Algebraic Statistics

Seth Sullivant

NORTH CAROLINA STATE UNIVERSITY

E-mail address: smsulli2@ncsu.edu
Contents

Preface xi

Chapter 1. Introduction 1
  §1.1. Discrete Markov Chain 2
  §1.2. Exercises 9

Chapter 2. Probability Primer 11
  §2.1. Probability 11
  §2.2. Random Variables and their Distributions 17
  §2.3. Expectation, Variance and Covariance 21
  §2.4. Multivariate Normal Distribution 28
  §2.5. Limit Theorems 31
  §2.6. Exercises 36

Chapter 3. Algebra Primer 39
  §3.1. Varieties 39
  §3.2. Ideals 43
  §3.3. Gröbner Bases 47
  §3.4. First Applications of Gröbner Bases 51
  §3.5. Computational Algebra Vignettes 54
  §3.6. Projective Space and Projective Varieties 59
  §3.7. Exercises 61

Chapter 4. Conditional Independence 65
  §4.1. Conditional Independence Models 66
Contents

§4.2. Primary Decomposition 73
§4.3. Primary Decomposition of CI Ideals 78
§4.4. Exercises 87

Chapter 5. Statistics Primer 89
§5.1. Statistical Models 89
§5.2. Types of Data 92
§5.3. Parameter Estimation 94
§5.4. Hypothesis Testing 98
§5.5. Bayesian Statistics 100
§5.6. Exercises 102

Chapter 6. Exponential Families 105
§6.1. Regular Exponential Families 106
§6.2. Discrete Regular Exponential Families 109
§6.3. Gaussian Regular Exponential Families 113
§6.4. Real Algebraic Geometry 115
§6.5. Algebraic Exponential Families 119
§6.6. Exercises 121

Chapter 7. Likelihood Inference 123
§7.1. Algebraic Solution of the Score Equations 124
§7.2. Concave Likelihood Functions 133
§7.3. Geometry of the ML-Degree 138
§7.4. Likelihood Ratio Tests 140
§7.5. Exercises 145

Chapter 8. The Cone of Sufficient Statistics 147
§8.1. Polyhedral Geometry 147
§8.2. Discrete Exponential Families 150
§8.3. Gaussian Exponential Families 156
§8.4. Exercises 162

Chapter 9. Fisher’s Exact Test 163
§9.1. Conditional Inference 163
§9.2. Markov Bases 167
§9.3. Markov Bases for Hierarchical Models 175
§9.4. Graver Bases and Applications 186
§9.5. Lattice Walks and Primary Decompositions 190
§9.6. Other Sampling Strategies 192
§9.7. Exercises 195

Chapter 10. Bounds on Cell Entries 197
§10.1. Motivating Applications 197
§10.2. Integer Programming and Gröbner Bases 203
§10.3. Quotient Rings and Gröbner Bases 205
§10.4. Linear Programming Relaxations 207
§10.5. Formulas for Bounds on Cell Entries 212
§10.6. Exercises 216

Chapter 11. Exponential Random Graph Models 219
§11.1. Basic Setup 219
§11.2. The Beta Model and Variants 222
§11.3. Models from Subgraphs Statistics 227
§11.4. Exercises 229

Chapter 12. Design of Experiments 231
§12.1. Designs 232
§12.2. Computations with the Ideal of Points 237
§12.3. The Gröbner Fan and Applications 239
§12.4. 2-level Designs and System Reliability 245
§12.5. Exercises 250

Chapter 13. Graphical Models 251
§13.1. Conditional Independence Description of Graphical Models 251
§13.2. Parametrizations of Graphical Models 258
§13.3. Failure of the Hammersley-Clifford Theorem 268
§13.4. Examples of Graphical Models from Applications 270
§13.5. Exercises 272

Chapter 14. Hidden Variables 275
§14.1. Mixture Models 276
§14.2. Hidden Variable Graphical Models 281
§14.3. The EM Algorithm 288
§14.4. Exercises 292

Chapter 15. Phylogenetic Models 295
Contents

§15.1. Trees and Splits 296
§15.2. Types of Phylogenetic Models 299
§15.3. Group-based Phylogenetic Models 306
§15.4. The General Markov Model 317
§15.5. The Allman-Rhodes-Draisma-Kuttler Theorem 323
§15.6. Exercises 326

Chapter 16. Identifiability 329
§16.1. Tools for Testing Identifiability 330
§16.2. Linear Structural Equation Models 337
§16.3. Tensor Methods 342
§16.4. State Space Models 347
§16.5. Exercises 353

Chapter 17. Model Selection and Bayesian Integrals 357
§17.1. Information Criteria for Regular Models 358
§17.2. Resolution of Singularities and the Log Canonical Threshold 359
§17.3. Information Criteria for Singular Models 359
§17.4. Exercises 359

Chapter 18. MAP Estimation 361
§18.1. Hidden Markov Models 362
§18.2. The Viterbi Algorithm and Tropical Arithmetic 365
§18.3. MAP Estimation, Parametric Inference, and Normal Fans 367
§18.4. Polytope Algebra 369
§18.5. Exercises 370

Chapter 19. Finite Metric Spaces 371
§19.1. Metric Spaces and The Cut Polytope 371
§19.2. Tree Metrics 378
§19.3. Finding an Optimal Tree Metric 381
§19.4. Toric Varieties Associated to Finite Metric Spaces 385
§19.5. Exercises 387

Bibliography 389
Preface

Algebraic statistics is a relatively young field based on the observation that many questions in statistics are fundamentally problems of algebraic geometry. This observation is now at least twenty years old and the time seems ripe for a comprehensive book that could be used as a graduate textbook on this topic.

Algebraic statistics represents an unusual intersection of mathematical disciplines, and it is rare that a mathematician or statistician would come to work in this area already knowing both the relevant algebraic geometry and statistics. I have tried to provide sufficient background in both algebraic geometry and statistics so that a newcomer to either area would be able to benefit from using the book to learn algebraic statistics. Of course both statistics and algebraic geometry are huge subjects and the book only scratches the surface on either of these disciplines.

I made the conscious decision to try to introduce algebraic concepts alongside statistical concepts where they can be applied, rather than having long introductory chapters on algebraic geometry, statistics, combinatorial optimization, etc. that must be waded through first, or flipped back to over and over again, before all the pieces are put together. Besides the three introductory chapters on probability, algebra, and statistics (Chapters 2, 3, 5, respectively), this perspective is followed throughout the text. While this choice might make the book less useful as a reference book on algebraic statistics, I hope that it will make the book more useful as an actual textbook that students and faculty plan to learn from.

Here is a breakdown of material that appears in each chapter in the book.
Chapter 1 is an introductory chapter that shows how ideas from algebra begin to arise when considering elementary problems in statistics. These ideas are illustrated with the simple example of a Markov Chain. As statistical and algebraic concepts are introduced the chapter makes forward reference to other sections and chapters in the book where those ideas are highlighted in more depth.

Chapter 2 provides necessary background information in probability theory which is useful throughout the book. This starts from the axioms of probability, works through familiar and important examples of discrete and continuous random variables, and includes limit theorems that are useful for asymptotic results in statistics.

Chapter 3 provides necessary background information in algebra and algebraic geometry, with an emphasis on computational aspects. This starts from definitions of polynomial rings, their ideals, and the associated varieties. Examples are typically drawn from probability theory to begin to show how tools from algebraic geometry can be applied to study families of probability distributions. Some computational examples using computer software packages are given.

Chapter 4 is an in depth treatment of conditional independence, an important property in probability theory that is essential for the construction of multivariate statistical models. To study implications between conditional independence models, we introduce primary decomposition, an algebraic tool for decomposing solutions of polynomial equations into constituent irreducible pieces.

Chapter 5 provides some necessary background information in statistics. It includes some examples of basic statistical models and hypothesis tests that can be performed in reference to those statistical models. This chapter has significantly fewer theorems than other chapters and is primarily concerned with introducing the philosophy behind various statistical ideas.

Chapter 6 provides a detailed introduction to exponential families, an important general class of statistical models. Exponential families are related to familiar objects in algebraic geometry like toric varieties. Nearly all models that we study in this book arise by taking semialgebraic subsets of the natural parameter space of some exponential family, making these models extremely important for everything that follows. Such models are called algebraic exponential families.

Chapter 7 gives an in depth treatment of maximum likelihood estimation from an algebraic perspective. For many algebraic exponential families maximum likelihood estimation amounts to solving a system of polynomial equations. For a fixed model and generic data, the number of critical points
of this system is fixed and gives an intrinsic measure of the complexity of calculating maximum likelihood estimates.

Chapter 8 concerns the geometry of the cone of sufficient statistics of an exponential family. This geometry is important for maximum likelihood estimation: maximum likelihood estimates exist in an exponential family if and only if the data lies in the interior of the cone of sufficient statistics. This chapter also introduces techniques from polyhedral and general convex geometry which are useful in subsequent chapters.

Chapter 9 describes Fisher’s exact test, a hypothesis test used for discrete exponential families. A fundamental computational problem that arises is that of generating random lattice points from inside of convex polytopes. Various methods are explored including methods that connect the problem to the study of toric ideals. This chapter also introduces the hierarchical models, a special class of discrete exponential family.

Chapter 10 concerns the computation of upper and lower bounds on cell entries in contingency tables given some lower dimensional marginal totals. One motivation for the problem comes from the sampling problem of Chapter 9: fast methods for computing bounds on cell entries can be used in sequential importance sampling, an alternate strategy for generating random lattice points in polytopes. A second motivation comes from certain data privacy problems associated with contingency tables. The chapter connects these optimization problems to algebraic methods for integer programming.

Chapter 11 describes the exponential random graphs models, a family of statistical models used in the analysis of social networks. While these models fit in the framework of the exponential families introduced in Chapter 6, they present a particular challenge for various statistical analyses because they have a large number of parameters and the underlying sample size is small. They also present a novel area of study for application of Fisher’s exact test and studying the existence of maximum likelihood estimates.

Chapter 12 concerns the use of algebraic methods for the design of experiments. Specific algebraic tools that are developed include the Gröbner fan of an ideal. Connections between the design of experiments and the toric ideals of Chapters 9 and 10 are also explored.

Chapter 13 introduces the graphical statistical models. In graphical models, complex interactions between large collections of random variables are constructed using graphs to specify interactions between subsets of the random variables. A key feature of these models is that they can be specified either by parametric descriptions or via conditional independence constructions. This chapter compares these two perspectives via the primary decompositions from Chapter 4.
Chapter 14 provides a general introduction of statistical models with hidden variables. Graphical models with hidden variables are widely used in statistics, but the presence of hidden variables complicates their use. This chapter starts with some basic examples of these constructions, including mixture models. Mixture models are connected to secant varieties in algebraic geometry.

Chapter 15 concerns the study of phylogenetic models, certain hidden variable statistical models used in computational biology. The chapter highlights various algebraic issues involved with studying these models and their equations.

Chapter 16 concerns the identifiability problem for parametric statistical models. Identifiability of model parameters is an important structural feature of a statistical model. Identifiability is studied for graphical models with hidden variables and structural equation models. Tools are also developed for addressing identifiability problems for dynamical systems models.

Chapter 17 concerns the topic of model selection. This is a well-developed topic in statistics and machine learning, but becomes complicated in the presence of model singularities that arise when working with models with hidden variables. The mathematical tools to develop corrections come from studying the geometry of certain integrals, and resolution of singularities of associated varieties. These singularity issues arise precisely at the points of parameter space where the model parameters are not identifiable.

Chapter 18 concerns the geometry of maximum a posteriori (MAP) estimation of the hidden states in a model. This involves performing computations in the tropical semiring. The related parametric inference problem studies how the MAP estimate changes as underlying model parameters change, and is related to problems in convex geometry.

Chapter 19 is a study of the geometry of finite metric spaces. Of special interest are the set of tree metrics and ultrametrics which play an important role in phylogenetics. More generally, the set of cut metrics are closely related to hierarchical models studied earlier in the book.

My first attempt at a book on algebraic statistics was in 2007 with Mathias Drton. That project eventually led to the set of lecture notes [DSS09] from our week long short course with Bernd Sturmfels at the Mathematisches Forschungsinstitut Oberwolfach (MFO). As part of Mathias’s and my first attempt at writing, we produced two background chapters on probability and algebra which were not used in [DSS09] and which Mathias has graciously allowed me to use here.
Chapter 1

Introduction

Algebraic statistics advocates using tools from algebraic geometry, commutative algebra, combinatorics and related tools from symbolic computation to address problems in probability theory, statistics, and their applications. The connection between the algebra and statistics sides goes both directions and statistical problems with algebraic character help to focus new research directions in algebra.

While the area called algebraic statistics is relatively new, connections between algebra and statistics are old going back to the beginnings of statistics. For instance, the constructions of different types of combinatorial designs use group theory and finite geometries, algebraic structures being used to describe central limit theorems in complex settings, or representation theoretic methods in the analysis of discrete data. In spite of these older contact points, the term algebraic statistics has primarily been used for the connection between algebraic geometry and statistics which is the focus of this book, a topic that has developed since the mid 1990’s.

Historically, the main thread of algebraic statistics started with the work of Diaconis and Sturmfels on conditional inference, establishing a connection between random walks on sets of contingency tables and generating sets of toric ideals. Inspired by Pistone, Riccomagno, and Wynn explored connections between algebraic geometry and the design of experiments, describing their work in the monograph, which coined the name algebraic statistics. Since then there has been an explosion of research in the area. The goal of this book is to illustrate and explain some of the advances in algebraic statistics highlighting the main areas of research directions since those first projects. Of course, it is impossible to highlight
everything, and new results are constantly being added, but we have tried to hit major points.

Whenever two fields come together, it is tempting to form a “dictionary” connecting the two areas. In algebraic statistics there are some concepts in statistics which directly correspond to objects in algebraic geometry, but there are many other instances where we only have a very rough correspondence. In spite of this, it can be useful to keep these correspondences in mind, some of which are illustrated in the table below.

<table>
<thead>
<tr>
<th>Probability/Statistics</th>
<th>Algebra/Geometry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probability distribution</td>
<td>Point</td>
</tr>
<tr>
<td>Statistical Model</td>
<td>(Semi)Algebraic set</td>
</tr>
<tr>
<td>Exponential family</td>
<td>Toric variety</td>
</tr>
<tr>
<td>Conditional inference</td>
<td>Lattice points in polytopes</td>
</tr>
<tr>
<td>Maximum likelihood estimation</td>
<td>Polynomial optimization</td>
</tr>
<tr>
<td>Model selection</td>
<td>Geometry of singularities</td>
</tr>
<tr>
<td>Multivariate Gaussian model</td>
<td>Spectrahedral geometry</td>
</tr>
<tr>
<td>Phylogenetic model</td>
<td>Tensor networks</td>
</tr>
<tr>
<td>MAP estimates</td>
<td>Tropical geometry</td>
</tr>
</tbody>
</table>

The goal of this book is to illustrate these connections. In the remainder of this chapter we illustrate some of the ways that algebra arises when thinking about statistics problems by illustrating it with the example of a discrete Markov chain. This is only intended as a single illustrative example to highlight some of the insights and connections we make in algebraic statistics. The reader should not concern themselves if they do not understand everything. More elementary background material will appear in later chapters.

1.1. Discrete Markov Chain

Let $X_1, X_2, \ldots, X_m$ be a sequence of random variables on the same state space $\Sigma$, a finite alphabet. Since these are random variables there is a joint probability distribution associated with them, i.e. to each tuple $x_1, \ldots, x_m \in \Sigma$ there is a real number

$$P(X_1 = x_1, X_2 = x_2, \ldots, X_m = x_m)$$

which is the probability that $X_1 = x_1, X_2 = x_2, \ldots, \text{et cetera}$. To be a probability distribution, these numbers are between 0 and 1, and the sum over all $(x_1, \ldots, x_m) \in \Sigma^m$ is one.

**Definition 1.1.1.** The sequence $X_1, X_2, \ldots, X_m$ is called a Markov chain if for all $i = 3, \ldots, m$ and for all $x_1, \ldots, x_i \in \Sigma$

$$(1.1.1) \quad P(X_i = x_i | X_1 = x_1, \ldots, X_{i-1} = x_{i-1}) = P(X_i = x_i | X_{i-1} = x_{i-1}).$$
1.1. Discrete Markov Chain

In other words, in a Markov chain, the conditional distribution of $X_i$ given all predecessors only depends on the most recent predecessor. Or said in another way, adding knowledge further back in the chain does not help in predicting the next step in the chain.

Let us consider the model of a discrete Markov chain, that is for a fixed $m$ and $\Sigma$, the set of all probability distributions consistent with the condition in Definition [1.1.1]. As for many statistical models, the underlying description of this model is fundamentally algebraic in character: in particular, it is described implicitly by polynomial constraints on the joint distribution. Here a specific example.

**Example 1.1.2.** Let $m = 3$ and $\Sigma = \{0, 1\}$ in the Markov chain model. We can naturally associate a probability distribution in this context with a point in $\mathbb{R}^8$. Indeed, the joint distribution is determined by the 8 values $P(X_1 = i, X_2 = j, X_3 = k)$ for $i, j, k \in \{0, 1\}$. We use the following shorthand for this probability distribution: $p_{ijk} = P(X_1 = i, X_2 = j, X_3 = k)$. Then a joint probability distribution for three binary random variables is a point

$$(p_{000}, p_{001}, p_{010}, p_{011}, p_{100}, p_{101}, p_{110}, p_{111}) \in \mathbb{R}^8.$$  

Computing conditional distributions gives rational expressions in terms of the joint probabilities:

$$P(X_3 = k|X_1 = i, X_2 = j) = \frac{p_{ijk}}{p_{ij+}}$$

where the “+” in the subscript denotes a summation, e.g. $p_{ij+} = \sum_{k \in \{0, 1\}} p_{ijk}$. The condition from [1.1.1] for a distribution to come from a Markov chain translates into the rational expression

$$(1.1.2) \quad \frac{p_{ijk}}{p_{ij+}} = \frac{p_{i'jk}}{p_{i'+j}}$$

for all $i, j, k \in \{0, 1\}$. We can also represent this as

$$\frac{p_{ijk}}{p_{ij+}} = \frac{p_{i'jk}}{p_{i'+j}}$$

for all $i, i', j, k \in \{0, 1\}$ by setting two different left hand sides of Equation [1.1.2] equal to each other for the same values of $j$ and $k$. Clearing denominators to get polynomial expressions and expanding and simplifying these expressions yields the following characterization of distributions that are Markov chains:

A vector $p = (p_{000}, p_{001}, p_{010}, p_{011}, p_{100}, p_{101}, p_{110}, p_{111}) \in \mathbb{R}^8$ is the probability distribution from the Markov chain model if and only if it satisfies

1. $p_{ijk} \geq 0$ for all $i, j, k \in \{0, 1\}$,
2. $\sum_{i,j,k \in \{0,1\}} p_{ijk} = 1$, 


1. Introduction

\( p_{000}p_{101} - p_{001}p_{100} = 0, \) and
\( p_{010}p_{111} - p_{011}p_{110} = 0. \)

**Remark 1.1.3.** Example 1.1.2 illustrates a theme that will recur throughout the book and is a hallmark of algebraic statistics: statistical models are semialgebraic sets, that is, they can be represented as the solutions sets of systems of polynomials equations and inequalities.

The Markov chain model is an example of a conditional independence model, that is, it is specified by conditional independence constraints on the random variables in the model. Equation 1.1.1 is equivalent to the conditional independence statement

\[ X_i \perp \perp (X_1, \ldots, X_{i-2}) | X_{i-1}. \]

Conditional independence models will be studied in more detail in Chapter 4 and play an important role in the theory of graphical models in Chapter 13. In spite of the commonality of conditional independence models, it is more typical to specify models parametrically, and the Markov chain model also has a natural parametrization. To “discover” the parametrization, we use a standard factorization for joint distributions into their conditional distributions:

\[ P(X_1 = x_1, \ldots, X_m = x_m) = \prod_{i=1}^{m} P(X_i = x_i | X_1 = x_1, \ldots, X_{i-1} = x_{i-1}) \]

then substitute in using Equation 1.1.1 to get

\[ P(X_1 = x_1, \ldots, X_m = x_m) = \prod_{i=1}^{m} P(X_i = x_i | X_{i-1} = x_{i-1}). \]

To discover the parametrization, we just treat each of the individual conditional distributions as free parameters. Let \( \pi_{j_1} = P(X_1 = j_1) \) and let \( \alpha_{i,j,k} = P(X_i = k | X_{i-1} = j) \). So we have the Markov chain model described by a polynomial parametrization:

\[ P_{j_1, j_2, \ldots, j_m} = \pi_{j_1} \prod_{i=2}^{m} \alpha_{i,j_{i-1}, j_i}. \]

**Remark 1.1.4.** The Markov chain example illustrates another key feature of algebraic statistics highlighted throughout the book: many parametric statistical models have their parametric representations given by polynomial functions of the parameters.

