribute to the integral are those for which $\mu^{-1} \circ g \approx e$. By definition,

$$\tilde{E}_i^r (\log(\mu^{-1} \circ g))^\vee = \frac{d}{dt} (\log((\mu \circ e^{tE_i})^{-1} \circ g))^\vee \bigg|_{t=0} = \frac{d}{dt} [\log(e^{-tE_i} \circ \mu^{-1} \circ g)]^\vee \bigg|_{t=0}.$$

Using the Baker–Campbell–Hausdorff formula

$$\log(e^X e^Y) \approx X + Y + \frac{1}{2}[X, Y]$$

with $X = -tE_i$ and $Y = \log(\mu^{-1} \circ g)$ together with the fact that $\mu^{-1} \circ g \approx e$ then gives

$$\int_G [\tilde{E}_i^r (\log(\mu^{-1} \circ g))^\vee] \rho(\mu^{-1} \circ g) \, dg \approx -\mathbf{e}_i. \tag{19.57}$$

The second term in the expansion of $\tilde{E}_i^r \phi(\mu)$ is

$$\int_G [\log(\mu^{-1} \circ g)]^\vee \rho(e^{-tE_i} \circ \mu^{-1} \circ g) \, dg \bigg|_{t=0} = \int_G [\log h]^\vee \rho(e^{-tE_i} \circ h) \, dh \bigg|_{t=0},$$

where the change of variables $h = \mu^{-1} \circ g$ has been made. Using the symmetry of ρ gives $\rho(e^{-tE_i} \circ h) = \rho(h^{-1} \circ e^{tE_i})$, and making the change of variables $h \to k^{-1}$ then reduces this term to $\int (\log k^{-1})^\vee (\tilde{E}_i^r \rho)(k) \, dk$. Recombining all of the parts means that $\tilde{E}_i^r \phi(\mu) = 0$ can be written in the form $\int_G a_i(k) b_j(k) \, dk = \delta_{ij}$, where $a_i(k) = [\rho(k)]^{\frac{1}{2}} (\log k^{-1})^\vee \cdot \mathbf{e}_i$ and $b_j(k) = [\rho(k)]^{\frac{1}{2}} \tilde{E}_j^r [\log \rho(k)]$. Then, as in the proof of the classical Cramér–Rao bound, using the Cauchy–Schwarz inequality gives the result in (19.54).

19.6.2 Maximum-Entropy Distributions

Recall that the Gaussian distribution on $\mathbb{R}^n$ has a number of remarkable properties, including the following: (1) It is closed under the operation of convolution; (2) it solves a linear diffusion equation with constant coefficients; and (3) it is the maximum-entropy distributution subject to constraints on the mean and covariance. A natural question to ask is whether such a distribution exists on unimodular Lie groups. With regard to (1) and (2), the answer is certainly yes, and this kind of Gaussian distribution appeared as the solution of (20.14) subject to Dirac delta initial conditions. However, this is not necessarily the maximum-entropy distribution subject to covariance constraints.

Equipped with a concept of mean and covariance, the concept of a maximum-entropy distribution on a unimodular Lie group subject to constraints on the mean and covariance can be defined and computed in the usual way using Lagrange multipliers, and the result is of the form

$$\rho(g; \mu, \Sigma) = \frac{1}{c(\boldsymbol{\mu}, \Sigma)} \exp\left(-\frac{1}{2} [\log(\mu^{-1} \circ g)]^\vee \cdot \Sigma^{-1} [\log(\mu^{-1} \circ g)]^\vee \right), \tag{19.58}$$

where

$$c(\boldsymbol{\mu}, \Sigma) = \int_G \exp\left(-\frac{1}{2} [\log(\mu^{-1} \circ g)]^\vee \cdot \Sigma^{-1} [\log(\mu^{-1} \circ g)]^\vee \right) dg.$$

Such distributions have been studied in the context of how the covariance of convolved Gaussians can be obtained from the covariances of those being convolved. As $\|\Sigma\|$ becomes small, $\rho(g; e, \Sigma)$ converges to the solution of a driftless diffusion with Dirac delta initial conditions at the identity, and $\Sigma = tD$. In this case, exponential coordinates $g = \exp X$ become Cartesian coordinates near the identity and $dg \approx d\mathbf{x}$ (the Lebesgue measure) by identifying the Lie algebra with $\mathbb{R}^n$. In this limit, the usual Gaussian on $\mathbb{R}^n$ results, $c(\boldsymbol{\mu}, \Sigma) = (2\pi)^{n/2} |\Sigma|^{1/2}$ and $S(\rho) = \log \left[(2\pi e)^{n/2} |\Sigma|^{1/2} \right]$.

However, as $\|\Sigma\|$ (or tD) becomes larger, then the concepts of Gaussians on Lie groups as solutions to diffusion equations and as maximum-entropy distributions become inconsistent with each other. Each of these concepts of Gaussian distribution has its advantages in different scenarios.

19.7 Entropy Powers and Lie Groups

19.7.1 The Entropy-Power Inequality Does Not Hold on Compact Lie Groups

On a compact Lie group, the Haar measure can be normalized such that $\int_G dg = 1$. When using such a measure, $\rho(g) \doteq 1$ is a pdf. This is the limiting pdf of any nondegenerate diffusion as $t \to \infty$. Therefore, $(\rho * \rho)(g) = \rho(g)$. Since $\log 1 = 0$, the entropy is computed as $S(\rho) = 0$, and the (unnormalized) entropy power[4] is $N'(\rho) = e^0 = 1$. Therefore,

$$N'(\rho * \rho) = 1 \quad \text{ and } \quad N'(\rho) = 1 \implies N'(\rho * \rho) < N'(\rho) + N'(\rho).$$

In other words, the entropy power inequality (which has a $\geq$ in place of the $<$ in the above equation) fails. This is a general result that depends on the topology of compact Lie groups.

19.7.2 A Weak Entropy-Power Inequality for Unimodular Lie Groups

For pdfs that are highly concentrated (in the sense of having covariance matrices with small entries), the tails decay before the topological properties are "felt." In this special case, convolution depends only on local geometry. For example, if $\rho_i(g)$ for $i = 1, 2$ are Gaussians on a unimodular Lie group in exponential coordinates with means and covariances (μ_i, Σ_i), then $(\rho_1 * \rho_2)(g)$ will be a Gaussian with mean and covariance $(\mu_1 \circ \mu_2, Ad(\mu_2^{-1})\Sigma_1 Ad^T(\mu_2^{-1}) + \Sigma_2)$. Recall that for a unimodular Lie group, $|Ad(g)| = 1$. Does the entropy-power inequality (EPI) hold here?

The EPI for $\mathbb{R}^n$ when applied to Gaussians with covariances Σ_1' and Σ_2' is equivalent to the matrix inequality

$$|\Sigma_1' + \Sigma_2'|^{1/n} \geq |\Sigma_1'|^{1/n} + |\Sigma_2'|^{1/n},$$

which is a form of Minkowski's inequality. Now, working in reverse and letting $\Sigma_1' = Ad(\mu_2^{-1})\Sigma_1 Ad^T(\mu_2^{-1})$ and $\Sigma_2' = \Sigma_2$, it follows from $|\Sigma_1'| = |\Sigma_1|$ that

$$N(\rho_1 * \rho_2) \geq N(\rho_1) + N(\rho_2).$$

Therefore, in this limited setting, a weak version of the EPI holds. Extensions of this are left as an exercise.

19.8 Conclusions

By collecting and reinterpreting results relating to the study of diffusion processes, harmonic analysis, and log-Sobolev inequalities on Lie groups and merging these results with definitions of Fisher information matrix and covariance, many inequalities of information theory were extended here to the context of probability densities on unimodular Lie groups. In addition, the natural decomposition of groups into cosets, double cosets, and the nesting of subgroups provides some inequalities that result from

[4] Unnormalized entropy powers can be defined as $N'(\rho) = e^{2S(\rho)/n}$, where $n = \dim(G)$, whereas the normalized one is $N(\rho) = N'(\rho)/2\pi e$.

the Kullback–Leibler divergence of probability densities on Lie groups. Some special inequalities related to finite groups (which are also unimodular) were also provided. The results presented in this chapter were first derived in [11]. One open issue is determining the conditions under which the entropy power inequality [7, 31] will hold for Lie groups.

19.9 Exercises

19.1. If in Section 19.7.1, an unnormalized Haar measure such that $\int_G dg = \mathrm{Vol}(G) \neq 1$ is used instead of the normalized one, will this affect the fact that the EPI does not hold?

19.2. Following up on Section 19.7.2, suppose that $\rho_i'(g) = (1 + \epsilon_i(g))\rho_i(g)$ where $|\epsilon_i(g)| \ll 1$ is a small perturbation that leaves the first few moments of a concentrated Gaussian on a unimodular Lie group unchanged: $\int_G \rho_i'(g)\, dg = 1$, $\mu_{i'} = \mu_i$, and $\Sigma_{i'} = \Sigma_i$. Will the EPI hold for $\rho_1'(g)$ and $\rho_2'(g)$?

19.3. Does the EPI hold for the Heisenberg group?

References

1. Amari, S., Nagaoka, H., *Methods of Information Geometry*, Translations of Mathematical Monographs Vol. 191, American Mathematical Society, Providence, RI, 2000.
2. Avez, A., "Entropy of groups of finite type," *C.R. Hebdomadaires Seances Acad. Sci. A*, 275, pp. 13–63, 1972.
3. Bakry, D., Concordet, D., Ledoux, M., "Optimal heat kernel bounds under logarithmic Sobolev inequalities," *ESAIM: Probability and Statistics*, 1, pp. 391–407, 1997.
4. Barron, A.R., "Entropy and the central limit theorem," *Ann. Probab.*, 14, pp. 336–342, 1986.
5. Beckner, W., "Sharp inequalities and geometric manifolds," *J. Fourier Anal. Applic.* 3, pp. 825–836, 1997.
6. Beckner, W., "Geometric inequalities in Fourier analysis," in *Essays on Fourier Analysis in Honor of Elias M. Stein*, pp. 36–68 Princeton University Press, Princeton, NJ, 1995.
7. Blachman, N.M., "The convolution inequality for entropy powers," *IEEE Trans. Inform. Theory*, 11(2), pp. 267–271, 1965.
8. Brown, L.D., "A proof of the Central Limit Theorem motivated by the Cramér–Rao inequality," in *Statistics and Probability: Essays in Honour of C.R. Rao*, G. Kallianpur, P.R. Krishnaiah, and J.K. Ghosh, eds., pp. 141–148, North-Holland, New York, 1982.
9. Carlen, E.A., "Superadditivity of Fisher's information and logarithmic Sobolev inequalities," *J. Funct. Anal.*, 101, pp. 194–211, 1991.
10. Chirikjian, G.S., *Stochastic Models, Information Theory, and Lie groups: Vol. 1*, Birkäuser, Boston, 2009.
11. Chirikjian, G.S., "Information-theoretic inequalities on unimodular Lie groups," *J. Geom. Mechan.*, 2(2), pp. 119–158, 2010.
12. Cover, T.M., Thomas, J.A., *Elements of Information Theory*, 2nd ed. Wiley-Interscience, Hoboken, NJ, 2006.
13. Csiszár, I., "*I*-Divergence geometry of probability distributions and minimization problems," *Ann. Probab.*, 3(1), pp. 146–158, 1975.
14. Dembo, A., "Information inequalities and concentration of measure," *Ann. Prob.*, 25, pp. 527–539, 1997.
15. Dembo, A., Cover, T.M., Thomas, J.A., "Information theoretic inequalities," *IEEE Trans. Inform. Theory.*, 37(6), pp. 1501–1518, 1991.

16. Gibilisco, P., Isola, T., "Fisher information and Stam inequality of a finite group," *Bull. London Math. Soc.*, 40, pp. 855–862, 2008.
17. Gibilisco, P., Imparato, D., Isola, T., "Stam inequality on $\mathbb{Z}_n$," *Statist. Probab. Lett.*, 78, pp. 1851–1856, 2008.
18. Grenander, U., *Probabilities on Algebraic Structures*, Dover Published, New York, 2008. (originally publicated by John Wiley and Sons 1963).
19. Gross, L., "Logarithmic Sobolev inequalities," *Am. J. Math.*, 97, pp. 1061–1083, 1975.
20. Gross, L., "Logarithmic Sobolev inequalities on Lie groups," *Illinois J. Math.*, 36(3), pp. 447–490, 1992.
21. Heyer, H., *Probability Measures on Locally Compact Groups*, Springer-Verlag, New York, 1977.
22. Johnson, O., Suhov, Y., "Entropy and convergence on compact groups," *J. Theoret. Probab.*, 13(3), pp. 843–857, 2000.
23. Johnson, O., *Information Theory and the Central Limit Theorem*, Imperial College Press, London, 2004.
24. Ledoux, M., *Concentration of Measure and Logarithmic Sobolev Inequalities*, Lecture Notes in Mathematics Vol. 1709, Springer, Berlin, 1999.
25. Ledoux, M., *The Concentration of Measure Phenomenon*, Mathematical Surveys and Monographs Vol. 89, American Mathematical Society, Providence, RI, 2001.
26. Lieb, E.H., Loss, M., *Analysis*, 2nd ed., American Mathematical Society, Providence, RI, 2001.
27. Linnik, Y.V., "An information-theoretic proof of the Central Limit Theorem with the Lindeberg condition," *Theory Probab. Applic.*, 4(3), pp. 288–299, 1959.
28. Maksimov, V.M., "Necessary and sufficient statistics for the family of shifts of probability distributions on continuous bicompact groups," *Theory Probab. Applic.*, 12(2), pp. 267–280, 1967.
29. Otto, F., Villani, C., "Generalization of an inequality by Talagrand and links with the logarithmic Sobolev inequality," *J. Funct. Anal.*, 173, pp. 361–400, 2000.
30. Roy, K.K., "Exponential families of densities on an analytic group and sufficient statistics," *Sankhyā*: *Indian J. Statist. A*, 37(1), pp. 82–92, 1975.
31. Stam, A.J., "Some inequalities satisfied by the quantities of information of Fisher and Shannon," *Inform. Control*, 2(2), pp. 101–112, 1959.
32. Sugiura, M., *Unitary Representations and Harmonic Analysis*, 2nd ed., Elsevier Science Publisher, Amsterdam, 1990.
33. Talagrand, M., "New concentration inequalities in product spaces," *Invent. Math.*, 126, pp. 505–563, 1996.
34. Wang, Y., Chirikjian, G.S., "Nonparametric second-order theory of error propagation on the Euclidean group," *Int. J. Robot. Res.*, 27(1112), pp. 1258–1273, 2008.

20

Stochastic Processes on Lie Groups

As has been discussed in earlier chapters, it is possible to define probability densities on Lie groups and to compute convolutions. Since Lie groups are by definition also analytic manifolds, the methodology from Chapter 8 of Volume 1 can be used to define SDEs and Fokker–Planck equations. However, the added structure provided by Lie groups means that these equations can be derived in completely Lie-theoretic terms without ever referring to coordinates or charts. In addition, the natural embedding of Lie groups into matrices means that SDEs can be written extrinsically as well. These topics are discussed here, along with related topics from the field of probability and statistics on Lie groups. These include answering the questions: "How can the concepts of mean and covariance of a pdf on a Lie group be defined?" "If I only care how the mean and covariance behave as a function of time, can I obtain these without solving the Fokker–Planck equation?"

The main ideas to take away from this chapter are as follows:

- It is possible to describe SDEs and corresponding Fokker–Planck equations on Lie groups in much the same way as was done in Chapter 4 for the case of $\mathbb{R}^n$. Moreover, the formulation here also can be viewed as a special case of the framework explained in Chapter 8 for more general manifolds.
- Concepts of mean and covariance of probability densities on Lie groups that have desirable properties under convolution can be defined and used to study what happens as the number of convolutions grows. In the compact connected case, this leads to a convergence to uniformity, and in the case of noncompact connected unimodular Lie groups, this results in a central limit theorem.
- Diffusion processes on Lie groups described in this chapter are precisely the kind that arise in applications such as DNA statistical mechanics, steering of flexible needles, and nonholonomic kinematic systems such as wheeled vehicles that are subject to rolling constraints.

This chapter is organized as follows. Section 20.1 discusses McKean–Gangolli injection, which is a way to take a stochastic trajectory defined in the tangent space of a Lie group and use the exponential map to create a stochastic trajectory in a Lie group. Section 20.2 derives the Fokker–Planck equation for the resulting McKean–Gangolli injection and shows that the result is the same as if the coordinate-dependent approach to stochastic calculus on manifolds from Chapter 8 is used. Sections 20.3 and 20.4 respectively discuss Stratonovich and Itô SDEs on Lie groups. The former is natural for

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_11,

intrinsic approaches, as transitions between coordinate charts are handled gracefully, whereas the latter is well suited to the extrinsic approach in which a Lie group is defined as a set of matrices with constraint equations. Section 20.5 discusses the limiting distribution for gradient flows on Lie groups. Section 20.6 reviews various dispersion measures presented in the literature. Section 20.7 addresses changes of Lie algebra basis and diagonalization of diffusion matrices. Section 20.8 relates these to the concept of central limit theorems for iterated convolutions on Lie groups. Section 20.9 describes the properties of the resulting limiting distributions.

20.1 McKean–Gangolli Injection

Stochastic processes on Lie groups can be generated in several ways. One way is to "inject" a stochastic process from the Lie algebra into the group using the exponential map and product integral formula, as introduced by McKean [48]. A second way is to restrict a stochastic process defined in an ambient Euclidean space so as to "stay on" a group manifold rather than meandering off into the larger space. A third way is through SDEs defined in some set of coordinates that are natural to a specific physical problem. All three of these are discussed in this chapter, with injection being the focus of this section.

Consider the linear SDE with constant or time-varying coefficients

$$d\mathbf{x} = \mathbf{h}(t)\,dt + H(t)\,d\mathbf{w}\,. \tag{20.1}$$

This describes stochastic sample paths that evolve in $\mathbb{R}^n$, and due to the fact that $H(t)$ does not depend on $\mathbf{x}$, (20.1) can be viewed either as an Itô or Stratonovich equation. If we identify this Euclidean space with an n-dimensional Lie algebra, $\mathcal{G}$, then through the exponential map, it is possible to transfer (or "inject") this sample path into the corresponding Lie group via the exponential map. However, as the exponentiated path meanders away from the identity element of the group, nonlinearities creep in. Therefore, the *McKean–Gangolli injection* process "resets" things at the identity at each step. So, at time $t = 0$, $g(0) = e$. At $t = dt$, $g(dt) = g(0) \circ \exp(\sum_i dx_i E_i)$, where dx_i is evaluated at time dt. At the next step, $g(2dt) = g(dt) \circ \exp(\sum_i dx_i E_i)$, where dx_i is evaluated at time $2dt$ and so forth. Then the path $g(t) \in G$ is defined recursively as

$$g(t + dt) = g(t) \circ \exp\left(\sum_i dx_i\, E_i\right), \quad \text{where } g(0) = e, \tag{20.2}$$

where $\{E_i\}$ is a basis for $\mathcal{G}$. The path $g(t)$ generated in this way is written as the *product integral*

$$g(t) = \bigcap_{0 \le \tau \le t} \exp\left(\sum_i dx_i(\tau)\, E_i\right). \tag{20.3}$$

For our purposes this is nothing more than shorthand for the infinite product of exponentials that results from (20.2) with infinitesimal dt. The next sections derive Fokker–Planck equations corresponding to this sort of stochastic process, both from coordinate-free and coordinate-dependent perspectives.

20.2 Fokker–Planck Equations on Unimodular Lie Groups

Let $\rho(g,t)$ denote a time-parameterized pdf on a unimodular Lie group[1] (e.g., the rotation or motion groups); that is,

$$\rho(g,t) \geq 0 \quad \text{and} \quad \int_G \rho(g,t)\, dg = 1$$

for all values of $t \in \mathbb{R}^+$, and assume that

$$\rho(g,0) = \delta(g).$$

As usual, the partial derivative with respect to time is defined as

$$\frac{\partial \rho}{\partial t} = \lim_{\Delta t \to 0} \frac{1}{\Delta t} \left[\rho(g, t+\Delta t) - \rho(g,t)\right].$$

However, for a homogeneous process that evolves on a Lie group, it should be the case that

$$\rho(g,t+\Delta t) = \rho(g,t) * \rho(g,\Delta t) = \int_G \rho(h,t)\rho(h^{-1}\circ g, \Delta t)\, dh \tag{20.4}$$

$$= \rho(g,\Delta t) * \rho(g,t) = \int_G \rho(h,\Delta t)\rho(h^{-1}\circ g, t)\, dh. \tag{20.5}$$

In fact, this can be taken as the definition of a homogeneous process.

As in the proof of the classical Fokker–Planck equation, this convolution integral is substituted into the definition of partial derivative,

$$\int_G \frac{\partial \rho}{\partial t} f(g)\, dg = \lim_{\Delta t \to 0} \frac{1}{\Delta t} \int_G \left[\rho(g,t+\Delta t) - \rho(g,t)\right] f(g)\, dg.$$

Either (20.4) or (20.5) can be chosen. In order to make things concrete, choose (20.5). Then

$$\int_G \rho(g,t+\Delta t) f(g)\, dg$$
$$= \int_G [\rho(g,\Delta t) * \rho(g,t)] f(g)\, dg - \int_G \left[\int_G \rho(h,\Delta t)\rho(h^{-1}\circ g,t)\, dh\right] f(g)\, dg. \tag{20.6}$$

Here, $f(g)$ is an arbitrary function.

Since Δt is small, $\rho(h,\Delta t) = 0$ when h is "far from the identity." In other words, for a small value of Δt, the function $\rho(h,\Delta t)$ must not be too different from $\rho(h,0) = \delta(h)$. Distance from the identity can be measured using any reasonable metric $d(h,e)$. Therefore, the only values of h that contribute to the integral are those when $h = \exp X$ for $X = \sum_i x_i(h) E_i$ with $|x_i(h)| \ll 1$.

Then by making the change of coordinates,

$$k = h^{-1}\circ g \quad \Longleftrightarrow \quad g = h \circ k,$$

[1] Recall from Chapter 10 that a unimodular Lie group is one for which the integration measure is bi-invariant (i.e., $d(h\circ g) = d(g \circ h)$). This is a less restrictive condition than the existence of a bi-invariant metric.

and switching the order of integration using Fubini's theorem, (20.6) is written as

$$\int_G \rho(g, t+\Delta t) f(g)\, dg = \int_G \int_G \rho(h, \Delta t)\rho(k,t) f(h\circ k)\, dk\, dh. \tag{20.7}$$

Expanding $f(h \circ k)$ in a "left" Taylor series for small h and integrating each term in the resulting sum leads to simplifications. First, the zeroth-order term becomes

$$\int_G \rho(h, \Delta t) f(k)\, dh = f(k)\cdot \int_G \rho(h,\Delta t)\, dh = f(k).$$

The first-order terms in $x_i(h)$ becomes

$$\int_G \int_G \rho(h,\Delta t)\rho(k,t)\left(\sum_i x_i(h)\tilde{E}_i^l f(k)\right) dk\, dh \\ = \sum_i \int_G \left(\int_G x_i(h)\rho(h,\Delta t)\, dh\right)\rho(k,t)\tilde{E}_i^l f(k)\, dk,$$

and the second-order term becomes

$$\int_G \int_G \rho(h,\Delta t)\rho(k,t)\left(\frac{1}{2}\sum_{i,j} x_i(h)x_j(h)\tilde{E}_i^l\tilde{E}_j^l f(k)\right) dk\, dh \\ = \frac{1}{2}\sum_{i,j}\int_G \left(\int_G x_i(h)x_j(h)\rho(h,\Delta t)\, dh\right)\rho(k,t)\tilde{E}_i^l\tilde{E}_j^l f(k)\, dk.$$

Note that near the identity, x_i serve as Cartesian coordinates and the integral over the group can be replaced by an integral over a small box containing the identity:

$$\int_G x_i(h)\rho(h,\Delta t)\, dh = \int_{-dx_1/2}^{dx_1/2} \cdots \int_{-dx_n/2}^{dx_n/2} y_i\, \rho(h(\mathbf{y}),\Delta t)\, dy_n\, dy_{n-1}\cdots dy_1 = \langle dx_i\rangle$$

and

$$\int_G x_i(h)x_j(h)\rho(h,\Delta t)\, dh \\ = \int_{-dx_1/2}^{dx_1/2} \cdots \int_{-dx_n/2}^{dx_n/2} y_i y_j\, \rho(h(\mathbf{y}),\Delta t)\, dy_n\, dy_{n-1}\cdots dy_1 = \langle dx_i\, dx_j\rangle.$$

The variables y_i here are dummy variables of integration.