As we have seen, algebra plays an important role in characterizing the distributions that belong to a statistical model. Various data analytic questions associated with using the statistical model also have an algebraic character. Here we discuss two such problems (which we state informally): fitting
the model to the data and determining whether or not the model fits the data well.  

There are many possible notions for fitting a model to data. Here we use the frequentist maximum likelihood estimate. First of all, there are many different types of data that one might receive that might be compatible with the analysis of a particular statistical model. Here we focus on the simplest which is independent identically distributed data. That is, we assume there is some true unknown distribution \( p \) according to which all of our data are independent samples from this underlying distribution. Focusing on the case of the Markov chain model of length 3 on a binary alphabet \( \Sigma = \{0, 1\} \), the data then would be collection of elements of \( \{0, 1\}^3 \) for example:

\[
000, 010, 110, 000, 101, 110, 100, 010, 110, 111, 000, 000, 010
\]

would be a data set with 13 data points. Since we assume the data is generated independently from the same underlying distribution, the probability of observing the data really only depends on the vector of counts \( u \), whose entry \( u_{ijk} \) records the number of times the configuration \( ijk \) occurred in the data. In this case we have

\[
(u_{000}, u_{001}, u_{010}, u_{011}, u_{100}, u_{101}, u_{110}, u_{111}) = (4, 0, 3, 0, 1, 1, 3, 1).
\]

The probability of observing the dataset \( D \) given the true unknown probability distribution \( p \) is then

\[
P(\text{Data}) = \prod_{ijk} p_{ijk}^{u_{ijk}} =: L(p|u).
\]

This probability is called the likelihood function. The data \( u \) is given to us and fixed, the probability \( p \) is the unknown.

The maximum likelihood estimate is the probability distribution in our model that maximizes the likelihood function. That is, for a given probabilistic model \( \mathcal{M} \), the maximum likelihood estimation problem is to compute

\[
\arg \max_{p \in \mathcal{M}} L(p|u) \quad \text{subject to} \ p \in \mathcal{M}.
\]

The argmax function asks for the maximizer rather than the maximum value of the function. For our discrete Markov chain model, we have representations of the model in both implicit and parametric forms, which means we can express this as either a constrained or unconstrained optimization problem, i.e.

\[
\arg \max \prod_{ijk} p_{ijk}^{u_{ijk}} \quad \text{subject to} \ p_{ijk} \geq 0, \ \sum_{ijk} p_{ijk} = 1, \text{ and }
\]

\[
p_{000}p_{101} - p_{001}p_{100} = p_{010}p_{111} - p_{011}p_{110} = 0.
\]
On the other hand, we can also express this as an unconstrained optimization problem, directly plugging in the parametrized form of the Markov chain.

\[
\arg\max \prod_{ijk} (\pi_i \alpha_{ij} \beta_{jk})^{u_{ijk}}.
\]

Note this optimization problem is not a completely unconstrained optimization problem, because we need \( \pi \) to be a probability distribution and \( \alpha \) and \( \beta \) to be conditional distribution. That is, we have the constraints

\[
\pi_i \geq 0, \quad \sum_i \pi_i = 1, \quad \alpha_{ij} \geq 0, \quad \sum_j \alpha_{ij} = 1, \quad \beta_{jk} \geq 0, \quad \sum_k \beta_{jk} = 1.
\]

A typical direct strategy to compute the maximum likelihood estimator is to compute the logarithm of the likelihood, and compute partial derivatives and set them equal to zero. Since our model is algebraic in nature, these score equations (or critical equations) give an algebraic system of polynomial equations which can be solved using symbolic techniques or numerically in specific instances. In this particular situation, there is a closed form rational expression for the maximum likelihood estimates. In terms of the parameters, these are

\[
(1.1.3) \quad \hat{\pi}_i = \frac{u_{i++}}{u_{++}}, \quad \hat{\alpha}_{ij} = \frac{u_{ij+}}{u_{i++}}, \quad \hat{\beta}_{jk} = \frac{u_{+jk}}{u_{+j+}}
\]

where

\[
u_{i++} = \sum_{j,k} u_{ijk}, \quad u_{++} = \sum_{i,j,k} u_{ijk}, \quad u_{ij+} = \sum_k u_{ijk}, \quad u_{+jk} = \sum_i u_{ijk}, \text{ etc.}
\]

In terms of probability distribution in the model we can multiply these together to get

\[
\hat{p}_{ijk} = \frac{u_{ij+} \cdot u_{+jk}}{u_{++} \cdot u_{+j+}}.
\]

In general, the score equations for a statistical model rarely have such simple closed form solutions – i.e. systems of polynomial equations often have multiple solutions. It is natural to ask: “For which statistical models does such a nice closed form solution arise?” “Can we say anything about the form of these closed form expressions?” Amazingly a complete, beautiful, yet still mysterious classification of models with rational formulas for maximum likelihood estimates exists and has remarkable connections to other areas in algebraic geometry. This was discovered by June Huh [Huh14] and will be explained in Chapter 7.

**Remark 1.1.5.** The classification of statistical models with rational maximum likelihood estimates illustrates a frequent point in algebraic statistics. Trying to classify and identify statistical models that satisfy some nice statistical property lead to interesting classification theorems in algebraic geometry and combinatorics.
Now that we have fit the model to the data, we can ask: how well does the model fit the data? In other words, do we think that the data was generated by some distribution in the model? In this case one often might be interested in performing a hypothesis test, to either accept or reject the model. (Caveat: usually in statistics we might only come to a conclusion about either rejecting the model or deciding that the test was inconclusive.)

Here is one typical way to try to test whether a given model fits the data. We instead pose the following question: Assuming that the true underlying distribution $p$ belongs to our model $\mathcal{M}$, among all data sets $v$ that could have been generated, what proportion of such data $v$ is more likely to have occurred than our observed data set $u$. From this we compute a $p$-value which might allow us to reject the hypothesis that the distribution $p$ actually belongs to the model $\mathcal{M}$. Essentially, we will reject data as coming from the model, if it had a (relatively) low probability of being generated from the model.

Of course, to measure the probability that a particular data vector $v$ appeared depends on the value of the (unknown) probability distribution $p$, and so it is impossible to directly measure the proportion from the previous paragraph. A key insight of Fisher’s, leading to Fisher’s Exact Test, is that for some statistical models, the dependence of the likelihood function on the data and the parameter values is only through a lower order linear function of the data vector. These lower order functions of the data are called sufficient statistics. Indeed, for a particular vector of counts $u$, for the two step Markov chain whose likelihood we viewed above, in terms of the parameters we have

$$P(u|\alpha, \beta, \gamma) = \prod_{ijk}(\pi_i \alpha_{ij} \beta_{jk})^{u_{ijk}}$$

$$= \left( \frac{n}{u} \right) \prod_{i,j}(\pi_i \alpha_{ij})^{u_{ij}+} \prod_{j,k} \beta_{jk}^{u_{jk}+}.$$}

The quantities $u_{ij+}, u_{+jk}$ with $i, j, k \in \Sigma$ are the sufficient statistics of the Markov chain model of length three. Note, since we have here written the probability of observing the vector of counts $u$, rather than an ordered list of observations, we include the multinomial coefficient in the likelihood. Fisher’s idea was that we can use this to pose a different question: among all possible data sets with the same sufficient statistics as the given data $u$ what proportion are more likely to occur than $u$?
From the standpoint of computing a probability, we are looking at the conditional probability distribution

\[ P(v|\alpha, \beta, \gamma, v_{ij+} = u_{ij+}, v_{+jk} = u_{+jk}) = \frac{n_v \prod_{i,j} (\pi_i \alpha_{ij})^{u_{ij+}} \prod_{j,k} \beta_{jk}^{u_{+jk}}}{\sum_v n_v \prod_{i,j} (\pi_i \alpha_{ij})^{u_{ij+}} \prod_{j,k} \beta_{jk}^{u_{+jk}}} \]

where the sum in the denominator is over all \( v \in \mathbb{N}^8 \) such that \( v_{ij+} = u_{ij+}, v_{+jk} = u_{+jk} \). Since the term that depends on \( p \) in this expression is the same in every summand, and equals the product in the numerator, we see that in fact

\[ P(v|\alpha, \beta, \gamma, v_{ij+} = u_{ij+}, v_{+jk} = u_{+jk}) = \frac{n_v}{\sum_v n_v} \]

and in particular, this probability does not depend on the unknown distribution \( p \). The fact that this probability does not depend on unknown distribution \( p \) is the reason for adding the condition “with the same sufficient statistics as the given data \( u \)”. It allows us to perform a hypothesis test without worrying about this unknown “nuisance parameter”.

Let

\[ \mathcal{F}(u) = \{ v \in \mathbb{N}^8 : v_{ij+} = u_{ij+}, v_{+jk} = u_{+jk} \text{ for all } i, j, k \} \]

that is, the set of all vectors of counts with the same sufficient statistics as \( u \). To carry out Fisher’s exact test amounts to computing the ratio

\[ \frac{\sum_{v \in \mathcal{F}(u)} \binom{n}{v} 1(\binom{n}{v} < \binom{n}{u}) \binom{n}{v}}{\sum_{v \in \mathcal{F}(u)} \binom{n}{v}} \]

where \( 1(\binom{n}{v} < \binom{n}{u}) \) denotes the indicator function of the event that \( \binom{n}{v} < \binom{n}{u} \).

The resulting number, the p-value of Fisher’s exact test, gives the probability that a random table drawn from \( \mathcal{F}(u) \) according to the generalized hypergeometric distribution (s.t. \( P(v) \propto \binom{n}{v} \)) has higher probability than the observed table \( u \). Of course, this raises all sorts of new questions, some of which we will explore in the present book. It is usually impossible to actually enumerate all the \( v \in \mathcal{F}(u) \) to calculate the sum, and one must find a way to generate them at random, using a sampling strategy. Note that the set \( \mathcal{F}(u) \) consists of the set of lattice points that satisfy a given system of linear equations and inequalities:

\[ \mathcal{F}(u) = \left\{ v \in \mathbb{Z}^8 : v_{ijk} \geq 0, \sum_k v_{ijk} = u_{ij+}, \text{ and } \sum_i v_{ijk} = u_{+jk} \right\} \]

This leads to the theory of Markov bases, studied in Chapter 9, and algebraic and combinatorial methods for sampling random lattice points in polytopes that allows one to apply Fisher’s exact test.
1.2. Exercises

**Exercise 1.1.** Derive the formula for the maximum likelihood estimates in the discrete Markov chain model from Equation [1.1.3]

**Exercise 1.2.** Call a Markov chain *homogeneous* if it satisfies the following extra condition:

\[ P(X_i = a | X_{i-1} = b) = P(X_j = a | X_{j-1} = b) \]

for all \( a, b \in \Sigma \) and \( i, j \in \{2, \ldots, n\} \).

(1) For \( n = 3 \) and \( \Sigma = \{0, 1\} \), find an implicit algebraic representation of the homogeneous Markov chain model.

(2) Find a parametric description of the model.

(3) Find closed form formulas for the maximum likelihood estimates in this model.

(4) Describe the minimal sufficient statistics of the model and the resulting polytope of data points satisfying the condition that those points have the same sufficient statistics as a given data point \( u \).
Probability Primer

Probability theory provides mathematical language to describe the observation of random quantities or quantities that arise in processes that are deterministic but too complicated to be predictable. This language of probability is fundamental to the design and evaluation of statistical methodology. In this chapter we review, at an elementary level, basic notions from probability theory such as random variables, expectation and limit theorems. We also define the normal or Gaussian distribution that will play a prominent role throughout the entire book. The discussion of the topics in this chapter will be brief and the reader will certainly benefit by consulting in-depth treatments of probability theory as found in [Bil95], [Chu01] or [Sho00].

2.1. Probability

Phrases such as “there is an 80% chance of rain this coming Saturday” testify to the fact that the concept of probability is omnipresent in our daily lives. Nevertheless it is not entirely straightforward to give a dictionary-definition of probability. Certainly, the probability of a coin toss resulting in heads being equal to 50% can be understood as a long-run frequency. If the coin is tossed repeatedly, then roughly 50% of the tosses will show heads. However, thinking of probability as a long-run frequency need not always be natural. For example, if the above statement about the probability of rain is to be interpreted in this way, then, strictly speaking, we would have to be able to relive this coming Saturday over and over again. Hence, it can sometimes be more appropriate to understand probability simply as the quantification of our belief about the occurrence of the event in question. Placing a bet on the event happening provides a way to quantify this belief.
We will not dwell on any further about the nature of probability and instead push towards mathematical abstraction, in which probability is turned into a mathematical object. This object is a map that assigns to each set of interest a non-negative real number, which is called the probability of the event represented by the set. Very reassuringly this framework to be presented next will lead to a theorem, the law of large numbers in §2.5, that recovers the interpretation in terms of long-run frequencies.

Before giving a first formal definition of probability, a clarification of language is in order. We will refer to a process that yields random outcomes as a random experiment. The set of all possible outcomes in such a random experiment is the sample space, denoted by Ω. An event is simply a subset A ⊆ Ω, and we say that the event A occurs if the random experiment results in an outcome ω ∈ A. The symbol Ψ(Ω) is used to denote the power set of the sample space Ω.

**Definition 2.1.1 (Countable sample spaces).** A probability measure on a finite or countably infinite sample space Ω is a map

$$P : Ψ(Ω) → [0, 1]$$

such that $P(Ω) = 1$ and

$$P\left( ∪_{i=1}^{∞} A_i \right) = ∑_{i=1}^{∞} P(A_i) \text{ if } A_i \cap A_j = ∅ \text{ for all } i \neq j.$$
for an increasing sequence of sets $A_1 \subseteq A_2 \subseteq \cdots$.

**Example 2.1.2** (Lottery). Suppose an urn contains 49 balls labelled by the integers 1 through 49. Six balls are drawn at random from this urn without replacement. What is the probability that exactly three of the balls show a number smaller than 10?

Assuming that the order in which the balls are drawn is not recorded, we can formalize the problem as follows. The sample space is the set of all six-element subsets of \([49] = \{1, \ldots, 49\}\), i.e.,

$$\Omega = \{A \subset [49] : \#A = 6\}.$$

The question then asks for the probability of the event

$$A = \{\{\omega_1, \ldots, \omega_6\} \in \Omega : \omega_i < 10, \ i = 1, 2, 3, \text{ and } \omega_i \geq 10, \ i = 4, 5, 6\}.$$

However, this question can be answered only if “drawing at random” is interpreted to specify a particular probability measure. As customary we will interpret the statement to mean that the probability measure $P$ assigns equal probability to each one of the

$$\#\Omega = \binom{49}{6} = 13,983,816$$

singletons $\{\omega\}$, $\omega \in \Omega$. This entails that the desired probability equals

$$(2.1.3) \quad P(A) = \frac{\#A}{\#\Omega} = \frac{9 \binom{40}{3}}{\binom{49}{6}} \approx 0.0593.$$

What if the order in which the balls are drawn was recorded? Clearly that would alter the sample space but does this change in sample space affect the probability of the considered event? The answer is no, and Exercise 2.1 asks you to go through the details of why the probability in question is still equal to the value found in (2.1.3).

Definition 2.1.1 was concerned with a finite or countably infinite sample space. However, when observing continuous quantities it is desirable to allow uncountably infinite sample spaces such as an interval. Unfortunately, it is then problematic to define probability measures on the power set $\mathcal{P}(\Omega)$.

**Proposition 2.1.3.** If the sample space in Definition 2.1.1 is allowed to be the uncountably infinite set $\Omega = [0, 1)$, then there does not exist a translation-invariant probability measure on $\mathcal{P}([0, 1))$.

**Proof.** Suppose $P$ was a translation-invariant probability measure on $\mathcal{P}([0, 1))$. Define $x, y \in [0, 1)$ to be equivalent if there exists a rational $q \in \mathbb{Q}$ such that
Choose a set $A$ that contains exactly one element of each equivalence class arising under this relation. For $q \in [0, 1) \cap \mathbb{Q}$, let

$$A_q = \{ q + a \mod 1 \mid a \in A \}.$$ 

Then the countably many sets $A_q$, $q \in \mathbb{Q}$, form a partition of $[0, 1)$. By translation-invariance of $P$, it must hold that

$$1 = P([0, 1)) = \sum_{q \in [0, 1) \cap \mathbb{Q}} P(A_q) = \sum_{q \in [0, 1) \cap \mathbb{Q}} P(A_0),$$

which is impossible. \hfill \Box

The inexistence of a ‘uniform distribution’ on $\mathcal{P}([0, 1))$ arises because an interval has too many subsets. The way around this problem is to define probability measures on suitable subsets of $\mathcal{P}(\Omega)$.

**Definition 2.1.4 (σ-Algebra).** A σ-algebra over a set $\Omega$ is a subset $\mathcal{A}$ of the power set $\mathcal{P}(\Omega)$ such that (i) $\Omega \in \mathcal{A}$, (ii) the complement $A^c \in \mathcal{A}$ if $A \in \mathcal{A}$, and (iii) a countable union $\bigcup_{i=1}^{\infty} A_i \in \mathcal{A}$ if $A_i \in \mathcal{A}$ for all $i \geq 1$.

**Definition 2.1.5 (Probability).** Let $\mathcal{A}$ be σ-algebra on a sample space $\Omega$. A probability measure on $(\Omega, \mathcal{A})$ is a map

$$P : \mathcal{A} \to [0, 1]$$

$$A \mapsto P(A)$$

such that $P(\Omega) = 1$ and

$$P\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i) \quad \text{if} \quad A_i \cap A_j = \emptyset \quad \text{for all} \quad i \neq j.$$ 

The triple $(\Omega, \mathcal{A}, P)$ is referred to as a probability space.

For finite or countably infinite sample spaces $\Omega$ the σ-algebra $\mathcal{A}$ can always be chosen to be the power set $\mathcal{P}(\Omega)$. The most important non-trivial σ-algebra is the Borel σ-algebra $\mathcal{B}_k$, which is the smallest σ-algebra over $\mathbb{R}^k$ that contains all rectangles of the form $(-\infty, b_1) \times \cdots \times (-\infty, b_k)$ with $b_i \in \mathbb{R}$. We will refer to the sets in the Borel σ-algebra, which include all open and all closed sets, as measurable sets. Measurable sets are of course a key ingredient to Lebesgue integration, which provides the following tool to define probability measures on $(\mathbb{R}^k, \mathcal{B}_k)$.

**Definition 2.1.6 (Density).** A density function is an integrable function $f : \mathbb{R}^k \to [0, \infty)$ with

$$\int_{\mathbb{R}^k} f(x) \, dx = 1.$$
Given a density function \( f \), the assignment

\[
P(A) = \int_A f(x) \, dx
\]
defines a probability measure \( P \) on \((\mathbb{R}^k, \mathcal{B}_k)\).

A density function of a probability measure is clearly not unique. If \( N \) is a set of Lebesgue measure zero, then altering the function values \( f(x) \) for \( x \in N \) yields another density function. However, two density functions \( f \) and \( g \) for the same probability measure are almost surely equal in the sense that the set \( \{ x \in \mathbb{R}^k : f(x) \neq g(x) \} \) has to have Lebesgue measure zero.

**Example 2.1.7** (Normal distribution). Suppose \( \mu \in \mathbb{R} \) and \( \sigma > 0 \). The probability measure \( N(\mu, \sigma^2) \) defined by the density function

\[
\phi_{\mu,\sigma}(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{ -\frac{(x-\mu)^2}{2\sigma^2} \right\}, \quad x \in \mathbb{R}
\]
is called the *normal distribution with mean \( \mu \) and variance \( \sigma^2 \)*. The fact that \( \phi_{\mu,\sigma} \) integrates to one can be seen as follows. First, using the substitution \( x = \sigma y + \mu \), we may assume that \( \mu = 0 \) and \( \sigma = 1 \) in which case the probability measure \( N(0,1) \) is known as the *standard normal distribution*. Now consider the squared integral

\[
\left( \int_{\mathbb{R}} \phi_{0,1}(x) \, dx \right)^2 = \int_{\mathbb{R}^2} \frac{1}{2\pi} \exp\left\{ -\frac{1}{2}(x^2 + y^2) \right\} \, d(x,y).
\]

Transforming to polar coordinates via \( x = r \cos \theta \) and \( y = r \sin \theta \) we find that

\[
\int_{r=0}^{\infty} \int_{\theta=0}^{2\pi} \frac{1}{2\pi} \exp\left\{ -r^2/2 \right\} \, r \, d\theta \, dr = \int_{r=0}^{\infty} \exp\left\{ -r^2/2 \right\} \, r \, dr = 1.
\]

Often one is concerned with not just a single event but two or more events, in which case it is interesting to ask questions of the type: what is the chance that event \( A \) occurs given the information that event \( B \) has occurred? This question could be addressed by redefining the sample space from \( \Omega \) to \( B \) and restricting the given probability measure \( P \) to \( B \). However, it is more convenient to adopt the following notion of conditional probability that avoids an explicit change of sample space.