It follows that if (20.1) holds, then

$$\langle x_i\rangle = h_i(t)\, dt \quad \text{and} \quad \langle x_i x_j\rangle = dt\sum_k H_{ik}H_{kj}^T. \tag{20.8}$$

This follows for exactly the same reasons as in the derivation in the Euclidean case. However, something that is different is that (20.1) is not a SDE valid over the whole group but rather only near the identity. This issue will be revisited momentarily.

First, the invariant derivation of the Fokker–Planck equation on a Lie group is completed by using integration by parts, resulting in the localization of the form

$$\int_G Af(g)\, dg = 0 \quad \Longrightarrow \quad A = 0,$$

where the expression $A = 0$ is the Fokker–Planck equation[2]

$$\frac{\partial \rho(g,t)}{\partial t} + \sum_{i=1}^{d} \tilde{E}_i^l (h_i(t)\rho(g,t)) - \frac{1}{2}\sum_{i,j=1}^{d} \tilde{E}_i^l \tilde{E}_j^l \left(\sum_{k=1}^{m} H_{ik}(t) H_{kj}^T(t) \rho(g,t) \right) = 0. \quad (20.9)$$

Instead of substituting (20.4) in (20.6) it is possible to use (20.5) with all other steps being the same. This results in

$$\frac{\partial \rho(g,t)}{\partial t} + \sum_{i=1}^{d} \tilde{E}_i^r (h_i(t)\rho(g,t)) - \frac{1}{2}\sum_{i,j=1}^{d} \tilde{E}_i^r \tilde{E}_j^r \left(\sum_{k=1}^{m} H_{ik}(t) H_{kj}^T(t) \rho(g,t) \right) = 0. \quad (20.10)$$

The local behavior near the identity captured by (20.1) can be extended over the whole group in the following two ways.

Method 1: The stochastic process can be extended to the whole group by defining $g(\mathbf{x})$ to satisfy the Stratonovich SDEs:

$$g^{-1}\, dg = d\mathbf{x} \quad \text{or} \quad dg\, g^{-1} = d\mathbf{x} \quad (20.11)$$

subject to the initial conditions $\mathbf{x}(0) = \mathbf{0}$. This reduces to

$$d\mathbf{x} = J_r^{-1}(\mathbf{x}) \left[\mathbf{h}(t)\, dt + H(t)\, d\mathbf{w} \right]. \quad (20.12)$$

This defines a stochastic trajectory $\mathbf{x}(t)$ where $g(\mathbf{x}(t) \in G$.

Method 2: Compute directly

$$g(t + dt) = g(t) \circ \exp[\mathbf{h}(t)\, dt + H(t)\, d\mathbf{w}]. \quad (20.13)$$

Both methods are consistent with (20.11).

Examples of (20.10) have been demonstrated in the context of gyroscopes, kinematic carts, and flexible needle steering, as will be discussed in the next chapter. Focusing on the “r” case, when $\mathbf{h}$ and H are constant, we can write

$$\frac{\partial \rho(g,t)}{\partial t} + \sum_{i=1}^{d} h_i\, \tilde{E}_i^r \rho(g,t)) - \frac{1}{2}\sum_{i,j=1}^{d} D_{ij} \tilde{E}_i^r \tilde{E}_j^r\, \rho(g,t) = 0, \quad (20.14)$$

where

$$D_{ij} = \sum_{k=1}^{m} H_{ik} H_{kj}^T.$$

When considering SDEs and the corresponding Fokker–Planck equations, it is usually important to specify whether the Itô or Stratonovich form is used. Without getting into too much detail, it suffices to say that the Itô form has been assumed in the derivation of both of the above Fokker–Planck equations. However, if the coupling matrices H are independent of the coordinates used (or do not depend explicitly on the group elements), then the Itô and Stratonovich forms of the Fokker–Planck equation will be identical. In the examples that we will consider, the Itô and Stratonovich forms of the Fokker–Planck equation are all the same unless otherwise specified.

[2] It is important when reading the mathematics literature to recall that our $\tilde{E}_i^l$ is often written as their $-\tilde{E}_i^r$ and our $\tilde{E}_i^r$ is often written as their $\tilde{E}_i^l$.

20.3 Extracting Stratonovich SDEs from Fokker–Planck Equations on Unimodular Lie Groups

In the previous section it was shown how to go from an SDE defined in exponential coordinates on a unimodular Lie group to the corresponding Fokker–Planck equation. Sometimes in applications, a Fokker–Planck equation is given and we wish to express the SDE in other coordinates. Here, some coordinate-dependent calculations are demonstrated for the case of Stratonovich SDEs.

Near the identity, the Jacobian in exponential coordinates is close to being the identity. Therefore, very close to the identity, the Itô and Stratonovich SDEs with $H = J^{-1}$ will be the same. Is this "zeroth-order" statement true to first order or higher? This question can be answered by expanding out the Jacobian for the exponential coordinate parameterization and doing the calculations.

On a unimodular Lie group, we encounter diffusion operators with drift of the form

$$\Delta^* = \frac{1}{2}\sum_{i,j=1}^{d} D_{ij}\tilde{E}_i\tilde{E}_j f - \sum_{i=1}^{d} d_i\tilde{E}_i,$$

where Δ^* is the adjoint of the operator Δ, and these differ from each other only in the sign of the drift term.

A natural question to address is, What SDEs have a Fokker–Planck equation of the form

$$\frac{\partial f}{\partial t} = \Delta^* f \ ?$$

In terms of coordinates,

$$\sum_{i,j=1}^{d} D_{ij}\tilde{E}_i\tilde{E}_j f = \sum_{i,j=1}^{d} D_{ij}\sum_{l=1}^{d} J_{li}^{-1}\frac{\partial}{\partial q_l}\left(\sum_{k=1}^{d} J_{kj}^{-1}\frac{\partial f}{\partial q_k}\right).$$

If $D = BB^T$, so that $D_{ij} = \sum_{m=1}^{d} B_{im}B_{jm}$, then the summation signs above can be rearranged to yield

$$\sum_{i,j=1}^{d} D_{ij}\tilde{E}_i\tilde{E}_j f = \sum_{m,l,k=1}^{d}\left(\sum_{i=1}^{d} J_{li}^{-1}B_{im}\right)\frac{\partial}{\partial q_l}\left(\sum_{j=1}^{d} J_{kj}^{-1}B_{jm}\frac{\partial f}{\partial q_k}\right).$$

If the matrix H is defined by

$$H = J^{-1}B, \tag{20.15}$$

then

$$\sum_{i,j=1}^{d} D_{ij}\tilde{E}_i\tilde{E}_j f = \sum_{m,l,k=1}^{d} H_{lm}\frac{\partial}{\partial q_l}\left(H_{km}\frac{\partial f}{\partial q_k}\right).$$

In a similar way,

$$\sum_{i=1}^{d} d_i\tilde{E}_i f = \sum_{i=1}^{d}\sum_{k=1}^{d} d_i J_{ki}^{-1}\frac{\partial f}{\partial q_k} = \sum_{k=1}^{d} h_k\frac{\partial f}{\partial q_k},$$

where

$$h_k = \sum_{i=1}^{d} d_i J_{ki}^{-1}. \tag{20.16}$$

From the conditions imposed on Jacobians that result from the discussion in Section 12.2.3, it follows that the coordinate-dependent Stratonovich SDE corresponding to the diffusion operator D is

$$d\mathbf{q} = \mathbf{h}(\mathbf{q})\, dt + H(\mathbf{q})\, d\mathbf{w},$$

where the components of $\mathbf{h}$ and H are given in (20.16) and (20.15), respectively.

20.4 Conditions for an Itô Equation to Evolve on Certain Matrix Lie Groups

Many matrix Lie groups are defined by conditions of the form

$$g^T Q\, g = Q, \tag{20.17}$$

where $Q = Q^T$ is a matrix such as $I(p,q)$.

Let the set of all $g \in \mathbb{R}^{N\times N}$ satisfying this condition be called G. (Elsewhere in this text, group elements are denoted as g in the context of more abstract settings, but here they are denoted as g to emphasize that these group elements are matrices.) Then it is easy to see that closure holds under matrix multiplication of elements of G because if $g_1, g_2 \in G$, then, by definition, $g_1^T Q\, g_1 = Q$ and $g_2^T Q\, g_2 = Q$ and $g_2^T g_1^T Q\, g_1 g_2 = g_2^T Q\, g_2 = Q$, indicating that $g_1 \circ g_2 \in G$ (where $\circ$ denotes matrix multiplication). Then multiplying (20.17) on the left by $(g^T)^{-1} = (g^{-1})^T$ and on the right by g^{-1} gives $(g^{-1})^T Q\, g^{-1} = Q$, indicating closure under the inversion of g. The identity element $e \in G$ is simply the identity matrix $\mathbb{I}_N$, the associative law holds from matrix multiplication, and since $\det(g^T Q\, g) = \det Q$ implies $(\det g)^2 = 1$, it must be the case that each $g \in G$ has an inverse.

More specifically, the groups $O(p,q)$, where $p+q=N$, consist of group elements g that satisfy the condition

$$g^T I(p,q)\, g = I(p,q), \tag{20.18}$$

where $I(p,q) = \mathbb{I}_p \oplus (-\mathbb{I}_q)$. In other words, $I(p,q)$ is the diagonal matrix consisting of blocks that are either the identity or the negative of the identity.

The group $SO(p,q)$ consists of the part of $O(p,q)$ where $\det g = +1$.

Conditions for an Itô stochastic process $X(t)$ to evolve on the group defined by (20.17) are

$$d(g^T Q\, g) = (dg)^T Q\, g + g^T Q\, dg + (dg)^T Q\, dg = \mathbb{O}. \tag{20.19}$$

In particular, if the discussion is restricted to matrix SDEs of the form

$$dg = A(g)\, dt + \sum_{i=1}^{m} B_i(g)\, dw_i$$

where $A(g)$ and $B_i(g)$ are both matrix-valued functions of matrix-valued argument, then substitution into (20.19) results in the conditions

$$[A(g)]^T Q\, g + g^T Q A(g) + \sum_{i=1}^{m} [B_i(g)]^T Q B_i(g) = \mathbb{O}$$

and

$$QB_j(g) + [B_j(g)]^T Q = 0 \quad \text{for } j = 1, \ldots, m.$$

In the special case when $B_i(g) = gY_i$, where each $Y_i \in \mathcal{G}$, then it can be shown that the following SDE satisfies (20.19) and hence evolves on the group defined by (20.17):

$$dg = g \sum_{i=1}^{m} \left(-\frac{1}{2} Q^{-1} Y_i^T Q E_i \, dt + Y_i \, dw_i \right) \quad \text{with } QY_j + Y_j^T Q = \mathbb{O} \quad \text{for } j = 1, \ldots, m. \tag{20.20}$$

Consider the case where

$$g = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$$

satisfies the following matrix Itô SDE from [9]:

$$\begin{pmatrix} dx_1 & dx_2 \\ dx_3 & dx_4 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & -\alpha \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} dt + \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} dw_1 & dw_2 \\ dw_3 & -dw_1 \end{pmatrix}. \tag{20.21}$$

As will be observed, this equation describes a stochastic process on the group $SL(2, R)$. In other words, $\det X(t) = +1$ if $\det X(0) = +1$.

The matrix equation (20.21) can be written in the vector form

$$d\mathbf{x} = A\,\mathbf{x}\,dt + \sum_{i=1}^{m} dw_i \, B_i \, \mathbf{x}, \tag{20.22}$$

where $\mathbf{x} = [x_1, x_2, x_3, x_4]^T$,

$$A = \begin{pmatrix} \alpha & 0 & \beta & 0 \\ 0 & \alpha & 0 & \beta \\ \gamma & 0 & -\alpha & 0 \\ 0 & \gamma & 0 & -\alpha \end{pmatrix},$$

and if $Y_i = E_i$, then

$$B_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad B_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The condition $\det X = x_1 x_4 - x_2 x_3 = 1$ can be written in the form $\frac{1}{2}\mathbf{x}^T Q \mathbf{x} = 1$, where

$$Q' = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

It is easy to verify that

$$B_i^T Q' + Q' B_i = \mathbb{O} \quad \text{and} \quad A^T Q' + Q' A = \mathbb{O},$$

indicating that the quadratic form $\frac{1}{2}\mathbf{x}^T Q' \mathbf{x} = 1$ is preserved by sample paths of the SDE (or, equivalently, $\det X(t) = 1$).

20.5 Gradient Flows

In $\mathbb{R}^N$, the stochastic differential equation (Stratonovitch or Itô)

$$d\mathbf{x} = -\frac{1}{2}\nabla\phi\, dt + d\mathbf{w}$$

has a corresponding Fokker–Planck equation

$$\frac{\partial f}{\partial t} = \frac{1}{2}\nabla \cdot (f\,\nabla\phi) + \frac{1}{2}\nabla^2 f.$$

If this equation is solved subject to the initial conditions $f(\mathbf{x},0) = \delta(\mathbf{x})$ (which corresponds to the SDE having initial conditions $\mathbf{x}(0) = \mathbf{0}$), then in the steady state this equation has the solution

$$f_\infty(\mathbf{x}) = \lim_{t\to\infty} f(\mathbf{x},t) = \frac{1}{Z}e^{-\phi(\mathbf{x})},$$

where

$$Z = \int_{\mathbb{R}^N} e^{-\phi(\mathbf{x})}\, d\mathbf{x}.$$

Now, let G be an n-dimensional unimodular Lie group and consider the Stratonovich SDE

$$(g^{-1}\,dg)^\vee = -\frac{1}{2}\,\mathrm{grad}(\phi)\,dt + d\mathbf{w}. \tag{20.23}$$

Recall that $\mathrm{grad}(\phi) = [\tilde{E}_1^r\phi, \ldots, \tilde{E}_n^r\phi]^T$. Writing (20.23) in coordinates,

$$J_r(\mathbf{q})\,d\mathbf{q} = -\frac{1}{2}[J_r(\mathbf{q})]^{-T}\nabla_{\mathbf{q}}\phi + d\mathbf{w}.$$

Multiplying both sides by the inverse of $J_r(\mathbf{q})$ and recalling that the matrix tensor is $G_r = J_r^T J_r$, the following SDE results:

$$d\mathbf{q} = -\frac{1}{2}[G_r(\mathbf{q})]^{-1}\nabla_{\mathbf{q}}\phi + [J_r(\mathbf{q})]^{-1}d\mathbf{w}.$$

The corresponding Fokker–Planck equation is

$$\frac{\partial f}{\partial t} = \frac{1}{2}|J|^{-1}\sum_{i,j=1}^{n}\frac{\partial}{\partial q_i}\left(|J|g^{ij}\frac{\partial\phi}{\partial q_j}f\right) + \frac{1}{2}|J|^{-1}\sum_{i,j,k=1}^{n}\frac{\partial}{\partial q_i}\left(J^{ik}\frac{\partial}{\partial q_j}(|J|\,J_{jk}f)\right), \tag{20.24}$$

where $|J| = |\det J_r|$. Using the properties of Lie derivatives of functions on unimodular groups, it can be shown that the steady-state solution to (20.24) is [10]

$$f_\infty(g) = \frac{1}{Z}e^{-\phi(g)}.$$

20.6 Measures of Dispersion

For a pdf in $\mathbb{R}^n$, it is possible to compute covariance, which gives a sense of “how spread out” the distribution is. In this section, several extensions of the concept of covariance to the setting of pdfs on groups are reviewed. First, the central limit theorem for the real line in reviewed in Section 20.6.1. Various ways of defining the distance between a pdf on a noncommutative group and its limiting distribution are reviewed in Section 20.6.1. In Section 20.6.2 concepts of covariance that are algebraic in nature are reviewed. These preserve properties such as the covariance of the convolution of two functions is the sum of the covariances. In Section 20.6.4, very different concepts of covariance that use some measure of distance between group elements are reviewed. The concepts in Sections 20.6.2 and 20.6.4 can, in fact, be applied to all kinds of groups: Lie groups, finite groups, discrete groups with an infinite number of elements, products of any of the above, and so forth. In contrast, in Section 20.6.5 a concept of covariance developed specifically for Lie groups is presented. This uses the logarithm operator. In principle, this concept can be applied not only to Lie groups but also to any subgroup of a Lie group, whether it be a Lie group itself, a finite group, and so forth. Whereas covariance concepts are defined to measure dispersion relative to the most concentrated distribution (i.e., the Dirac delta function), where they take a value of 0, it is possible to view the problem from an opposite perspective—namely how far is a pdf from its limiting distribution?

20.6.1 Measures of Distance from the Limiting Distribution

For homogeneous diffusion processes with drift on $\mathbb{R}^n$, the distribution $f(\mathbf{x},t)$ subject to the initial conditions $f(\mathbf{x},0) = \delta(g)$ is self-similar; that is, a uniform rescaling of the spatial variable and renormalization of the function so as to remain a pdf will have the property

$$f(\mathbf{x},t;D,\mathbf{d}) = c(t)f(\mathbf{x},1;tD,t\mathbf{d}). \tag{20.25}$$

In contrast, diffusion processes on noncommutative Lie groups will generally not not have this property. Rather, the "shape" of the distribution will evolve over time.

For diffusion processes on compact Lie groups, the time-evolving pdf $f(g,t)$ will have the property that

$$f_{lim}(g) = \lim_{t\to\infty} f(g,t) = 1$$

as long as the volume element is normalized such that

$$\int_G 1\, dg = 1.$$

It then follows that for any pdf $\phi(g)$,

$$(f_{lim} * \phi)(g) = \int_G 1 \cdot \phi(h^{-1} \circ g)\, dh = \int_G \phi(g^{-1} \circ h)\, dh = \int_G \phi(h)\, dh = 1 = f_{lim}(g).$$

Stated in words, the convolution of the limiting distribution with any other pdf on a compact Lie group returns the limiting distribution. Thus, in the compact case the limiting distribution is very special, and it makes sense to ask how close any distribution is to the limiting distribution. This closeness of a given distribution, $\phi(g)$, to the limiting one can be defined in a number of ways, such as

$$d_p(\phi, f_{lim}) = \left(\int_G |\phi(g) - f_{lim}(g)|^p\, dg\right)^{\frac{1}{p}} \tag{20.26}$$

or

$$D_{KL}(\phi \,\|\, f_{lim}) = \int_G \phi(g) \log[\phi(g)/f_{lim}(g)]\, dg. \tag{20.27}$$

The rates of convergence to uniformity under iterated convolution has been studied in a number of works, including [14].

In the case of noncompact and noncommutative groups, the concept of limiting distribution of a diffusion process needs to be modified, because although the shape of the pdf evolves, it does not converge to the uniform distribution. Put simply, it is not possible to be a pdf and to be uniform on a space of infinite extent. In this case, the limiting distributions have been studied far less than the compact case, but in cases when they have been obtained, (20.26) and (20.27) can still be used.

20.6.2 Algebraic Covariance

Referring back to the way covariance matrices are defined for pdfs on $\mathbb{R}^n$, one might conclude that the "essential" property of covariances is that $\Sigma_{f_1 * f_2} = \Sigma_{f_1} + \Sigma_{f_2}$ and that the concept of covariance should be extended to more abstract domains in a way that preserves this property. In fact, this is the approach taken in [28, 30]. This concept uses ideas of group representation theory and harmonic analysis to define covariances. Part of the attractiveness of this approach is that it generalizes to wide classes of groups. However, for the purposes of illustration, only compact Lie groups will be discussed here.

Because the spectrum of an n-dimensional compact Lie group is discrete, it is possible to "pick any n" of the inequivalent irreducible unitary representations from the countably infinite number of them that are available. Let these chosen IURs be labeled as $U_i(g)$ for $i = 1, \ldots, n$. The corresponding Fourier transforms of the pdf $f(g)$ be computed as

$$\hat{f}_i = \int_G f(g) U_i(g^{-1})\, dg.$$

Denote the dimension of $\hat{f}_i$ (which is obviously the same as the dimension of $U_i(g)$) as d_i.

Now, let

$$V_{\mathbf{k}}(f) = \prod_{i=1}^{n} |\det \hat{f}_i|^{k_i},$$

where $\mathbf{k} = [k_1, k_2, \ldots, k_n]^T \in (\mathbb{R}^+)^n$. It follows that evaluating this definition at $f(g) = \delta(g)$ (the Dirac delta function), then $\hat{\delta}_i = I_{d_i}$ and $V_{\mathbf{k}}(\delta) = 1$ for any valid choice of $\mathbf{k}$. Likewise, if $f(g) = f_{lim}(g) = 1$, then for all values of i for which $d_i > 1$, the orthogonality of IURs forces $\hat{f}_i = 0$, and so, $V_{\mathbf{k}}(1) = 0$.

Using the convolution theorem and the property that $\det(AB) = \det A \det B$, it follows that

$$V_{\mathbf{k}}(f_1 * f_2) = V_{\mathbf{k}}(f_1) V_{\mathbf{k}}(f_2).$$

Since it is natural to think of a covariance as something that should be 0 for a delta function, take a large value for the limiting distribution, add under convolution, and be an $n \times n$-dimensional symmetric matrix for a pdf on an n-dimensional space, the following definition is used [28, 30]:

$$\sigma_{ij}(f) = -\log V_{\mathbf{e}_i + \mathbf{e}_j}(f) \quad \text{for } i, j = 1, \ldots, n. \tag{20.28}$$

In the case when $i = j$, $\sigma_{ii}(f) = -\log V_{2\mathbf{e}_i}(f) = -2 \log V_{\mathbf{e}_i}(f)$. An *algebraic covariance matrix* is then defined as $\Sigma_f = [\sigma_{ij}(f)]$.

Now, consider how this definition behaves under left shifts of the pdf:

$$\begin{aligned}\mathcal{F}(f(h^{-1}\circ g)) &= \int_G f(a^{-1}\circ g)U(g^{-1},\lambda)\,dg\\ &= \int_G f(h)U(h^{-1}\circ a^{-1},\lambda)\,dh\\ &= \left[\int_G f(h)U(h^{-1}\lambda)\,dh\right]U(a^{-1},\lambda)\\ &= \hat{f}(\lambda)U^*(a,\lambda).\end{aligned}$$

Since $U(a,\lambda)$ is special unitary, $\det U(a,\lambda)=1$, and so,

$$\sigma_{ij}(f(h^{-1}\circ g)) = \sigma_{ij}(f(g)).$$

Let $f_{D,\mathbf{d}}(g,t)$ denote the solution to the diffusion equation in (14.48) subject to the initial conditions $f_{D,\mathbf{d}}(g,t)=\delta(g)$. The Fourier space solution is

$$\hat{f}_{D,\mathbf{d}}(\lambda,t) = \exp t\left[\frac{1}{2}\sum_{i,j=1}^{n} D_{ij}u_i(\lambda)u_j(\lambda) - \sum_{k=1}^{n} d_k u_k(\lambda)\right].$$

Since $\det(\exp A)=e^{\mathrm{tr}(A)}$ and since $\mathrm{tr}(u_k(\lambda))=0$, it follows that

$$\det\hat{f}_{D,\mathbf{d}}(\lambda,t) = \exp t\left[\frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\mathrm{tr}\left\{u_i(\lambda)u_j(\lambda)\right\}\right] = \det\hat{f}_{D,\mathbf{0}}(\lambda,t),$$

and so, $\sigma_{ij}(f_{D,\mathbf{d}}(g,t)) = \sigma_{ij}(f_{D,\mathbf{0}}(g,t))$. In other words, the algebraic concept of covariance depends only on the diffusion constants, not the drifts.

To summarize, the algebraic covariance matrix $\varSigma=[\sigma_{ij}]$ with entries defined in (20.28) has the following properties:

$$\varSigma_\delta = \mathbb{O}, \tag{20.29}$$

$$(\sigma_{ij})_{f_{lim}} = \infty, \tag{20.30}$$

$$\varSigma_{f_1 * f_2} = \varSigma_{f_1} + \varSigma_{f_2}, \tag{20.31}$$

$$\varSigma_{L(h)f} = \varSigma_{R(h)f} = \varSigma_f, \tag{20.32}$$

$$\varSigma_{f_{D,\mathbf{d}}} = \varSigma_{f_{D,\mathbf{0}}}. \tag{20.33}$$

Whereas this concept seems to be the most widely articulated definition of covariance in the mathematical probability literature, the geometric/Lie-theoretic ideas in the following subsections arise more naturally in the context of the applications that follow in later chapters.

20.6.3 Dual-Space Covariance

Grenander [28] discussed a measure of dispersion of the form

$$d(f) = -\int_{\hat{G}} \alpha(\lambda)\log|||\hat{f}(\lambda)|||d\lambda, \quad \text{where } \alpha(\lambda)\geq 0, \quad \forall\,\lambda\in\hat{G}, \tag{20.34}$$

where G is a unimodular group and $|||\cdot|||$ is a matrix norm that is assumed to have the properties of being submultiplicative and $|||U||| = 1$ for $U \in SU(n)$. With these properties it is easy to see that

$$\begin{aligned}|||\hat{f}(\lambda)||| &= \left|\left|\left|\int_G f(g)U(g^{-1},\lambda)\,dg\right|\right|\right| \\ &\leq \int_G f(g)|||U(g^{-1},\lambda)|||\,dg \\ &= \int_G f(g)\,dg \\ &= 1,\end{aligned}$$

and so,

$$|||\hat{f}(\lambda)||| \leq 1, \tag{20.35}$$

In particular, if $|||A||| = \sqrt{\lambda_{max}(AA^*)}$, then the useful properties $|||AU||| = |||UA||| = |||A|||$ also hold and

$$|||\mathcal{F}(f(a^{-1}\circ g))||| = |||\hat{f}|||.$$

This invariance is true for right shifts also.

With such a norm, equality in (20.35) will hold when $f(g) = \delta(a^{-1}\circ g)$ for some $a \in G$ or if $U(g,\lambda) = 1$ (which can be true for a single value of λ in the case of a compact Lie group).

Furthermore,

$$|||\widehat{f_1 * f_2}||| = |||\hat{f}_2\hat{f}_1||| \leq |||\hat{f}_1|||\cdot|||\hat{f}_2||| \leq 1.$$

Substituting this into (20.34) means that $d(f_1 * f_2) \leq d(f_1) + d(f_2)$. From this it is also clear that as a pdf is convolved many times with itself (or with other pdfs), the norm $|||\cdot|||$ of the Fourier matrices that result will tend toward the zero matrix and (20.34) will therefore tend to infinity. To summarize, this measure of dispersion has the properties

$$0 \leq d(f) \leq \infty, \quad d(f_1 * f_2) \leq d(f_1) + d(f_2), \quad d(L(a)f) = d(R(a)f) = d(f). \tag{20.36}$$

A simple extension of this concept that the author has not seen in the literature would be to define a *dual-space covariance* as

$$\sigma_{ij}(f) = -\int_{\hat{G}} [\alpha_i(\lambda) + \alpha_j(\lambda)] \log |||\hat{f}(\lambda)|||d\lambda, \tag{20.37}$$

where

$$\alpha_i(\lambda) \geq 0, \quad \forall\ \lambda \in \hat{G}, \quad \text{and} \quad i \in \{1,2,\ldots,\dim(G)\}.$$

20.6.4 Geometric Covariance

In a sense, the core ideas of geometry all revolve around measuring distances and angles. By defining a metric (or distance) function on a Lie group, then a geometric concept of mean and covariance can be defined. There is more than one way to measure distances between group elements. In order to be a valid distance function, the following properties are required for all $g_1, g_2, g_3 \in G$:

$$d(g_1, g_2) = d(g_2, g_1), \tag{20.38}$$

$$d(g_1, g_2) \geq 0, \quad \text{where } d(g_1, g_1) = 0, \quad \text{and} \tag{20.39}$$

$$d(g_1, g_2) = 0 \quad \Longrightarrow \quad g_1 = g_2, \tag{20.40}$$

$$d(g_1, g_3) \leq d(g_1, g_2) + d(g_2, g_3). \tag{20.41}$$

For example, the conceptually simplest metric for matrix Lie groups is

$$d_F(g_1, g_2) = \|g_1 - g_2\|,$$

where $\|\cdot\|$ is a matrix norm, such as the Frobenius norm.

Additionally, if $U(g, \lambda) \in SU(d_\lambda)$ is a finite-dimensional irreducible unitary representation of G, then

$$d_\lambda(g_1, g_2) = \|U(g_1, \lambda) - U(g_2, \lambda)\|$$

satisfies these definitions.

The following are also valid metrics for all but a set of measure zero on the groups of interest in most applications:

$$d_l(g_1, g_2) = \| \, [\log(g_1^{-1} \circ g_2)]^\vee \, \|$$

and

$$d_r(g_1, g_2) = \| \, [\log(g_2 \circ g_1^{-1})]^\vee \, \|.$$

In general, $d_\lambda(g_1, g_2)$ can be defined for compact Lie groups. It has the property of being bi-invariant:

$$d_\lambda(h \circ g_1, h \circ g_2) = d_\lambda(g_1, g_2) = d_\lambda(g_1 \circ h, g_2 \circ h).$$

For the noncompact case, IURs are infinite dimensional and $d_\lambda(g_1, g_2)$ cannot be defined. However, in both compact and noncompact cases, the distance functions $d_l(\cdot, \cdot)$ and $d_r(\cdot, \cdot)$ can be defined for all pairs for which the logarithm map is defined.

Additionally, although bi-invariance is generally not preserved,

$$d_l(h \circ g_1, h \circ g_2) = d_l(g_1, g_2)$$

and

$$d_r(g_1 \circ h, g_2 \circ h) = d_r(g_1, g_2).$$

Armed with a variety of metrics from which to choose, the geometric mean of a pdf on a Lie group is defined as [14, 28]

$$\mu_d(f) = \arg \min_{g_1 \in G} \int_G d^2(g_1, g_2) f(g_2) \, dg_2. \tag{20.42}$$

The corresponding *geometric variance* about the geometric mean is

$$\sigma_d^2(f) = \int_G d^2(\mu, g_2) f(g_2) \, dg_2, \tag{20.43}$$

where d can be any metric.

Similarly, the *geometric median* and *geometric spread* about the median can be defined as

$$m_d(f) = \arg\min_{g_1 \in G} \int_G d(g_1, g_2) f(g_2)\, dg_2 \tag{20.44}$$

and

$$s_d(f) = \int_G d(m_d(f), g_2) f(g_2)\, dg_2. \tag{20.45}$$

Now, given functions $f_1(g)$ and $f_2(g)$, consider the values of $\sigma_d^2(f_i)$ and $s_d(f_i)$ assuming that $\mu_d(f_i) = m_d(f_i) = e$. This is not a severe constraint since if $d(\cdot, \cdot)$ is left invariant, the mean or median can be moved to any desired group element by shifting the function. However, computing the geometric mean or median of the convolution of two pdfs is not trivial. Therefore, the more restrictive constraint $\mu_d(f_1 * f_2) = m_d(f_1 * f_2) = e$ will also be assumed.

Due to the metric property and the above assumptions,

$$\begin{aligned}
s_d(f_1 * f_2) &= \int_G d(e, g_2)(f_1 * f_2)(g_2)\, dg_2 \\
&= \int_G \int_G d(e, g_2) f_1(h) f_2(h^{-1} \circ g_2)\, dg_2\, dh \\
&= \int_G \int_G d(e, h \circ k) f_1(h) f_2(k)\, dk\, dh \qquad (20.46) \\
&= \int_G \int_G d(h^{-1}, k) f_1(h) f_2(k)\, dk\, dh \\
&\leq \int_G \int_G \{d(h^{-1}, e) + d(e, k)\} f_1(h) f_2(k)\, dk\, dh \\
&= \int_G d(e, h) f_1(h)\, dh + \int_G d(e, k) f_2(k)\, dk \\
&= s_d(f_1) + s_d(f_2). \qquad (20.47)
\end{aligned}$$

In (20.46) the substitution $k = h^{-1} \circ g_2$ means that $g_2 = h \circ k$. In the equality prior to that, the order of integration over h and g_2 was switched when the definition of convolution was substituted.

A similar calculation shows

$$\begin{aligned}
\sigma_d^2(f_1 * f_2) &= \int_G d^2(e, g_2)(f_1 * f_2)(g_2)\, dg_2 \\
&= \int_G \int_G d^2(h^{-1}, k) f_1(h) f_2(k)\, dk\, dh \\
&\leq \int_G \int_G \{d(h^{-1}, e) + d(e, k)\}^2 f_1(h) f_2(k)\, dk\, dh \\
&= \sigma_d^2(f_1) + \sigma_d^2(f_2) + 2 s_d(f_1) \cdot s_d(f_2), \qquad (20.48)
\end{aligned}$$

where the details analogous to steps (20.46)–(20.47) have been abbreviated.

Using an alternative logical route starting at equality (20.46), the definition of the median implies that

$$s_d(f_2) \leq \int_G d(e, h \circ k) f_2(k)\, dk \quad \text{and} \quad s_d(f_1) \leq \int_G d(e, h \circ k) f_1(h)\, dh.$$

Therefore,

$$\max\{s_d(f_1), s_d(f_2)\} \leq s_d(f_1 * f_2).$$

The same logic follows for the variance.

In summary, when the geometric mean and median of the original and convolved probability density functions are all located at the identity,

$$\max\{s_d(f_1), s_d(f_2)\} \leq s_d(f_1 * f_2) \leq s_d(f_1) + s_d(f_2), \tag{20.49}$$

$$\max\{\sigma_d^2(f_1), \sigma_d^2(f_2)\} \leq \sigma_d^2(f_1 * f_2) \leq \sigma_d^2(f_1) + \sigma_d^2(f_2) + 2s_d(f_1) \cdot s_d(f_2). \tag{20.50}$$

20.6.5 Lie-theoretic Covariance

For any Lie group G, it is possible to map a region around the identity element to the Lie algebra using the logarithm map. This means that if $f(g)$ is a pdf on G supported on this region around the identity, then the *covariance of* f,

$$\Sigma_f = \int_G (\log g)^\vee [(\log g)^\vee]^T f(g)\, dg, \tag{20.51}$$

is well defined.[3] In fact, for the groups of interest in many applications (which typically are connected), the exponential and logarithm maps are well defined "almost everywhere"; that is, if a set of measure zero in the group is excluded (which corresponds to singularities in the exponential map), then the mapping between the remaining part of the group and the corresponding region in the Lie algebra can be made bijective. Additionally, since the removal of sets of measure zero for well-behaved probability densities does not affect the computation of integrals, the condition that $f(g)$ is compactly supported can be relaxed.

For a unimodular Lie group, a transformation of coordinates of the form $g \to h \circ g \circ h^{-1}$ leaves integrals invariant. Therefore,

$$\begin{aligned}
\Sigma_f &= \int_G (\log h \circ g \circ h^{-1})^\vee [(\log h \circ g \circ h^{-1})^\vee]^T f(h \circ g \circ h^{-1})\, dg && (20.52)\\
&= \int_G [Ad(h)](\log g)^\vee [(\log g)^\vee]^T [Ad(h)]^T f(h \circ g \circ h^{-1})\, dg && (20.53)\\
&= [Ad(h)] \Sigma_{Ad(h^{-1})f} [Ad(h)]^T, && (20.54)
\end{aligned}$$

where $Ad(h^{-1})f(g) = f(h \circ g \circ h^{-1})$. This definition of $Ad(\cdot)$ acting on a *function* is opposite that for the definition of $Ad(g)$ acting on a *Lie algebra* element, in the same way that a left shift $(L(h)f)(g) = f(h^{-1} \circ g)$, whereas the left shift of a group element itself would be $g \to h \circ g$.

By a change of coordinates, (20.54) is rewritten as

$$\Sigma_{Ad(h)f} = [Ad(h)] \Sigma_f [Ad(h)]^T. \tag{20.55}$$

In the special case when $f(g)$ is a class function, it follows that $[Ad(h)]\Sigma_f[Ad(h)]^T = \Sigma_f$. This fact is used in [67] to obtain a formula for computing the Lie-theoretic (or "kinematic") covariance of the convolution product $(f_1 * f_2)(g)$ when each $f_i(g)$ is relatively concentrated.

[3] Usually when there is no question about which pdf is being used, the subscript f is omitted.

20.6.6 Other Measures of Dispersion

The concepts of covariance discussed in the previous sections are not the only ways to describe how spread out or concentrated a pdf is. Here, some other measures are discussed.

The Square of a Probability Density Function

Given a time-evolving pdf $f(g,t)$, the quantity

$$-\frac{1}{2}\|f\|_2^2 = -\frac{1}{2}\int_G |f(g,t)|^2\, dg \tag{20.56}$$

can also be used as a measure of dispersion since it will be more negative for values of t when $f(g,t)$ is concentrated and will approach its minimal value as $f(g,t)$ spreads out.

For solutions of the diffusion equation with drift,

$$\begin{aligned}
-\frac{1}{2}\frac{d\|f\|_2^2}{dt} &= -\int_G f\frac{\partial f}{\partial t}\, dg = -\int_G f\Delta^* f\, dg \\
&= \int_G \left\{ \sum_{i,j=1}^{3} D_{ij}(\tilde{E}_i^r f)(\tilde{E}_j^r f) \right\} dg \\
&\geq 0.
\end{aligned}$$

In the above, integration by parts has been used (resulting in the change in sign on the third line above). The reason why the drift terms disappear is that for any differentiable function $\phi(g)$,

$$\int_G \phi\,(\tilde{E}_i^r \phi)\; dg = 0.$$

The final inequality is a result of the fact that the quantity in braces is a quadratic form and D is a positive semi-definite matrix.

The measure of dispersion $-\frac{1}{2}\|f\|_2^2$ is also convenient from a Fourier perspective since from the Plancherel equality,

$$\frac{d\|f\|_2^2}{dt} = -\frac{1}{2}\frac{d}{dt}\int_{\hat{G}} \|\hat{f}(\lambda,t)\|^2 d\lambda \geq 0 \quad\Longrightarrow\quad \frac{d}{dt}\|\hat{f}(\lambda,t)\|^2 \leq 0, \quad \forall\ \lambda \in \hat{G}. \tag{20.57}$$

The Entropy of a Probability Density Function

The entropy of a pdf on a Lie group is defined as

$$S_\phi = -\int_G \phi(g)\log\phi(g)\, dg. \tag{20.58}$$

If $f(g,t)$ is a pdf that satisfies a diffusion equation (regardless of the details of the initial conditions), then some interesting properties of $S_f(t)$ can be studied. In particular, if $\dot{S}_f = dS_f/dt$, then differentiating under the integral sign gives

$$\dot{S}_f = -\int_G \left\{ \frac{\partial f}{\partial t}\log f + \frac{\partial f}{\partial t} \right\} dg.$$

However, from the properties of a diffusion equation,

$$\int_G \frac{\partial f}{\partial t}\, dg = \frac{d}{dt}\int_G f(g,t)\, dg = 0,$$

and so, the second term in the above braces integrates to 0.

Substitution of

$$\frac{\partial f}{\partial t} = \frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\tilde{E}_i^r \tilde{E}_j^r f - \sum_{k=1}^{n} d_k \tilde{E}_k^r f$$

into the integral for $\dot{S}_f$ gives

$$\begin{aligned}
\dot{S}_f =& -\int_G \left\{ \frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\tilde{E}_i^r \tilde{E}_j^r f - \sum_{k=1}^{n} d_k \tilde{E}_k^r f \right\} \log f\, dg \\
=& -\frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\int_G (\tilde{E}_i^r \tilde{E}_j^r f) \log f\, dg - \sum_{k=1}^{n} d_k \int_G (\tilde{E}_k^r f)\, \log f\, dg \\
=& \frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\int_G (\tilde{E}_j^r f)(\tilde{E}_i^r \log f)\, dg + \sum_{k=1}^{n} d_k \int_G f\, (\tilde{E}_k^r \log f)\, dg \\
=& \frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\int_G \frac{1}{f}(\tilde{E}_j^r f)(\tilde{E}_i^r f)\, dg + \sum_{k=1}^{n} d_k \int_G \tilde{E}_k^r f\, dg \\
=& \frac{1}{2}\sum_{i,j=1}^{n} D_{ij}\int_G \frac{1}{f}(\tilde{E}_j^r f)(\tilde{E}_i^r f)\, dg \\
=& \frac{1}{2}\int_G \frac{1}{f}\, (\nabla^r f)^T D\, (\nabla^r f)\, dg \\
\geq& \, 0.
\end{aligned}$$

This result parallels the one developed for manifolds in Volume 1.

20.7 Changes of Coordinates to Diagonalize a Diffusion Operator

Diffusion equations with drift discussed previously can be solved using methods of noncommutative harmonic analysis. As a computation matter, these solutions can be obtained with fewer numerical operations in some cases if the matrix D in the expression

$$\varDelta = \frac{1}{2}\sum_{ij} D_{ij}\tilde{E}_i^r \tilde{E}_j^r + \sum_k d_k \tilde{E}_k^r$$

is diagonal. Therefore, this section explores the cases when D can be diagonalized. In order to accomplish this, some preliminary results regarding the interactions of shifts, derivatives, and group Fourier transforms are presented.

20.7.1 Left Shifts and Right Derivatives Commute

Recall that left-shift operators of the form $(L(g_0)f)(g) = f(g_0^{-1} \circ g)$ commute with the operators $(\tilde{E}_i^r f)(g)$. This is easy to see because

$$\begin{aligned}(L(g_0)\tilde{E}_i^r f)(g) &= L(g_0)\frac{d}{dt}f(g\circ\exp(tE_i))\bigg|_{t=0}\\ &= \frac{d}{dt}f(g_0^{-1}\circ g\circ\exp(tE_i))\bigg|_{t=0}\\ &= (\tilde{E}_i^r f)(g_0^{-1}\circ g)\\ &= (\tilde{E}_i^r L(g_0)f)(g).\end{aligned} \tag{20.59}$$

A similar expression holds for left derivatives and right shifts (20.59). In contrast, in general, $(R(g_0)\tilde{E}_i^r f)(g) \neq (\tilde{E}_i^r R(g_0)f)(g)$ and likewise for left shifts and left Lie derivatives.

The adjoint operator applied to a function is defined as

$$(Ad(g_0)f)(g) = (R(g_0)L(g_0)f)(g) = (L(g_0)R(g_0)f)(g) = f(g_0^{-1}\circ g\circ g_0). \tag{20.60}$$

Now, consider what happens when the right Lie derivative of $(Ad(g_0)f)(g)$ is computed:

$$\begin{aligned}(\tilde{E}_i^r Ad(g_0)f)(g) &= \tilde{E}_i^r[f(g_0^{-1}\circ g\circ g_0)]\\ &= \frac{d}{dt}f(g_0^{-1}\circ(g\circ\exp(tE_i))\circ g_0)\bigg|_{t=0}\\ &= \frac{d}{dt}f((g_0^{-1}\circ g)\circ(\exp(tE_i)\circ g_0))\bigg|_{t=0}\\ &= \frac{d}{dt}f((g_0^{-1}\circ g)\circ(g_0\circ g_0^{-1})\circ(\exp(tE_i)\circ g_0))\bigg|_{t=0}\\ &= \frac{d}{dt}f((g_0^{-1}\circ g\circ g_0)\circ(g_0^{-1}\circ\exp(tE_i)\circ g_0))\bigg|_{t=0}\\ &= \frac{d}{dt}f((g_0^{-1}\circ g\circ g_0)\circ\exp(t\,g_0^{-1}E_i g_0))\bigg|_{t=0}\\ &= (Ad(g_0)[\widetilde{Ad(g_0^{-1})E_i}]^r f)(g).\end{aligned} \tag{20.61}$$

In other words, the adjoint applied to a scalar function does not commute with the Lie derivative, but there is a Lie derivative in a different direction defined by the adjoint that can be applied in reverse order to obtain the same result.

20.7.2 Using Harmonic Analysis to Elucidate Interactions Between Shifts and Derivatives

The evaluations of multiple shifts and derivatives such as those in Section 20.7 can be quite confusing, and it is easy to make an error in the order in which operations are applied. Fortunately, notation from harmonic analysis can be used as a convenient check on these calculations.

The Fourier reconstruction formula for a well-behaved function on a unimodular Lie group is given by

$$f(g) = \int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g,\lambda)\right]d\lambda, \tag{20.62}$$

where $U(g,\lambda)$ is an IUR with the property $U(g_1 \circ g_2, \lambda) = U(g_1,\lambda)U(g_2,\lambda)$ and $U(g^{-1},\lambda) = U^*(g,\lambda)$.

Evaluating the right Lie derivative then means

$$\begin{aligned}(\tilde{E}_i^r f)(g) &= \frac{d}{dt}\left[\int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g \circ e^{t\,E_i},\lambda)\right] d\lambda\right]_{t=0} \\ &= \int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g,\lambda)\frac{d}{dt}U(e^{t\,E_i},\lambda)\right]_{t=0} d\lambda \\ &= \int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g,\lambda)u(E_i,\lambda)\right] d\lambda = \int_{\hat{G}} \mathrm{tr}\left[u(E_i,\lambda)\hat{f}(\lambda)U(g,\lambda)\right] d\lambda,\end{aligned}$$

where

$$u(E_i,\lambda) = \left.\frac{d}{dt}U(e^{t\,E_i},\lambda)\right|_{t=0}.$$

Note that this “little u” matrix has the property that

$$U(g,\lambda)u(E_i,\lambda)U(g^{-1},\lambda) = u(g\,E_i\,g^{-1},\lambda). \tag{20.63}$$

Below, (20.59) is reexamined within this context. From the equations above, it follows that

$$\begin{aligned}(L(g_0)\tilde{E}_i^r f)(g) &= L(g_0)\int_{\hat{G}} \mathrm{tr}\left[u(E_i,\lambda)\hat{f}(\lambda)U(g,\lambda)\right] d\lambda \\ &= \int_{\hat{G}} \mathrm{tr}\left[u(E_i,\lambda)\hat{f}(\lambda)U(g_0^{-1}\circ g,\lambda)\right] d\lambda \\ &= \int_{\hat{G}} \mathrm{tr}\left[u(E_i,\lambda)\hat{f}(\lambda)U^*(g_0,\lambda)U(g,\lambda)\right] d\lambda.\end{aligned}$$

On the other hand,

$$\begin{aligned}(\tilde{E}_i^r L(g_0)f)(g) &= \tilde{E}_i^r \int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g_0^{-1}\circ g,\lambda)\right] d\lambda \\ &= \frac{d}{dt}\left[\int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g_0^{-1}\circ g \circ e^{t\,E_i},\lambda)\right] d\lambda\right]_{t=0} \\ &= \int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U^*(g_0,\lambda)U(g,\lambda)u(E_i,\lambda)\right] d\lambda \\ &= \int_{\hat{G}} \mathrm{tr}\left[u(E_i,\lambda)\hat{f}(\lambda)U^*(g_0,\lambda)U(g,\lambda)\right] d\lambda.\end{aligned}$$

From this, it is clear that (20.59) is verified.