**Definition 2.1.8** (Conditional probability). Let \( A, B \in \mathfrak{A} \) be two events such that the probability measure \( P \) on \((\Omega, \mathfrak{A})\) assigns positive probability \( P(B) > 0 \) to event \( B \). Then the conditional probability of event \( A \) given event \( B \) is the ratio

\[
P(A \mid B) = \frac{P(A \cap B)}{P(B)}.
\]
The following rules for computing with conditional probabilities are immediate consequences of Definition 2.1.8.

**Lemma 2.1.9** (Total probability and Bayes’ rule). Suppose $P$ is a probability measure on $(\Omega, \mathcal{A})$ and $A_1, \ldots, A_n \in \mathcal{A}$ are pairwise disjoint sets that form a partition of $\Omega$. Then we have the two equalities

$$P(A) = \sum_{i=1}^{n} P(A | B_i)P(B_i)$$

and

$$P(B_i | A) = \frac{P(A | B_i)P(B_i)}{\sum_{j=1}^{n} P(A | B_j)P(B_j)},$$

which are known as the law of total probability and Bayes’ rule, respectively.

**Example 2.1.10** (Urn). Suppose an urn contains two green and four red balls. In two separate draws two balls are taken at random and without replacement from the urn and the ordered pair of their colors is recorded. What is the probability that the second ball is red? To answer this we can apply the law of total probability. Let $A = \{(r, r), (g, r)\}$ be the event of the second ball being red, and $B_r = \{(r, r), (r, g)\}$ and $B_g = \{(g, r), (g, g)\}$ the events defined by fixing the color of the first ball. Then we can compute

$$P(A) = P(A | B_r)P(B_r) + P(A | B_g)P(B_g) = \frac{3}{5} \cdot \frac{4}{6} + \frac{4}{5} \cdot \frac{2}{6} = \frac{2}{3};$$

What is the probability that the first ball is green given that the second ball is red? Now Bayes’ rule yields

$$P(B_g | A) = \frac{P(A | B_g)P(B_g)}{P(A | B_r)P(B_r) + P(A | B_g)P(B_g)} = \frac{4}{5} \cdot \frac{2}{6} \cdot \frac{3}{2} = \frac{2}{5}.$$

In the urn example, the conditional probability $P(B_g | A)$ is larger than the unconditional probability of the first ball being green, which is $P(B_g) = 1/3$. This change in probability under conditioning captures the fact that due to the draws occurring without replacement knowing the color of the second ball provides information about the color of the first ball.

**Definition 2.1.11** (Independence). An event $A$ is independent of a second event $B$ if either $P(B) > 0$ and $P(A | B) = P(A)$ or $P(B) = 0$.

The following straightforward characterization of independence shows that the relation is symmetric.

**Lemma 2.1.12** (Multiplication of probabilities). Two events $A$ and $B$ are independent if and only if $P(A \cap B) = P(A)P(B)$. 
In light of Lemma \ref{lem:2.1.12} we use the following definition to express that the occurrence of any subset of these events provides no information about the occurrence of the remaining events.

**Definition 2.1.13** (Mutual Independence). The events $A_1, \ldots, A_n$ are mutually independent if

$$P\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} P(A_i), \quad \text{for all } I \subseteq [n].$$

Under mutual independence of the events $A_1, \ldots, A_n$, it holds that

$$P\left(\bigcap_{i \in I} A_i \mid \bigcap_{j \in J} A_j\right) = P\left(\bigcap_{i \in I} A_i\right)$$

for any pair of disjoint index sets $I, J \subseteq [n]$. Exercise \ref{ex:2.4} discusses an example in which it becomes clear that it does not suffice to consider independence of all pairs $A_i$ and $A_j$ in a definition of mutual independence of several events.

### 2.2. Random Variables and their Distributions

Many random experiments yield numerical quantities as outcomes that the observer may modify using arithmetic operations. Random variables are a useful concept for tracking the change of probability measures that is induced by calculations with random quantities. At an intuitive level a random variable is simply a “random number” and the distribution of a random variable determines the probability with which such a random number belongs to a given interval. The concept is formalized as follows.

**Definition 2.2.1** (Random variables and vectors). Let $(\Omega, \mathcal{A}, P)$ be a probability space. A random variable is a function $X : \Omega \to \mathbb{R}$ such that for every measurable set $B$ it holds that the preimage $X^{-1}(B) = \{X \in B\} \in \mathcal{A}$. The distribution of a random variable $X$ is the probability measure $P^X$ on $(\mathbb{R}, \mathcal{B})$ that is defined by

$$P^X(B) := P(X \in B) = P(X^{-1}(B)), \quad B \in \mathcal{B}.$$  

A random vector in $\mathbb{R}^k$ is a vector of random variables $X = (X_1, \ldots, X_k)$ that are all defined on the same probability space. The distribution of this random vector is defined by as above but considering set $B \in \mathcal{B}_k$. It is sometimes referred to as the joint distribution of $X$. For Cartesian products, $B = B_1 \times \cdots \times B_k$ we also write $P(X_1 \in B_1, \ldots, X_k \in B_k)$ to denote $P(X \in B)$. 
All random variables appearing in this book will be of one of two types. Either the random variable takes values in a finite or countably infinite set, in which case it is called a discrete random variable, or its distribution has a density function, in which case we will call the random variable continuous. Note that in more advanced treatments of probability a continuous random variable would be referred to as absolutely continuous. For a random vector, we will use the terminology discrete and continuous if the component random variables are all discrete or all continuous, respectively.

Example 2.2.2 (Binomial distribution). Suppose a coin has chance \( p \in (0,1) \) to show heads, and that this coin is tossed \( n \) times. It is reasonable to assume that the outcomes of the \( n \) tosses define independent events. The probability of seeing a particular sequence \( \omega = (\omega_1, \ldots, \omega_n) \) in the tosses is equal to \( p^k (1-p)^{n-k} \) where \( k \) is the number of heads among the \( \omega_i \). If we define \( X \) to be the discrete random variable

\[
X : \omega \mapsto \sum_{i=1}^{n} 1_{\{\omega_i = H\}}
\]

that counts the number of heads, then the distribution \( P^X \) corresponds to the probability vector with components

\[
p_k = \binom{n}{k} p^k (1-p)^{n-k}, \quad k = 0, \ldots, n.
\]

The distribution is known as the Binomial distribution \( B(n,p) \).

For a random vector \( X \) in \( \mathbb{R}^k \), we define the cumulative distribution function (cdf) to be the function

\[
F_X : \mathbb{R}^k \to [0,1],
\]

\[
x \mapsto P(X \leq x) = P(X_1 \leq x_1, \ldots, X_k \leq x_k).
\]

The fact that the Borel \( \sigma \)-algebra \( \mathbb{B}_k \) is the smallest \( \sigma \)-algebra containing the rectangles \((-\infty, b_1) \times \cdots \times (-\infty, b_k)\) can be used to show that the cdf uniquely determines the probability distribution of a random vector. A cdf exhibits monotonocity and continuity properties that follow from (2.1.1) and (2.1.2). In particular, the cdf \( F \) of a random variable is non-decreasing, right-continuous function with \( \lim_{x \to -\infty} F(x) = 0 \) and \( \lim_{x \to \infty} F(x) = 1 \). For continuous random vectors, the fundamental theorem of calculus yields the following relationship.

Lemma 2.2.3 (Density and cdf). If the random vector \( X = (X_1, \ldots, X_k) \) has density \( f \) that is continuous at \( x \in \mathbb{R}^k \), then

\[
f(x) = \frac{\partial^n}{\partial x_1 \cdots \partial x_n} F_X(x).
\]
Two natural probabilistic operations can be applied to a random vector \( X = (X_1, \ldots, X_k) \). On one hand, we can consider the distribution of a subvector \( X_I = (X_i \mid i \in I) \) for an index set \( I \subseteq [k] \). This distribution is referred to as the **marginal distribution** of \( X \) over \( I \). If \( X \) has density \( f \), then the marginal distribution over \( I \) has the **marginal density**

\[
(2.2.2) \quad f_{X_I}(x_I) = \int_{\mathbb{R}^J} f(x_I, x_J) \, dx_J,
\]

where \( J = [k] \setminus I \). On the other hand, given two index sets \( I, J \subseteq [k] \) and a vector \( x_J \in \mathbb{R}^J \), one can form the **conditional distribution** of \( X_I \) given \( X_J = x_J \). This distribution assigns the conditional probabilities \( P(X_I \in B \mid X_J = x_J) \) to the measurable sets \( B \in \mathcal{B}_I \). Clearly this definition of a conditional distribution is meaningful only if \( P(X_J = x_J) > 0 \). This seems to prevent us from defining conditional distributions for continuous random vectors as then \( P(X_J = x_J) = 0 \) for all \( x_J \). However, measure theory provides a way out that applies to arbitrary random vectors; see e.g. [Bil95, Chap. 6]. For random vectors with densities, this leads to intuitive ratios of densities.

**Definition 2.2.4** (Conditional distribution with densities). Let the random vector \( X = (X_1, \ldots, X_k) \) have density \( f \) and consider two index sets \( I, J \subseteq [k] \) that partition \( [k] \). For a vector \( x_J \in \mathbb{R}^J \), the conditional distribution of \( X_I \) given \( X_J = x_J \) is the probability distribution on \((\mathbb{R}^I, \mathcal{B}_I)\) that has density

\[
f(x_I \mid x_J) = \begin{cases} 
\frac{f(x_I, x_J)}{f_{X_J}(x_J)} & \text{if } f_{X_J}(x_J) > 0, \\
0 & \text{otherwise.}
\end{cases}
\]

The function \( f(x_I \mid x_J) \) is indeed a density as it is non-negative by definition and is easily shown to integrate to one by using (2.2.2).

When modelling random experiments using the language of random variables, an explicit reference to an underlying probability space can often be avoided by combining particular distributional assumptions with assumptions of independence.

**Definition 2.2.5** (Independence of random vectors). Let \( X_1, \ldots, X_n \) be random vectors on the probability space \((\Omega, \mathcal{A}, P)\). Then \( X_1, \ldots, X_n \) are independent if

\[
P(X_1 \in B_1, \ldots, X_n \in B_n) = \prod_{i=1}^{n} P(X_i \in B_i)
\]

for all measurable sets \( B_1, \ldots, B_n \) in the appropriate Euclidean spaces.

**Example 2.2.6** (Bernoulli random variables). Suppose we toss the coin from Example 2.2.2 and record a one if heads shows and a zero otherwise.
This yields a random variable \( X_1 \) with \( P(X_1 = 1) = p \) and \( P(X_1 = 0) = 1 - p \). Such a random variable is said to have a Bernoulli\((p)\) distribution. If we now toss the coin \( n \) times and these tosses are independent, then we obtain the random variables \( X_1, \ldots, X_n \) that are independent and identically distributed (i.i.d.) according to Bernoulli\((p)\). We see that

\[
Y = \sum_{i=1}^{n} X_i
\]

has a Binomial distribution, in symbols, \( Y \sim B(n, p) \). More generally, \( X \sim B(n, p) \) and \( Y \sim B(m, p) \) are independent, then \( X + Y \sim B(n + m, p) \). This fact is also readily derived from the form of the probability vector of the Binomial distribution. By Lemma 2.1.9

\[
P(X + Y = k) = \sum_{j=0}^{m} P(X + Y = k \mid Y = j)P(Y = j)
\]

\[
= \sum_{j=0}^{m} P(X = k - j \mid Y = j)P(Y = j).
\]

Under the assumed independence \( P(X = k - j \mid Y = j) = P(X = k - j) \) and we find that

\[
P(X + Y = k) = \sum_{j=0}^{m} \binom{n}{k-j} p^{k-j}(1-p)^{n-k+j} \binom{m}{j} p^j (1-p)^{m-j}
\]

\[
= p^k (1-p)^{n+m-k} \sum_{j=0}^{m} \binom{n}{k-j} \binom{m}{j},
\]

which is equal to (2.2.1).

The following result gives a simplified criterion for checking independence of random vectors. It can be established as a consequence of the Borel \( \sigma \)-algebra being defined in terms of rectangular sets.

**Lemma 2.2.7** (Independence and cdf). The random vectors \( X_1, \ldots, X_n \) on \((\Omega, \mathcal{A}, P)\) are independent if and only if

\[
F_{(X_1, \ldots, X_n)}(x) = \prod_{i=1}^{n} F_{X_i}(x_i)
\]

for all vectors \( x = (x_1, \ldots, x_n) \) in the appropriate Euclidean space.

If densities are available then it is often easier to recognize independence in a density factorization.
Lemma 2.2.8 (Independence and densities). Suppose the random vectors \(X_1, \ldots, X_n\) on \((\Omega, \mathcal{A}, P)\) have density functions \(f_1, \ldots, f_n\). If \(X_1, \ldots, X_n\) are independent, then the random vector \((X_1, \ldots, X_n)\) has the density function

\[
 f_{X_1,\ldots,X_n}(x) = \prod_{i=1}^{n} f_{X_i}(x_i).
\]

If the random vector \((X_1, \ldots, X_n)\) has the density function \(f_{X_1,\ldots,X_n}\), then \(X_1, \ldots, X_n\) are independent if and only if the equality (2.2.3) holds almost surely.

Proof. The first claims follows by induction and the observation that

\[
 P(X_1 \in B_1) P(X_2 \in B_2) = \int_{B_1} \int_{B_2} f(x_1) f(x_2) \, dx_2 \, dx_1.
\]

The second claim can be verified using this same observation for one direction and Lemma 2.2.7 in combination with the relation between cdf and density in Lemma 2.2.3 for the other direction. \(\square\)

As Example 2.2.6 shows, the changes in distribution when performing arithmetic operations with discrete random variables are not too hard to track. For random vector with densities we can employ the change of variables theorem from analysis.

Theorem 2.2.9 (Transformations). Suppose the random vector \(X = (X_1, \ldots, X_k)\) has density \(f_X\) that vanishes outside the set \(\mathcal{X}\), which may be equal to all of \(\mathbb{R}^k\). Suppose further that \(g : \mathcal{X} \to \mathcal{Y} \subseteq \mathbb{R}^k\) is a differentiable bijection whose inverse map \(g^{-1}\) is also differentiable. Then the random vector \(Y = g(X)\) has the density function

\[
 f_Y(y) = \begin{cases} 
 f_X(g^{-1}(y)) |Dg^{-1}(y)| & \text{if } y \in \mathcal{Y}, \\
 0 & \text{otherwise.}
\end{cases}
\]

Here, \(Dg^{-1}(y)\) is the Jacobian matrix of \(g^{-1}\) at \(y\).

Remark 2.2.10. The differentiability, in fact the continuity of \(g\) in Theorem 2.2.9 is sufficient for the vector \(Y = g(X)\) to be a random vector according to Definition 2.2.1 [Bil95, Thm. 13.2].

2.3. Expectation, Variance and Covariance

When presented with a random variable then it is natural to ask for numerical features of its distribution. The expectation, or in different terminology the expected value or mean, is a numerical description of the center of the distribution.
2. Probability Primer

Definition 2.3.1 (Expectation). If $X$ is a discrete random variable taking values in $\mathcal{X}$ and $\sum_{x \in \mathcal{X}} |x| P(X = x) < \infty$, then the expectation of $X$ is defined as the weighted average

$$E[X] = \sum_{x \in \mathcal{X}} x P(X = x).$$

If $\sum_{x \in \mathcal{X}} |x| P(X = x)$ diverges, then we say that the expectation of $X$ does not exist. If $X$ is a continuous random variable with density $f$, then the expectation exists if $\int_{\mathbb{R}} |x| f(x) \, dx < \infty$, in which case it is defined as the integral

$$E[X] = \int_{\mathbb{R}} x f(x) \, dx.$$

For a random vector, we define the expectation as the vector of expectations of its components.

Example 2.3.2 (Binomial expectation). If $X \sim B(n, p)$, then the expected value exists because $X = \{0, 1, \ldots, n\}$ is finite. It is equal to

$$E[X] = \sum_{x=0}^{n} x \binom{n}{x} p^x (1 - p)^{n-x}$$

$$= np \sum_{x=1}^{n} \binom{n-1}{x-1} p^{x-1} (1 - p)^{(n-1)-(x-1)}$$

$$= np.$$

The following result allows to compute the expectation of functions of random variables without having to work out their distributions. It is easily proven for the discrete case and is a consequence of Theorem 2.2.9 in special cases of the continuous case. For the most general version of this result see [Bil95, pp. 274, 277].

Theorem 2.3.3 (Transformation and expectation). (i) Suppose $X$ is a discrete random vector taking values in $\mathcal{X}$. If the function $g : \mathcal{X} \to \mathbb{R}$ defines a random variable $g(X)$, then the expectation of $g(X)$ is equal to

$$E[g(X)] = \sum_{x \in \mathcal{X}} g(x) P(X = x)$$

if it exists. It exists if the sum obtained by replacing $g(x)$ by $|g(x)|$ is finite.

(ii) Suppose $X$ is a continuous random vector with density $f$ that vanishes outside the set $\mathcal{X}$. If the function $g : \mathcal{X} \to \mathbb{R}$ defines a random variable $g(X)$, then the expectation of $g(X)$ is equal to

$$E[g(X)] = \int_{\mathcal{X}} g(x) f(x) \, dx$$

if it exists, which it does if the integral replacing $g(x)$ by $|g(x)|$ is finite.
Corollary 2.3.4. Suppose that the expectation of the random vector \( X = (X_1, \ldots, X_k) \) exists. If \( a_0 \in \mathbb{R} \) and \( a \in \mathbb{R}^k \) are constants, then the expectation of an affine function \( Y = a_0 + a^t X \) exists and is equal to
\[
E[Y] = a_0 + a^t E[X] = a_0 + \sum_{i=1}^k a_i E[X_i].
\]

Proof. The existence of \( E[Y] \) follows from the triangle inequality and the form of \( E[Y] \) follows from Theorem 2.3.3 \( \Box \)

In the case of discrete random vectors the following corollary is readily obtained from Definition 2.2.5 and Theorem 2.3.3. In the case of densities it follows using Lemma 2.2.8.

Corollary 2.3.5. If the random variables \( X_1, \ldots, X_k \) are independent with finite expectations, then the expectation of their product exists and is equal to
\[
E[X_1 X_2 \cdots X_k] = \prod_{i=1}^k E[X_i].
\]

Another natural measure for the distribution a random variable is the spread around the expectation, which is quantified in the variance.

Definition 2.3.6 (Variance). Suppose \( X \) is a random variable with finite expectation. The variance \( \text{Var}[X] = E[(X - E[X])^2] \) is the expectation of the squared deviation from \( E[X] \).

The variance can be computed using Theorem 2.3.3 but often it is in fact easier to compute the variance as
\[
\]

Note that we employed Corollary 2.3.4 for the second equality and that \( E[X] \) is a constant. Using Corollary 2.3.4 we can also easily show that
\[
(2.3.2) \quad \text{Var}[a_1 X + a_0] = a_1^2 \text{Var}[X].
\]

If a unit is attached to a random variable, then the variance is measured in the square of that unit. Hence, one often quotes the standard deviation \( \sqrt{\text{Var}[X]} \), which is measured in the original unit.

We next derive a simple but useful bound on the probability that a random variable \( X \) deviates from its expectation by a certain amount. This bound is informative if the variance of \( X \) is finite. One consequence of this bound is that if \( \text{Var}[X] = 0 \), then \( X \) is equal to the constant \( E[X] \) with probability one.
Lemma 2.3.7 (Chebyshev’s inequality). Let $X$ be a random variable with finite expectation $E[X]$ and finite variance $\text{Var}[X] < \infty$. Then
\[
P(|X - E[X]| \geq t) \leq \frac{\text{Var}[X]}{t^2} \quad \text{for all } t > 0.
\]

Proof. We will assume that $X$ is continuous with density $f$; the case of discrete $X$ is analogous. Define $Y = g(X) = (X - E[X])^2$ such that $E[Y] = \text{Var}[X]$ and $P(Y \geq 0) = 1$. Let $f_Y$ be the density function of $Y$. The fact that $Y$ has a density follows from two separate applications of the substitution rule from analysis (compare Theorem 2.2.9). The two separate applications consider $g$ over $(E[X], \infty)$ and $(-\infty, E[X])$.

Now,
\[
E[Y] = \int_0^\infty y f_Y(y) \, dy \geq \int_{t^2}^{\infty} t^2 f_Y(y) \, dy = t^2 P(Y \geq t^2).
\]
It follows that
\[
P(|Y| \geq t) \leq \frac{E[Y]}{t^2},
\]
which is the claim if all quantities are re-expressed in terms of $X$. \qed

We now turn to a measure of dependence between two random variables.