Now, consider (20.61) in the light of the harmonic-analysis expansion:

$$\begin{aligned}(\tilde{E}_i^r Ad(g_0)f)(g) &= \tilde{E}_i^r \int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g_0^{-1}\circ g \circ g_0,\lambda)\right] d\lambda \\ &= \tilde{E}_i^r \int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g_0^{-1},\lambda)U(g,\lambda)U(g_0,\lambda)\right] d\lambda \\ &= \int_{\hat{G}} \mathrm{tr}\left[\hat{f}(\lambda)U(g_0^{-1},\lambda)U(g,\lambda)u(E_i,\lambda)U(g_0,\lambda)\right] d\lambda.\end{aligned}$$

On the other hand,

$$
\begin{aligned}
&(Ad(g_0)[Ad(g_0^{-1})\tilde{E}_i]^r f)(g) \\
&= Ad(g_0)\int_{\hat{G}} \operatorname{tr}\left[\hat{f}(\lambda)U(g,\lambda)u(g_0^{-1}E_i g_0,\lambda)\right] d\lambda \\
&= \int_{\hat{G}} \operatorname{tr}\left[\hat{f}(\lambda)U(g_0^{-1}\circ g\circ g_0,\lambda)u(g_0^{-1}E_i g_0,\lambda)\right] d\lambda \\
&= \int_{\hat{G}} \operatorname{tr}\left[\hat{f}(\lambda)\left(U(g_0^{-1},\lambda)U(g,\lambda)U(g_0,\lambda)\right)\left(U(g_0^{-1},\lambda)u(E_i,\lambda)U(g_0,\lambda)\right)\right] d\lambda \\
&= \int_{\hat{G}} \operatorname{tr}\left[\hat{f}(\lambda)U(g_0^{-1},\lambda)U(g,\lambda)u(E_i,\lambda)U(g_0,\lambda)\right] d\lambda
\end{aligned}
$$

The fact that these are the same verifies (20.61).

It is also easy to see that for general functions, $f(g)$, right derivatives do not commute with right shifts, and similarly for the left case.

20.8 The Central Limit Theorem for Unimodular Lie Groups

For probability densities that are highly concentrated around their mean, the Lie-theoretic definition of mean and covariance makes the most sense, because a d-dimensional unimodular Lie group "looks like" $\mathbb{R}^d$ locally.

To be more precise, if $d(g_1,g_2)=\|(\log g_1^{-1}\circ g_2)^\vee\|$ and if there exists $\mu\in G$ such that

$$\int_{d(\mu,g)<\epsilon} \rho(g)\,dg \approx 1, \quad \text{where } \epsilon \ll 1,$$

then $\rho(g)$ will be called *highly concentrated*. This happens, for example, when $\rho(g)$ has compact support on the ϵ-ball centered on the mean, in which case $\approx$ becomes $=$. For highly concentrated distributions, the mean will be μ and the Lie-theoretic covariance will be

$$\Sigma = \int_{\mathbb{R}^d} \mathbf{x}\mathbf{x}^T \rho(\mu\circ\exp X)\,d\mathbf{x}.$$

Suppose that n such functions $\rho_1(g),\rho_2(g),\dots,\rho_n(g)$ are given and they all have means and covariances defined by

$$(\log\mu_i)^\vee = \frac{1}{n}\mathbf{d} \quad \text{and} \quad \Sigma_i = \frac{1}{n}D.$$

Then the central limit theorem for Lie groups states that [28]

$$\lim_{n\to\infty}(\rho_1 * \rho_2 * \cdots * \rho_n)(x) = f(g,1,D,\mathbf{d}), \tag{20.64}$$

where $f(g,1,D,\mathbf{d})$ is the solution to the Fokker–Planck equation with $t=1$.

The proof of this follows in much the same way as for the case on the real line. The case when $\rho_i=\rho$ for all $i=1,\dots,n$ is considered below to reduce the number of indices, which would clutter the picture without adding much conceptually.

Basically, the Fourier transform matrices for such distributions will be

$$\begin{aligned}\hat{\rho}(\lambda) &= \int_G \rho(g) U(g^{-1}, \lambda)\, dg \\ &= \int_{d(\mu,g)<\epsilon} \rho(g) U(g^{-1}, \lambda)\, dg \\ &= \int_{\|\mathbf{x}\|<\epsilon} \rho(\mu \circ \exp X) U([\mu \circ \exp X]^{-1}, \lambda)\, d\mathbf{x} \\ &= \int_{\|\mathbf{x}\|<\epsilon} \rho(\mu \circ \exp X) U(\exp -X, \lambda) U(\mu^{-1}, \lambda)\, d\mathbf{x}.\end{aligned}$$

Since $\|\mathbf{x}\| \ll 1$, the second-order Taylor series approximation

$$\begin{aligned}U(\exp -X, \lambda) &= \exp\left[\sum_{i=1}^{n} -x_i u(E_i, \lambda)\right] \\ &\approx I - \sum_{i=1}^{d} x_i u(E_i, \lambda) + \frac{1}{2} \sum_{i=1}^{d} \sum_{i=1}^{d} x_i x_j u(E_i, \lambda) u(E_j, \lambda)\end{aligned}$$

is appropriate. Integrating term by term the product of the above series approximation with $\rho(\mu \circ \exp X)$ over the ball $\|\mathbf{x}\| < \epsilon$ then gives

$$\hat{\rho}(\lambda) U(\mu, \lambda) \approx I + \frac{1}{2n} \sum_{i=1}^{d} \sum_{i=1}^{d} D_{ij}\, u(E_i, \lambda) u(E_j, \lambda).$$

The first-order terms drop out because the ball is centered on the mean.

$U(\mu^{-1}, \lambda)$ can be expanded in a similar way as

$$U(\mu^{-1}, \lambda) \approx I - \frac{1}{n} \sum_{i=1}^{d} d_i u(E_i, \lambda) + \frac{1}{2n^2} \sum_{i=1}^{d} \sum_{i=1}^{d} d_i d_j\, u(E_i, \lambda) u(E_j, \lambda).$$

However, since $n \to \infty$, the second-order terms in this last expression can be ignored. Therefore, multiplying $\hat{\rho}(\lambda) U(\mu, \lambda)$ and $U(\mu^{-1}, \lambda)$ and keeping terms to $O(1/n)$,

$$\hat{\rho}(\lambda) \approx I - \frac{1}{n} \sum_{i=1}^{d} d_i u(E_i, \lambda) + \frac{1}{2n} \sum_{i=1}^{d} \sum_{i=1}^{d} D_{ij}\, u(E_i, \lambda) u(E_j, \lambda).$$

Therefore, using the convolution theorem, $\mathcal{F}\left(\lim_{n\to\infty} (\rho_1 * \rho_2 * \cdots * \rho_n)(x)\right)$ can be written as

$$\begin{aligned}\lim_{n\to\infty} (\hat{\rho}(\lambda))^n &= \lim_{n\to\infty} \left[I - \frac{1}{n} \sum_{i=1}^{d} d_i u(E_i, \lambda) + \frac{1}{2n} \sum_{i=1}^{d} \sum_{i=1}^{d} D_{ij}\, u(E_i, \lambda) u(E_j, \lambda)\right]^n \\ &= \exp\left[-\sum_{i=1}^{d} d_i u(E_i, \lambda) + \frac{1}{2} \sum_{i=1}^{d} \sum_{i=1}^{d} D_{ij}\, u(E_i, \lambda) u(E_j, \lambda)\right] \\ &= \hat{f}(\lambda; t, D, \mathbf{d}).\end{aligned}$$

Application of the inverse Fourier transform completes the proof.

While, in principle, information-theoretic proofs of this result could follow in a similar way as the Abelian case, the author is not aware of any such proofs. One difficulty not encountered in the case of Lie groups that is not encountered in Euclidean space is that the definition of covariance breaks down for distributions that are very spread out. This means that the "maximum-entropy distribution" on a Lie group cannot be defined by simply maximizing the entropy subject to a constraint on covariance, since the covariance concept itself becomes questionable. This issue with the information-theoretic formulation disappears if the problem of convergence to the stable distribution is considered.

20.9 Limiting Distributions of Evolution Equations on Groups

The sorts of evolution equations examined in this book include degenerate and nondegenerate diffusions (with and without drifts) as well as processes that converge to a nontrivial limiting distribution (e.g., Ornstein–Uhlenbeck processes). In all of these cases, two natural questions arise: (1) What does the solution $f(g,t)$ look like as $t \to \infty$? (2) Given some initial distribution, how fast does the solution converge to this limiting distribution?

These questions are addressed naturally using methods of noncommutative harmonic analysis, because linear diffusion equations on noncommutative groups are solved in Fourier space in a transparent way. This is analogous to the way that Fourier analysis is used to arrive at the central limit theorem in $\mathbb{R}^n$.

Let G be a unimodular Lie group and let the diffusion operator be $\Delta(\lambda)$. Observing the behavior of the solution as time increases, it is easy to see from the Plancherel equality that

$$\frac{d}{dt}\int_G |f(g,t)|^2\,dg \leq 0 \quad\Longrightarrow\quad \frac{d}{dt}\int_{\hat{G}} \|\hat{f}(\lambda,t)\|^2 d\lambda \leq 0 \quad\Longrightarrow\quad \frac{d}{dt}\|\hat{f}(\lambda,t)\|^2 \leq 0.$$

Moreover, it follows from the definition of $\hat{f}(\lambda,t)$ and the fact that $f(g,t)$ is a pdf for each fixed value of t that the entries of $\hat{f}(\lambda,t)$ must be bounded for all values of t, since $U(g,\lambda)$ is unitary and hence the modulus of each of its entries is bounded from above by unity. This means that when writing

$$\hat{f}(\lambda,t) = e^{t\hat{\Delta}^*(\lambda)},$$

all of the eigenvalues of $\hat{\Delta}(\lambda)$ must have nonpositive real parts. Otherwise, some matrix element of $\hat{f}(\lambda,t)$ would grow without bound as $t \to \infty$, which would be a contradiction.

In the case of compact Lie groups, all Fourier matrices of nondegenerate diffusions without drift will have negative eigenvalues, except for the "lowest-frequency" (scalar) one, corresponding to the scalar IUR that is nothing more than unity. The speed with which the limiting distribution is approached depends on the eigenvalue of the Fourier diffusion matrix (other than the zero eigenvalue) that has smallest absolute value.

The noncompact case behaves somewhat differently. As with the classical central limit theorem, the limiting distributions for diffusion processes on noncompact Lie groups (commutative or noncommutative) will not be a single static function analogous to a uniform distribution. Rather, the limiting distribution itself will retain dependence on time. Thus, if T denotes an adequate amount of time for an initial distribution to decay to within some small deviation from this form, it makes sense to determine how T

depends on the structure of the group. Such problems are studied in the references provided at the end of this chapter.

20.10 Chapter Summary

This chapter has presented properties of diffusion processes that are described as SDEs or probability flows on Lie groups. The principles described here build on concrete applications from previous chapters in which such equations arise. In particular, the McKean–Gangolli injection process and corresponding Fokker–Planck equations were discussed, and concepts of mean and covariance were reviewed, the central limit theorem for diffusions on Lie groups was explained. Of course, the brief treatment presented here is necessarily incomplete and should be augmented by further reading, as described below.

The McKean–Gangolli injection process is described in [24, 48], and studies of its properties and generalizations can be found in [29, 39].

For further reading on the topic of diffusions on Lie groups and manifolds, see [1, 5, 8, 16–18, 20, 21, 28, 35–37, 42, 47]. For approaches involving martingales, see [3, 32, 34, 41].

A large subarea of study relating to diffusion processes and Lie groups has been hypoelliptic diffusion equations for which the diffusion matrix is singular [33, 57]. Indeed, this is relevant to the diffusion processes describing DNA in Chapter 14 and laser phase noise in Chapter 17, as well as those described in [52], many of which are degenerate.

Although the emphasis here has been stochastic processes forced by Wiener process noise, the topic of Lévy processes (i.e., Wiener process noise punctuated by occasional random jumps) has been the subject of a growing body of recent work [2, 45].

Random walks on groups and manifolds are studied in [23, 56]. Connections between diffusion processes on Lie groups and control theory are explored in [10, 15]. Applications of covariance propagation in robotics are explored in [61, 67].

Works focusing on the rotation group [26, 43, 44, 50, 53, 70] and Euclidean motion group [27, 63] are also relevant to applications. For physical phenomena involving diffusions on Lie groups, see [11, 13, 19, 40].

The behavior of Brownian motion can be related to the local and global geometric and topological properties of the manifolds/Lie groups on which the trajectories evolve, leading to results beyond the scope of this book that can be found in [4, 7, 25, 49, 55, 62]. Roughly speaking, short-time behavior provides some information about local curvature, and long-time behavior says something about topological structure. For more on limiting behavior as time (or the number of convolutions) becomes large, see [6, 46, 58, 59, 65, 69].

Other important works involving probabilities on Lie groups include [12, 14, 22, 30, 31, 38, 51, 54, 60, 64, 66, 68].

Some of the concepts discussed in this chapter will be used in the next chapter when formulating noise models that arise in locomotion (such as robots and microorganisms), and perception/sensing.

20.11 Exercises

20.1. Defining $y_{kl} = g_{kl}(X) = \sum_{j,k} x_{ik} q_{ij} x_{jl}$, where $Q = [q_{ij}]$, use Itô 's rule (see Vol. 1) with g_{kl} in place of g_k and the entries in the matrix $X = [x_{ij}]$ as the variables in place of the vector components to verify (20.19) by setting $dy_{kl} = 0$.

20.2. Address the above question where in place of class functions, one considers symmetric functions (i.e., $f_i(g) = f_i(g^{-1})$). What happens if $(f_1 * f_2)(g)$ and $(f_2 * f_1)(g)$ are also symmetric?

20.3. Can Cauchy–Schwartz equality for $L^2(G)$ and/or $L^2(\hat{G})$ be used to bound the temporal behavior of $\|f\|_2^2$ defined in (20.56)?

20.4. Show that, in analogy with (20.59), if

$$(E_i^l f)(g) = \frac{d}{dt} f(\exp(-tE_i) \circ g)\bigg|_{t=0} \quad \text{and} \quad (R(g_0)f)(g) = f(g \circ g_0),$$

then

$$(R(g_0)E_i^l f)(g) = (E_i^l R(g_0)f)(g). \tag{20.65}$$

20.5. Show that left shifts, right shifts, and the adjoint transformation of a function have the properties

$$(L(g_1 \circ g_2)f)(g) = (L(g_1)L(g_2)f)(g) \quad \text{and} \quad (R(g_1 \circ g_2)f)(g) = (R(g_1)R(g_2)f)(g), \tag{20.66}$$

$$(Ad(g_1 \circ g_2)f)(g) = (Ad(g_1)Ad(g_2)f)(g) \quad \text{and} \quad (R(g_1)L(g_2)f)(g) = (L(g_2)R(g_1)f)(g). \tag{20.67}$$

20.6. Using the expansion in (20.62), verify that (20.60) holds.

20.7. Let $f(g,t)$ be a solution to the (forward) evolution equation

$$\frac{\partial f}{\partial t} = \Delta^* f, \qquad \text{where} \qquad f(g,0) = \delta(g).$$

Using the Fourier form of the solution $f(g,t)$, show that $f(g^{-1},t)$ satisfies the backward equation (i.e., the evolution equation with Δ^* replaced by Δ).

20.8. If Δ is self-adjoint, show that $f(g,t) = f(g^{-1},t)$. What limitations does being self-adjoint place on the parameters $\{D, \mathbf{d}\}$ that define Δ for a unimodular Lie group?

20.9. Determine the symmetry operations for the heat equation on $SO(3)$.

References

1. Albeverio, S., Arede, T., Haba, Z., "On left invariant Brownian motions and heat kernels on nilpotent Lie groups," *J. Math. Phys.*, 31(2), pp. 278–286, 1990.
2. Applebaum, D., Kunita, H., "Lévy flows on manifolds and Lévy processes on Lie groups," *J. Math. Kyoto. Univ.*, 33/34, pp. 1103–1123, 1993.
3. Arnaudon, M., "Connexions et martingales dans les groupes de Lie," *Sémin. Probab. XXVI.* LMN 1526, pp. 146–155, Springer, 1992.
4. Atiyah, M., Bott, R., Patodi, V.K., "On the heat equation and the Index theorem," *Invent. Math.*, 19, pp. 279–330, 1973.
5. Azencott, R., "Behavior of diffusion semi-groups at infinity," *Bull. Soc. Math. France*, 102, pp. 193–240, 1974.
6. Bellman, R., "Limit theorems for noncommutative operations, I," *Duke Math. J.*, 21, 1954.

7. Berline, N., Getzler, E., Vergne, M., *Heat Kernels and Dirac Operators*, Springer-Verlag, Berlin, 1992.
8. Bochner, S., "Diffusion equations and stochastic processes," *PNAS*, 35, pp. 369–370, 1949.
9. Brockett, R.W., "Lie algebras and Lie groups in control theory," in *Geometric Methods in System Theory*, D.Q. Mayne and R.W. Brockett, eds., Reidel Publishing Company, Dordrecht, 1973.
10. Brockett, R.W., "Notes on stochastic processes on manifolds," in *Systems and Control in the Twenty-First Century*, C.I. Byrnes et al. eds., Birkhäuser, Boston, 1997.
11. Coffey, W.T., Kalmykov, Yu. P., Waldron, J.T., *The Langevin Equation*, World Scientific, Singapore, 2004.
12. Dani, S.G., Graczyk, P., eds., *Probability Measures on Groups: Recent Directions and Trends*, Narosa Publishing House, New Delhi, 2006.
13. Dankel, T.G., Jr., "Mechanics on manifolds and the incorporation of spin into Nelson's stochastic mechanics," *Arch. Rat. Mech. Anal.*, 31(3), pp. 192–222, 1970.
14. Diaconis, P., *Group Representations in Probability and Statistics*, Institute of Mathamatical Statistics, Hayward, CA, 1988.
15. Duncan, T.E., "Stochastic systems in Riemannian manifolds," *J. Optim. Theory Applic.*, 27, pp. 175–191, 1976.
16. Elworthy, K.D., *Stochastic Differential Equations on Manifolds*, Cambridge University Press, Cambridge, 1982.
17. Emery, M., *Stochastic Calculus in Manifolds*, Springer-Verlag, Berlin, 1989.
18. Epperson, J.B., Lohrenz, T., "Brownian motion and the heat semigroup on the path space of a compact Lie group," *Pacific J. Math.*, 161(2), pp. 233–253, 1993.
19. Ermakov, S.M., Nekrutkin, V.V., Sipin, A.S., *Random processes for classical equations of mathematical physics*, Kluwer Academic, Dordeclet, 1989.
20. Fegan, H.D., "The heat equation on a compact Lie group," *Trans. Am. Math. Soc.*, 246, pp. 339–357, 1978.
21. Fegan, H.D., "The fundamental solution of the heat equation on a compact Lie group," *J. Diff. Geom.*, 18, pp. 659–668, 1983.
22. Furman, A., "Random walks on groups and random transformations," in *Handbook of Dynamical Systems, Vol. 1A*, B. Hasselblatt and A. Katok, eds., pp. 931–1014, Elsevier, Amsterdam, 2002.
23. Furstenberg, H., "Random walks and discrete subgroups of Lie groups," in *Advances in Probability and Related Topics, Vol.* 1, P. Ney, ed., Marcel Dekker, New York, 1971.
24. Gangolli, R., "On the construction of certain diffusions on a differentiable manifold," *Z. Wahrscheinlichkeitstheorie Geb.*, 2, pp. 406–419, 1964.
25. Gilkey, P.B., *Invariance Theory, the Heat Equation, and the Atiyah-Singer Index Theorem*, CRC Press, Boca Raton, FL, 1995.
26. Gorman, C.D., "Brownian motion of rotation," *Trans. Am. Math. Soc.*, 94, pp. 103–117, 1960.
27. Gorostiza, L.G., "The Central Limit Theorem for random motions of d-dimensional Euclidean space," *Ann. Probab.*, 1(4), pp. 603–612, 1973.
28. Grenander, U., *Probabilities on Algebraic Structures*, John Wiley and Sons, New York, 1963 (reprinted by Dover, Mineola, NY, 2008)
29. Hakim-Dowek, M., Lépingle, D., "L'exponentielle stochastique des groupes de Lie," in *Séminaire de Probabilités XX* Lecture Notes in Mathematics, 1204, pp. 352–374, eds. J. Azéma, M. Yor, Springer 1986.
30. Heyer, H., "Moments of probability measures on a group," *Int. J. Math. Math. Sci.*, 4(1), pp. 1–37, 1981.
31. Heyer, H., *Probability Measures on Locally Compact Groups*, Springer-Verlag, New York, 1977.
32. Hida, T., "Brownian Motion," *Applic. Math.* # 11, Springer 1980.
33. Hörmander, L., "Hypoelliptic second order differential equations," *Acta Math.*, 119, pp. 147–171, 1967.

34. Ikeda, N., Watanabe, S., *Stochastic Differential Equations and Diffusion Processes*, 2nd ed., North-Holland, Amsterdam, 1989.
35. Itô, K., “Brownian motions in a Lie group,” *Proc. Japan Acad.*, 26, pp. 4–10, 1950.
36. Itô, K., “Stochastic differential equations in a differentiable manifold,” *Nagoya Math. J.* 1, pp. 35–47, 1950.
37. Itô, K., “Stochastic differential equations in a differentiable manifold (2),” *Sci. Univ. Kyoto Math. Series A*, 28(1), pp. 81–85, 1953.
38. Itô, K., McKean, H.P., Jr., *Diffusion Processes and their Sample Paths*, Springer, New York, 1996.
39. Jorgensen, E., “Construction of the Brownian motion and the Ornstein-Uhlenbeck process in a Riemannian manifold on the basis of the Gangolli-McKean injection scheme,” *Z. Wahrscheinlichkeitstheorie Geb.*, 44, pp. 71–87, 1978.
40. Kree, P., Soize, Ch., *Mécanique aléatoire*, Dunod, Paris, 1983.
41. Kunita, H., *Stochastic Flows and Stochastic Differential Equations*, Cambridge University Press, Cambridge, 1997.
42. Lewis, J., “Brownian motion on a submanifold of Euclidean space,” *Bull. London Math. Soc.*, 18(6), pp. 616–620, 1986.
43. Liao, M., ”Random motion of a rigid body,” *J. Theoret. Probab.*, 10(1), pp. 201–211, 1997.
44. Liao, M., Wang, L., “Motion of a rigid body under random perturbation,” *Electron. Commun. Probab.*, 10, pp. 25–243, 2005.
45. Liao, M., *Lévy Processes in Lie Groups*, Cambridge University Press, Cambridge, 2004.
46. Major, P., Shlosman, S.B., “A local limit theorem for the convolution of probability measures on a compact connected group,” *Zeitschr. Wahrscheinlichkeitstheorie Gebiete*, 50, pp. 137–148, 1979.
47. Malliavin, P., Stroock, D., “Short time behavior of the heat kernel and its logarithmic derivatives,” *J. Diff. Geom.*, 44, pp. 550–570, 1996.
48. McKean, H.P., Jr., *Stochastic Integrals*, Academic Press, New York, 1969 (reprinted in 2005).
49. McKean, H., Jr., Singer, I.M., “Curvature and the eigenvalues of the Laplacian,” *J. Diff. Geom.*, 1, pp. 43–69, 1967.
50. McKean, H.P., Jr., “Brownian motions on the 3-dimensional rotation group,” *Mem. College Sci., Univ. Kyoto Series A*, 33(1), pp. 25–38, 1960.
51. Pap, G., “Construction of processes with stationary independent increments in Lie groups,” *Arch. Math.*, 69, pp. 146–155, 1997.
52. Park, W., Liu, Y., Moses, M., Zhou, Y., Chirikjian, G.S., “Kinematic state estimation and motion planning for stochastic nonholonomic systems using the exponential map” *Robotica*, 26(4), pp. 419–434, 2008.
53. Parthasarathy, K.R., “The Central Limit Theorem for the rotation group,” *Probab. Theory Applic.*, 9(2), pp. 248–257, 1964.
54. Pinsky, M., “Isotropic transport process on a Riemannian manifold,” *TAMS*, 218, pp. 353–360, 1976.
55. Pinsky, M., *Brownian motion and Riemannian geometry*, Probability Theory (Chen, L., Choi, K.P., Hu, K., Lou, J.-H., eds.), de Gruyter, 1991.
56. Roberts, P.H., Ursell, H.D., ”Random walk on a sphere and on a Riemannian manifold,” *Philos. Trans. R. Soc. London*, A252, pp. 317–356, 1960.
57. Robinson, D.W., *Elliptic operators and Lie groups*, Clarendon Press, Oxford, 1991.
58. Shlosman, S.B., “Limit theorems of probability theory on compact topological groups,” *Theory Probab. Applic.*, 25, pp. 604–609, 1980.
59. Shlosman, S.B., “The influence of noncommutativity on limit theorems,” *Zeitschr. Wahrscheinlichkeitstheorie Geb.,* 65, pp. 627–636, 1984.
60. Stromberg, K., “Probabilities on a compact group,” *Trans. Am. Math. Soc*, 94, pp. 295–309, 1960.
61. Su, S., Lee, C.S.G., “Manipulation and propagation of uncertainty and verification of applicability of actions in assembly tasks,” *IEEE Trans. Syst. Man Cybernet.*, 22(6), pp. 1376–1389, 1992.

62. Taira, K., *Brownian Motion and the Index Formulas for the de Rham Complex*, Wiley-VCH, Berlin, 1998.
63. Tutubalin, V.N., "The Central Limit Theorem for random motions of a Euclidean space," *Selected Transl. Math.: Statist. Probab.*, 12, pp. 47–57, 1973.
64. Varopoulos, N.Th., Saloff-Coste, L., Coulhon, T., *Analysis and Geometry on Groups*, Cambridge University Press, Cambridge, 1992.
65. Virtzer, A.D., "Central limit theorem for semi-simple Lie groups," *Theor. Probab. Appl.*, 15, pp. 667–687, 1970.
66. Voiculescu, D., "Entropy of random-walks on groups and the Macaev norm," *Proc.* AMS, 119(3), pp. 971–977, 1993.
67. Wang, Y., Chirikjian, G.S., "Error propagation on the Euclidean group with applications to manipulator kinematics," *IEEE Trans. Robot.*, 22(4), pp. 591–602, 2006.
68. Wehn, D.F., "Probabilities on Lie groups," *PNAS*, 48, pp. 791–795, 1962.
69. Wehn, D.F., "Limit distributions on Lie groups," PhD Dissertation, Dept. of Mathematics, Yale University, 1962.
70. Yosida, K., "Brownian motion on the surface of the 3-sphere," *Ann. Math. Statist.*, 20, pp. 292–296, 1949.

21

Locomotion and Perception as Communication over Principal Fiber Bundles

This chapter can be viewed as a demonstration of applications of the Lie-theoretic methods presented in Chapters 10–12, the inequalities in Chapter 19, and the stochastic processes on Lie groups in Chapter 20. As in Chapter 1, the simple system used to illustrate these concepts is the nonholonomic kinematic cart. When any trajectory of the cart is discretized into smaller segments which are drawn from a set of intended maneuvers, then this set serves as an alphabet of basic moves. As the cart moves and noise is added to these intended moves, it will not move exactly as planned. This corruption of the resulting output position and orientation can be viewed as an injection of noise through the combined space of pose and wheel angles. This space is an example of the differential geometric structure called a *principal fiber bundle*.[1] An external observer (which might be a human or another robot) watching the motion of the robot can then attempt to infer the robot's intent and functionality. The combination of stochastic models, information theory, and Lie groups is helpful in studying such scenarios. Therefore, this chapter has several goals:

- To provide a detailed treatment of the geometry of fiber bundles that augments the discussion in Chapter 7;
- To explain how a natural rate-distortion theory extends from the classical information-theory context to more geometric settings;
- To discuss problems in locomotion and perception that require multiple concepts and methodologies developed in earlier chapters and are brought together in the context of fiber bundle structures.

This chapter is organized as follows. Section 21.1 revisits the kinematic cart that was introduced in Chapter 1 from the perspective of the methods developed in the chapters of Volume 2. In addition, this is a simple system that evolves on a (principal) fiber bundle and therefore serves as an important example in illustrating the definitions that will follow. Section 21.2 provides detailed definitions and examples of principal fiber bundles. Section 21.3 generalizes the classical theory of the communication channel with Gaussian noise (called the "Gaussian channel") to the geometric context in which the "message" is generated and received in a copy of the base space of the bundle and the channel is the fiber space. Scenarios in which this formulation may be useful are demonstrated in Section 21.4 in the context of robotics problems. Section 21.5 then provides a pointer to the literature on mathematical vision, perception, and psychology

[1] This has nothing to do with fiber optic communications or the transmission of intercontinental information via undersea cables. In that sense, the title of this chapter is a bit of a pun.

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_12,

in which fiber bundle structures and corresponding stochastic differential equations have been studied.

21.1 The Kinematic Cart (Revisited)

Consider the kinematic cart in Figure 21.1 that was initially introduced in Chapter 1. Recall that the two wheels each have radii r and let the wheelbase be denoted as L; the nonholonomic equations of motion are

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{\theta} \end{pmatrix} = \begin{pmatrix} \frac{r}{2}\cos\theta & \frac{r}{2}\cos\theta \\ \frac{r}{2}\sin\theta & \frac{r}{2}\sin\theta \\ \frac{r}{L} & -\frac{r}{L} \end{pmatrix} \begin{pmatrix} \dot{\phi}_1 \\ \dot{\phi}_2 \end{pmatrix}. \tag{21.1}$$

This can be written in coordinate-free notation as

$$\left(g^{-1}\frac{dg}{dt}\right)^{\vee} = A\,\dot{\boldsymbol{\phi}}, \qquad \text{where} \qquad A = \frac{r}{2}\begin{pmatrix} 1 & 1 \\ 0 & 0 \\ 2/L & -2/L \end{pmatrix}, \tag{21.2}$$

where $g = g(x, y, \theta) \in SE(2)$ is of the same form as in (10.75).

In the case of a single stochastic trajectory for $g(t)$ that evolves when the robot intends to go straight but is influenced by wheel slippage and other noise, a SDEs of the form in Chapter 1 and [80] results from the substitution of

$$d\phi_1 = \omega\,dt + \sqrt{D}\,dw_1 \qquad \text{and} \qquad d\phi_2 = \omega\,dt + \sqrt{D}\,dw_2 \tag{21.3}$$

into either of the above equations after multiplication on both sides by dt, where dw_i each represent uncorrelated unit-strength white noise and D scales the strength of the noise. Here the constant rate of rotation of both wheels would be ω if there were no

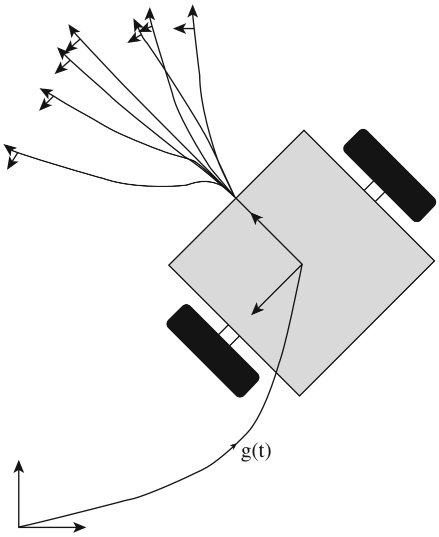


Fig. 21.1. A Kinematic Cart with an Uncertain Future Position and Orientation

noise, in which case the robot would move straight forward and $g_{odo} = g(\omega T, 0, 0)$, which is what would result from integrating odometry measurements.

Usually to be precise it is important to specify whether an SDE is of Itô or Stratonovich type. In this example, both interpretations yield the same equation and this distinction is unimportant because the matrix on the right-hand side in (21.2) is constant. However, for the sake of definiteness, consider the combination of (21.2) and (21.3) to be an Itô equation.

If such an equation is simulated many times, each time starting from the same initial conditions (say, $x = y = \theta = 0$), then a function $f(x, y, \theta; t)$ that records the distribution of positions and orientations of the cart at the same value of time, t, in each trajectory can be defined. (This pdf also depends on r, L, ω, and D, but the dependence on these constants is suppressed.)

As explained in detail in [80] and in Volume 1, a well-developed theory for linking SDEs such as (21.1) to functions such as $f(x, y, \theta; t)$ exists. This theory produces a *Fokker–Planck equation* for $f(x, y, \theta; t)$. In the present context, this equation is of the form [80]

$$\begin{aligned}\frac{\partial f}{\partial t} &= -r\omega\cos\theta\frac{\partial f}{\partial x} - r\omega\sin\theta\frac{\partial f}{\partial y}\\ &\quad + \frac{D}{2}\left(\frac{r^2}{2}\cos^2\theta\frac{\partial^2 f}{\partial x^2} + \frac{r^2}{2}\sin 2\theta\frac{\partial^2 f}{\partial x\partial y} + \frac{r^2}{2}\sin^2\theta\frac{\partial^2 f}{\partial y^2} + \frac{2r^2}{L^2}\frac{\partial^2 f}{\partial\theta^2}\right),\end{aligned}$$

which is subject to the initial conditions $f(x, y, \theta; 0) = \delta(x - 0)\delta(y - 0)\delta(\theta - 0)$. The coordinate-free version of the above Fokker–Planck equation can be written compactly in terms of these Lie derivatives as [80]

$$\frac{\partial f}{\partial t} = -r\omega\tilde{E}_1^r f + \frac{r^2 D}{4}(\tilde{E}_1^r)^2 f + \frac{r^2 D}{L^2}(\tilde{E}_3^r)^2 f \tag{21.4}$$

with initial conditions $f(g; 0) = \delta(g)$. The resulting time-evolving pdf is denoted as $f(g; t)$, or with the shorthand $f_t(g)$. Additionally, the operational poperties of the $SE(2)$ Fourier transform discussed in Chapter 12 can be used to solve this equation, as was done in [58].

Although efficient techniques for solving this sort of equation exist for both the long-time and short-time cases (see, e.g., [80] and references therein), the emphasis here is not solution techniques but rather to serve as a test case for the various definitions and concepts that follow.

It is interesting to note that models similar to this have been used to characterize the motion of biological organisms [59, 60], and the steering of flexible needles in three dimensions [76]. As we will see later in this chapter, the configuration space of this cart has the geometric structure of a fiber bundle (in particular, a trivial principal fiber bundle), and ensembles of stochastic trajectories evolving on this space have Fokker–Planck equations that have a more specialized structure than typical diffusion processes on generic Riemannian manifolds. However, first, in the next section fiber bundles are described in more detail than in Chapter 7, where they were mentioned in passing.

21.2 Principal Fiber Bundles and Lie Groups

The concept of a fiber bundle was discussed qualitatively in Chapter 7. A particular kind of fiber bundle, called a *principal fiber bundle*, is reviewed here since it has strong ties to the theory of Lie groups. The presentation here follows those in [35, 36, 64].

21.2.1 General Facts About Fiber Bundles

First, recall that, in general, a fiber bundle consists of the objects (E, B, π, F), where E, B, and F are spaces (called the entire space, base space, and fiber space, respectively) and π is a surjective mapping, $\pi : E \to B$.

In the present context, let E, B, and F denote manifolds with dimensions that satisfy the constraint

$$\dim E = \dim B + \dim F.$$

Let $\{U_\alpha\}_{\alpha \in I}$ be an open cover of B, where I is an index set. Let $\varphi_\alpha : U_\alpha \times F \to E$ be injective. Then $\{\varphi_\alpha(U_\alpha \times F)\}_{\alpha \in I}$ is an open cover of E. For each $\alpha \in I$, let $\phi_\alpha : \varphi_\alpha(U_\alpha \times F) \to \mathbb{R}^{\dim E}$ so that $(\varphi_\alpha(U_\alpha \times F), \phi_\alpha)$ is a coordinate chart, and $\{(\varphi_\alpha(U_\alpha \times F), \phi_\alpha)\}_{\alpha \in I}$ is the corresponding atlas for E. Although $\varphi_\alpha : U_\alpha \times F \to E$ is usually only injective, $\varphi_\alpha : U_\alpha \times F \to \varphi_\alpha(U_\alpha \times F)$ is obviously bijective.

The standard constraint that defines a fiber bundle is that the diagram

$$\begin{tikzcd}
U_\alpha \times F \arrow[r, "\varphi_\alpha"] \arrow[dr, "\text{proj}"'] & \pi^{-1}(U_\alpha) \arrow[d, "\pi"] \\
 & U_\alpha
\end{tikzcd} \tag{21.5}$$

commutes, where for any $(x, y) \in U_\alpha \times F$, the projection operation "proj" is defined by $\text{proj}(x, y) \doteq x$. For any $x \in U_\alpha \subset B$, the "fiber over x" is the preimage of the projection π; that is, $\pi^{-1}(x)$ is an individual fiber in the space of all such fibers, F. The above diagram is equivalent to the equation

$$\pi(\varphi_\alpha(x, y)) = x, \quad \forall\, (x, y) \in U_\alpha \times F \text{ and } \alpha \in I. \tag{21.6}$$

A convenient property to enforce is that each φ_α is a homeomorphism, so

$$U_\alpha \times F \cong \pi^{-1}(U_\alpha).$$

A map $s : B \longrightarrow E$ is called a *cross section* if for each $x \in U_\alpha \subset B$,

$$s(x) \in \varphi_\alpha(U_\alpha \times F) = \pi^{-1}(U_\alpha) \quad \text{and} \quad \pi(s(x)) = x. \tag{21.7}$$

Now, suppose that there are two open sets $U_\alpha, U_\beta \subset B$ such that $U_\alpha \cap U_\beta \neq \emptyset$. Then inverse maps φ_α^{-1} and φ_β^{-1} exist, each of which can be used to map $\pi^{-1}(U_\alpha \cap U_\beta)$ into $(U_\alpha \cap U_\beta) \times F$. Therefore, the composition of maps $\varphi_{\alpha\beta} \doteq \varphi_\alpha^{-1} \circ \varphi_\beta$ is a map from $(U_\alpha \cap U_\beta) \times F$ into itself (and likewise for $\varphi_{\beta\alpha}$).

As with charts on any manifold, certain compatibility conditions must hold. These are described by having the diagram

$$\begin{tikzcd}
(U_\alpha \cap U_\beta) \times F \arrow[r, "\varphi_\alpha"] \arrow[dr, "\text{proj}"'] & \pi^{-1}(U_\alpha \cap U_\beta) \arrow[d, "\pi"] & (U_\alpha \cap U_\beta) \times F \arrow[l, "\varphi_\beta"'] \arrow[dl, "\text{proj}"] \\
 & U_\alpha \cap U_\beta &
\end{tikzcd} \tag{21.8}$$

commute. Each loop of this diagram produces an equation, and altogether there are four equations:

$$\pi(\varphi_\alpha(x,y)) = \pi(\varphi_\beta(x,y)) = \mathrm{proj}((\varphi_\beta^{-1}\circ\varphi_\alpha)(x,y)) = \mathrm{proj}((\varphi_\alpha^{-1}\circ\varphi_\beta)(x,y)) = x. \tag{21.9}$$

Given three overlapping open sets, $U_\alpha, U_\beta, U_\gamma \subset B$, and $U_\alpha \cap U_\beta \cap U_\gamma \neq \emptyset$, then the following diagram commutes:

$$\begin{tikzcd}
(U_\alpha \cap U_\beta \cap U_\gamma) \times F \arrow[r, "\varphi_\alpha"] \arrow[rr, bend left, "\varphi_{\beta\alpha} \doteq \varphi_\beta^{-1} \circ \varphi_\alpha"] \arrow[dr, "\varphi_{\gamma\alpha} \doteq \varphi_\gamma^{-1} \circ \varphi_\alpha"'] & \pi^{-1}(U_\alpha \cap U_\beta \cap U_\gamma) & (U_\alpha \cap U_\beta \cap U_\gamma) \times F \arrow[l, "\varphi_\beta"'] \arrow[dl, "\varphi_{\gamma\beta} \doteq \varphi_\gamma^{-1} \circ \varphi_\beta"] \\
 & (U_\alpha \cap U_\beta \cap U_\gamma) \times F \arrow[u, "\varphi_\gamma"'] &
\end{tikzcd} \tag{21.10}$$

Reading off equations from the loops gives

$$\varphi_{\gamma\beta} \circ \varphi_{\beta\alpha} = (\varphi_\gamma^{-1} \circ \varphi_\beta) \circ (\varphi_\beta^{-1} \circ \varphi_\alpha) = \varphi_\gamma^{-1} \circ \varphi_\alpha = \varphi_{\gamma\alpha}.$$

Hence, $(\varphi_{\alpha\beta})^{-1} = \varphi_{\beta\alpha}$, and $\varphi_{\alpha\alpha}$ is the identity map.[2]

It is possible to define mappings from one bundle into another, $(E', B', \pi', F') \rightarrow (E, B, \pi, F)$, by introducing two maps, $m_1 : E' \rightarrow E$ and $m_2 : B' \rightarrow B$ such that the diagram

$$\begin{tikzcd}
E' \arrow[r, "m_1"] \arrow[d, "\pi'"'] & E \arrow[d, "\pi"] \\
B' \arrow[r, "m_2"'] & B
\end{tikzcd} \tag{21.11}$$

commutes. This works when a homeomorphism exists between each fiber $(\pi')^{-1}(x') \in F'$ and $\pi^{-1}(m_2(x')) \in F$ for every $x' \in B'$. If $B = B'$ so that there is no need for m_2, then (E', B, π', F') and (E, B, π, F) are called *equivalent* if m_1 is a homeomorphism and the diagram

$$\begin{tikzcd}
E' \arrow[r, "m_1"] \arrow[dr, "\pi'"'] & E \arrow[d, "\pi"] \\
 & B
\end{tikzcd} \tag{21.12}$$

commutes.

[2] The set of all such mappings together with the composition operation $\circ$ forms a group called the structure group. In some books, the definition of principal fiber bundles includes this group as one of the constituent parts, along with (E, B, π, F).

21.2.2 Relationships to Lie Groups

Lie groups and fiber bundles interact at several levels. For example, in applications, an open cover does not simply present itself; it must be constructed. If $U \subset B$ is a suitable open set (such as an open ball defined relative to some metric), then one way to construct an open cover of B is by the action of a group. In particular, if G is a Lie group that acts transitively on B, then B can be covered by translated copies of U; that is, $g \cdot U$ or $U \cdot g$ can take the place of U_α in the previous section. The index set is then some subset $I \subset G$, which is typically discrete.

Even deeper connections between Lie groups and fiber bundles result when E, F, B, or any combination thereof are Lie groups as described in the following definition.

Definition 21.1: A *(right) principal fiber bundle* or *principal bundle* for short[3] is a special kind of fiber bundle where the following three conditions hold:

1. The manifold F is homeomorphic to a Lie group G (i.e., $F \cong G$), but in general F does not have a group operation, identity element, or any of the algebraic properties of $(G, \circ)$. For principal bundles, P is used to denote the entire space (instead of E). G acts freely on P from the right so that $p \cdot g \in P$ for all $g \in G$ and $p \in P$, and $p \cdot g = p \Longrightarrow g = e$.
2. $B = P/G$, the set of equivalence classes generated by the action described above. A projection map can be defined using this action, and so, $\pi : P \to P/G$.
3. Every point $x \in P/G$ has a neighborhood U_x such that $x \in U_x \subset P/G$ and $\pi^{-1}(U_x)$ is isomorphic with $U_x \times G$; that is, for every $v \in \pi^{-1}(U_x)$, there is a diffeomorphism $\psi : \pi^{-1}(U_x) \to U_x \times G$, where $\vartheta : \pi^{-1}(U_x) \to G$ such that for a given right action $\bullet$ of G on itself,

$$\psi(v) = (\pi(v), \vartheta(v)) \qquad \text{and} \qquad \vartheta(v \cdot g) = \vartheta(v) \bullet g.$$

The resulting $(P, P/G, \pi, G)$ (with ϑ and the two actions $\cdot$ and $\bullet$ implicit) is a principal fiber bundle, and it can be shown that G is isomorphic with the structure group. In the special case when $P \cong P/G \times G$ and the action of G on P has the property $(x, a) \cdot g = (x, a \bullet g)$ for all $g \in G$ and $(x, a) \in P$ then is called a *trivial principal fiber bundle* [55].

Two common examples of principal fiber bundles are discussed below, following [35, 36].

Example 21.2.1: If H is a proper Lie subgroup of a Lie group G, then a natural projection map $p : G \longrightarrow G/H$ is defined by $p(g) \doteq gH$, resulting in a bundle $(E, B, \pi, F) = (G, G/H, p, H)$. In general, mappings from $G/H \times H$ onto G are not one-to-one (a fact that is important in the proof of Weyl's integration formula in Chapter 12). Therefore, there cannot be a diffeomorphism $G/H \times H \longleftrightarrow G$, and so there will not be smooth cross sections for bundles of this type.

Example 21.2.2: Since a Lie group, G, has a manifold structure, associated with each element $g \in G$ is a tangent space T_gG. A vector in this tangent space is $\mathcal{X}_g \in T_gG$.

[3] In the classical mathematics literature these are the principal fiber bundles that are primarily studied, and therefore the prefix "right" does not appear. In contrast, in modern applications in geometric mechanics the action of G on P is often from the left, resulting in a switching of the order of the terms. Hence it is sometimes useful to distinguish between right and left principal bundles. When G is specified and the left/right aspect is clear, the terminology "principal G-bundle" is often used.

The collection of all such tangent spaces is called the *tangent bundle* and is denoted as TG. A vector field is an element of this tangent bundle, $\mathcal{X} \in TG$, which can be identified with the set of all possible vector fields on G. The set of all *smooth* vector fields can then be viewed as the subset $\mathfrak{X}(G) \subset TG$. A projection map associated with the tangent bundle is $\pi' : TG \longrightarrow G$ defined as $\pi'(\mathcal{X}_g) = g$. Therefore, in this case, $(E, B, \pi, F) = (TG, G, \pi', T_gG \cong \mathcal{G})$, where $\mathcal{G}$ is the Lie algebra associated with G and $(\mathcal{G}, +)$ is a commutative Lie group (not to be confused with $(G, \circ)$).

The configuration space of the kinematic cart is an example of a trivial principal fiber bundle, in that $E = \mathbb{T}^2 \times SE(2)$, $B = \mathbb{T}^2$, and $F = SE(2)$. This example will be important in the next section to illustrate how an important result from information theory (i.e., rate-distortion theory for Gaussian channels) generalizes to the geometric setting.

More widely, there has been interest in using differential-geometric and Lie-theoretic methods to study locomotion, controls, and computer vision [3, 5, 8, 12, 13, 20, 37, 40, 41, 45–47, 52, 61, 67, 79], including the author's own work [43, 57]. Stochastic processes on fiber bundles offers a unifying theme to many problems in action and perception in the physical world.

21.3 Gaussian Channels and Principal Bundles

This section gives some highlights of the classical rate-distortion theory and the Shannon–Hartley theorem for classical Gaussian channels and then shows how these concepts naturally extend to Lie groups and principal G-bundles.

21.3.1 Classical Rate-Distortion Theory

Given a set of source symbols, U, and a set of sink symbols, V, a *distortion measure* $d : U \times V \rightarrow \mathbb{R}_{\geq 0}$ assigns values $d(u, v)$ that are high when two symbols $u \in U$ and $v \in V$ are far from being in proper correspondence and assigns a value of 0 when they correspond exactly. Often $U \subset V$, and $d(\cdot, \cdot)$ can be taken to be a metric (or the square of a metric) for V, but this is not required. U and V could both be continuous or discrete. For example, U and V could both be the Roman alphabet (plus empty space) in which case a 27×27 table of values $\{d(u, v) \mid u \in U, v \in V\}$ could be defined as $d(u, v) = 1 - \delta_{u,v}$, and so, the table would have zeros on the diagonal. Or, if the symbols are two real numbers, we could define $d(u, v) = |u - v|^2$. In general, given an injective mapping $m : U \rightarrow V$, if $m(u) = v$ then u and v are said to be in proper correspondence, in which case $d(m(u), v) = 0$ when $d(\cdot, \cdot)$ is a metric for V.