Definition 2.3.8 (Covariance). Suppose $X$ and $Y$ are two random variables whose expectations exist. The covariance of $X$ and $Y$ is defined as
\[
\text{Cov}[X,Y] = E[(X - E[X])(Y - E[Y])].
\]

In analogy with (2.3.1) it holds that
\[
\text{Cov}[X,Y] = E[XY] - E[X]E[Y]. \tag{2.3.3}
\]
It follows from Corollary 2.3.5 that if $X$ and $Y$ are independent then they are uncorrelated, which refers to a zero covariance. The reverse implication is not true: one can construct uncorrelated random variables that are dependent. By Corollary 2.3.4 if $X$ and $Y$ are two random vectors in $\mathbb{R}^k$ and $\mathbb{R}^m$, respectively, then
\[
\text{Cov} \left[ a_0 + \sum_{i=1}^{k} a_i X_i, b_0 + \sum_{j=1}^{m} b_j Y_j \right] = \sum_{i=1}^{k} \sum_{j=1}^{m} a_i b_j \text{Cov}[X_i,Y_j]. \tag{2.3.4}
\]
Since $\text{Var}[X] = \text{Cov}[X,X]$ it follows that
\[
\text{Var} \left[ a_0 + \sum_{i=1}^{k} a_i X_i \right] = \sum_{i=1}^{k} a_i^2 \text{Var}[X_i] + 2 \sum_{i=1}^{k} \sum_{j=i+1}^{k} a_i a_j \text{Cov}[X_i,X_j]. \tag{2.3.5}
\]
If $X_1, \ldots, X_k$ are independent, then

\begin{equation}
\text{Var} \left[ a_0 + \sum_{i=1}^{k} a_i X_i \right] = \sum_{i=1}^{k} a_i^2 \text{Var}[X_i].
\end{equation}

**Example 2.3.9** (Binomial variance). Suppose $X \sim B(n, p)$. Then we can compute $\text{Var}[X]$ in a similar fashion as we computed $E[X]$ in Example 2.3.2. However, it is easier to exploit that $X$ has the same distribution as the sum of independent Bernoulli($p$) random variables $X_1, \ldots, X_n$; recall Example 2.2.6. The expectation of $X_1$ is equal to $E[X_1] = 0 \cdot (1-p) + 1 \cdot p = p$ and thus the variance of $X_1$ is equal to $E[X_1^2] - E[X_1]^2 = E[X_1] - E[X_1]^2 = p(1-p)$.

By (2.3.6), we obtain that $\text{Var}[X] = np(1-p)$.

**Definition 2.3.10** (Covariance matrix). The covariance matrix $\text{Var}[X]$ of a random vector $X = (X_1, \ldots, X_k)$ is the $k \times k$-matrix with entries $\text{Cov}[X_i, X_j]$.

Using the covariance matrix, we can rewrite (2.3.5) as

$$\text{Var}[a_0 + a^t X] = a^t \text{Var}[X] a,$$

which reveals more clearly the generalization of (2.3.2). Since $\text{Var}[a_0 + a^t X] \geq 0$ for any choice of $a \in \mathbb{R}^k$ we see that the set of all covariance matrices is equal to the cone of (symmetric) positive semi-definite matrices.

An inconvenient feature of covariance is that it is affected by changes of scales and thus its numerical value is not directly interpretable. This dependence on scales is removed in the measure of correlation.

**Definition 2.3.11** (Correlation). The correlation between random variables $X$ and $Y$ where all the expectations $E[X], E[Y], \text{Var}[X], \text{Var}[Y]$, and covariance $\text{Cov}[X, Y]$ exist is a standardized covariance defined as

$$\text{Corr}[X, Y] = \frac{\text{Cov}[X, Y]}{\sqrt{\text{Var}[X] \text{Var}[Y]}}.$$

A correlation is indeed unaffected by (linear) changes of scale in that

$$\text{Corr}[a_0 + a_1 X, b_0 + b_1 Y] = \text{Corr}[X, Y].$$

As shown next, a correlation is never larger than one in absolute value and the extremes indicate a perfect linear relationship.

**Proposition 2.3.12** (Extreme correlation). Let $\rho = \text{Corr}[X, Y]$. Then $\rho \in [-1, 1]$. If $|\rho| = 1$ then there exist $a \in \mathbb{R}$ and $b \neq 0$ with $\text{sign}(b) = \text{sign}(\rho)$ such that $P(Y = a + bX) = 1$. 


Proof. Let $\sigma_X = \sqrt{\text{Var}[X]}$ and $\sigma_Y = \sqrt{\text{Var}[Y]}$. The claims follow from the inequality
\[ 0 \leq \text{Var} \left[ \frac{X}{\sigma_X} \pm \frac{Y}{\sigma_Y} \right] = 2(1 \pm \rho) \]
and the fact that a random variable with zero variance is constant almost surely. \qed

Remark 2.3.13. Proposition 2.3.12 shows that
\[ \text{Cov}[X_1, X_2]^2 \leq \text{Var}[X_1] \text{Var}[X_2], \]
which implies that the covariance of two random variables exists if both their variances are finite.

Considering conditional distributions can be helpful when computing expectations and (co-)variances. We will illustrate this in Example 2.3.16 but it also plays an important role in hidden variable models. If a random vector is partitioned into subvectors $X$ and $Y$ then we can compute the expectation of $X$ if $X$ is assumed to be distributed according to its conditional distribution given $Y = y$. This expectation, in general a vector, is referred to as the conditional expectation denoted $E[X \mid Y = y]$. Its components $E[X_i \mid Y = y]$ can be computed by passing to the marginal distribution of the vector $(X_i, Y)$ and performing the following calculation.

Lemma 2.3.14 (Conditional expectation). Suppose a random vector is partitioned as $(X, Y)$ with $X$ being a random variable. Then the conditional expectation of $X$ given $Y = y$ is equal to
\[ E[X \mid Y = y] = \begin{cases} \sum_x xP(X = x \mid Y = y) & \text{if } (X, Y) \text{ is discrete}, \\ \int_x x f(x \mid y) \, dx & \text{if } (X, Y) \text{ has density } f. \end{cases} \]

Similarly, we can compute conditional variances $\text{Var}[X \mid Y = y]$ and covariances $\text{Cov}[X_1, X_2 \mid Y = y]$. The conditional expectation is a function of $y$. Plugging in the random vector $Y$ for the value $y$ we obtain a random vector $E[X \mid Y]$.

Lemma 2.3.15 (Iterated expectation). Suppose a random vector is partitioned as $(X,Y)$ where $X$ and $Y$ may be arbitrary subvectors. Then the expectation of $X$ is equal to
\[ E[X] = E \left[ E[X \mid Y] \right], \]
and the covariance matrix of $X$ can be computed as
\[ \text{Var}[X] = \text{Var} \left[ E[X \mid Y] \right] + E \left[ \text{Var}[X \mid Y] \right]. \]

Proof. Suppose that $(X,Y)$ has density $f$ on $\mathbb{R}^{k+1}$ and that $X$ is a random variable. (If $(X,Y)$ is discrete, then the proof is analogous.) Let $f_Y$ be the
marginal density of $Y$; compare (2.2.2). Then $f(x, y) = f(x \mid y)f_Y(y)$ such that we obtain

$$
E[X \mid Y] = \int_{\mathbb{R}} \left( \int_{\mathbb{R}} xf(x \mid y) \, dx \right) f_Y(y) \, dy
= \int_{\mathbb{R}^k+1} \int_{\mathbb{R}} xf(x, y) \, d(x, y)
= E[X].
$$

Note that the last equality follows from Theorem 2.3.3. The vector-version of the equality $E[X] = E[E[X \mid Y]]$ follows by component-wise application of the result we just derived.

The claim about the covariance matrix follows if we can show that for a random vector $(X_1, X_2, Y)$ with random variable components $X_1$ and $X_2$ it holds that

$$(2.3.7) \quad \text{Cov}[X_1, X_2] = \text{Cov}[E[X_1 \mid Y], E[X_2 \mid Y]] + E[\text{Cov}[X_1, X_2 \mid Y]].$$

For the first term in (2.3.7) we obtain by (2.3.3) and the result about the expectation that

$$\text{Cov}[E[X_1 \mid Y], E[X_2 \mid Y]] = E[E[X_1 \mid Y] \cdot E[X_2 \mid Y]] - E[X_1]E[X_2].$$

Similarly, the second term in (2.3.7) equals

$$E[\text{Cov}[X_1, X_2 \mid Y]] = E[X_1X_2] - E[E[X_1 \mid Y] \cdot E[X_2 \mid Y]].$$

Hence, adding the two terms gives $\text{Cov}[X_1, X_2]$ as claimed. \qed

**Example 2.3.16** (Penalty kicks). Suppose a soccer player in the German Bundesliga is selected at random and takes two penalty kicks against goalie Manuel Neuer. Let $X_1$ and $X_2$ be the two Bernoulli random variables that indicate whether the player makes kicks 1 and 2. We would like to compute the correlation $\text{Corr}[X_1, X_2]$ under the assumption that the random variable $Y$ that denotes the probability of a randomly selected player making a penalty kick against Oliver Kahn has density $f(y) = 6y(1-y)1_{[0,1]}(y)$.

Clearly, $\text{Corr}[X_1, X_2]$ will not be zero as the two kicks are taken by the same player. However, it is reasonable to assume that conditional on the player’s skill level $Y = y$, success in the first and success in the second kick are independent. This implies that $\text{Cov}[X_1, X_2 \mid Y = y] = 0$ and thus the second term in (2.3.7) is zero. Since the expectation of a Bernoulli($y$) random variable is equal to $y$ we obtain that $E[X_1 \mid Y] = Y$, which implies that the first term in (2.3.7) equals $\text{Var}[Y]$. We compute

$$E[Y] = \int_0^1 6y^2(1-y) \, dy = 1/2$$
\[ E[Y^2] = \int_0^1 6y^3(1 - y) \, dy = 3/10 \]

and obtain by (2.3.1) that

\[ \text{Cov}[X_1, X_2] = \text{Var}[Y] = 3/10 - (1/2)^2 = 1/20. \]

Similarly, using the variance formula in Lemma 2.3.15 and the fact \( \text{Var}[X_i \mid Y] = Y(1 - Y) \), we find that

\[ \text{Var}[X_i] = \text{Var}[Y] + E[Y(1 - Y)] = 1/20 + 1/2 - 3/10 = 1/4. \]

The correlation thus equals

\[ \text{Corr}[X_1, X_2] = \frac{1/20}{1/4} = 1/5. \]

We remark that the set-up of Example 2.3.16 does not quite fit in our previous discussion in the sense that we discuss a random vector \((X_1, X_2, Y)\) that has two discrete and one continuous component. However, all our results carry over to this mixed case if multiple integrals (or multiple sums) are replaced by a mix of summations and integrations.

### 2.4. Multivariate Normal Distribution

In this section we introduce a multivariate generalization of the normal distribution \( \mathcal{N}(\mu, \sigma^2) \) from Example 2.1.7 where the parameters \( \mu \) and \( \sigma \) were called mean and standard deviation. Indeed it is an easy exercise to show that if an \( \mathcal{N}(\mu, \sigma^2) \) random variable \( X \) has expectation \( \mathbb{E}[X] = \mu \) and variance \( \text{Var}[X] = \sigma^2 \).

To begin, let us recall that the (univariate) standard normal distribution \( \mathcal{N}(0, 1) \) has as density function the Gaussian bell curve

\[ \phi(x) = \phi_{0,1}(x) = \frac{1}{\sqrt{2\pi}} \exp \left\{ -\frac{1}{2} x^2 \right\}. \tag{2.4.1} \]

Let \( I \in \mathbb{R}^{k \times k} \) be the identity matrix. Then we say that a random vector \( X = (X_1, \ldots, X_k) \) is distributed according to the \textit{standard multivariate normal distribution} \( \mathcal{N}_k(0, I) \) if its components \( X_1, \ldots, X_k \) are independent and identically distributed (i.i.d.) as \( X_i \sim \mathcal{N}(0, 1) \). Thus, by Lemma 2.2.8 the distribution \( \mathcal{N}_k(0, I) \) has the density function

\[ \phi_{0,I}(x) = \prod_{i=1}^k \frac{1}{\sqrt{2\pi}} \exp \left\{ -\frac{1}{2} x_i^2 \right\} \]

\[ = \frac{1}{(2\pi)^{k/2}} \exp \left\{ -\frac{1}{2} x^T x \right\}. \tag{2.4.2} \]
2.4. Multivariate Normal Distribution

Let \( \Lambda \in \mathbb{R}^{k \times k} \) be a matrix of full rank and let \( \mu \in \mathbb{R}^k \). Suppose \( X \sim \mathcal{N}_k(0, I) \) and define \( Y = \Lambda X + \mu \). By Theorem \[2.2.9\] the random vector \( Y \) has the density function

\[
\phi_Y(y) = \frac{1}{(2\pi)^{k/2}} \exp \left\{ -\frac{1}{2} (y - \mu)^t \Lambda^{-t} \Lambda^{-1} (y - \mu) \right\} |\Lambda^{-1}|,
\]

where \( |.| \) denotes the determinant. Define \( \Sigma = \Lambda \Lambda^t \). Then the density \( \phi_Y \) is seen to depend only on \( \mu \) and \( \Sigma \) and can be rewritten as

\[\tag{2.4.3}\]
\[
\phi_{\mu, \Sigma}(y) = \frac{1}{(2\pi)^{k/2} |\Sigma|^{1/2}} \exp \left\{ -\frac{1}{2} (y - \mu)^t \Sigma^{-1} (y - \mu) \right\},
\]

Note that since standard multivariate normal random vector has expectation 0 and covariance matrix \( I \), it follows from Corollary \[2.3.4\] and \[2.3.4\] that \( Y \) has expectation \( \Lambda 0 + \mu = \mu \) and covariance matrix \( \Lambda I \Lambda^t = \Sigma \).

**Definition 2.4.1** (Multivariate normal distribution). Suppose \( \mu \) is a vector in \( \mathbb{R}^k \) and \( \Sigma \) is (symmetric) positive definite \( k \times k \)-matrix. Then a random vector \( X = (X_1, \ldots, X_k) \) is said to be distributed according to the multivariate normal distribution \( \mathcal{N}_k(\mu, \Sigma) \) with mean vector \( \mu \) and covariance matrix \( \Sigma \) if it has the density function in \[2.4.3\].

One of the many amazing properties of the multivariate normal distribution is that its marginal distributions as well as its conditional distributions are again multivariate normal.

**Theorem 2.4.2** (Marginal and conditional normal distributions). Let \( X \sim \mathcal{N}_k(\mu, \Sigma) \) and let \( A, B \subseteq [k] \) be two disjoint index sets.

(i) The marginal distribution of \( X \) over \( B \), that is, the distribution of the subvector \( X_B = (X_i \mid i \in B) \) is multivariate normal, namely,

\[
X_B \sim \mathcal{N}_{\#B}(\mu_B, \Sigma_{B,B}),
\]

where \( \mu_B \) is the respective subvector of the mean vector \( \mu \) and \( \Sigma_{B,B} \) is the corresponding principal submatrix of \( \Sigma \).

(ii) For every \( x_B \in \mathbb{R}^B \), the conditional distribution of \( X_A \) given \( X_B = x_B \) is the multivariate normal distribution

\[
\mathcal{N}_{\#A} \left( \mu_A + \Sigma_{A,B} \Sigma_{B,B}^{-1} (x_B - \mu_B), \Sigma_{A,A} - \Sigma_{A,B} \Sigma_{B,B}^{-1} \Sigma_{B,A} \right).
\]

The matrix \( \Sigma_{A,B} \Sigma_{B,B}^{-1} \) appearing in Theorem \[2.4.2\] is the matrix of regression coefficients. The positive definite matrix

\[\tag{2.4.4}\]
\[
\Sigma_{A,A} = \Sigma_{A,A} - \Sigma_{A,B} \Sigma_{B,B}^{-1} \Sigma_{B,A}
\]

is the conditional covariance matrix. We also note that \( (X_A \mid X_B = x_B) \) is not well-defined as a random vector. It is merely a way of denoting the conditional distribution of \( X_A \) given \( X_B = x_B \).
Proof of Theorem 2.4.2. Suppose that $A \cup B = [k]$. Then we can partition the covariance matrix as

$$
\Sigma = \begin{pmatrix}
\Sigma_{A,A} & \Sigma_{A,B} \\
\Sigma_{B,A} & \Sigma_{B,B}
\end{pmatrix}.
$$

Using the same partitioning, $\Sigma^{-1}$ can be factored as

$$
\Sigma^{-1} = \begin{pmatrix}
I & 0 \\
-\Sigma_{B,B}^{-1}\Sigma_{B,A} & I
\end{pmatrix}
\begin{pmatrix}
(\Sigma_{A,B})^{-1} & 0 \\
0 & \Sigma_{B,B}^{-1}
\end{pmatrix}
\begin{pmatrix}
I & -\Sigma_{A,B}\Sigma_{B,B}^{-1} \\
0 & I
\end{pmatrix}.
$$

Plugging this identity into (2.4.3) we obtain that

$$
(2.4.5) \quad \phi_{\mu,\Sigma}(x) = \phi_{\mu_A + \Sigma_{A,B}\Sigma_{B,B}^{-1}(x_B - \mu_B)}(x_A) \phi_{\mu_B,\Sigma_{B,B}}(x_B).
$$

Integrating out $x_A$, we see that $X_B \sim \mathcal{N}_{\#B}(\mu_B, \Sigma_{B,B})$, which concludes the proof of claim (i).

By Definition 2.2.4 it also follows that (ii) holds if, as we have assumed, $A \cup B = [k]$. If this does not hold we can use (i) to pass the marginal distribution of $X_{A \cup B}$ first. Hence, we have also shown (ii).

The multivariate normal distribution is the distribution of a non-singular affine transformation of standard normal random vector. Consequently, further affine transformations remain multivariate normal.

Lemma 2.4.3 (Affine transformation). If $X \sim \mathcal{N}_k(\mu, \Sigma)$, $A$ is a full rank $m \times k$-matrix with $m \leq k$ and $b \in \mathbb{R}^m$, then $AX + b \sim \mathcal{N}_m(A\mu + b, A\Sigma A^t)$.

Proof. If $m = k$ the claim follows from Theorem 2.2.9. If $m < k$ then complete $A$ to a full rank $k \times k$-matrix and $b$ to a vector in $\mathbb{R}^k$, which allows to deduce the result from Theorem 2.4.2(i). □

In §2.3 we noted that uncorrelated random variables need not be independent in general. However, this is the case for random variables that form a multivariate normal random vector.

Proposition 2.4.4 (Normal independence). If $X \sim \mathcal{N}_k(\mu, \Sigma)$ and $A, B \subseteq [k]$ are two disjoint index sets, then the subvectors $X_A$ and $X_B$ are independent if and only if $\Sigma_{A,B} = 0$.

Proof. Combining Lemma 2.2.8 and Definition 2.2.4 we see that independence holds if and only if the conditional density of $X_A$ given $X_B = x_B$ does not depend on $x_B$. By Theorem 2.4.2 the latter condition holds if and only if $\Sigma_{A,B}\Sigma_{B,B}^{-1} = 0$ if and only if $\Sigma_{A,B} = 0$ because $\Sigma_{B,B}$ is of full rank. □

An important distribution intimately related to the multivariate normal distribution is the chi-squared distribution.
Definition 2.4.5. Let $Z_1, Z_2, \ldots, Z_k$ be i.i.d. $N(0, 1)$ random variables. Then the random variable $Q = \sum_{i=1}^{k} Z_i^2$ has a chi-squared distribution with $k$ degrees of freedom. This is denoted $Q \sim \chi_k^2$.

The chi-squared distribution is rarely used to model natural phenomena. However, it is the natural distribution that arises in limiting phenomena in many hypothesis tests, since it can be interpreted as the distribution of squared distances in many contexts. A typical example is the following.

Proposition 2.4.6. Let $X \in \mathbb{R}^m \sim N(0, I)$, let $L$ be a linear space of dimension $d$ through the origin, and let $Z = \min_{y \in L} \|y - X\|_2$. Then $Z \sim \chi^2_{m-d}$.