Given two discrete sequences $u^{(n)} \doteq \{u_1, \ldots, u_n\}$ and $v^{(n)} \doteq \{v_1, \ldots, v_n\}$, the distortion between them is defined as

$$d(u^{(n)}, v^{(n)}) \doteq \frac{1}{n} \sum_{i=1}^{n} d(u_i, v_i).$$

Similarly, given continuous signals $u_{[0,T]}$ and $v_{[0,T]}$ defined by continuous functions $u(t)$ and $v(t)$ over the time interval $[0, T]$, we could take

$$d(u_{[0,T]}, v_{[0,T]}) \doteq \frac{1}{T} \int_0^T d(u(t), v(t))\, dt.$$

In the absence of noise, a mapping between corresponding symbols $m : U \rightarrow V$ exists and applies to sequences of symbols in a term-by-term fashion so that $m(\{u_1, \ldots, u_n\} \in$

$U^n) = \{m(u_1), \ldots, m(u_n)\} \in V^n$. Given the frequency of occurrence of sequences of symbols in U described as a probability distribution (or density in the continuous case), $p(u^{(n)})$, the average rate of distortion over the set of sequences/messages of length n will be

$$D(R) \doteq \sum_{u^{(n)}} p(u^{(n)})\, d\left(u^{(n)}, m_R^n(u^{(n)})\right), \tag{21.13}$$

where R and m_R^n are defined as follows. The mapping m_R^n can be broken up into two maps that are composed. The first, $f_R^n : U^n \to \{1, 2, \ldots, 2^{nR}\}$, converts the source message into a standard alphabet (such as binary), and the second converts the message represented in the standard alphabet into $v^{(n)}$ (i.e., $g_R^n : \{1, 2, \ldots, 2^{nR}\} \to V^n$). Then $m_R^n(u^{(n)}) = g_R^n(f_R^n(u^{(n)}))$, or, equivalently, $m_R^n = g_R^n \circ f_R^n$. These implicitly define R. The pair (R, D') is called an achievable *rate-distortion pair* if $D(R) \leq D'$ as $n \to \infty$. The *rate-distortion function*, $R(D')$, is defined as the infimum of values of R over all achievable rate-distortion pairs (R, D').

Since a channel has noise, there is always some probability (rather than certainty) that the intended message will be communicated, which is described using the mutual information $\mathcal{I}(U; V)$ and the probability distribution $p(u, v)$. When noise is present, the the average distortion can be computed in the discrete case as

$$\overline{D} \doteq \sum_{u \in U} \sum_{v \in V} p(u, v)\, d(u, v),$$

with sums being replaced by integrals in the continuous case. The famous *rate-distortion theorem* then states that

$$\boxed{R(D) = \min_{p(v|u) | \overline{D} \leq D} \mathcal{I}(U; V).} \tag{21.14}$$

The continuous version of this would replace probability distributions with densities.

In the context of the mobile robot discussed in Section 21.1, the set of symbols/signals in U is the allowable basic maneuvers defined by the wheel angle trajectories $(\phi_1(t), \phi_2(t))$, or equivalently the wheel speeds $(\dot{\phi}_1(t), \dot{\phi}_2(t))$, over a short duration of time, and the message is the full intended wheel trajectory. The wheel speeds are converted into poses of the robot by the nonholonomic kinematics in (21.1), which together with numerical integration, defines the mapping m in this case. In this problem $V = SE(2)$, and the original message can be transmitted via an overhead camera that observes the resulting trajectory. The rate distortion then can be computed using a metric $d(\cdot, \cdot)$ for $SE(2)$. Noise is injected into the channel both through wheel slippage and observation error due to limited camera resolution.

21.3.2 The Shannon–Hartley Theorem

The subjects of stochastic modeling and information theory intersect when studying noisy channels. A typical noise model for a channel is the same sort of Gaussian (Wiener process) noise studied in Chapters 3 and 4. If one seeks to send a message over a noisy channel, a natural question to ask is what the trade-off between the signal amplitude (which is related to the power of the signal) is and the probability that the message will be successfully delivered. Clearly, increasing the power can be used to overcome fixed-amplitude background noise. However, given finite bounds on the amount of power that a signal can have and given fixed noise characteristics of the channel, there is a natural trade-off in how much information can be sent. In the case of a Gaussian channel, this trade-off is described by the Shannon–Hartley theorem, the derivation of which is briefly reviewed here. The reason for including this classical result here rather than earlier is to more directly draw parallels to the case of information flow in principal G-bundles subject to noise.

If the source has Gaussian statistics $\mathcal{N}(0,\sigma^2)$ and the rate distortion of function is the squared error of the source and sink signals, it can be shown that when $\sigma^2 \geq D$,

$$R(D) \geq \frac{1}{2}\log\frac{\sigma^2}{D}.$$

For a discrete memoryless channel with Gaussian noise with power constraint on the signal

$$\frac{1}{n}\sum_{i=1}^{n} x_i^2 \leq P$$

and noise intensity $\sigma^2 = N$, the capacity (measured in bits/transmission) will be

$$C = \frac{1}{2}\log\left(1+\frac{P}{N}\right). \tag{21.15}$$

Moreover, for a continous channel with power of the input signal bounded by P, information measured in bits, and the bandwidth of the channel B, then then the Shannon–Hartley theorem states that the capacity of the channel (when measured in bits per second) will be

$$\boxed{C = B\log_2\left(1+\frac{S}{N}\right),} \tag{21.16}$$

where C is the capacity of the channel, B is its bandwidth (in Hertz), $S = P/B$ is the total (integrated) received signal power divided by the bandwidth, and N is the total noise. S/N is the signal-to-noise ratio, and $\log_2(\cdot)$ is measured in units of bits.

The proofs of (21.14)–(21.16) can be found in the references on information theory provided in Chapter 17. Examples of why it is worthwhile to consider generalizations of this theory to the context of principal bundles are given in the following section.

21.3.3 Rate-Distortion Theory for Principal Bundles and Noisy Locomotion

Recall from Chapter 7 and the discussion in Section 21.1 that a fiber bundle consists of an entire space E, base space B, fiber space F, and a projection map π that satisfies certain properties. Roughly speaking, E locally "looks like" the Cartesian product of B and F. A principal bundle is one where the fiber space is homeomorphic to a Lie group. For example, the configuration space of the kinematic cart consists of the space of wheel angles $(\phi_1, \phi_2) \in \mathbb{T}^2$ and its pose $g \in SE(2)$. In this case, $E = \mathbb{T}^2 \times SE(2)$, and this is a trivial principal bundle. This situation generalizes to many scenarios in which mechanical systems demonstrate locomotion. Indeed, the locomotion of mechanical systems generally can be written in the form [10, 55, 56]

$$\left(g^{-1}\dot{g}\right)^{\vee} = A(\boldsymbol{\phi})\,\dot{\boldsymbol{\phi}} + [I(\boldsymbol{\phi})]^{-1}\,\mathbf{p}, \tag{21.17}$$

where $A(\boldsymbol{\phi})$ is called the "mechanical connection," $[I(\boldsymbol{\phi})]$ is called the "locked inertia," $\mathbf{p}$ is the generalized momentum, and $\boldsymbol{\phi}$ are the "internal coordinates." Kinematic systems, such as the cart, are characterized by $\mathbf{p} = \mathbf{0}$. Although (21.17) is usually studied in the context of deterministic motion, in order to obtain planning and control laws for a mechanical system to execute a desired pattern of motion (see, e.g., [26, 50] in which Stokes' theorem is used to select locomotion strategies or [16, 38] in which the fiber bundle structure is exploited to provide simplified feedback control), the problem discussed here is somewhat different. Suppose that we consider kinematic systems subjected to noise. Then (21.17) might become an SDE of the form

$$(g^{-1}\,dg)^{\vee} = A(\boldsymbol{\phi})\,[d\boldsymbol{\phi}_0 + H\,d\mathbf{w}], \tag{21.18}$$

where $d\phi = d\boldsymbol{\phi}_0 + H\,d\mathbf{w}$ is an SDE in shape space that "injects" noise and results in a stochastic trajectory in the G-bundle.[4] Indeed, the kinematic cart equations in Chapter 1 are exactly of this form where in that case the connection $A(\boldsymbol{\phi})$ is a constant matrix that describes the nonholonomic constraint.

A "message" in this context is the intended trajectory $(\phi_1(t), \phi_2(t)) \in \mathbb{T}^2$. The pose $g \in SE(2)$ of the robot can then be observed by an overhead camera. The wheels may slip, the camera has discretization effects, and so forth, so the pose that is observed will not be the ideal one that would be obtained by integrating the nonholonomic equations of motion of the cart. Nevertheless, from the trajectory $g(t)$ observed by the camera, it is possible to "decode" the intended message with knowledge of the nonholonomic kinematics, to back out a "received message" $(\tilde{\phi}_1(t), \tilde{\phi}_2(t)) \in \mathbb{T}^2$. This is an example of "communication over fiber bundles." This word usage is a bit of a pun since the term "fiber bundle" means something entirely different to the communications engineer. Here, the fibers are copies of $SE(2)$.

In the current context, Figure 17.1 applies where noise can be added in several places. It can be added at the arrow from transmitter to physical channel (which in the current context would be noise added at the level of wheel angles); or noise can be added in the physical channel (which would be, e.g., due to wheel slippage or surface roughness, which are not explicitly modeled here); or it can be added in the arrow from the physical channel to the receiver (which would be, e.g., discretization or other noise in an external camera that observes the motion of the cart). Treating the fiber space in a fiber bundle as a model of the physical channel allows for analytical modeling of how noise is injected in a variety of ways.

In general, for a G-bundle, the channel consists of fibers that are copies of the Lie group G, which serves as the medium through which communication takes place. In the simple example above, the Lie group is simply $SE(2)$ since the camera is assumed to be far enough away that it captures the scene as a parallel projection. However, if the camera were closer, then the affine group would enter, or if it were very close, then true projective transformations would become relevant. Regardless, with the tools of harmonic analysis on Lie groups discussed in Chapter 12, it is possible to define a concept of bandlimited signals and to define an analog of B in (21.16) that captures practical limitations on the physical movements of the robot. Moreover, the Gaussian statistics of the channel in the classical information-theory version of the rate-distortion theorem is replaced by the statistical properties of Fokker–Planck equations such as those in Chapters 1, 14, and 20, which characterize the extent to which noise in the kinematic system corrupts the intended motion.

This sort of view of the relationship between intended and actual motion can be used in the diagnose of systems, as in [39]. Some amount of wheel slippage or other noise is expected. By simulating a system under many different fault conditions (e.g.,

[4] The injection here reduces to the McKean–Gangolli injection described in Chapter 20 when A is constant and $d\boldsymbol{\phi}_0 = \mathbf{0}$.

if a wheel fails and its angle locks), the relationship between its intended and actual behavior, as observed in the solution to the corresponding Fokker–Planck equation, will be radically different when the pdfs for both scenarios are compared. Such comparisons can be made in the the sense of L^2 error or KL divergence. A decision as to the most likely system state (resulting in a diagnosis of either a fault state or the nominal fault-free state) can be obtained from the computed probability densities evaluated on the observed trajectories, providing likelihood information.

Several kinds of coding problems for this sort of robotics problem can be imagined. For example, we can ask "what constitutes a basic set of moves that can serve as a sufficiently rich alphabet to construct any desired trajectory to within an acceptable discretization error?" And since $(\phi_1(t), \phi_2(t))$ defines both the shape of a trajectory and its parameterization, it is possible to separate this into two different parts and ask "For fixed shape of a trajectory how can we optimally reparameterize so as to reject noise?" For example, a parameterization that speeds up as the robot makes a sharp turn would be bad from the perspective of transmitting intention to the observer for two reasons. First, the wheels would be more likely to slip. And second, as a result of limitations on the camera sample rate, a very abrupt event may be missed. In contrast, if a trajectory of given shape is parameterized to evolve in time as smoothly as possible, the intended message is more likely to get through. The development of a quantitative theory of source and channel coding over principal bundles in the context of robotics is yet to be formulated. But the variational tools of Chapter 13 and notions from information theory and coding from Chapters 17 and 18 appear to be promising in this regard.

21.4 Sensor Fusion in Mobile Robotics

Assume that the nonholonomic kinematic cart robot with two independently actuated wheels moves in a square room of known size. Relative to a frame of reference fixed in the room, the velocity of a frame of reference fixed in the robot is a function of the wheel speeds. The equations for this system are well known. See, for example, [10, 53, 80]. The reference frame that results from numerically integrating these nonholonomic governing equations can be thought of as the time-dependent rigid-body motion $g(t) = g(x(t), y(t), \theta(t)) \in SE(2)$. If the robot's motion could be observed with infinite precision, then $g(t)$ would be known for all times $t \geq 0$. However, of course, infinitely precise observations are not possible. The question then becomes one of estimating $g(t)$ given whatever sensory data is available. Such problems have become popular over the past decade, as reviewed in [49, 71].

In the present example, it is assumed that two noisy sensing modalities are present on the robot: (1) The wheel speeds can be measured (or calculated from wheel angle measurements) with sensors co-located with the motors resulting; (2) two range sensors fixed on the robot (one in front and one in back) point directly forward and behind the robot along its symmetry axis and measure the distance to the walls ahead of and behind the robot.[5] The scenario is that the robot starts at the center of the room with known initial heading, $\theta = 0$, estimates $g(t)$ from odometry for $t \in [0, T]$, and then switches on

[5] Although real-world range sensors spin and provide panoramic information about the proximity of neighboring objects, the range sensors alluded to in this section are far less capable. These are taken to be fixed in orientation relative to the robot and only provide distance information along a single line of sight that depends on the robot's orientation relative to the environment.

its range sensors at time T. Given models for the noise in both sensing modalities, how should these measurements be pooled to obtain the best estimate of the robot's current pose? Additionally, how can the quality of this estimate be compared with the estimates obtained from each individual sensing modality? Several of the theorems derived earlier in this chapter can be used to address these problems.

This is the question of fusing odometric (or "dead-reckoning") data with range data. In odometry, the nonholonomic kinematic equations of motion are numerically integrated given knowledge of the wheel speeds as a function of time. However, such measurements are noisy, and so the path that the robot actually takes diverges from the predicted one as time increases. The result is a conditional probability density $f(g_{act} \mid g_{odo}) \in \mathcal{N}(SE(2) \times SE(2))$, where g_{act} denotes the actual pose of the robot and g_{odo} denotes the pose predicted by odometry.

The function $f(g;T)$ generated by solving (21.4) is in fact $f(g_{act} \mid g_{odo})$ because the dead-reckoning path for a robot with fixed L, r, and D is completely defined by ω and T, which, in turn, define the shape of $f(g;T)$. It is interesting to note in passing that if the robot continues to move for an additional amount of time, t_2, then the distribution will be updated as a convolution over $SE(2)$ of the form

$$f_{t_1+t_2}(g) = (f_{t_1} * f_{t_2})(g); \tag{21.19}$$

that is, solutions to (21.4), or more generally (20.14), subject to Dirac delta initial conditions form a commutative semigroup under the operation of group convolution.

If the actual pose of the robot (which is unknown to the robot) is g_{act} and the distance/range range sensors take measurements from that pose, they will generate noisy distance measurements that can be used together with elementary geometry and trigonometry to develop a discrete set (or cloud) of reference frames. If the sensors are accurate, this cloud will be tightly clustered around g_{act}. The resulting histogram normalized to be a pdf in its first argument for any fixed value of $g_{act} \in SE(2)$ will be $f(g_{dis} \mid g_{act})$, where g_{dis} is the pose of the robot predicted from distance measurements. The peak value of g_{dis} need not coincide exactly with g_{act}. Any discrepancy between the peak value of g_{dis} for a given g_{act} represents bias in the range sensors. Models for $f(g_{act} \mid g_{odo})$ and $f(g_{dis} \mid g_{act})$ are developed in the following subsections and then fused to obtain $f(g_{act} \mid g_{odo}, g_{dis})$, the estimate of the actual robot position and orientation given measurements from both odometry and distance sensors.

21.4.1 A Maximum Entropy Model for Range-Finder Measurements

In the scenario described at the beginning of this section, the robot is equipped with two range sensors arranged with their beams pointing in diametrically opposed directions on the x axis passing through the center of the robot in Figure 21.1. If the range sensors could measure the distance to the walls exactly and if the robot behaved exactly as the nonholonomic kinematic cart, then the robot could spin around its z axis through 180°, generate an exact map of the environment, and exactly know its location modulo symmetries. It is these symmetries that make the discussions of discrete groups, cosets, and double cosets in Sections 5.2 and 5.3 relevant to this application. For a robot that has 180° rotational symmetry around its z axis, there is no distinction in the observation of $g_{act} = g(x, y, \theta)$ and $g(x, y, \theta + \pi) = g_{act} \circ g(0, 0, \pi)$. This means that no matter what shape room the robot is in, it will localize in a bounded subset of the coset space $SE(2)/C_2$ (where C_n is the cyclic group, isomorphic to the group of rotational symmetry operations of the regular n-gon, and the boundaries result from the walls of the room). Similarly, for a robot in a square room with no landmarks, there is no distinction between range sensor data when the robot is at the pose g_{act} and when it is at $g(0, 0, k\pi/2) \circ g_{act}$ for any $k \in \{0, 1, 2, 3\}$. This is true regardless of how the sensors are arranged on the robot. Therefore, the localization problem for a robot in a square room is one of finding a point in the coset space $C_4 \backslash SE(2)$. Now, if the robot and its range finders have C_2 symmetry and the room is square, then the localization problem becomes one in a bounded subset of the double coset space $C_4 \backslash SE(2)/C_2$.

Suppose that the robot is placed at the pose g_{act} where it remains while its front and back range sensors take a stream of synchronized distance measurements. A natural estimator for the pairs of distances of the front and back of the robot to the walls that the two beams hit results from simply computing the sample mean and covariance of pairs of distances. A roboticist might then define a bivariate Gaussian distribution with mean and variance given by the sample mean and sample variance of these two sets of measured distances. This is akin to the maximum entropy principle under the assumption that distances can be mapped to poses and the mean and covariance are sufficient statistics; that is, with all other things being unknown, choose the maximum-entropy distribution with specified mean and covariance, which is the Gaussian. The result is $f(g_{dis} \mid g_{act})$, a distribution of measured distances (which can be converted to a distribution of reference frames) when g_{act} is specified (although not known to the robot).

Taking a stream of measurements when the robot is at a fixed pose certainly does not offer as much information as when it does a full sweep. However, since it is implicit in this scenario that the geometry of the robot and the room are both known in advance, the above situation can be turned around. If we assume that g_{act} is not known, then we can ask for each pair of measured front/back distances what all possible poses of the robot can be in order for such distance measurements to be replicated, under the constraint that the robot fits in the room without penetrating any walls. From this, a maximum-entropy distribution $f(g_{act} \mid d_{front}, d_{back})$ can be constructed, where d_{front} and d_{back} are respectively the measured distances to walls in front and behind the robot.

In summary, an error model for distance measurements is presented that takes into account known symmetries of the robot and the room. Even if range finders could measure distance perfectly, due to symmetries they would not be sufficient to localize in the room, but only to within a bounded region in the double coset described above. The odometry data, as imperfect as it is, provides a means to resolve the ambiguity in the range measurements. Additionally, information theory on groups provides a language in which to address questions such as How much information is being provided by the range sensors versus odometry? How much improvement is there in estimates of g_{act} when data is pooled versus using each sensor modality independently? These questions can only be answered using the theorems presented previously in this chapter after a strategy for pooling the measurements is articulated. One such strategy is the Baysian filter (see [71] and references therein), a version of which is described in the following subsection.

21.4.2 Sensor Fusion

One form of Bayes' rule, which holds for probabilities and pdfs alike, is

$$p(A \mid B, C) = \frac{p(B \mid A, C)\, p(A \mid C)}{p(B \mid C)}.$$

Taking $A = g_{act}$, $B = g_{dis}$, and $C = g_{odo}$ and using the pdfs generated in the previous sections gives

$$f(g_{act} \mid g_{dis}, g_{odo}) = \frac{f(g_{dis} \mid g_{act}, g_{odo}) f(g_{act} \mid g_{odo})}{f(g_{dis} \mid g_{odo})}.$$

If g_{act} is known, then knowledge of g_{odo} adds nothing. Therefore, in this application, $f(g_{dis} \mid g_{act}, g_{odo}) = f(g_{dis} \mid g_{act})$. This is analogous to how conditioning on states at all prior times reduces to conditioning on the immediate predecessor for a Markov process. Therefore, the sensor fusion equation becomes

$$f(g_{act} \mid g_{dis}, g_{odo}) = \frac{f(g_{dis} \mid g_{act}) f(g_{act} \mid g_{odo})}{f(g_{dis} \mid g_{odo})}. \tag{21.20}$$

Each term on the right-hand side of this equation can be evaluated using the individual sensor models presented in the previous two subsections.

If nothing were known other than the speed of the robot, ω, and the duration of travel, T, and if $r\omega T$ is less than the distance to the nearest wall, then the robot position will be constrained to be within a circular disk of radius $r\omega T$. If its orientation is completely unknown, then an upper bound on the entropy of $f(g_{act})$ (without conditioning on any odometry data) can be computed from the maximum-entropy distribution on $SE(2)$ that is independent of θ, constant on this circular disk in the x-y plane and 0 for $\sqrt{x^2+y^2} > r\omega T$. The entropy associated with this distribution must necessarily be greater than that obtained when sensor measurements are obtained:

$$S(f_{max\,ent}(g_{act})) \geq S(f(g_{act} \mid g_{odo})) \geq S(f(g_{act} \mid g_{dis}, g_{odo})).$$

This follows from the general information-theoretic property that conditioning reduces entropy and does not use any Lie-group properties. In contrast, inequalities that directly use the results of the theorems presented earlier in this chapter are reviewed in the following subsection.

21.4.3 Application of Information-Theoretic Inequalities on Groups

The theorems presented in Chapter 19 describe relationships between several measures of dispersion for pdfs on Lie groups, including entropy, covariance, and the (inverse) Fisher information matrix. The reason for performing the sensor fusion described above is to reduce the dispersion of the resulting pdf in the variable $g_{act} \in SE(2)$ compared to the pdfs obtained from individual sensor modalities. This is now verified using (21.20), where g_{dis} and g_{odo} are fixed values and g_{act} is the unknown to be estimated. Below, examples of the applicability of the theorems presented earlier are given.

Example 12.4.1: Since the dead-reckoning distribution $f(g_{act}|g_{odo}) = f(g_{act}; t)$ is the solution of (21.4), it satisfies (21.19). From Theorem 19.1 we know that the entropy of a pdf increases under convolution, and from Theorem 19.10, the Fisher information decreases under convolution. These indicate that an estimate of the pose of the robot obtained by selecting the value of g that maximizes $f_t(g)$ will become more and more unreliable as an estimator of the actual pose as t increases, and the amount of this unreliability is quantifiable.

Example 12.4.2: Due to the symmetry of the room and of the range sensors, the entropy of the range only sensing modality can be bounded using the result of Theorem 19.4, which holds both when the subgroups K and H are Lie groups and when they are finite. If both elements of C_2 and all four elements of C_4 are equally likely, computation of the entropies $S(f_{C_2})$ and $S(f_{C_4})$ becomes trivial, and $S(f_{C_4 \backslash SE(2)/C_2})$

is computed by focusing on a single asymmetrical region of the configuration space. Theorem 19.4 then allows for the bounding of the actual entropy as the sum of these individual quantities, each of which is easier to compute than a mixture model of the form

$$f(g_{act} \mid d_{front}, d_{back}) = \frac{1}{8}\sum_{i=0}^{3}\sum_{j=0}^{1} f_{C_4\backslash SE(2)/C_2}(g(0,0,i\pi/2) \circ g_{act} \circ g(0,0,j\pi)).$$

This mixture model reflects maximal uncertainty induced by the symmetries but does not lend itself to closed-form entropy evaluations, which is one reason why the result of Theorem 19.4 is useful.

Example 12.4.3: Since $f(g_{act} \mid g_{odo}) = f(g_{act}, t)$ in (21.4), which is a specific example of (20.14), the de Bruijn inequality in Section 19.4 (with α set to the Dirac delta function on $SE(2)$) gives the rate of entropy increase of the odometry model in terms of the Fisher information matrix corresponding to the solution of the Fokker-Planck equation for the robot's SDE.

Example 12.4.4: Using nothing more than the product rule for the Lie derivatives, the Fisher information matrix for $f(g_{act} \mid g_{dis}, g_{odo})$ in (21.20) can be computed from models of $f(g_{dis} \mid g_{act})$ and $f(g_{act} \mid g_{odo})$, and through the CR-bound in Theorem 19.16, this can be used to bound the covariance of $f(g_{act} \mid g_{dis}, g_{odo})$.

Example 12.4.5: The Fourier-space solution for dead-reckoning models are described in [80], the $SE(2)$ and $SE(3)$ group-Fourier transforms, their properties, and applications are described in detail in Chapter 12, and $\hat{f}(\lambda)$ is completely characterized for equations such as the odometry model in (21.4). Therefore, the bounds in Theorem 19.2 can be applied.

Example 12.4.6: Theorems 19.6 and 19.7(b) are applicable to symmetric functions, including Gaussians on $SE(2)$ with $\mu = e$. The solution of the odometry equation (21.4) is not a symmetric function. However, $f_t(g) * f_t(g^{-1})$ is symmetric. Therefore, if a robot does an initial sensor sweep in a room without symmetry, which results in an $SE(2)$ Gaussian, then the robot moves under the open-loop odometry model for time t, and then it tries to return to its starting location, the resulting pose distribution will be the convolution of the $SE(2)$ Gaussian constructed from range-finder data and the symmetric function $f_t(g) * f_t(g^{-1})$. Theorems 19.6 and 19.7(b) allow for the isentropic reordering of some of these convolutions, even though convolution on noncommutative groups is generally order dependent.

Example 12.4.7: The bounds on entropy powers and relative information in (19.47) and (19.50) resulting from log-Sobolev inequalities provides a means to respectively evaluate and compare additional informational quantities associated with $f(g_{act} \mid g_{dis}, g_{odo})$ and $f(g_{act} \mid g_{odo})$.

In summary, the efficacy of 9 out of the 15 theorems presented have been illustrated in the context of a single example in robotics. By establishing the language and principles with which to articulate information theory on Lie groups, other applications that utilize all of these theorems will be explored in the future. For example, Theorems 19.7(a) and 19.8 pertaining to convolution and class functions are not relevant to robot localization in $SE(2)$ because there are no pdfs that are class functions in $\mathcal{N}(SE(2))$. However, solutions to the heat equation on $SO(3)$ are both symmetric and class functions, and so these theorems become immediately applicable to spacecraft and submarine orientational estimation problems.

21.4.4 Relationship to Information-Driven Motion

A topic that has become popular in the robotics community in the past few years has been endowing robots with "information-foraging" capabilities; that is, how should a mobile robot move so as to increase the amount of information that it collects in an optimal way. Such information may be in regard to a chemical plume or radioactive source, about the structure of its a priori unknown environment, or about its position in a known environment. Works in this area include [19, 63, 66, 75]. One such method involves the use of the Cramér–Rao bound (or CRB) [11, 72–74]. In the classical CRB, the Fisher information figures prominently. However, the author is unaware of any statement of the concept of Fisher information for Lie groups prior to the present work.[6] Having such a concept would be critical for the extension of the CRB to the Lie-group setting. An application of this is described below.

Previous works treat a robot as holonomic point-particle vehicles and they treat the problem as one of pure translation in the plane. One reason for this may be because information theory on $\mathbb{R}^2$ is well developed and information theory on noncommutative Lie groups is not. However, since information gathering and locomotion capabilities are really body-fixed phenomena, vehicles are essentially rigid bodies that observe nonholonomic locomotion constraints, "$SE(2)$ versions" of all of the methods mentioned above should become possible with the assistance of the derivations provided in this chapter. In particular, if a robot wants to analyze the intensity of radiation in an area, it might deploy detectors on antipodal points of a long boom. Any measurements would then become measurements in $SE(2)$ as the robot moves, rather than point measurements in the plane. Then the methods developed in the works cited above would extend in a natural way to include orientation using the definitions and properties described in the theorems presented here. In short, the methods developed here provide a link among information theory, the geometric approach to robotics expressed in [10, 53], and work on localization such as [49, 71]. Work in the area of computer vision such as [70] in which actionable information is extracted from visual images is also relevant to the overall goal of information-driven motion.

21.5 Stochastic Models in Vision

Three intertwined areas of research pertaining to the study of vision involve stochastic models, information theory, and Lie groups. They are (1) the structure and function of the visual cortex in mammals, (2) the mathematics of perception and visual hallucination, and (3) algorithms for the processing of occluded visual scenes in computer vision systems. A brief review of this literature is provided here. Equipped with the mathematical tools explained in these volumes, this literature can be understood without difficulty.

The idea that visual perception is a kind of communication channel that can be addressed using methods of information theory is almost as old as information theory itself (see, e.g., [2]). Remarkably, researchers in the field of mathematical psychology have been interested in tools from geometry and topology for almost as long as physicists have (and for longer than these tools have been used by engineers) [9, 44, 54].

[6] As is the case in the field of information geometry, Smith [69] addresses the issue of the intrinsic CRB for pdfs of the form $f(\mathbf{x} \,|\, \boldsymbol{\theta})$ where $\mathbf{x} \in \mathbb{R}^n$ and $\boldsymbol{\theta}$ is in a manifold, but the issue of when $\mathbf{x}$ is replaced by $g \in G$ was not the concern of that work.

The work by Hubel and Wiesel on the mammalian visual cortex [32–34] that started half a century ago and was recognized with the 1981 Nobel Prize in Physiology or Medicine (shared with Sperry) has led to mathematical modeling work in the field of mammalian vision that is related to the topic of this book. In particular, the topic of visual perception has been studied from a Lie-group/fiber bundle perspective for decades [28–31, 65].

Occlusion is a big problem in vision—namely based on a two-dimensional image of the three-dimensional world, how can one make reasonable guesses as to what objects are in front of others (i.e., closer to the eye or camera taking the image) in the three-dimensional world? In order to address this problem, work on stochastic completion fields propagates probabilities on the special Euclidean group $SE(2)$ to make an informed guesses as to where hidden edges of a partially occluded object are likely to intersect. This has been an active area of work spanning a number of years [51, 77, 78, 81] and remains of interest today [27]. In these works, the same sort of diffusion equations that describe the stochastic kinematic cart or DNA conformational statistics discussed earlier arise.

The mathematics of visual hallucination and its connection to the structure of the visual cortex in the mammalian brain have been studied using differential geometric tools in [7, 14, 62].

Such tools have become popular in the analysis and understanding of images [17, 18, 23, 24].

21.6 Conclusions

Although the emphasis of this chapter was on the discovery of fundamental inequalities, the motivation for this study originated with applications in robotics and other areas. Indeed, it was the problem of quantifying the difficulty of robotic assembly [42] and self-repair [39] tasks using the concept of "parts entropy" discussed in Chapter 15 that led the author to link group theory and information theory. A detailed example in mobile robot localization was provided here to illustrate the efficacy of the presented theorems.

Eye movements (in particular, saccades) are studied from the perspective of Lie groups and differential geometry in [25]. Fax and Murray applied tools from graph theory and the topology of the communication network of multiple vehicles that coordinate to move in formation [22]. The stability of the formation depends on the communication capabilities and the control law used. This is a perfect example of how information, geometry of motion, and topology can come together in the context of an application, although in a different way than emphasized in this book.

As another example, the idea that a robot or animal should move (in $SE(2)$) so as to maximize the rate at which its sensors gain information is attracting attention [1, 4, 6, 11, 15, 21, 48, 63, 66, 68, 72–75]. Analogous problems can be formulated in medical imaging in which only X-rays in directions that maximize the generation of new information need be taken rather than exposing a patient to the radiation of a whole CT scan. Related to this problem is that of biomolecular structure determination from disparate data sets such as cryo-electron microscopy, NMR, X-ray crystallography, and so forth. Each is related to the structure of molecules, their ensemble motion, and/or their quantum state—all of which are described in terms of probability densities on Lie groups. A first step toward information fusion of data on Lie groups is the version of information theory developed here and demonstrated on an example in the context of a mobile robot.

References

1. Atema, J., "Eddy chemotaxis and odor landscapes: exploraton of nature with animal sensors," *Biol. Bull.*, 191(1), pp. 129–138, 1996.
2. Attneave, F., "Some informational aspects of visual perception," *Psychol. Rev.*, 61(3), pp. 183–193, 1954.
3. Baldwin, G., Mahony, R., Trumpf, J., "A nonlinear observer for 6 DOF pose estimation from inertial and bearing measurements," *IEEE International Conference on Robotics and Automation*, Kobe, Japan, May 2009.
4. Berg, H.C., *E. coli in Motion*, Springer, New York, 2003.
5. Bloch, A. M., et al. *Nonholonomic Mechanics and Control.* Springer, New York, 2003.
6. Bray, D., *Cell Movements*, Garland Pubishing, Inc., New York, 1992.
7. Bressloff, P.C., Cowan, J.D., Golubitsky, M., Thomas, P., Wiener, M., "Geometric visual hallucinations, Euclidean symmetry, and the functional architecture of striate cortex," *Philos. Trans. Soc. London B*, 356(1407), pp. 299-330, 2001.
8. Brockett, R.W., "System theory on group manifolds and coset spaces," *SIAM J. Control*, 10(2), pp. 265–284, 1972.
9. Brown, J.F., Voth, A.C., "The path of seen movement as a function of the vector field," *Am. J. Psychol.*, 49, pp. 543–563, 1937.
10. Bullo, F., Lewis, A.D., *Geometric Control of Mechanical Systems*, Springer, New York, 2004.
11. Censi, A., "On achievable accuracy for pose tracking," *IEEE International Conference on Robotics and Automation*, Kobe, Japan, May 2009.
12. Censi, A., "On achievable accuracy for range-finder localization," in Proc. of the IEEE Int. Conf. on Robotics and Automation (ICRA), pp. 4170–4175, 2007.
13. Choset, H., Lynch, K.M., Hutchinson, S., Kantor, G., Burgard, W., Kavraki, L.E., Thrun, S., *Principles of Robot Motion: Theory, Algorithms, and Implementations*, MIT Press, Boston, 2005.
14. Citti, G., Sarti, A., "A Cortical Based Model of Perceptual Completion in the Roto-Translation Space," *J. Math. Imaging Vision*, 24(3), pp. 307–326, 2006.
15. Cortez, R.A., Tanner, H.G., Lumia, R., "Distributed robotic radiation mapping," *Experimental Robotics, Springer Tracts in Advanced Robotics*, Vol. 54, pp. 147–156, 2009.
16. Cowan, N.J., Chang, D.E., "Geometric visual servoing," *IEEE Trans. Robot.*, 21(6), pp. 1128–1138, 2005.
17. Duits, R., Franken, E., "Left-invariant parabolic evolutions on $SE(2)$ and contour enhancement via invertible orientation scores Part I: Linear left-invariant diffusion equations on $SE(2)$," *Q. Appl. Math.*, 68, pp. 255–292, 2010.
18. Duits, R., van Almsick, M., Duits, M., Franken, E., Florack, L.M.J., "Image processing via shift-twist invariant operations on orientation bundle functions," *Pattern Recognition and Image Analysis*, 15(1), pp. 151–156, 2005.
19. Durrant-Whyte, H.F., "sensor models and multisensor integration," *Int. J. Robot. Res.*, 7(6), pp. 97–113, 1988.
20. Durrant-Whyte, H.F., *Integration, Coordination and Control of Multi-Sensor Robot Systems*, Kluwer Academic Publishers, Boston, 1988.
21. Dusenbery, D.B., *Sensory Ecology: How Organisms Acquire and Respond to Information*, Freeman, New York, 1992.
22. Fax, J.A., Murray, R.M., "Information Flow and Cooperative Control of Vehicle Formations," *IEEE Trans. Autom. Control*, 49(9), pp. 1465–1476, 2004.
23. Ferraro, M., Caelli, T.M., "Lie transformation groups, integral transforms, and invariant pattern recognition," *Spatial Vison*, 8(1), pp. 33–44, 1994.

24. Franken, E.M., *Enhancement of Crossing Elongated Structures in Images*, Ph.D. thesis, Department of Biomedical Engineering, Eindhoven University of Technology, 2008.
25. Handzel, A.A., Flash, T., "The geometry of eye rotations and Listing's law," *Adv. Neural Inform. Process. Syst.*, 8, pp. 117–123, 1996.
26. Hatton, R.L., Choset, H., "Geometric motion planning: The local connection, Stokes's theorem, and the importance of coordinate choice," *Int. J. Robot. Res.*, 30(8), pp. 988–1014, 2011.
27. Hladky, R.K., Pauls, S.D., "Minimal surfaces in the roto-translation group with applications to a neuro-biological image completion model," *J. Math. Imaging Vision*, 36(1), pp. 1–27, 2010.
28. Hoffman, W.C., "The Lie algebra of visual perception," *J. Math. Psychol.*, 3, pp. 65–98, 1966.
29. Hoffman, W.C., "Higher visual perception as prolongation of the basic Lie transformation group," *Math. Biosci.*, 6, pp. 437–471, 1970.
30. Hoffman, W.C., "Some reasons why algebraic topology is important in neuropsychology: perceptual and cognitive systems as fibrations," *Int. J. Man-Machine Studies*, 22, pp. 613–650, 1985.
31. Hoffman, W.C., "The visual cortex is a contact bundle," *Appl. Math. Comput.*, 32, pp. 137–167, 1989.
32. Hubel, D.H., Wiesel, T.N., "Receptive fields of single neurones in the cat's striate cortex," *J. Physiol.*, 148, pp. 574–591, 1959.
33. Hubel, D.H., Wiesel, T.N., "Receptive fields, binocular interaction and functional architecture in the cat's visual cortex," *J. Physiol.*, 160, pp. 106–154, 1962.
34. Hubel, D.H., Wiesel, T.N., "Ferrier lecture: Functional architecture of macaque monkey visual cortex," *Proc. R. Soc. London B: Biol. Sci.*, 198, pp. 1–59, 1977.
35. Husemoller, D., *Fibre Bundles*, 3rd ed., Springer, New York, 1993.
36. Isham, C.J., *Modern Differential Geometry for Physicists*, World Scientific Publishing, Singapore, 1989.
37. Jurdjevic, V., Sussmann, H.J., "Control systems on Lie groups," *J. Diff. Eq.*, 12, pp. 313–329, 1972.
38. Kallem, V., Chang, D.E., Cowan, N.J., "Task-induced symmetry and reduction with application to needle steering,"*IEEE Trans. Automa. Control*, 55(3), pp. 664–673, 2010.
39. Kutzer, M.D.M., Armand, M., Lin, E., Scheidt, D., Chirikjian, G.S., "Toward cooperative team-diagnosis in multi-robot systems," *Int. J. Robot. Res.*, 27, pp. 1069–1090, 2008.
40. Kwon, J., Choi, M., Park, F.C., Chu, C., "Particle filtering on the Euclidean group: Framework and applications, " *Robotica*, 25, pp. 725–737, 2007.
41. LaValle, S.M., *Planning Algorithms*, Cambridge University Press, Cambridge, 2006.
42. Lee, K., Chirikjian, G.S., Robotic self-replication from low-complexity parts. *IEEE Robot. Automa. Mag.*, 14(4), pp. 34–43, 2007.
43. Lee, K., Moses, M., Chirikjian, G.S., "Robotic self-replication in partially structured environments: Physical demonstrations and complexity measures," *Int. J. Robot. Res.*, 27(3–4), pp. 387–401, 2008.
44. Lewin, K., *Principles of Topological Psychology*, McGraw-Hill, New York, 1936.
45. Mahony, R., Hamel, T., Pflimlin, J.-M., "Nonlinear complementary filters on the special orthogonal group," *IEEE Trans. on Autom. Control*, 53(5), pp. 1203–1218, 2008.
46. Makadia, A., Daniilidis, K., "Rotation estimation from spherical images," *IEEE Trans. Pattern Anal. Mach. Intell.*, 28, pp. 1170–1175, 2006.
47. Malis, E., Hamel, T., Mahony, R., Morin, P., "Dynamic estimation of homography transformations on the special linear group for visual servo control," *IEEE International Conference on Robotics and Automation*, Kobe, Japan, May 12–17, 2009; paper 0538.pdf on CD Rom Proceedings.
48. Manyika, J., Durrant-Whyte, H., *Data Fusion and Sensor Management: A Decentralized Information-Theoretic Approach*, Ellis Horwood, New York, 1994.
49. Mourikis, A., Roumeliotis, S., "On the treatment of relative-pose measurements for mobile robot localization," *ICRA'06*, Orlando, FL, 2006.

50. Mukherjee, R., Anderson, D.P., "Nonholonomic motion planning using Stokes' theorem," *Proceedings of the IEEE International Conference on Robotics and Automation*, 1993.
51. Mumford, D., "Elastica and computer vision," in *Algebraic Geometry and Its Applications*, C. Bajaj ed., Springer-Verlag, New York, 1994.
52. Murray, R., Sastry, S., "Nonholonomic motion planning: Steering using sinusoids," *IEEE Trans. Autom. Control*, 38(5), pp. 700–715, 1993.
53. Murray, R., Li, Z., Sastry, S., *A Mathematical Introduction to Robotics*, CRC Press, Boca Raton, FL, 1994.
54. Orbison, W.D., "Shape as a function of the vector-field," *Am. J. Psychol.*, 52, pp. 31–45, 1939.
55. Ostrowski, J.P., *The Mechanics and Control of Undulatory Robotic Locomotion*, Ph.D. dissertation, Caltech, 1996.
56. Ostrowski, J., Burdick, J., "The mechanics and control of undulatory locomotion," *Int. J. Robot. Res.*, 17(7), pp. 683–701, 1998.
57. Park, W., Liu, Y., Moses, M., Chirikjian, G.S., "Kinematic state estimation and motion planning for stochastic nonholonomic systems using the exponential map," *Robotica*, 26(4), pp. 419–434, 2008.
58. Park, W., Wang, Y., Chirikjian, G.S., "The path-of-probability algorithm for steering and feedback control of flexible needles," *Int. J. Robot. Res.*, 29, pp. 813–830, 2010.
59. Patlak, C.S., "Random walk with persistence and external bias," *Bull. Math. Biophys.*, 15, pp. 311–338, 1953.
60. Patlak, C.S., "A mathematical contribution to the study of orientation of organisms," *Bull. Math. Biophys.*, 15, pp. 431–476, 1953.
61. Pennec, X., "Intrinsic statistics on Riemannian manifolds: Basic tools for geometric measurements," *J. Math. Imaging Vision*, 25(1), pp. 127–154, 2006.
62. Petitot, J., "The neurogeometry of pinwheels as a sub-Riemannian contact structure," *J. Physiol. (Paris)*, 97, pp. 265–309, 2003.
63. Porat, B., Nehorai, A., "Localizing vapor-emitting sources by moving sensors," *IEEE Trans. Signal Process.*, 44(4), pp. 1018–1021, 1996.
64. Porter, R.D., *Introduction to Fibre Bundles*, Marcel Dekker, New York, 1977.
65. Resnikoff, H.L., "Differential geometry and color perception," *J. Math. Biol.*, 1, pp. 97–131, 1974.
66. Russell, R.A., *Odour Detection by Mobile Robots*, World Scientific, Singapore, 1999.
67. Shapere, A., Wilczek, F., "Geometry of self-propulsion at low Reynolds number," *Journal of Fluid Mechanics*, 198, pp. 557–585, 1989.
68. Smith, P., Drummond, T., Roussopoulos, K., "Computing MAP trajectories by representing, propagating and combining PDFs over groups," *Proceedings of the 9th IEEE International Conference on Computer Vision*, Vol. 2, Nice, France, 2003, pp. 1275–1282.
69. Smith, S.T., "Covariance, Subspace, and Intrinsic Cramér-Rao Bounds," *IEEE Transactions on Signal Processing*, 53(5): 1610–1630, May 2005.
70. Soatto, S., "Actionable Information in Vision," *Proceedings of the International Conference on Computer Vision*, Kyoto, Japan, October 2009.
71. Thrun, S., Burgard, W., Fox, D., *Probabilistic Robotics*, MIT Press, Cambridge, MA, 2005.
72. Tzanos, P., Zefran, M., Nehorai, A., "Information based distributed control for biochemical source detection and localization," *ICRA'05*, pp. 4457–4462.
73. Tzanos, P., Zefran, M., "Stability analysis of information based control for biochemical source localization," *ICRA'06*, pp. 3116–3121.
74. Tzanos, P., Zefran, M., "Locating a circular biochemical source: Modeling and control," *ICRA'07*, pp. 523–528.
75. Vergassola1, M., Villermaux, E., Shraiman, B.I., " 'Infotaxis' as a strategy for searching without gradients," *Nature*, 445(25), pp. 406–409, 2007.
76. Webster, R.J., III, Kim, J.-S., Cowan, N.J., Chirikjian, G.S., Okamura, A.M., "Nonholonomic modeling of needle steering," *Int. J. Robot. Res.*, 25(5–6), pp. 509–525, 2006.
77. Williams, L.R., Jacobs, D.W., "Stochastic completion fields: A neural model of illusory contour shape and salience," *Neural Comput.*, 9(4), pp. 837–858, 1997.

78. Williams, L.R., Jacobs, D.W., "Local parallel computation of stochastic completion fields," *Neural Comput.*, 9(4), pp. 859–881, 1997.
79. Willsky, A.S., "Dynamical systems defined on groups: Structural properties and estimation," Ph.D. dissertation, Dept. Aeronautics and Astronautics, MIT,, Cambridge, MA, 1973.
80. Zhou, Y., Chirikjian, G.S., "Probabilistic models of dead-reckoning error in nonholonomic mobile robots," *ICRA'03*, Taipei, Taiwan, September 2003.
81. Zweck, J., Williams, L.R., "Euclidean group invariant computation of stochastic completion fields using shiftable-twistable functions," *J. Math. Imaging Vision*, 21, pp. 135–154, 2004.

22

Summary

This chapter summarizes Volume 2 of this two-volume set. Whereas the emphasis of Volume 1 was on establishing terminology and review of fundamental definitions from information theory, geometry, and probability theory on Euclidiean space, Volume 2 has focused on analogous concepts in the setting of Lie groups. A survey of problems that simultaneously involve Lie groups and information theory was provided, including the encoding/decoding of spatial pose (position and orientation). The physics that govern different kinds of communication systems gives rise to SDEs and their corresponding Fokker–Planck equations. In some instances, such as laser phase noise, these can be viewed as a probability flows on a group manifold. In other instances, such as the telegraph equation, Lie groups describe the symmetries of a PDE on Euclidean space. Stochastic models of phenomena such as the conformational fluctuations of DNA and the motions of robotic systems were examined. These lead to probability densities on the group of rigid-body motions, and properties of the corresponding conformational and parts entropy were studied. Numerical tools for solving Fokker–Planck equations on Lie groups such as the rotation group and group of rigid-body motions were reviewed.

The goals of the remaining sections in this chapter are to (1) return to Problems 1–5 listed at the beginning of Volume 1 and to sketch their solutions using the methods of both books and (2) enumerate possible future research directions for which the methods in these volumes may be applicable.

22.1 Return to the Problems Stated in Volume 1

At the beginning of Volume 1, five problems were stated to motive the development of the methods presented in both volumes. Here, these problems are restated together with pointers to methods enclosed in these volumes that address their solution.

Problem 1: A random walker on a sphere starts at the North Pole. After some period of time, what will the probability be that the walker is at a particular location? How long will it take before the walker's location on the sphere is completely randomized (i.e., how long will it be before the initial location of the walker becomes irrelevant)?

Solution: We know from Chapters 4, 5, and 8 how to write an SDE for isotropic Brownian motion on the sphere. The most natural way to do this using spherical coordinates is to write a Stratonovich equation as was done in Section 8.5.2. Or, an Itô process on the sphere can be defined extrinsically using Cartesian coordinates as was done in

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9_13,

Section 8.5.3. Either way, a corresponding Fokker–Planck equation can be written. This is a linear PDE that can be solved by separation of variables. Alternatively, the operational properties of spherical harmonics that follow from their definition relative to IURs of $SO(3)$ in Chapter 12 can be used to write a solution. Knowing explicitly the form of the probability density $f(\mathbf{u}, t)$ that solves the Fokker–Planck equation subject to initial condition that $f(\mathbf{u}, 0)$ is concentrated at the North Pole, we can evaluate probabilities at any location and time. Additionally, we can compare $f(\mathbf{u}, t)$ with the uniform distribution on the sphere using L^2 or KL measures and observe how these changes as a function of time to assess how rapidly the effects of initial conditions decay.

Problem 2: A cartlike robot moves around in the plane by turning each of its two wheels. Relative to a frame of reference fixed in the plane, the frame of reference fixed in the robot moves as a function of the torque inputs imparted by the motors to the wheels. Given models describing these uncertainties, what will the most likely position and orientation of the robot be at a given future time?