Proof. There is an orthogonal change of coordinates $Q$ so that $L$ becomes a coordinate subspace, consisting of, saying the last $d$ coordinates in $\mathbb{R}^m$. Let $L_d$ be the resulting coordinate subspace. The standard normal distribution is rotationally invariant so $Z$ has the same distribution as

$$Z = \min_{y \in L_d} \|y - X\|_2^2 = \sum_{i=1}^{m-d} X_i^2$$

so $Z \sim \chi^2_{m-d}$. \qed

2.5. Limit Theorems

According to Definition 2.2.1 a random vector is a map from a sample space $\Omega$ to $\mathbb{R}^k$. Hence, when presented with a sequence of random vectors $X_1, X_2, \ldots$ all defined on the same probability space $(\Omega, \mathcal{F}, P)$ and all taking values in $\mathbb{R}^k$, then we can consider their pointwise convergence to a limiting random vector $X$. Such a limit $X$ would need to satisfy that

$$X(\omega) = \lim_{n \to \infty} X_n(\omega)$$

for all $\omega \in \Omega$. While pointwise convergence is a useful concept in analysis it presents an unnaturally strong requirement for probabilisty purposes. For example, it is always possible to alter the map defining a continuous random vector at countably many elements in $\Omega$ without changing the distribution of the random vector. A more appropriate concept is almost sure convergence, denoted by $X_n \to a.s. X$, in which (2.5.1) is required to hold for all $\omega$ in a set with probability one.
Example 2.5.1 (Dyadic intervals). Suppose that $\Omega = (0, 1]$ and that $\mathfrak{A}$ is the $\sigma$-algebra of measurable subsets of $(0, 1]$. Let $P$ be the uniform distribution on $\Omega$, that is, $P$ has density function $f(\omega) = 1_{[0, 1]}(\omega)$. Define 

$$X_{2^j+i}(\omega) = 1_{((i-1)/2^j, i/2^j]}(\omega), \quad j = 1, 2, \ldots, \ i = 1, \ldots, 2^j.$$ 

Then for all $\omega \in \Omega$ it holds that 

$$\lim \inf_{n \to \infty} X_n(\omega) = 0 \neq 1 = \lim \sup_{n \to \infty} X_n(\omega)$$ 

such that the sequence $(X_n)_{n \geq 1}$ has no limit under almost sure convergence.

In Example 2.5.1, the probability $P(X_{2^j+i} \neq 0) = 2^{-j}$ converges to zero as $j$ grows large, from which it follows that the sequence $(X_n)_{n \geq 1}$ converges to the constant 0 in the weaker sense of the next definition.

Definition 2.5.2 (Convergence in probability). Let $X$ be a random vector and $(X_n)_{n \geq 1}$ a sequence of random vectors on $(\Omega, \mathfrak{A}, P)$ that all take values in $\mathbb{R}^k$. We say that $X_n$ converges to $X$ in probability, in symbols $X_n \xrightarrow{\text{p}} X$ if for all $\epsilon > 0$ it holds that 

$$\lim_{n \to \infty} P(||X_n - X|| > \epsilon) = 0.$$ 

Equipped with the notion of convergence we can give a long-run average interpretation of expected values.

Theorem 2.5.3 (Weak law of large numbers). Let $(X_n)_{n \geq 1}$ be a sequence of random variables with finite expectation $E[X_n] = \mu$ and finite variance $\text{Var}[X_n] = \sigma^2 < \infty$. Suppose further that the random variables are pairwise uncorrelated, that is, $\text{Cov}[X_n, X_m] = 0$ for $n \neq m$. Then, as $n \to \infty$, 

$$\bar{X}_n = \frac{1}{n} \sum_{i=1}^{n} X_i \xrightarrow{\text{p}} \mu.$$ 

Proof. By Corollary 2.3.4 and (2.3.6), $E[\bar{X}_n] = \mu$ and $\text{Var}[\bar{X}_n] = \sigma^2/n$. Thus by Lemma 2.3.7, 

$$P(||\bar{X}_n - \mu|| > \epsilon) \leq \frac{\sigma^2}{n\epsilon^2} \to 0.$$ 

Suppose $X_n$ is the Bernoulli$(p)$ indicator for the heads in the $n$-th toss of a coin. Then $\bar{X}_n$ is the proportion of heads in $n$ tosses. Assuming independence of the repeated tosses, Theorem 2.5.3 implies that the proportion converges to the probability $p$. This is the result promised in the beginning of this chapter.

The version of the law of large numbers we presented is amenable to a very simple proof. With more refined techniques, the assumptions made can be weakened. For example, it is not necessary to require finite variances.
Moreover, if independence instead of uncorrelatedness is assumed then it is also possible to strengthen the conclusion from convergence in probability to almost sure convergence in which case one speaks of the strong law of large numbers. We state without proof one version of the strong law of large numbers; compare Theorem 22.1 in \cite{Bil95}.

**Theorem 2.5.4** (Strong law of large numbers). If the random variables in the sequence \((X_n)_n\) are independent and identically distributed with finite expectation \(E[X_n] = \mu\), then \(X_n\) converges to \(\mu\) almost surely.

**Example 2.5.5** (Cauchy distribution). An example to which the law of large numbers does not apply is the Cauchy distribution, which has density function

\[
f(x) = \frac{1}{\pi(1 + x^2)}, \quad x \in \mathbb{R}.
\]

If \(X_1, X_2, \ldots\) are i.i.d. Cauchy random variables, then Theorem 2.2.9 can be used to show that \(X_n\) has again a Cauchy distribution and thus does not converge in probability or almost surely to a constant. The failure of the law of large numbers to apply is due to the fact that the expectation of a Cauchy random variable does not exist, i.e., \(E[|X_1|] = \infty\).

All convergence concepts discussed so far require that the sequence and its limiting random variable are defined on the same probability space. This is not necessary in the following definition.

**Definition 2.5.6** (Convergence in distribution). Let \(X\) be a random vector and \((X_n)_n\) a sequence of random vectors that all take values in \(\mathbb{R}^k\). Denote their cdfs by \(F_X\) and \(F_{X_n}\). Then \(X_n\) converges to \(X\) in distribution, in symbols \(X_n \overset{d}{\rightarrow} X\) if for all points \(x \in \mathbb{R}^k\) at which \(F_X\) is continuous it holds that

\[
\lim_{n \to \infty} F_{X_n}(x) = F(x).
\]

Exercise 2.7 explains the necessity of excluding the points of discontinuity of \(F_X\) when defining convergence of distribution. What is shown there is that without excluding the points of discontinuity convergence in distribution may fail for random variables that converge to a limit in probability and almost surely. We summarize the relationship among the three convergence concepts we introduced.

**Theorem 2.5.7** (Convergence implications). Almost sure convergence implies convergence in probability which in turn implies convergence in distribution.

**Proof.** We prove the implication from convergence in probability to convergence in distribution; for the other implication see Theorem 5.2 in \cite{Bil95}.
Suppose that $X_n \xrightarrow{p} X$ and let $\epsilon > 0$. Let $x$ be a point of continuity of the cdf $F_X$, which implies that $P(X = x) = 0$. If $X_n \leq x$ and $|X_n - X| \leq \epsilon$, then $X \leq x + \epsilon$. Hence, $X > x + \epsilon$ implies that $X_n > x$ or $|X_n - X| > \epsilon$. Consequently,

$$1 - P(X \leq x + \epsilon) \leq 1 - P(X_n \leq x) + P(|X_n - X| > \epsilon)$$

from which we deduce that

$$P(X_n \leq x) \leq F_X(x + \epsilon) + P(|X_n - X| > \epsilon).$$

Starting the same line of reasoning with the fact that $X \leq x - \epsilon$ and $|X_n - X| \leq \epsilon$ imply that $X_n \leq x$ we find that

$$P(X_n \leq x) \geq F_X(x - \epsilon) - P(|X_n - X| > \epsilon).$$

Combining the two inequalities and letting $n$ tend to infinity we obtain that

$$F_X(x - \epsilon) \leq \lim \inf_{n \to \infty} P(X_n \leq x) \leq \lim \sup_{n \to \infty} P(X_n \leq x) \leq F_X(x + \epsilon).$$

Now letting $\epsilon$ tend to zero, the continuity of $F_X$ at $x$ yields

$$\lim_{n \to \infty} P(X_n \leq x) = F_X(x),$$

which is what we needed to show. \qed

**Remark 2.5.8.** In general none of the reverse implications in Theorem 2.5.7 hold. However, if $c$ is a constant and $X_n$ converges to $c$ in distribution, then one can show that $X_n$ also converges to $c$ in probability.

Convergence in distribution is clearly the relevant notion if one is concerned with limits of probabilities of events of interest. The next result is a powerful tool that allows to approximate difficult to evaluate probabilities by probabilities computed under a normal distribution.

**Theorem 2.5.9 (Central limit theorem).** Let $(X_n)_n$ be a sequence of independent and identically distributed random vectors with existent expectation $E[X_n] = \mu \in \mathbb{R}^k$ and positive definite covariance matrix $\text{Var}[X_n] = \Sigma$. Then, as $n \to \infty$,

$$\sqrt{n}(\bar{X}_n - \mu) \xrightarrow{d} \mathcal{N}_k(0, \Sigma).$$

The literature offers two types of proofs for central limit theorems. The seemingly simpler approach employs so-called characteristic functions and a Taylor-expansion; compare Sections 27 and 29 in [Bil95]. However, this argument relies on the non-trivial fact that characteristic functions uniquely determine the probability distribution of a random vector or variable. The second approach known as Stein’s method is perhaps more elementary and is discussed for example in [Sho00]. Instead of attempting to reproduce a general proof of the central limit theorem here, we will simply illustrate its conclusion in the example that is at the origin of the modern result.
Example 2.5.10 (Laplace DeMoivre Theorem). Let $X_1, X_2, \ldots$ be independent Bernoulli($p$) random variables. Then

$$S_n = \sum_{i=1}^{n} X_i$$

follows the Binomial $B(n, p)$ distribution. Let $Z \sim \mathcal{N}(0, p(1 - p))$. Then it holds for all $a < b$ that

$$\lim_{n \to \infty} P \left( a < \frac{S_n - np}{\sqrt{n}} \leq b \right) = P(a < Z \leq b).$$

We conclude this review of probability by stating two useful results on transformations, which greatly extend the applicability of asymptotic approximations.

Lemma 2.5.11 (Continuous mapping). Suppose the random vectors $X_n$ converge to $X$ almost surely, in probability or in distribution. If $g$ is a continuous map that defines random vectors $g(X_n)$ and $g(X)$, then the sequence $g(X_n)$ converges to $g(X)$ in the same mode as the original sequence.

The claim is trivial for almost sure convergence. For the proofs for convergence in probability and in distribution see Theorem 25.7 in [Bil95] and also Theorem 2.3 in [vdV98].

Lemma 2.5.12 (Delta method). Let $X_n$ and $X$ be random vectors in $\mathbb{R}^k$ and $(a_n)_n$ a diverging sequence of real numbers with $\lim_{n \to \infty} a_n = \infty$. Suppose there exists a vector $b \in \mathbb{R}^k$ such that

$$a_n(X_n - b) \rightarrow_d X.$$

Let $g: \mathbb{R}^k \rightarrow \mathbb{R}^m$ be a map defining random vectors $g(X_n)$ and $g(X)$.

(i) If $g$ is differentiable at $b$ with total derivative matrix $D = Dg(b) \in \mathbb{R}^{m \times k}$, then

$$a_n(g(X_n) - g(b)) \rightarrow_d D X.$$

(ii) If $g$ is a function, i.e., $m = 1$, that is twice differentiable at $b$ with gradient $Dg(b)^t \in \mathbb{R}^k$ equal to zero and Hessian matrix $H = Hg(b) \in \mathbb{R}^{k \times k}$, then

$$a_n(g(X_n) - g(b)) \rightarrow_d \frac{1}{2} X^t H X.$$

Proof sketch. A rigorous proof is given for Theorem 3.1 in [vdV98]. We sketch the idea of the proof. Apply a Taylor expansion to $g$ at the point $b$ and multiply by $a_n$ to obtain that

$$a_n(g(X_n) - g(b)) \approx D \cdot a_n(X_n - b).$$
By Lemma 2.5.11, the right hand side converges to $DX$ in distribution, which is claim (i). For claim (ii) go one order higher in the Taylor-expansion.

We remark that if the limiting random vector $X$ in Lemma 2.5.12 has a multivariate normal distribution $\mathcal{N}_k(\mu, \Sigma)$ and the derivative matrix $D$ is of full rank then it follows from Lemma 2.4.3 that $DX \sim \mathcal{N}_m(D\mu, D\Sigma D^t)$. If $D$ is not of full rank then $DX$ takes its values in the linear subspace given by the image of $D$. Such distributions are often called singular normal distributions [Rao73, Chap. 8a].

2.6. Exercises

Exercise 2.1. An urn contains 49 balls labelled by the integers 1 through 49. Six balls are drawn at random from this urn without replacement. The balls are drawn one by one and the numbers on the balls are recorded in the order of the draw. Define the appropriate sample space and show that the probability of exactly three balls having a number smaller than 10 is equal to (2.1.3).

Exercise 2.2. (i) Show that a $\sigma$-algebra contains the empty set and is closed under countable intersections. (ii) Show that the Borel $\sigma$-algebra $\mathcal{B}$ on $\mathbb{R}$ contains all open subsets of $\mathbb{R}$. (iii) Show that the Borel $\sigma$-algebra $\mathcal{B}_k$ on $\mathbb{R}^k$ is not the $k$-fold Cartesian product of $\mathcal{B}$.

Exercise 2.3. The exponential distribution is the probability measure $P$ on $(\mathbb{R}, \mathcal{B})$ defined by the density function $f(x) = e^{-x}1_{\{x > 0\}}$. For $t, s > 0$, show that $P((0, s]) = P((t, t + s] \mid (t, \infty))$.

Exercise 2.4. A fair coin showing heads and tails with equal probability is tossed twice. Show that the any two of the events Heads with the first toss, Heads with exactly one toss and Heads with the second toss are independent but that the three events are not mutually independent.

Exercise 2.5. Show that if $X \sim \mathcal{N}(0, 1)$, then the sign of $X$ and the absolute value of $X$ are independent.

Exercise 2.6. Find the density of $X + Y$ for $X$ and $Y$ being independent random variables with an exponential distribution (cf. Exercise 2.3).

(Hint: One way of approaching this problem is to consider the map $g : (x, y) \mapsto (x + y, y)$ and employ Theorem 2.2.9.)

Exercise 2.7. Let the discrete random variable $X$ have a Poisson($\lambda$) distribution, i.e.,

$$P(X = k) = e^{-\lambda} \lambda^k / k!, \quad k = 0, 1, 2, \ldots$$

where the parameter $\lambda$ is a positive real. Show that $E[X] = \text{Var}[X] = \lambda$. 

Exercise 2.8. Suppose the random vector \((X_1, X_2, X_3)\) follows the multivariate normal distribution \(N_3(0, \Sigma)\) with

\[
\Sigma = \begin{pmatrix}
\frac{3}{2} & 1 & \frac{1}{2} \\
1 & 2 & 1 \\
\frac{1}{2} & 1 & \frac{3}{2}
\end{pmatrix}.
\]

Verify that the conditional distribution of \(X_1\) given \((X_2, X_3) = (x_2, x_3)\) does not depend on \(x_3\). Compute the inverse \(\Sigma^{-1}\); do you see a connection?

Exercise 2.9. Let \((X_n)_n\) be a sequence of independent discrete random variables that take the values \(\pm 1\) with probability \(1/2\) each. Let \(F_{\bar{X}_n}\) denote the cdf of \(\bar{X}_n\). By the weak law of large numbers it holds that \(\bar{X}_n\) converges to zero in probability. Let \(F_X(x) = 1_{[0, \infty)}(x)\) be the cdf of the constant zero. Show that \(F_{\bar{X}_n}(x)\) converges to \(F_X(x)\) if and only if \(x \neq 0\). What is the limit if \(x = 0\)?

Exercise 2.10. Let \((X_n)_n\) be a sequence of independent and identically distributed random variables that follow a uniform distribution on \((0, 1]\), which has density \(f(x) = 1_{(0,1]}(x)\). What does the central limit theorem say about the convergence of \(\bar{X}_n\)? Consider the parametrized family of functions \(g_t(x) = (x - t)^2\) with parameter \(t \in (0, 1]\). Use the delta method from Lemma 2.5.12 to find a convergence in distribution result for \(g_t(\bar{X}_n)\). Contrast the two cases \(t \neq 1/2\) and \(t = 1/2\).

Exercise 2.11. Suppose \((X_n)_n\) is a sequence of independent and identically distributed random variables that follow an exponential distribution. Find the cdf of \(M_n = \max\{X_1, \ldots, X_n\}\). Show that \(M_n - \log n\) converges in distribution and find the limiting distribution.
Chapter 3

Algebra Primer

The basic geometric objects that are studied in algebraic geometry are algebraic varieties. On the algebraic side, varieties will form the main object of study in this book, in particular, we will be interested in ways to using algebraic techniques to understand properties of these varieties. This chapter will be devoted to laying the groundwork for algebraic geometry. We introduce algebraic varieties, and the tools used to study them, in particular, their vanishing ideals, and Gröbner bases of these ideals. In Section 3.4 we will describe some applications of Gröbner bases to computing features of algebraic varieties.

Our aim in this chapter is to provide a concise introduction to the main tools we will use. Thus, it will be highly beneficial for the reader to also consult some texts that go into more depth on these topics, for instance [CLO07].

3.1. Varieties

Let \( \mathbb{K} \) be a field. For the purposes of this book, there are three main fields of interest: the rational numbers \( \mathbb{Q} \), which are useful for performing computations, the real numbers \( \mathbb{R} \), which are fundamental because probabilities are real, and the complex number \( \mathbb{C} \), which we will need in some circumstances for proving precise theorems in algebraic geometry.

Let \( p_1, p_2, \ldots, p_r \) be polynomial variables or indeterminates (we will generally use the word indeterminate instead of variable to avoid confusion with random variables). A monomial in these indeterminates is an expression of the form

\[
p^u := p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r}
\]
where \( u = (u_1, u_2, \ldots, u_r) \in \mathbb{N}^r \) is a vector of nonnegative integers. The set of integers is denoted by \( \mathbb{Z} \) and the set of nonnegative integers is \( \mathbb{N} \). The notation \( p^u \) is monomial vector notation for the monomial in Equation 3.1.1.

A polynomial in indeterminates \( p_1, p_2, \ldots, p_m \) over \( \mathbb{K} \) is a linear combination of finitely many monomials, with coefficients in \( \mathbb{K} \). That is, a polynomial can be represented as a sum

\[
f = \sum_{u \in A} c_u p^u
\]

where \( A \) is a finite subset of \( \mathbb{N}^m \), each each coefficient \( c_u \in \mathbb{K} \). Alternately, we could say that \( f = \sum_{u \in \mathbb{N}^r} c_u p^u \) where only finitely many of the coefficients \( c_u \) are nonzero elements of the field \( \mathbb{K} \).

For example, so for example, the expression \( p_2^2 p_3^4 \) is a monomial in the indeterminates \( p_1, p_2, p_3 \), with \( u = (2, 0, 4) \), whereas \( p_2^2 p_3^{-4} \) is not a monomial because there is a negative in the exponent of indeterminate \( p_3 \). An example of a polynomial is

\[
f = p_1^2 p_3^4 + 6 p_1^2 p_2 - \sqrt{2} p_1^3 p_2 p_3^2
\]

which has three terms. The power series

\[
\sum_{i=0}^{\infty} p_1^i
\]

is not a polynomial because it has infinitely many terms with nonzero coefficients.

Let

\[
\mathbb{K}[p] := \mathbb{K}[p_1, p_2, \ldots, p_r]
\]

be the set of all polynomials in the indeterminates \( p_1, p_2, \ldots, p_r \) with coefficients in \( \mathbb{K} \). This set of polynomials forms a ring, because the sum of two polynomials is a polynomial, the product of two polynomials is a polynomials, and these two operations follow all the usual properties of a ring, (e.g. multiplication distributes over addition of polynomials). Each polynomial is naturally considered as a multivariate function from \( \mathbb{K}^r \to \mathbb{K} \), by evaluation. For this reason, we will often refer to the ring \( \mathbb{K}[p] \) as the ring of polynomial functions.

Definition 3.1.1. Let \( S \subseteq \mathbb{K}[p] \) be a set of polynomials. The variety defined by \( S \) is the set

\[
V(S) = \{a \in \mathbb{K}^r : f(a) = 0 \text{ for all } f \in S\}.
\]

The variety \( V(S) \) is also called the zero set of \( S \).

Note that the set of points in the variety depends on which field \( \mathbb{K} \) we are considering. Most of the time, the particular field of interest should be clear from the context. In nearly all situations explored in this book, this will either be the real numbers \( \mathbb{R} \) or the complex numbers \( \mathbb{C} \). When we wish
3.1. Varieties

to call attention to the nature of the particular field under consideration, we will use the notation $V_{K}(S)$ to indicate the variety in the $K$.