Solution: Models for this sort of problem were described in Chapter 20 and references to the literature were given that solve this problem for the kinematic cart, the nonholonomic car model, and so forth. The process involves first writing an SDE that defines sample paths on the group $SE(2)$, converts them to Fokker–Planck equations, and then solves them using the operational properties of the $SE(2)$ Fourier transform. The original SDEs could be generated either in coordinates or in coordinate-free form. The SDEs and corresponding Fokker–Planck equations for this problem are closely related to those presented in Chapter 17 in the context of laser phase noise in optical communications and also to the equations used in the study of stochastic completion fields discussed in Chapter 20.

Problem 3: A long and slender semi-flexible biological macromolecule, such as double-helical DNA composed of 300 stacked basepairs, is subjected to random Brownian motion bombardment by the surrounding solvent molecules. If reference frames are attached to both ends of the DNA, what will the distributions of rigid-body motions between these reference frames look like as a function of temperature and the stiffness of the molecule?

Solution: This problem was addressed in detail in Chapter 14 using two models. One was the rigid-base model in which spatially proximal bases were connected by six-dimensional springs that store energy under infinitesimal rigid-body motions, and a Gaussian on the space $SE(3) \times \cdots \times SE(3)$ resulted where the number of copies of $SE(3)$ is the number of bases in the DNA. The other model was the continuum filament model in which the backbone of the DNA was a continuous curve perturbed by Brownian motion forcing, resulting in a diffusion equation describing the evolution of a pdf $f(g, s)$ on one copy of $SE(3)$ indexed by arc length along the filament, s.

Problem 4: An isolated *E. coli* bacterium swims in a medium and, based on sensory information, randomly reorients. For a given starting position, nutrient environment and temperature, what will the probability be that it reaches a particular position at a particular time?

Solution: This is a variant of the kinematic cart problem in three dimensions. It is also very similar to the problem of kinematic needle steering that was discussed in the context of Taylor series on Lie groups in Chapter 11, where the goal is to steer the needle in order for the tip to hit a target. The two minor differences are that arc length of the needle is replaced by time traveled and the baseline path in the present case is not differentiable due to the tumbling phase. The "straight" sections of its motion are not perfectly straight and can be described by the same mathematics as in the DNA statistical mechanics problem discussed in Chapter 14. These parts of the path are connected by distributions that describe tumbling, which are essentially a product of delta functions in position and distributions over $SO(3)$ which have been modeled as uniform in the literature but could be any distribution informed by experiment. Let $g = (\mathbf{x}, R) \in SE(3)$. Then the iterated convolution on $SE(3)$ of the form $f_{1,n}(g) \doteq (s_1 * t_1 * s_2 * t_2 * \cdots t_{n-1} * s_n)(g)$, where $s_k(g)$ describes the distribution for the kth straight path and $t_k(g)$ describes the distribution for the kth tumbling phase, produces the joint distribution in position and orientation up to the nth time. A maximum likelihood foraging strategy would put the mode of the marginal of this probability density integrated over orientation,

$$f_{1,n}(\mathbf{x}) = \int_{SO(3)} f_{1,n}(\mathbf{x}, R)\, dR,$$

over the location of the food.

Problem 5: (a) One rigid body is set at a fixed pose (or position and orientation) in a box, and a second rigid body is allowed to move uniformly at random in the box under the constraint that it cannot intersect the first body. How much free space is there for the second body to move? (b) If the opposing faces of the box are identified with each other (by "gluing them together"), then the boundaries are removed, but the volume in this toroidal world will be the same as that of the original box. How much free space is there for the second body to move in this scenario?

Solution: In both of these problems, if the amount (i.e., volume) of allowable motion in $SE(3)$ can be obtained first in the case when there is no obstacle and then the effects of interactions between obstacle and moving body are taken into account to reduce this volume, then we can solve the problem. When the obstacle and moving object are both small enough that the moving object never gets "jammed," then in both cases we can simply compute the volume of allowable motion without the obstacle. This is actually easier in the toroidal world because this volume is equal to the product of the volume of the unit cell that describes the range of allowable translations and the volume of $SO(3)$, which is $8\pi^2$ when computed using the unnormalized Haar measure. Again, this assumes that the body is small enough that it does not self-occlude as it undergoes rotational motion in a toroidal world. The allowable motion of a convex body moving in a convex box, the latter of which has minimum radius of curvature and diameter that are always larger than the maximal radius of curvature and diameter of the moving body, can be computed from a variant of the principal kinematic formula from Chapter 15. Even when these conditions do not hold, good approximations of the allowable motion in the obstacle-free case can still be obtained. When accounting for the effects of the obstacle, in the case when both bodies are convex we can use the principal kinematic formula to compute the volume of motions corresponding to all possible collisions and then subtract this from the former quantity. If the bodies are not convex, then the bounds computed in Chapter 15 can be used to provide estimates. In more difficult cases where the bodies occupy a relative large fraction of the volume of the box or unit cell containing them, the situation is not so easy and becomes more computational than analytical. This is the subject of current research [18, 19].

22.2 Future Directions

Usually the fields of stochastic modeling, information theory, and Lie groups are considered to be disjoint from each other. Perhaps this is because experts in one of these fields may not know about either of the other two. These two volumes have sought to illustrate connections between these three fields both from a theoretical perspective (using methods of differential geometry and analysis techniques) and from the perspective of motivating applications (robotics, DNA statistical mechanics, laser communications, etc.). In a sense, the applications discussed may be the tip of an iceberg. With these few examples serving to illustrate connections, the door opens to many other possibilities. For example, information theory could be used as a tool to link the information processing and stochastic motion in living systems such as in chemotaxis or in cell signal transduction between motile cells.

One result of this book has been the observation that a number of inequalities from classical information theory can be extended to the context of group-valued probability density functions. A natural question to ask is how these inequalities might be used in applications. Here short descriptions of potential applications and how they relate to the derived inequalities are provided. Several different application areas are described below.

Before getting to these examples, it is worth repeating what was stated in the preface: The webpage of the author's lab will post an evolving bibliography pointing toward the growing body of literature on applications at the intersection of the fields of stochastic models, information theory, and Lie groups. Therefore, the examples described below are only a few of the many possible future directions. Readers who contribute to this area are welcome to contact the author for possible inclusion of their work in that web-based bibliography.

22.2.1 Limited Tomographic Reconstruction

Computed tomography (CT) scans are used regularly in hospitals to obtain three-dimensional information about the internal structure of patients. They are very useful and have many benefits. However, since they require rotating scanners around a patient and taking X-rays in finely spaced angular increments, the result can be a radiation dose of approximately 500 times that of a normal chest X-ray—or the approximate equivalent of what someone standing 2.5 km from ground zero of the Hiroshima bomb experienced (http://www.newscientist.com/article/dn11827-ct-scan-radiation-can-equal-nuclear-bomb-exposure.html).

Although it has been estimated that each CT scan only increases the risk of cancer by a small fraction of a percent, CT has become a means of follow-up that is used more routinely than perhaps is desirable. This is because sometimes patients are given multiple CT scans over relatively short time scales.

One way that multiple CT scans can be used effectively and simultaneously reduce the radiation exposure of patients is to take slices at coarser (perhaps irregular) angles during scans subsequent to the first one and compare the results to a prior baseline scan. In principle, with the design of new machinery, such projections could be taken from any orientation rather than around a fixed axis. If the goal is to minimize radiation exposure while obtaining the most useful information, the issue then becomes one of how to select the slices. The relationship to information theory is that this can be done so as to increase the expected amount of information gain. A strategy to optimally select angles drawn from $SO(2)$ (or in the case of new equipment paradigms, S^2), would be to assess the information content in each slice of a prior CT reconstruction (perhaps sliced in different planes than those used to form the original CT scan). The information in each of these slices (which can be equated to the classical discrete entropy of the pixelized images in each of these planes) will be a non-negative function of the orientation of the slice taken and a point on the plane and, hence, will be of $SO(3) \times \mathbb{R}^2$-valued argument (or at least $S^2 \times \mathbb{R}^2$-valued argument). If the discrete entropy of the image in each of these planes is computed and the results are normalized, then this actually defines a pdf on the space of all slices. From this, a first best guess as to what single new CT slice to take would be the one that maximizes this probability. Additional slices would need to be chosen to maximize the amount of information gain in this non-Euclidean product group, taking into account the cumulative information obtained up to the current point. Having a language for quantities such as entropy and Fisher information on groups provides a starting point to articulate such problems.

22.2.2 Information Fusion in Biomolecular Structure Determination

Many experimental modalities exist to provide insight into the structure of biological macromolecules. These include X-ray crystallography, nuclear magnetic resonance (NMR), and cryo-electron microscopy (cry-EM), among others. Each of these modalities provide partial information about a biomolecular structure of interest. Each involves the spatial position and orientation of molecules given with some probability. Stochastic modeling opportunities exist in the context of each individual method. For example, geometric packing models that involve stochastic searches over $SE(3)^N$ for fitting articulated multi-rigid-body models of proteins to X-ray crystallography data benefit from the methods and terminology presented in this book [18, 19]. In addition, information theory provides a framework for merging or “fusing” information from these various sources.

As an example of opportunities within a particular modality, cryo-EM is described here. The objective in cryo-EM is the reconstruction of three-dimensional object densities from two-dimensional projections. The “object” is usually a large biomolecular structure such as a viral capsid, ion channel, or rhibosome. The added difficulty in cryo-EM is that the method of data collection does not usually couple the direction from which a projection is taken to the projection data itself. Therefore, the added difficulty of simultaneously obtaining projection directions and reconstruction exists. This is a problem of not only reconstructing a density in $\mathbb{R}^3$ but also assigning and refining probabilities on $SO(3)$ that describe the projection directions and how the projections are rotated in the image plane relative to the body-fixed coordinates of the three-dimensional density. The density of the object that is being reconstructed as well as the experimental projections can be taken as pdfs on $\mathbb{R}^3$ and marginals on copies of $\mathbb{R}^2$, respectively. An initial pdf on $SO(3)$ may be used to assign projection directions to the obtained projections. Ultimately, this pdf should converge to one consisting of peaks corresponding to the actual projection directions that gave rise to the images. This convergence could be information-driven, in the sense that the mutual information between pairs of images can be computed under optimal alignment (superposition under rigid-body motion in the plane so as to maximize mutual information). Then the relative relationship between projection directions (i.e., determining if they are close or far from each other) can be assessed using the mutual information between the optimally superimposed images. Stochastic issues in cryo-EM are addressed in [11, 14] and references therein.

22.2.3 Evaluation of Human Motor Skills

Another area in which the methods of this book may find applications is in evaluation of human motor skills when performing tele-operation procedures. Such could be in the context of remote operations in space, such as the robotic repair of satellites under human control [21], or in robotic surgery, which is the emphasis here. In particular, a new area of growing interest is the "language of surgery" [8, 16]. In this research area, expert surgeons perform operations using a medical robotic system, which records every movement and the forces and torques experienced. Though not currently articulated in Lie-theoretic terminology, the above problem is a perfect example of how the methods in this book might be applied in the future.

Let the normalized time interval $[0, 1]$ parameterize the surgical task from the beginning to the end. From an ensemble of such paths that are recorded in the space consisting of all tool poses, g, and wrenches, w (six-dimensional vector of forces and torques), $SE(3) \times se^*(3)$, it is possible to generate an indexed set of probabilities $f(g, w; t)$ that describe the range of expert performance in a surgical task with $t \in [0, 1]$ denoting a particular value of normalized time.[1] Then as a medical student or resident trains to perform the procedure, an individual trajectory that they generate, $(g_s(t), w_s(t))$, can be evaluated as

$$P \doteq \int_0^1 f(g_s(t), w_s(t); t)\, dt$$

to assess overall performance. The higher the value of P, the closer their single performance is the mode behavior of the expert. Or, if an ensemble of student trajectories are performed resulting in $f_s(g, w; t)$, then costs such as

$$c_1(t) \doteq \int_{SE(3)\times se^*(3)} |f_s(g, w; t) - f(g, w; t)|^2\, dg\, dw$$

or

$$c_2(t) \doteq \int_{SE(3)\times se^*(3)} f_s(g, w; t) \log \frac{f_s(g, w; t)}{f(g, w; t)}\, dg\, dw$$

or any of the generalized information measures discussed in Chapter 17 can be used to evaluate ensemble performance.

22.2.4 Deconvolution over Lie Groups

A number of problems that arise in applications require solving the convolution equation

$$(k * f)(g) = h(g)$$

for $f(g)$ where $g \in G$, a Lie group, where $k(g)$ and $h(g)$ are given functions. The author initially studied this problem in the context of designing robot arms for the case when

[1] The space $se^*(3)$ is the dual space of $se(3)$, both of which can be identified with $\mathbb{R}^6$ by an appropriate $\vee$ operation.

$G = SE(2)$ [1], and others have made more recent advances [6, 20] that have appeared in the information theory literature. In general, exact solutions are not possible, and some form of regularization is required.

Another variation of this problem is the solution of the nonlinear convolution equation

$$(f * f)(g) = h(g)$$

which was studied in [7] in the context of robot arms where $G = SE(3)$. The use of methods from harmonic analysis on groups and the convolution theorem play central roles in addressing both problems.

22.2.5 Quantum Information, Computing, Estimation, and Control

The topics of quantum information theory, quantum computing, and estimating and control of quantum systems have received considerable attention in the literature over the past decade. Indeed, so many works have been published that it would be impossible to provide a complete survey without devoting a whole book to these topics. Several recent books that provide comprehensive overviews of the problems in these fields include [9, 10, 12]. Classical works that address quantum estimation and measurement include [2–4]. Quantum control is addressed in many works, including [5, 13, 15, 17]. In these topics, the concepts of Brownian motion, integration, and probability densities on unitary groups have a role, and hence the tools discussed in Chapters 12, 16, 19, and 20 may find applications.

References

1. Chirikjian, G.S., “Fredholm integral equations on the Euclidean motion group.” *Inverse Problems* 12, pp. 579–599, 1996.
2. Davies, E.B., *Quantum Theory of Open Systems*, Academic Press, New York, 1976.
3. Helstrom, C.W., *Quantum Detection and Estimation Theory*, Academic Press, New York, 1976.
4. Holevo, A.S., *Statistical Structure of Quantum Theory*, Springer, New York, 2001.
5. Khaneja, N., Brockett, R., Glaser, S.J., “Time optimal control in spin systems,” *Phys. Rev. A*, 63, 032308, 2001.
6. Koo, J.-Y., Kim, P.T., “Asymptotic minimax bounds for stochastic deconvolution over groups,” *IEEE Trans. Inform. Theory*, 54(1), pp. 289–298, 2008.
7. Kyatkin, A.B., Chirikjian, G.S., “Regularization of a nonlinear convolution equation on the Euclidean group,” *Acta Appl. Math*, 53, pp. 89–123, 1998.
8. Lin, H.C., Shafran, I., Yuh, D., Hager, G.D., “Towards automatic skill evaluation: Detection and segmentation of robot-assisted surgical motions,” *Computer Aided Surgery*, 11(5), pp. 220–230, 2006.
9. Marinescu, D.C., Marinescu, G.M., *Classical and Quantum Information*, Academic Press, New York, 2012.
10. Nielsen, M.A., Chuang, I.L., *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.
11. Park, W., Madden, D.R., Rockmore, D.N., Chirikjian, G.S., “Deblurring of class-averaged images in single-particle electron microscopy,” *Inverse Problems*, 26(3), 035002, 2010.
12. Schumacher, B., Westmoreland, M., *Quantum Processes, Systems, and Information*, Cambridge University Press, Cambridge, 2010.
13. Shapiro, M., Brumer, P., *Principles of the Quantum Control of Molecular Processes*, Wiley-VCH, Weinhein, 2003.

14. Singer, A., “Angular synchronization by eigenvectors and semidefinite programming,” *Appl. Comput. Harmon. Anal.* 30, pp. 20–36, 2011.
15. Vandersypen, L.M.K., Chuang, I.L., “NMR techniques for quantum control and computation,” *Rev. Mod. Phys.* 76, pp. 1037–1069, 2005.
16. Varadarajan, B., Reiley, C., Lin, H., Khudanpur, S., Hager, G.D., Data-derived models for segmentation with application to surgical assessment and training. Medical Image Computing and Computer-Assisted Intervention – MICCAI 2009, pp. 426–434, 2009.
17. Wiseman, H.M., *Quantum Measurement and Control*, Cambridge University Press, 2009.
18. Yan, Y., Chirikjian, G.S., “A Gaussian packing model for phasing in macromolecular crystallography,” *BIOCOMP*, 2011.
19. Yan, Y., Chirikjian, G.S., “Molecular replacement for multi-domain structures using packing models,” *Proceedings of the ASME 2011 International Design Engineering Technical Conferences & Computers and Information in Engineering Conference* (*IDETC/CIE 2011*), paper DETC2011-48583, Washington, DC, August 28–31, 2011.
20. Yazici, B., “Stochastic deconvolution over groups,” *IEEE Trans. Inform. Theory*, 50, pp. 494–510, 2004.
21. Zimmerman, W., Backes, P., Chirikjian, G., “Telerobot control mode performance assessment,” *Adv. Astron. Sci.*, 78, pp. 305–318, 1992.

Index

G.S. Chirikjian, *Stochastic Models, Information Theory, and Lie Groups, Volume 2: Analytic Methods and Modern Applications*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4944-9,

Applied and Numerical Harmonic Analysis

J.M. Cooper: *Introduction to Partial Differential Equations with MATLAB* (ISBN 978-0-8176-3967-9)

C.E. D'Attellis and E.M. Fernández-Berdaguer: *Wavelet Theory and Harmonic Analysis in Applied Sciences* (ISBN 978-0-8176-3953-2)

H.G. Feichtinger and T. Strohmer: *Gabor Analysis and Algorithms* (ISBN 978-0-8176-3959-4)

T.M. Peters, J.H.T. Bates, G.B. Pike, P. Munger, and J.C. Williams: *The Fourier Transform in Biomedical Engineering* (ISBN 978-0-8176-3941-9)

A.I. Saichev and W.A. Woyczyński: *Distributions in the Physical and Engineering Sciences* (ISBN 978-0-8176-3924-2)

R. Tolimieri and M. An: *Time-Frequency Representations* (ISBN 978-0-8176-3918-1)

G.T. Herman: *Geometry of Digital Spaces* (ISBN 978-0-8176-3897-9)

A. Procházka, J. Uhlíř, P.J.W. Rayner, and N.G. Kingsbury: *Signal Analysis and Prediction* (ISBN 978-0-8176-4042-2)

J. Ramanathan: *Methods of Applied Fourier Analysis* (ISBN 978-0-8176-3963-1)

A. Teolis: *Computational Signal Processing with Wavelets* (ISBN 978-0-8176-3909-9)

W.O. Bray and C.V. Stanojević: *Analysis of Divergence* (ISBN 978-0-8176-4058-3)

G.T Herman and A. Kuba: *Discrete Tomography* (ISBN 978-0-8176-4101-6)

J.J. Benedetto and P.J.S.G. Ferreira: *Modern Sampling Theory* (ISBN 978-0-8176-4023-1)

A. Abbate, C.M. DeCusatis, and P.K. Das: *Wavelets and Subbands* (ISBN 978-0-8176-4136-8)

L. Debnath: *Wavelet Transforms and Time-Frequency Signal Analysis* (ISBN 978-0-8176-4104-7)

K. Gröchenig: *Foundations of Time-Frequency Analysis* (ISBN 978-0-8176-4022-4)

D.F. Walnut: *An Introduction to Wavelet Analysis* (ISBN 978-0-8176-3962-4)

O. Bratteli and P. Jorgensen: *Wavelets through a Looking Glass* (ISBN 978-0-8176-4280-8)

H.G. Feichtinger and T. Strohmer: *Advances in Gabor Analysis* (ISBN 978-0-8176-4239-6)

O. Christensen: *An Introduction to Frames and Riesz Bases* (ISBN 978-0-8176-4295-2)

L. Debnath: *Wavelets and Signal Processing* (ISBN 978-0-8176-4235-8)

J. Davis: *Methods of Applied Mathematics with a MATLAB Overview* (ISBN 978-0-8176-4331-7)

G. Bi and Y. Zeng: *Transforms and Fast Algorithms for Signal Analysis and Representations* (ISBN 978-0-8176-4279-2)

J.J. Benedetto and A. Zayed: *Sampling, Wavelets, and Tomography* (ISBN 978-0-8176-4304-1)

E. Prestini: *The Evolution of Applied Harmonic Analysis* (ISBN 978-0-8176-4125-2)

O. Christensen and K.L. Christensen: *Approximation Theory* (ISBN 978-0-8176-3600-5)

L. Brandolini, L. Colzani, A. Iosevich, and G. Travaglini: *Fourier Analysis and Convexity* (ISBN 978-0-8176-3263-2)

W. Freeden and V. Michel: *Multiscale Potential Theory* (ISBN 978-0-8176-4105-4)

O. Calin and D.-C. Chang: *Geometric Mechanics on Riemannian Manifolds* (ISBN 978-0-8176-4354-6)

J.A. Hogan and J.D. Lakey: *Time-Frequency and Time-Scale Methods* (ISBN 978-0-8176-4276-1)

C. Heil: *Harmonic Analysis and Applications* (ISBN 978-0-8176-3778-1)

K. Borre, D.M. Akos, N. Bertelsen, P. Rinder, and S.H. Jensen: *A Software-Defined GPS and Galileo Receiver* (ISBN 978-0-8176-4390-4)

T. Qian, V. Mang I, and Y. Xu: *Wavelet Analysis and Applications* (ISBN 978-3-7643-7777-9)

Applied and Numerical Harmonic Analysis (Cont'd)

G.T. Herman and A. Kuba: *Advances in Discrete Tomography and Its Applications* (ISBN 978-0-8176-3614-2)

M.C. Fu, R.A. Jarrow, J.-Y. J. Yen, and R.J. Elliott: *Advances in Mathematical Finance* (ISBN 978-0-8176-4544-1)

O. Christensen: *Frames and Bases* (ISBN 978-0-8176-4677-6)

P.E.T. Jorgensen, K.D. Merrill, and J.A. Packer: *Representations, Wavelets, and Frames* (ISBN 978-0-8176-4682-0)

M. An, A.K. Brodzik, and R. Tolimieri: *Ideal Sequence Design in Time-Frequency Space* (ISBN 978-0-8176-4737-7)

B. Luong: *Fourier Analysis on Finite Abelian Groups* (ISBN 978-0-8176-4915-9)

S.G. Krantz: *Explorations in Harmonic Analysis* (ISBN 978-0-8176-4668-4)

G.S. Chirikjian: *Stochastic Models, Information Theory, and Lie Groups, Volume 1* (ISBN 978-0-8176-4802-2)

C. Cabrelli and J.L. Torrea: *Recent Developments in Real and Harmonic Analysis* (ISBN 978-0-8176-4531-1)

M.V. Wickerhauser: *Mathematics for Multimedia* (ISBN 978-0-8176-4879-4)

P. Massopust and B. Forster: *Four Short Courses on Harmonic Analysis* (ISBN 978-0-8176-4890-9)

O. Christensen: *Functions, Spaces, and Expansions* (ISBN 978-0-8176-4979-1)

J. Barral and S. Seuret: *Recent Developments in Fractals and Related Fields* (ISBN 978-0-8176-4887-9)

O. Calin, D. Chang, K. Furutani, and C. Iwasaki: *Heat Kernels for Elliptic and Sub-elliptic Operators* (ISBN 978-0-8176-4994-4)

C. Heil: *A Basis Theory Primer* (ISBN 978-0-8176-4686-8)

J.R. Klauder: *A Modern Approach to Functional Integration* (ISBN 978-0-8176-4790-2)

J. Cohen and A. Zayed: *Wavelets and Multiscale Analysis* (ISBN 978-0-8176-8094-7)

D. Joyner and J.-L. Kim: *Selected Unsolved Problems in Coding Theory* (ISBN 978-0-8176-8255-2)

J.A. Hogan and J.D. Lakey: *Duration and Bandwidth Limiting* (ISBN 978-0-8176-8306-1)

G. Chirikjian: *Stochastic Models, Information Theory, and Lie Groups, Volume 2* (ISBN 978-0-8176-4943-2)