**Example 3.1.2.** The variety $V(\{p_1 - p_2^2\}) \subset \mathbb{R}^2$ is the familiar parabolic curve, facing towards the right, whereas the variety $V(\{p_1^2 + p_2^2 - 1\}) \subset \mathbb{R}^2$ is a circle centered at the origin. The variety $V(\{p_1 - p_2^2, p_1^2 + p_2^2 - 1\})$ is the set of points that satisfy both of the equations

$$p_1 - p_2^2 = 0 \quad p_1^2 + p_2^2 - 1 = 0$$

and thus is the intersection $V(\{p_1 - p_2^2\}) \cap V(\{p_1^2 + p_2^2 - 1\})$. Thus, the variety $V(\{p_1 - p_2^2, p_1^2 + p_2^2 - 1\})$ is a finite number of points. It makes a difference which field we consider this variety over, and the number of points varies with the field. Indeed,

$$V_{\mathbb{Q}}(\{p_1 - p_2^2, p_1^2 + p_2^2 - 1\}) = \emptyset$$

$$V_{\mathbb{R}}(\{p_1 - p_2^2, p_1^2 + p_2^2 - 1\}) = \left\{ \left( \frac{-1 + \sqrt{5}}{2}, \pm \sqrt{\frac{-1 + \sqrt{5}}{2}} \right) \right\}$$

$$V_{\mathbb{C}}(\{p_1 - p_2^2, p_1^2 + p_2^2 - 1\}) = \left\{ \left( \frac{-1 \pm \sqrt{5}}{2}, \pm \sqrt{\frac{-1 \pm \sqrt{5}}{2}} \right) \right\}.$$

In many situations, it is natural to consider polynomial equations like $p_1^2 + 4p_2 = -17$, that is, polynomial equations that are not of the form $f(p) = 0$, but instead of the form $f(p) = g(p)$. These can, of course, be transformed into the form discussed previously, by moving all terms to one side of the equation, i.e. $f(p) - g(p) = 0$. Writing equations in this standard form is often essential for exploiting the connection to algebra which is at the heart of algebraic geometry.

In many situations in algebraic statistics, varieties are presented as parametric sets. That is, there is some polynomial map $\phi : \mathbb{K}^d \to \mathbb{K}^r$, such that $V = \{\phi(t) : t \in \mathbb{K}^d\}$ is the image of the map. We will also use $\phi(\mathbb{K}^d)$ as shorthand to denote this image.

**Example 3.1.3 (Twisted Cubic).** Consider the polynomial map

$$\phi : \mathbb{C} \to \mathbb{C}^3, \quad \phi(t) = (t, t^2, t^3)$$

The image of this map is the twisted cubic curve in $\mathbb{C}^3$. Every point on the twisted cubic satisfies the equations $p_1^3 = p_2$ and $p_1^2 = p_3$, and conversely every point satisfying these two equations is in the image of the map $\phi$.

The next example concerns a parametric variety which arises naturally in the study of statistical models.
Example 3.1.4 (Binomial Random Variables). Consider the polynomial map \( \phi : \mathbb{C} \to \mathbb{C}^{r+1} \) whose \( i \)th coordinate function is

\[
\phi_i(t) = \binom{r}{i} t^i (1-t)^{r-i}, \quad i = 0, 1, \ldots, r.
\]

For a real parameter \( \theta \in [0, 1] \), the value \( \phi_i(\theta) \) is the probability \( P(X = i) \) where \( X \) is a binomial random variable with success probability \( \theta \). That is, if \( \theta \) is the probability of getting a head in one flip of a biased coin, \( \phi_i(\theta) \) is the probability of seeing \( i \) heads in \( r \) independent flips of the same biased coin. Hence, the vector \( \phi(\theta) \) denotes the probability distribution of a binomial random variable.

The image of the real interval \([0, 1]\), is a curve inside the probability simplex

\[
\Delta_r = \left\{ p \in \mathbb{R}^{r+1} : \sum_{i=0}^{r} p_i = 1, p_i \geq 0 \text{ for all } i \right\}.
\]

which consists of all possible probability distributions of a binomial random variable. For example, in the case of \( r = 2 \), the curve \( \phi([0,1]) \) is the red curve inside the probability simplex in the figure.

\[\text{Figure 3.1.1.} \text{ The set of all binomial random variables for } r = 2 \text{ flips of a biased coin.}\]

The image of the complex parametrization \( \phi(\mathbb{C}) \) is a curve in \( \mathbb{C}^{r+1} \) that is also an algebraic variety. In particular, it is the set of points satisfying the trivial equation \( \sum_{i=0}^{r} p_i = 1 \) together with the vanishing of all \( 2 \times 2 \) subdeterminants of the following \( 2 \times m \) matrix:

\[
\begin{pmatrix}
p_0/\binom{r}{0} & p_1/\binom{r}{1} & p_2/\binom{r}{2} & \cdots & p_{r-1}/\binom{r}{r-1} \\
p_1/\binom{r}{1} & p_2/\binom{r}{2} & p_3/\binom{r}{3} & \cdots & p_r/\binom{r}{r}
\end{pmatrix}.
\]

In applications in algebraic statistics, it is common to consider not only maps whose coordinates functions are polynomial functions, but also maps whose coordinate functions are rational functions. Such, functions have the form \( f/g \) where \( f \) and \( g \) are polynomials. Hence, a rational map is a map \( \phi : \mathbb{C}^d \to \mathbb{C}^r \), where each coordinate function \( \phi_i = f_i/g_i \) where each \( f_i, g_i \in \mathbb{K}[t] := \mathbb{K}[t_1, \ldots, t_d] \) are polynomials. Note that the map \( \phi \) is not defined on all of \( \mathbb{C}^d \), it is only well defined off of the hypersurface \( V(\{\prod_i g_i\}) \).
If we speak of the image of \( \phi \), we mean the image of the set \( \mathbb{C}^d \setminus V(\prod_i g_i) \), where the rational map \( \phi \) is well-defined. The symbol \( \rightarrow \rightarrow \) is used in the notational definition of a rational map to indicate that the map need not be defined everywhere.

### 3.2. Ideals

In the preceding section, we showed how to go from a collection of polynomials (an algebraic object) to their common zero set (a geometric object). This construction can be reversed: from a geometric object we can construct the set of polynomials that vanish on it. The sets of polynomials that can arise in this way have the algebraic structure of a radical ideal. This interplay between varieties and ideals is at the heart of algebraic geometry. We describe the ingredients here.

**Definition 3.2.1.** Let \( W \subset \mathbb{K}^r \). The set of polynomials

\[
I(W) = \{ f \in \mathbb{K}[p] : f(a) = 0 \text{ for all } a \in W \}
\]

is the **vanishing ideal** of \( W \) or the defining ideal of \( W \).

Recall that a subset \( I \) of a ring \( R \) is an ideal if for all \( f, g \in I \), \( f + g \in I \), and for all \( f \in I \) and \( h \in R \), \( hf \in I \). As the name implies, the set \( I(W) \) is an ideal (e.g. Exercise 3.1).

A collection of polynomials \( F \) is said to generate an ideal \( I \), if it is the case that every polynomial \( f \in I \) can be written as a finite linear combination of the form \( f = \sum_{i=1}^{k} h_i f_i \) where \( f_i \in F \) and the \( h_i \) are arbitrary polynomials in \( \mathbb{K}[p] \). The number \( k \) might depend on \( f \). In this case we use the notation \( \langle F \rangle = I \) to denote that \( I \) is generated by \( F \).

**Theorem 3.2.2** (Hilbert Basis Theorem). For every ideal \( I \) in a polynomial ring \( \mathbb{K}[p_1, \ldots, p_r] \) there exists a finite set of polynomials \( F \subset I \) such that \( I = \langle F \rangle \). That is, every ideal in \( \mathbb{K}[p] \) has a finite generating set.

Note that the Hilbert Basis Theorem only holds for polynomial rings in finitely many variables. In general, a ring that satisfies the property that every ideal has a finite generating set is called a Noetherian ring.

When presented with a set \( W \subset \mathbb{K}^r \), we are often given the task of finding a finite set of polynomials in \( I(W) \) that generate the ideal. The special case where the set \( W = \phi(\mathbb{K}^d) \) for some rational map \( \phi \) is called an **implicitization problem** and many problems in algebraic statistics can be interpreted as implicitization problem.
Example 3.2.3 (Binomial Random Variables). Let $\phi : \mathbb{C} \to \mathbb{C}^{r+1}$ be the map from Example 3.1.4. Then the ideal $I(\phi(\mathbb{C})) \subseteq \mathbb{C}[p_0, \ldots, p_r]$ is generated by the polynomials $\sum_{i=0}^r p_i - 1$ plus the $2 \times 2$ minors of the matrix from Equation (3.1.2).

In the special case where $r = 2$, we have

$$I(\phi(\mathbb{C})) = \langle p_0 + p_1 + p_2 - 1, 4p_0p_2 - p_1^2 \rangle.$$ 

So the two polynomials $p_0 + p_1 + p_2 - 1$ and $4p_0p_2 - p_1^2$ solve the implicitization problem in this instance. We will describe computational techniques for solving the implicitization problem in Section 3.4.

If we are given an ideal, we can iteratively compute the variety defined by the vanishing of that ideal, and then compute the vanishing ideal of the resulting variety. We always have $I \subseteq I(V(I))$. However, this containment need not be an equality, as the example $I = \langle p_1^2 \rangle$ indicates. The ideals that can arise as vanishing ideals are forced to have some extra structure.

Definition 3.2.4. An ideal $I$ is called radical if $f^k \in I$ for some polynomial $f$ and positive integer $k$ implies that $f \in I$. The radical of $I$, denoted $\sqrt{I}$, is the smallest radical ideal that contains $I$ and consists of the polynomials:

$$\sqrt{I} = \left\{ f \in \mathbb{K}[p] : f^k \in I \text{ for some } k \in \mathbb{N} \right\}.$$

Proposition 3.2.5. For any field and any set $W \subset \mathbb{K}^m$, the ideal $I(W)$ is a radical ideal.

Theorem 3.2.6 (Nullstellensatz). Suppose that $\mathbb{K}$ is algebraically closed (e.g. $\mathbb{C}$). Then the vanishing ideal of the variety of an ideal is the radical of the ideal: $I(V(I)) = \sqrt{I}$.

When $\mathbb{K}$ is algebraically closed, the radical provides a closure operation for ideals, by determining all the functions that vanish on the underlying varieties $V(I)$. Computing $V(I(W))$ provides the analogous algebraic closure operations for subsets of $\mathbb{K}^m$.

Proposition 3.2.7. The set $V(I(W))$ is called the Zariski closure of $W$. It is the smallest algebraic variety that contains $W$.

A set $W \subset \mathbb{K}^r$ is called Zariski closed if it is a variety, that is of the form $W = V(S)$ for some $S \subseteq \mathbb{K}[p]$. Note that since polynomial functions are continuous in the standard Euclidean topology, the Zariski closed sets are also closed in the standard Euclidean topology.

Example 3.2.8. As an example of a Zariski closure let $W \subset \mathbb{K}^2$ consists of the $p_1$ axis with the origin $(0,0)$ removed. Because polynomials are continuous, any polynomial that vanishes on $W$ vanishes on the origin as well.
Thus, the Zariski closure contains the $p_1$ axis. On the other hand, the $p_1$ axis is the variety defined by the ideal $\langle p_2 \rangle$, so the Zariski closure of $W$ is precisely the $p_1$ axis. In this case, if the field $\mathbb{K}$ was some subfield of the complex numbers, the Zariski closure merely corresponded to the closure operation in the standard topology. □

**Example 3.2.9** (Binomial Random Variable). Let $\phi : \mathbb{C} \to \mathbb{C}^{r+1}$ be the map from Example 3.1.4. The image of the interval $[0,1]$ in $\Delta_r$ is not a Zariski closed set. The Zariski closure of $\phi([0,1])$ equals $\phi(\mathbb{C})$. This is because $\phi(\mathbb{C})$ is Zariski closed, and the Zariski closure of $[0,1] \subseteq \mathbb{C}$ is all of $\mathbb{C}$.

Note that the Zariski closure of $[0,1]$ is not $\mathbb{R} \subseteq \mathbb{C}$. While $\mathbb{R} = \{z : z = \overline{z}\}$, $\mathbb{R}$ is not a variety when considered as a subset of $\mathbb{C}$, since complex conjugation is not a polynomial operation.

If we only care about subsets of $\Delta_r$, then $\phi([0,1])$ is equal to the Zariski closure intersected with the probability simplex. In this case, the variety gives a good approximation to the statistical model. □

Complements of Zariski closed sets are called Zariski open. The Zariski topology is the topology whose closed sets are the Zariski closed sets. The Zariski topology is a much coarser topology than the standard topology, as the following example illustrates.

**Example 3.2.10** (Mixture of Binomial Random Variables). Let $\mathcal{P} \subseteq \Delta_{r-1}$ be a family of probability distributions (i.e., a statistical model) and let $s > 0$ be an integer. The $s$th mixture model $\text{Mixt}^s(\mathcal{P})$ consists of all probability distributions which arise as convex combinations of $s$ distributions in $\mathcal{P}$. That is,

$$
\text{Mixt}^s(\mathcal{P}) = \left\{ \sum_{j=1}^{s} \pi_j p^{(j)} : \pi \in \Delta_{s-1} \text{ and } p^{(j)} \in \mathcal{P} \text{ for all } j \right\}.
$$

Mixture models allow to build a complex model from a simple model $\mathcal{P}$. The motivation for modeling with a mixture model will be explained in Chapter 14.

The special case of mixtures of binomial random variables arises in Bayesian statistics through its connection to exchangeability via de Finetti’s Theorem (see e.g. [DF80]). Focusing on the case $r = 2$ and $s = 2$, we see that $\text{Mixt}^2(\mathcal{P})$ is precisely the region below the curve in Figure 3.1.1. Since $\text{Mixt}^2(\mathcal{P})$ is a 2-dimensional subset of $\Delta_2$, we see that the Zariski closure of $\text{Mixt}^2(\mathcal{P})$ is the entire plane $V(p_0 + p_1 + p_2 - 1)$. Thus, the intersection of the Zariski closure and the probability simplex $\Delta_2$ is not the mixture model. This example illustrates the fact that in some situations in algebraic statistics, it might not be sufficient to only consider varieties. Indeed, sometimes
constraints using inequalities are necessary. In this example, the mixture
model is the set
\[ \Delta_2 \cap \left\{ p : \det \begin{pmatrix} 2p_0 & p_1 \\ p_1 & 2p_2 \end{pmatrix} \geq 0 \right\}. \]
We will return to the issues of real algebraic geometry in later chapters. □

Building on the Nullstellensatz, and the notion of Zariski closures, there
is a natural correspondence between radical ideals on the one hand, and
varieties on the other.

Theorem 3.2.11. Let \( K \) be an algebraically closed field. Then the maps
\[ V : \left\{ I \subseteq K[p] : I = \sqrt{I} \right\} \rightarrow \{ W \subseteq K^m | W = V(J) \text{ for some } J \subseteq K[p] \} \]
\[ I : \{ W \subseteq K^m | W = V(J) \text{ for some } J \subseteq K[p] \} \rightarrow \left\{ I \subseteq K[p] : I = \sqrt{I} \right\} \]
are inclusion reversing bijections between the set of radical ideals and the set
of varieties.

Note that the condition that \( K \) is algebraically closed is necessary (see
Exercise 3.4).

Theorem 3.2.11 is the Rosetta stone for decyphering the “algebra-geometry”
dictionary. Natural operations on the ideal or variety side lead to natural
related operations on the opposing side. For example consider the sum of
two ideals:
\[ I + J := \{ f + g : f \in I \text{ and } g \in J \}. \]
Note that if \( I \) and \( J \) are generated by \( \mathcal{F} \) and \( \mathcal{G} \) respectively, then \( I + J \) is
generated by \( \mathcal{F} \cup \mathcal{G} \), since the polynomial 0 belongs to any ideal.

Proposition 3.2.12.
\[ V(I + J) = V(I) \cap V(J) \]
and over an algebraically closed field
\[ I(V \cap W) = \sqrt{I(V)} + I(W). \]

Proof. It suffices to show the first equation, since the second follows by the
ideal-variety correspondence. Suppose that \( a \in V(I + J) \). Then \( f(a) = 0 \)
for all \( f \in I \) and for all \( f \in J \). This implies that \( a \in V(I) \cap V(J) \) and
implies the containment \( V(I + J) \subseteq V(I) \cap V(J) \). On the other hand, if
\( a \in V(I) \cap V(J) \), it satisfies all polynomials in \( I \) and in \( J \), and hence, all
polynomials in \( I + J \). □

Proposition 3.2.13.
\[ V(I \cap J) = V(I) \cup V(J) \]
\[ I(V \cup W) = I(V) \cap I(W) \]
3.3. Gröbner Bases

Gröbner bases are the algebraic tool for studying ideals computationally. The most basic use for Gröbner bases to answer the ideal membership problem; that is, to decide whether or not a given polynomial $f$ belongs to a particular ideal $I$. The fact that Gröbner bases solve the ideal membership problem allows for a great many further applications. We highlight some of these uses in this chapter and defer other applications until later in the book.

Definition 3.3.1. A term order $\prec$ is a total order on the set of monomials in the polynomial ring $\mathbb{K}[p]$ which satisfies the two conditions

(1) $1 = p^0 \leq p^u$ for all $u \in \mathbb{N}^r$ and

(2) $p^u \prec p^v$ implies that $p^w \cdot p^u \prec p^w \cdot p^v$ for all $w \in \mathbb{N}^r$.

Three common examples of terms orders are the lexicographic, reverse lexicographic, and weight term orders.

Example 3.3.2 (Lexicographic Term Order). The lexicographic term order $\prec_{\text{lex}}$ is defined by the rule $p^u \prec_{\text{lex}} p^v$ if and only if the leftmost nonzero element of $v - u$ is positive. For instance, the following is a chain of valid inequalities in the lexicographic order:

$$p_1^3 \succ_{\text{lex}} p_1^2 p_2^3 \succ_{\text{lex}} p_1^2 p_3^3 \succ_{\text{lex}} p_2^3 \succ_{\text{lex}} p_3^3.$$

The lexicographic order we have defined is with respect to a particular ordering of the variables. In particular, we are assuming that $p_1 \succ_{\text{lex}} p_2 \succ_{\text{lex}} \cdots \succ_{\text{lex}} p_m$. However, any permutation of the set of indices $\{1, 2, \ldots, m\}$ yields a different lexicographic term order.

Example 3.3.3 (Reverse Lexicographic Term Order). The reverse lexicographic term order $\succ_{\text{rev}}$ is defined by the rule $p^u \succ_{\text{rev}} p^v$ if and only if

(1) $\sum_{i=1}^m u_i < \sum_{i=1}^m v_i$, or

(2) $\sum_{i=1}^m u_i = \sum_{i=1}^m v_i$ and the rightmost nonzero entry of $v - u$ is negative.

For instance, the following is a chain of valid inequalities in the reverse lexicographic term order:

$$p_1^5 \succ_{\text{rev}} p_2^3 p_3^2 \succ_{\text{rev}} p_2^3 p_3^1 \succ_{\text{rev}} p_2^3 p_3^3 \succ_{\text{rev}} p_1.$$

As with the lexicographic order, we can get many different reverse lexicographic term order, by permuting the roles that the variables have to play.
3. Algebra Primer

Example 3.3.4 (Weight Orders). The weight orders are an important class of term orders that will play a role in Chapter 10. Let \( c \in \mathbb{Q}^r \) be a rational vector, and \( \prec \) an arbitrary term order. The weight order \( \prec_c \) is defined by the rule \( p^u \prec_c p^v \) if and only if

1. \( c^T u < c^T v \) or
2. \( c^T u = c^T v \) and \( p^u \prec p^v \).

The interpretation of the weight orders that will be useful later is that the vector \( c \) is a cost vector. Then monomials are larger in the weight order if they have larger cost with respect to the linear cost function \( c^T x \), and ties are broken with the tie breaking term order \( \prec \). Note that as we have defined term orders, the weight order is only a term order if \( c_i \geq 0 \) for all \( i \), an issue that we will remedy later.

Besides being a useful tool for its connections to integer programming that we will see later on, the weight orders also provide a useful mnemonic for remembering the definitions of the lexicographic and reverse lexicographic term orders. While neither of these term orders can be realized as weight orders, the idea of variable weight is natural in this context. Indeed, for the lexicographic order, the most expensive variables (\( p_1 \) then \( p_2 \), etc.) are so expensive that they make any monomial containing them large in the term order \( \prec_{\text{lex}} \). On the other hand, for the reverse lexicographic order, the cheap variables (\( p_m \), then \( p_{m-1} \), etc.) are so cheap that they make any monomial containing them small in the term order \( \prec_{\text{rev}} \).

Definition 3.3.5. Given a term order \( \prec \) and a polynomial \( f \in \mathbb{K}[p] \), the initial monomial of \( f \) with respect to \( \prec \) is the largest monomial \( p^u \) with respect to the ordering \( \prec \) among all the monomials appearing in \( f \) with nonzero coefficient. The initial monomial of \( f \) is denoted \( \text{in}_{\prec}(f) \).

Example 3.3.6. Let \( f = p_1^2 - 3p_1^2 p_2 + 6p_1^2 p_3 + \frac{\pi}{\sqrt{3}} p_4^2 + p_1^2 p_3^2 \). Then \( \text{in}_{\text{lex}}(f) = p_1^2 p_2 \) whereas \( \text{in}_{\text{rev}}(f) = p_2^4 \).

Initial terms extend naturally from polynomials to ideals.

Definition 3.3.7. The initial ideal \( \text{in}_{\prec}(I) \) of an ideal \( I \subseteq \mathbb{K}[p] \) with respect to the term order \( \prec \) is the monomial ideal generated by the initial monomials of all polynomials in \( I \):

\[
\text{in}_{\prec}(I) = \langle \text{in}_{\prec}(f) : f \in I \rangle.
\]

A Gröbner basis of the ideal \( I \) with respect to the term order \( \prec \) is a finite collection of polynomials \( \mathcal{G} \subset I \) such that the initial monomials of the elements of \( \mathcal{G} \) generate the initial ideal:

\[
\langle \text{in}_{\prec}(g) : g \in \mathcal{G} \rangle = \text{in}_{\prec}(I).
\]
Note that the initial ideal is not, in general, generated by the initial terms of a generating set of an ideal. For instance, consider the ideal \( I = \langle p_1^2, p_1p_2 + p_2^2 \rangle \). Then \( \text{in}_{\text{lex}} \) contains both the monomials \( p_1^2 \) and \( p_1p_2 \). These two monomials do not generate the initial ideal because the polynomial \( p_1^2 - (p_1 - p_2) \cdot (p_1p_2 + p_2^2) = p_2^3 \) belongs to \( I \), but its initial term \( p_2^3 \) does not belong to the monomial ideal \( \langle p_1^2, p_1p_2 \rangle \). The goal of the remainder of this section is to describe how to compute Gröbner bases and initial ideals, for instance, to explain how we found the polynomial \( p_2^3 \).

**Algorithm 3.3.8 (Division Algorithm).** Let \( \mathcal{G} = \{g_1, \ldots, g_k \} \) be a finite set of polynomials, \( f \) another polynomial, and \( < \) a term order.

Output of algorithm: A representation \( f = \sum h_i g_i + r \) such that no term of \( r \) is divisible by a leading term of any of the polynomials in \( \mathcal{G} \).

1. Set \( h_i = 0 \) for all \( i \) and \( r = f \).
2. While \( r \) has a term \( c_a p^a \) divisible by a leading term of some \( g_i \), replace \( h_i \) by \( h_i + c_a p^a / \text{in}_{\prec}(g_i) \) and replace \( r \) by \( r - c_a p^a / \text{in}_{\prec}(g_i) \cdot g_i \)

The algorithm terminates because a term ordering is a well ordering: there is no infinite decreasing sequence of monomials with respect to a term order.

The remainder \( r \) upon dividing \( f \) by \( \mathcal{G} \) is called the normal form of \( f \), and is denoted by the shorthand notation \( NF_{\mathcal{G}}(f) \). Of course, one must be careful with this definition because the normal form is not uniquely determined by the \( \mathcal{G} \) and \( f \) in general. In particular, it might depend on the order we choose to divide polynomials into each other.

In the special case where \( \mathcal{G} \) consists of a single polynomial \( g \), the normal form computation directly allows us to decide whether or not the polynomial \( f \) belongs to the ideal \( \langle g \rangle \). In particular, in this case \( NF_{\mathcal{G}}(f) = 0 \) if and only if \( f \in \langle g \rangle \). The division algorithm also gives a method for addressing the ideal membership problem for arbitrary ideals, but one must work with a Gröbner basis. Indeed, this is given an alternate characterization of a Gröbner basis.

**Theorem 3.3.9.** Let \( I \) be an ideal, \( < \) a term order, and \( \mathcal{G} \) a finite subset of \( I \). Then \( NF_{\mathcal{G}}(f) = 0 \) for all \( f \in I \) if and only if \( \mathcal{G} \) is a Gröbner basis for \( I \) with respect to \( < \).

**Corollary 3.3.10.** Let \( I \) be an ideal \( < \) a term order, and \( \mathcal{G} \) a Gröbner basis for \( I \) with respect to \( < \). Then \( \mathcal{G} \) is a generating set of \( I \).

**Proof.** Let \( f \in I \) and \( \mathcal{G} = \{g_1, \ldots, g_k \} \). Theorem 3.3.9 shows that \( NF_{\mathcal{G}}(f) = 0 \). This, in turn, shows that there are \( h_1, \ldots, h_k \) in \( \mathbb{K}[p] \) such that \( f = h_1 g_1 + \cdots + h_k g_k \). In other words, every element of \( f \) can be expressed as a
polynomial combination of the elements of $G$. Hence, $G$ is a generating set of $I$. □

Let $f$ and $g$ be two polynomials with $\prec$ leading terms $p^u$ and $p^v$ respectively. In the quest to find new polynomials in the ideal containing $f$ and $g$ with new leading terms, we can form the polynomial

$$S(f, g) = \frac{p^v}{\gcd(p^u, p^v)} f - \frac{p^u}{\gcd(p^u, p^v)} g$$

which is called the $S$-polynomial of $f$ and $g$. Note that the $S$-polynomial cancels the leading terms of $f$ and $g$ in the most economical way possible, and $S(f, g)$ gives a candidate for a new polynomial which might need to appear in a Gröbner basis. If $f$ and $g$ were part of a Gröbner basis $G$ of $I$ with respect to $\prec$, then $NF_{G}(S(f, g)) = 0$, by Theorem 3.3.9. The converse is also true.

**Theorem 3.3.11** (Buchberger’s Criterion). Let $I$ be an ideal, $\prec$ a term order and $G$ a finite generating set of $I$. Then $G$ is a Gröbner basis of $I$ with respect to $\prec$ if and only if $NF_{G}(S(f, g)) = 0$ for all $f, g \in G$.

Buchberger’s criterion leads to a straightforward algorithm for computing Gröbner bases of ideals from their generating sets.

**Algorithm 3.3.12** (Buchberger’s Algorithm). *Input:* Finite generating set $F$ of $I$, and a term order $\prec$.

*Output:* Gröbner basis $G$ for $I$ with respect to $\prec$.

(1) Set $G := F$

(2) While $G$ does not satisfy Buchberger’s criterion, do:

- There exists a pair $f, g \in G$ such that $NF_{G}(S(f, g)) = h \neq 0$.
- Set $G := G \cup \{h\}$

(3) Output: $G$ is a Gröbner basis for $I$ with respect to $\prec$.

Note that the algorithm is guaranteed to terminate by the Hilbert basis theorem. At each step we have a candidate initial ideal $J_i = \langle \text{in}_{\prec}(f) : f \in G \rangle$ which form an ascending chain. Then Exercise 3.5 guarantees these ideals, and hence the set $G$, must stabilize. Algorithms which are implemented to compute Gröbner bases are all based on Buchberger’s Algorithm. There are many refinements and extensions of Buchberger’s algorithm which can be used to speed up the computation and are implemented in practice.

**Example 3.3.13.** Consider the ideal $I = \langle p_1^2, p_1p_2 + p_2^2 \rangle$ and the lexicographic term order. We will describe how to compute a Gröbner basis using Buchberger’s algorithm. We compute the $S$-polynomial

$$S(p_1^2, p_1p_2 + p_2^2) = p_2 \cdot p_1^2 - p_1 \cdot (p_1p_2 + p_2^2) = -p_1p_2^2.$$
Performing long-division by $p_1^2, p_1p_2 + p_2^2$ produces the normal form $NF_G(S(p_1^2, p_1p_2 + p_2^2)) = p_2^3$, which is nonzero. Hence, our new candidate Gröbner basis becomes $G = \{p_1^2, p_1p_2 + p_2^2, p_3^2\}$. Computing the normal forms of the $S$-polynomials for all pairs in $G$ reveals that $G$ is a Gröbner basis for $I$ with respect to the lexicographic term order.

\[ \square \]

### 3.4. First Applications of Gröbner Bases

The Buchberger algorithm and its generalizations are the major workhorse of computational algebra packages, because many useful invariants of an ideal $I$, and hence, a variety, can be read off from properties of the initial ideal. Furthermore, Gröbner bases can be used to solve the implicitization problem for rational maps, which we describe here.

For a variety, the dimension is simply the dimension as a topological space, which can be determined by the implicit function theorem by looking at smooth points. For an ideal $I$, we define the dimension to simply be the dimension of the variety $V(I)$. For this to make sense, it is essential that we work over an algebraically closed field. When referring to the dimension of an ideal when the underlying field is not algebraically closed, we will mean the dimension over the algebraic closure (which corresponds to more general algebraic definitions of dimension, for instance, in [Eis95]). Rather than using the implicit function theorem, it turns out that this fundamental invariant of a variety can be computed directly from any initial ideal.

**Proposition 3.4.1.** Let $\mathbb{K}$ be an algebraically closed field. Then $\dim I = \dim \text{in}_\prec(I)$ for any term order $\prec$. Furthermore, for a monomial ideal $M$, the dimension is equal to the cardinality of the largest subset $S \subseteq [m]$ such that the monomial $\prod_{i \in S} p_i^k$ is not in $M$ for all $k \in \mathbb{N}$.

Proposition 3.4.1 gives a straightforward method to compute the dimension of a variety, and is the standard method for computing dimensions in computational algebra packages.

Among the most important geometric objects for algebraic statistic are parametrized algebraic sets, which will play a major role throughout the book.

That is, suppose we are given a polynomials $\phi_1, \phi_2, \ldots, \phi_r \in \mathbb{K}[t] := \mathbb{K}[t_1, t_2, \ldots, t_d]$. Consider the map

$$\phi: \mathbb{K}^d \to \mathbb{K}^r$$

$$(\theta_1, \ldots, \theta_d) \mapsto (\phi_1(\theta), \ldots, \phi_r(\theta)).$$

If $\Theta \subseteq \mathbb{K}^d$ is a subset of the domain of $\phi$,

$$\phi(\Theta) = \{\phi(\theta) : \theta \in \Theta\}$$
is the image of the parametrization $\phi$. More generally, we could consider this problem in the case of rational of a rational map $\phi : \Theta \rightarrow K^r$. The *implicitization problem* asks to take the sets $\Theta$ and the rational map $\phi$ and compute the vanishing ideal $I(\phi(\Theta))$.

As we saw with the example of the twisted cubic, the image of a parametrization can be a variety. Note that this need not be the case in general.

**Example 3.4.2.** Consider the parametrization $\phi : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ given by 
\[
\phi_1(\theta_1, \theta_2) = \theta_1, \quad \phi_2(\theta_1, \theta_2) = \theta_1 \theta_2.
\]
The image of this parametrization $\phi(\mathbb{C}^2)$ consists of all points $(a_1, a_2)$ in $\mathbb{C}^2$ such that $a_1 \neq 0$ together with the origin. The set $\phi(\mathbb{C}^2)$ is not a variety: the Zariski closure is equal to all of $\mathbb{C}^2$, since any polynomial that vanishes on a dense subset of $\mathbb{C}^2$ is the zero polynomial.

While the image of a parametrization need not be a variety, in the algebraically closed case, it is close to being a variety.

**Theorem 3.4.3.** Let $V$ be a variety and $\phi$ a rational map $\phi : V \rightarrow \mathbb{K}^m$. Then there is a finite sequence of varieties $W_1 \supset W_2 \supset \cdots \subset W_k$ in $W$ such that
\[
\phi(V) = W_1 \setminus (W_2 \setminus (\cdots \setminus W_k)\cdots)).
\]

Note that Theorem 3.4.3 only holds when $\mathbb{K}$ is algebraically closed. For example consider the map $\phi : \mathbb{R} \rightarrow \mathbb{R}$, $\phi(\theta) = \theta^2$. The image $\phi(\mathbb{R})$ is the half-ray $[0, \infty)$ which is not of the constructible form in Theorem 3.4.3.

The images of real algebraic varieties under rational maps do have special structure and are the subject of Tarski-Seidenberg theorem, which we will return to later in the book.

To understand how to solve the implicitization problem for general rational maps, we must first get a handle on linear maps. After a change of coordinates, we can assume such a linear map is a coordinate projection. The next proposition and theorem show that the vanishing ideal of a coordinate projection can be computed using Gröbner bases.

**Proposition 3.4.4.** Let $\phi : \mathbb{K}^{r_1+r_2} \rightarrow \mathbb{K}^{r_1}$ be the coordinate projection 
\[
(a_1, \ldots, a_{r_1}, b_1, \ldots, b_{r_2}) \mapsto (a_1, \ldots, a_{r_1}).
\]
Let $V \subseteq \mathbb{K}^{r_1+r_2}$ be a variety and $I = I(V) \subseteq \mathbb{K}[p, q] := \mathbb{K}[p_1, \ldots, p_{r_1}, q_1, \ldots, q_{r_2}]$ be its vanishing ideal. Then the vanishing ideal of the image $\phi(V)$ is the elimination ideal
\[
I(\phi(V)) = I \cap \mathbb{K}[p].
\]

Generators for the elimination ideals can be determined by computing a Gröbner basis.
Theorem 3.4.5. Let $I \subseteq \mathbb{K}[p,q]$ and let $\prec$ be a lexicographic term order such that
\[ q_1 \succ \cdots \succ q_r \succ p_1 \succ \cdots \succ p_r. \]
If $G$ is a Gröbner basis of $I$ with respect to $\prec$ then
\[ I \cap \mathbb{K}[p] = \langle G \cap \mathbb{K}[p] \rangle \]
and furthermore $G \cap \mathbb{K}[p]$ is a Gröbner basis for the elimination ideal $I \cap \mathbb{K}[p]$.

Aside from the lexicographic term order used in Theorem 3.4.5, any other elimination term ordering can be used. An elimination ordering is a term ordering where any monomial with a $q$ indeterminate appearing to any nonzero power is larger than every monomial only in the $p$ indeterminates.

From linear projections, it is only a single step to computing the images of general rational maps. We first consider the case of polynomial maps. Suppose that $\phi : \mathbb{K}^{r_2} \to \mathbb{K}^{r_1}$ is a polynomial map (each component function is a polynomial). The graph of the map is the set of points
\[ \Gamma_\phi = \{(\phi(\theta), \theta) : \theta \in \mathbb{K}^{r_2}\} \subset \mathbb{K}^{r_1+r_2}. \]
If $\mathbb{K}$ is an infinite field the vanishing ideal of the graph is
\[ I(\Gamma_\phi) = \langle p_1 - \phi_1(q), \ldots, p_r - \phi_r(q) \rangle. \]

Proposition 3.4.6. Let $I \subset \mathbb{K}[q]$ be the vanishing ideal of a variety $V \subset \mathbb{K}^{r_2}$. Let $\phi$ be a polynomial map $\phi : \mathbb{K}^{r_2} \to \mathbb{K}^{r_1}$. Then the vanishing ideal of the Zariski closure is the elimination ideal
\[ I(\phi(V)) = (I + I(\Gamma_\phi)) \cap \mathbb{K}[p]. \]

The ideal $I + I(\Gamma_\phi)$ has as its generating set all the polynomial generators of $I$ (\subseteq $\mathbb{K}[q]$) plus the $r_1$ polynomials $p_1 - \phi_1(q), \ldots, p_r - \phi_r(q)$. Hence the implicitization problem can be solved computationally by computing a Gröbner basis.

To handle rational maps requires only a small modification to the construction above. In particular, we need a way to handle the denominators that appear in the rational functions $\phi_i = f_i/g_i$.

Proposition 3.4.7. Let $I \subset \mathbb{K}[q]$ be the vanishing ideal of a variety $V \subset \mathbb{K}^{r_2}$. Let $\phi$ be a rational map $\phi : \mathbb{K}^{r_2} \to \mathbb{K}^{r_1}$, with coordinate functions $\phi_i = f_i/g_i$. Then the vanishing ideal of the Zariski closure is the elimination ideal
\[ I(\phi(V)) = (I + \langle g_1p_1 - f_1, \ldots, g_r p_r - f_r, zg_1 \cdots g_r\rangle) \cap \mathbb{K}[p]. \]

Note that the ideal in parentheses on the right hand side of the equality in Proposition 3.4.7 belongs to the ring $\mathbb{K}[p,q,z]$, where $z$ is an extra indeterminate. This extra indeterminate is the added feature which is necessary
to clear the denominators. Note that the equation \( zg_1 \cdots g_{r_1} - 1 \) guarantees that we only consider points in the graph where none of the denominators are zero.

### 3.5. Computational Algebra Vignettes

Gröbner bases are the primary tool for computing with algebraic varieties. Fortunately, they have been implemented in most software for performing symbolic computation. Many computations which use Gröbner bases can be performed directly without understanding how the Buchberger algorithm works, nor how certain computations are translated into Gröbner basis calculations. We illustrate some of the basic things that can be done with these computational algebra software packages in this section. Two pieces of software we illustrate here are Macaulay2 and Singular. Throughout the book we will return to these two pieces of computational algebraic geometry software to illustrate various points and to demonstrate examples that go beyond what can easily be computed by hand. We stress, however, that in practice in algebraic statistics, we use the computational algebra software to gain insight by studying small example. Then we usually try to prove theorems that generalize the small examples to more general settings.

Macaulay 2. Macaulay 2 is a computational algebraic geometry software developed by Dan Grayson and Mike Stillman with contributions of packages from many mathematicians. We display some elementary computations with Gröbner bases here.

```plaintext
R1 = QQ[p0,p1,p2,p3,p4, MonomialOrder => Lex];
```

This command declares the ring \( R_1 \). Note that the monomial order is a fixed feature of the ring.

```plaintext
i2 : M = matrix{
   {p0, p1/4, p2/6, p3/4},
   {p1/4, p2/6, p3/4, p4}};
```

```plaintext
2  4
o2 : Matrix R1 <--- R1
```

```plaintext
i3 : I = ideal(p0 + p1 + p2 + p3 + p4 -1) + minors(2, M);
```

```plaintext
o3 : Ideal of R1
```

```plaintext
i4 : gb I
```

```plaintext
o4 = GroebnerBasis[status: done; S-pairs encountered up to degree 4]
```

```plaintext
o4 : GroebnerBasis
```
3.5. Computational Algebra Vignettes

i5 : gens gb I

\[
\begin{align*}
&\mathbf{p}_3^4+16\mathbf{p}_3^3\mathbf{p}_4+96\mathbf{p}_3^2\mathbf{p}_4^2+256\mathbf{p}_3\mathbf{p}_4^3+256\mathbf{p}_4^4-256\mathbf{p}_4^3 8\mathbf{p}_2\mathbf{p}_4-3\mathbf{p}_3^2 \\
&\mathbf{p}_2\mathbf{p}_3^2+6\mathbf{p}_3^3+36\mathbf{p}_3^2\mathbf{p}_4+96\mathbf{p}_3\mathbf{p}_4^2+96\mathbf{p}_4^3-96\mathbf{p}_4^2 \\
&2\mathbf{p}_2^2+12\mathbf{p}_2\mathbf{p}_3+27\mathbf{p}_3^2+72\mathbf{p}_3\mathbf{p}_4+72\mathbf{p}_4^2-72\mathbf{p}_4 \\
&6\mathbf{p}_1\mathbf{p}_4-\mathbf{p}_2\mathbf{p}_3 \\
&3\mathbf{p}_1\mathbf{p}_3+8\mathbf{p}_2\mathbf{p}_3+18\mathbf{p}_3^2+48\mathbf{p}_3\mathbf{p}_4+48\mathbf{p}_4^2-48\mathbf{p}_4 \\
&\mathbf{p}_1\mathbf{p}_2-10\mathbf{p}_2\mathbf{p}_3-30\mathbf{p}_3^2-90\mathbf{p}_3\mathbf{p}_4-6\mathbf{p}_3-96\mathbf{p}_4^2+96\mathbf{p}_4 \\
&3\mathbf{p}_1^2+40\mathbf{p}_2\mathbf{p}_3-8\mathbf{p}_2+135\mathbf{p}_3^2+432\mathbf{p}_3\mathbf{p}_4+48\mathbf{p}_3+480\mathbf{p}_4^2-480\mathbf{p}_4 \\
&\mathbf{p}_0+\mathbf{p}_1+\mathbf{p}_2+\mathbf{p}_3+\mathbf{p}_4-1 \quad | \\
&1 \quad 9 \\
\end{align*}
\]

This command creates the vanishing ideal of the binomial random variable from Example 3.1.4 for \( r = 4 \). Note that the command `gb I` computes the Gröbner basis of the ideal \( I \) with respect to the lexicographic order declared in the ring \( \mathbb{R}_1 \). However, to see the result of the computation, use the command `gens gb I`. The operator `%` computes the normal form with respect to the Gröbner basis. The calculation `dim I` shows that the variety of this ideal is one dimensional.

i6 : p0^3 % I

\[
\begin{align*}
&-3\mathbf{p}_1-33\mathbf{p}_2\mathbf{p}_3+5\mathbf{p}_2-\mathbf{p}_3-\mathbf{p}_3-\mathbf{p}_3-\mathbf{p}_3-\mathbf{p}_4-\mathbf{p}_4-135\mathbf{p}_3\mathbf{p}_4- \\
&16 \quad 8 \quad 4 \\
&330\mathbf{p}_3\mathbf{p}_4-31\mathbf{p}_3-165\mathbf{p}_4-165\mathbf{p}_4+329\mathbf{p}_4+1 \\
\end{align*}
\]

i7 : dim I

\( \text{o7} = 1 \)

The next collection of computations shows how to compute the vanishing ideal of the mixture model \( \text{Mixt}^2(\mathcal{P}) \) where \( \mathcal{P} \subseteq \Delta_4 \) is the model of a binomial random variable with \( r = 4 \) flips of a biased coin (which we have been computing with, above). To be able to use Proposition 3.4.6 we realize
the mixture model as the image of the parametrization
\[ \phi : \mathcal{P} \times \mathcal{P} \times \Delta_1 \rightarrow \mathbb{R}^5, \quad (p^{(1)}, p^{(2)}, \pi) \mapsto \pi p^{(1)} + (1 - \pi) p^{(2)}. \]
This means we can compute the vanishing ideal \( I(\text{Mixt}^2(\mathcal{P})) \) by performing a Gröbner basis computation in 16 indeterminates. This is presented here:

```plaintext
i1 : R2 = QQ[q10,q11,q12,q13,q14, q20,q21,q22,q23,q24, p, p0,p1,p2,p3,p4, MonomialOrder => Eliminate 11];

i2 : M1 = matrix{
    {q10, q11/4, q12/6, q13/4},
    {q11/4, q12/6, q13/4, q14}};

2 4
o2 : Matrix R2 <--- R2

i3 : I1 = ideal(q10 + q11 + q12 + q13 + q14 -1) + minors(2, M1);

o3 : Ideal of R2

i4 : M2 = matrix{
    {q20, q21/4, q22/6, q23/4},
    {q21/4, q22/6, q23/4, q24}};

2 4
o4 : Matrix R2 <--- R2

i5 : I2 = ideal(q20 + q21 + q22 + q23 + q24 -1) + minors(2, M2);

o5 : Ideal of R2

i6 : I3 = ideal( p0 - p*q10 - (1-p)*q20,
    p1 - p*q11 - (1-p)*q21,
    p2 - p*q12 - (1-p)*q22,
    p3 - p*q13 - (1-p)*q23,
    p4 - p*q14 - (1-p)*q24);

o6 : Ideal of R2

i7 : J = I1 + I2 + I3;

o7 : Ideal of R2

i8 : betti gens gb J

  0 1
o8 = total: 1 77
```
0: 1 3
1: . 16
2: . 22
3: . 18
4: . 17
5: . 1

\texttt{o8 : BettiTally}

\texttt{i9 : Mixt2I = ideal selectInSubring(1, gens gb J);} 

\texttt{o9 : Ideal of R2}

\texttt{i10 : gens Mixt2I}

\texttt{o10 = | p0+p1+p2+p3+p4-1 2p2^3-9p1p2p3-27p1p3^2-27p2p3^2-27p3^3+27p1^}
\texttt{2p4+72p1p2p4+72p2^2p4+72p2p3p4-27p3^2p4+72p2p4^2+27p3^2-72p2p4 |}

\texttt{1 2}

\texttt{o10 : Matrix R2 \leftarrow R2}

Note that we have declared our ring with an elimination term ordering that eliminates the first 11 indeterminates in the ring. The command \texttt{betti gens gb J} gives the number in each degree of the elements in the Gröbner basis of the ideal of the graph \textit{J}, with respect to the elimination ordering. There are 3 polynomials of degree 1, 16 of degree 2, \ldots, down to 1 of degree 5. The command \texttt{selectInSubring(1, gens gb J)} retrieves only those elements which are in the \textit{p}_i indeterminates.

The vanishing ideal \textit{I}(Mixt^2(\mathcal{P})) is generated by the trivial linear polynomial \(p_0 + p_1 + p_2 + p_3 + p_4 - 1\) and a complicated looking cubic. Just as the model of binomial random variables had a vanishing ideal generated by \(2 \times 2\) minors, its mixture model has vanishing ideal generated by a \(3 \times 3\) minor, as the following computation verifies.

\texttt{i11 : M3 = matrix{}
  \{p0, p1/4, p2/6},
  \{p1/4, p2/6, p3/4},
  \{p2/6, p3/4, p4\};}

\texttt{3 3}

\texttt{o11 : Matrix R2 \leftarrow R2}

\texttt{i12 : K = ideal(p0 + p1 + p2 + p3 + p4 -1) + minors(3, M3);} 

\texttt{o12 : Ideal of R2}
An alternate strategy for computing the vanishing ideal of this mixture model is to use the fact that the underlying model \( \mathcal{P} \) is itself the image of a parametrization. Indeed, it is the image of a parametrization

\[
\phi : \Delta_1 \times \Delta_1 \times \Delta_1 \to \mathbb{R}^5
\]

\[
\phi_i(\theta_1, \theta_2, \pi) = \binom{4}{i} \pi (1 - \theta_1)^{4-i} \theta_1^i + \binom{4}{i} (1 - \pi)(1 - \theta_2)^{4-i} \theta_2^i.
\]

This induces the pullback ring homomorphism

\[
\phi^* : \mathbb{K}[p_0, p_1, p_2, p_3, p_4] \to \mathbb{K}[\pi, \theta_1, \theta_2]
\]

\[
\phi^*_i(p_i) = \binom{4}{i} \pi (1 - \theta_1)^{4-i} \theta_1^i + \binom{4}{i} (1 - \pi)(1 - \theta_2)^{4-i} \theta_2^i.
\]

The vanishing ideal \( I(\text{Mixt}^2(\mathcal{P})) \) is the kernel of \( \phi^* \). The following code realizes the computation of the vanishing ideal in this manner.

\[
\text{i1 : } S = \mathbb{Q}[a_1, a_2, p];
\]

\[
\text{i2 : } R = \mathbb{Q}[p_0, p_1, p_2, p_3, p_4];
\]

\[
\text{i3 : } f = \text{map}(S, R, \{ 
1 p*(1-a1)^4*a1^0 + (1-p)*(1-a2)^4*a2^0, 
4*p*(1-a1)^3*a1^1 + 4*(1-p)*(1-a2)^3*a2^1, 
6*p*(1-a1)^2*a1^2 + 6*(1-p)*(1-a2)^2*a2^2, 
4*p*(1-a1)^1*a1^3 + 4*(1-p)*(1-a2)^1*a2^3, 
p*(1-a1)^0*a1^4 + (1-p)*(1-a2)^0*a2^4 \});
\]

\[
\text{i4 : } K = \text{kernel } f
\]

\[
\text{o4 : Ideal of } R
\]

Singular. Grobner basis

Solving Polynomial Equations
3.6. Projective Space and Projective Varieties

In some problems in algebraic statistics, it is useful to consider varieties as varieties in projective space, rather than as varieties in affine space. While to newcomers, the passage to projective space seems to make life more complicated, the primary reason for considering varieties in projective space is that it makes certain things simpler. In algebraic statistics we will have two reasons for passing to projective space to simplify life.

First, projective space is compact (unlike the affine space $\mathbb{K}^r$) and various theorems in algebraic geometry require this compactness to be true. As a simple example from algebraic geometry: Bezout’s theorem says that the intersection of two curves of degree $d$ and $e$ in the plane without common components with have exactly $de$ points, when counted with multiplicity. This theorem is only true when considered in the projective plane (and over an algebraically closed field). For example, the intersection of two circles in the plane always has 4 intersection points when counted with multiplicity, but two of these are always complex points “at infinity”.

A second reason for passing to projective varieties is aesthetic. When considering statistical models for discrete random variables in projective space, the vanishing ideal tends to look simpler and more easy to interpret. This is especially true when staring at the output of symbolic computation software.

**Definition 3.6.1.** Let $\mathbb{K}$ be a field. The projective space $\mathbb{P}^{r-1}$ is the set of all lines through the origin in $\mathbb{K}^r$. Equivalently, it is equal to the set of equivalence classes in $\mathbb{K}^r \setminus \{0\}$ under the equivalence relation $a \sim b$ if there is $\lambda \in \mathbb{K}^*$ such that $a = \lambda b$.

The lines or equivalence classes in the definition are the points of the projective space. The equivalence classes that arise in the definition of projective space could be represented by any element of that equivalence class. Note, however, that it does not make sense to evaluate a polynomial $f \in \mathbb{K}[p]$ at an equivalence class, since, in general $f(\lambda a) \neq f(a)$ for $\lambda \in \mathbb{K}^*$. The exception to this comes when considering homogeneous polynomials.

**Definition 3.6.2.** A polynomial is homogeneous if all of its terms have the same degree. An ideal is homogeneous if it has a generating set consisting of homogeneous polynomials.

For example, the polynomial $p_1^3p_2 - 17p_1p_3p_4^2 + 12p_4^4$ is homogeneous of degree 4. For a homogeneous polynomial, we always have $f(\lambda a) = \lambda^{\deg f} f(a)$. Hence, it is well defined to say that a homogeneous polynomial evaluates to zero at a point of projective space.
Definition 3.6.3. Let $\mathcal{F} \subseteq \mathbb{K}[p]$ be a set of homogeneous polynomials. The projective variety defined by $\mathcal{F}$ is the set
\[ V(\mathcal{F}) = \{ a \in \mathbb{P}^{r-1} : f(a) = 0 \text{ for all } f \in \mathcal{F} \}. \]
If $I \subseteq \mathbb{K}[p]$ is a homogeneous ideal, then
\[ V(I) = \{ a \in \mathbb{P}^{r-1} : f(a) = 0 \text{ for all homogeneous } f \in I \}. \]
If $S \subseteq \mathbb{P}^{r-1}$ its homogeneous vanishing ideal is
\[ I(S) = \langle f \in \mathbb{K}[p] \text{ homogeneous} : f(a) = 0 \text{ for all } a \in S \rangle. \]

The projective space $\mathbb{P}^{r-1}$ is naturally covered by patches that are isomorphic to the affine space $\mathbb{K}^{r-1}$. Each patch is obtained by taking a nonzero homogeneous linear polynomial $\ell \in \mathbb{K}[p]$, and taking all points in $\mathbb{P}^{r-1}$ where $\ell \neq 0$. This is realized as an affine space, because it is isomorphic to the linear affine variety $V(\ell - 1) \subseteq \mathbb{K}^{r}$. This suggests that if we are presented with a variety $V \subseteq \mathbb{K}^{r}$ whose vanishing ideal $I(V)$ contains a linear form $\ell - 1$, we should realize that we are merely looking at an affine piece of a projective variety. This issue arises in algebraic statistics when considering statistical models $\mathcal{P}$ for discrete random variables. Since such a model is contained in the probability simplex $\Delta_{r-1}$, and hence $I(\mathcal{P})$ contains the linear polynomial $p_1 + \cdots + p_r - 1$, we should really consider this model as (part of) a patch of a projective variety in $\mathbb{P}^{k-1}$.

Given a radical ideal $I \in \mathbb{K}[p]$, containing a linear polynomial $\ell - 1$, and hence defining a patch of a projective variety, we can use Gröbner bases to compute the homogeneous vanishing ideal of the Zariski closure of $V(I)$ (in projective space).

Proposition 3.6.4. Let $I \in \mathbb{K}[p]$ be a radical ideal containing a linear form $\ell - 1$. The Zariski closure of $V(I)$ in projective space has homogeneous vanishing ideal
\[ J := (I(q) + \langle p_i - tq_i : i = 1, \ldots, r \rangle) \cap \mathbb{K}[p]. \]

The notation $I(q)$ means to take the ideal $I \in \mathbb{K}[p]$ and rewrite it in terms of the new variables $q_1, \ldots, q_r$, substituting $q_1$ for $p_1$, $q_2$ for $p_2$, etc. Note that the ideal in parentheses on the right hand side of the equation in Proposition 3.6.4 is in the ring $\mathbb{K}[p, q, t]$ in $2r + 1$ indeterminates. When a variety is given parametrically and the image would contain a linear polynomial $\ell - 1$, that parametrization can be homogenized as well, to compute the homogeneous vanishing ideal of the Zariski closure in projective space. This is illustrated below using Macaulay 2, to compute the ideal of the projective closure of the mixture model $\text{Mixt}^2(\mathcal{P})$ where $\mathcal{P} \subseteq \Delta_4$ is the model for a binomial random variable with 4 trials.
3.7. Exercises

Exercise 3.1.  
(1) Verify that $I(W)$ is an ideal for any $W \subseteq \mathbb{K}^m$.

(2) Show that $\sqrt{I}$ is an ideal and that it is radical.

(3) Prove Proposition 3.2.5.

(4) Prove Proposition 3.2.7.

Exercise 3.2. Let $M$ be an $m \times m$ nonsingular matrix of integers. Define an order relation $\prec_M$ on the set of monomials in $\mathbb{K}[p]$ by the rule $p^u \prec_M p^v$ if and only if the first nonzero entry in $M(v - u)$ is positive.

(1) Show that if the first row of $M$ consists of nonnegative integers, then $\prec_M$ is a term order.
(2) Show that every term order \( \prec \) arises as a term order \( \prec_M \) for some \( M \).

(3) Determine the matrices \( M_{\text{lex}} \) and \( M_{\text{rev}} \) which realize the lexicographic and reverse lexicographic term orders.

**Exercise 3.3.**

1. Show that if \( \text{in}_{\prec}(I) \) is prime, then \( I \) is also prime.
2. Show that if \( \text{in}_{\prec}(I) \) is radical, then \( I \) is also radical.
3. Find examples to show that a prime ideal need not have any prime initial ideals and that a radical ideal need not have any radical initial ideals.

**Exercise 3.4.**

1. Show that the duality between radical ideals and varieties fails if the underlying field \( K \) is not algebraically closed, by exhibiting two radical ideals with the same zero set.
2. An ideal \( I \) in \( K[p] \) such that \( \mathcal{I}(\mathcal{V}(I)) = I \) is called a real radical ideal. Show that \( \mathcal{I} \) and \( \mathcal{V} \) are inclusion reversing bijections between the set of real radical ideals and the set of real algebraic varieties.

**Exercise 3.5.** Show that the Hilbert basis theorem implies that for any infinite ascending chain of ideals

\[
I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq \mathbb{K}[x]
\]

there exist a \( j \geq 1 \) such that \( I_i = I_j \) for all \( i > j \). A ring with the property that every infinite ascending sequence of ideals stabilizes is called a Noetherian ring.

**Exercise 3.6.** Prove proposition 3.2.13.

**Exercise 3.7.**

1. Show that the vanishing ideal of the twisted cubic curve is \( I = \langle p_1^2 - p_2, p_1^3 - p_3 \rangle \).
2. Show that every point in \( V(I) \) is in the image of the parametrization of the twisted cubic.
3. Determine Gröbner bases for \( I \) with respect to the lexicographical term order with \( p_1 \prec p_2 \prec p_3 \) and \( p_3 \prec p_2 \prec p_1 \).

**Exercise 3.8.**

1. A Gröbner basis \( G \) is minimal if no leading term of \( g \in G \) divides the leading term of a different \( g' \in G \), and all the leading coefficients are equal to 1. Explain how to construct a minimal Gröbner basis of an ideal.
2. A Gröbner basis \( G \) is reduced if it is minimal and no leading term of \( g \in G \) divides any term of a different \( g' \in G \). Explain how to construct a reduced Gröbner basis of an ideal.
3. Show that with a fixed term order, the reduced Gröbner basis of an ideal \( I \) is uniquely determined.
(4) Show that if \( I \) is a homogeneous ideal, then any reduced Gröbner basis of \( I \) consists of homogeneous polynomials.
Conditional independence constraints are simple and intuitive restrictions on the probability densities that allow one to express the notion that two sets of random variables are unrelated, typically given knowledge of the values of a third set of random variables. A conditional independence model is the family of probability distributions that satisfy all the conditional independence constraints in a given set. In the case where the underlying random variables are discrete or follow a jointly normal distribution, conditional independence constraints are algebraic (polynomial) restrictions on the density function: directly on the joint distribution in the discrete case, and on the covariance matrix in the Gaussian case. The most common source of conditional independence models is from graphical models. These families of conditional independence constraints will be explored in a later chapter.

In this Chapter, we introduce the basic theory of conditional independence. The study of conditional independence structures is a natural place to begin to study the connection between probabilistic concepts and methods from algebraic geometry. In particular, we will tie conditional independence to algebraic statistics through the conditional independence ideals. Section 4.1 introduces conditional independence models, the associate algebraic object (the conditional independence ideal), and the notion of conditional independence implication. In Section 4.2, the algebraic concept of primary decomposition is introduced. The primary decomposition provides an algebraic method to decompose a variety into its irreducible subvarieties. We put special emphasis on the case of primary decomposition of binomial
Conditional Independence Ideals, as this important case arises in a number of different examples of conditional independence ideals. In Section 4.3, the primary decomposition is applied to study conditional independence models. It is shown in a number of examples, how conditional independence implications can be detected using primary decomposition.

4.1. Conditional Independence Models

Let $X = (X_1, \ldots, X_m)$ be an $m$ dimensional random vector that takes its values on a Cartesian product space $\mathcal{X} = \prod_{i=1}^m \mathcal{X}_i$. We assume throughout that the joint probability distribution of $X$ has a density function $f(x) = f(x_1, \ldots, x_n)$ with respect to a product measure $\nu$ on $\mathcal{X}$, and that $f$ is continuous on $\mathcal{X}$. In the case where $\mathcal{X}$ is a finite set, the continuity assumption places no restrictions on the resulting probability distribution.

For each subset $A \subseteq [m]$, let $X_A = (X_a)_{a \in A}$ be the subvector of $X$ indexed by the elements of $A$. Similarly $\mathcal{X}_A = \prod_{a \in A} \mathcal{X}_a$. Given a partition $A_1|\cdots|A_k$ of $[m]$, we frequently use notation like $f(x_{A_1}, \ldots, x_{A_k})$ to denote the function $f(x)$, but with some variables grouped together. Recall the definitions of marginal and conditional densities from Chapter 2:

**Definition 4.1.1.** Let $A \subseteq [m]$. The **marginal density** $f_A(x_A)$ of $X_A$ is obtained by integrating out $x_{[m]\setminus A}$:

$$f_A(x_A) := \int_{\mathcal{X}_{[m]\setminus A}} f(x_A, x_{[m]\setminus A}) \, d\nu_{[m]\setminus A}(x_{[m]\setminus A}), \quad x_A \in \mathcal{X}_A.$$ 

Let $A, B \subseteq [m]$ be disjoint subsets and $x_B \in \mathcal{X}_B$. If $f_B(x_B) > 0$, the **conditional density** of $X_A$ given $X_B = x_B$ is defined as:

$$f_{A|B}(x_A|x_B) := \begin{cases} \frac{f_{A\cup B}(x_{A\cup B})}{f_B(x_B)} & \text{if } f_B(x_B) > 0 \\ 0 & \text{otherwise.} \end{cases}$$

Note that we use interchangeably various notation that can denote the same marginal or conditional densities, e.g. $f_{A\cup B}(x_A, x_B) = f_{A\cup B}(x_{A\cup B})$.

**Definition 4.1.2.** Let $A, B, C \subseteq [m]$ be pairwise disjoint. The random vector $X_A$ is **conditionally independent of $X_B$ given $X_C$** if and only if

$$f_{A\cup B\cup C}(x_A, x_B|x_C) = f_{A\cup C}(x_A|x_C) \cdot f_{B\cup C}(x_B|x_C)$$

for all $x_A, x_B, x_C$ such that $f_C(x_C) > 0$. The notation $X_A \perp\!\!\!\!\perp X_B | X_C$ is used to denote that the random vector $X$ satisfies the conditional independence statement that $X_A$ is conditional independent of $X_B$ given $X_C$. This is often further abbreviated to $A \perp\!\!\!\!\perp B | C$. 

4. Conditional Independence
Suppose we have some values \( x_B \) and \( x_C \) such that \( f_{B|C}(x_B|x_C) \) is defined and positive, and conditional independence statement \( X_A \perp \!\!\!\!\!\perp X_B | X_C \) holds. Then we can compute the conditional density \( f_{A|B\cup C}(x_A|x_B, x_C) \) as

\[
f_{A|B\cup C}(x_A|x_B, x_C) = \frac{f_{A\cup B|C}(x_A, x_B|x_C)}{f_{B|C}(x_B|x_C)} = f_{A|C}(x_A|x_C).
\]

This consequence of the definition of conditional independence gives a useful way to think about the conditional independence constraint. It can be summarized in plain English as saying “given \( X_C \), knowing \( X_B \) does not given any information about \( X_A \).” This gives us a useful down-to-earth interpretation of conditional independence, which can be easier to digest than the abstract definition.

**Example 4.1.3.** A statement of the form \( X_A \perp \!\!\!\!\!\perp X_B := X_A \perp \!\!\!\!\!\perp X_B | X_\emptyset \) is called a **marginal independence statement**, since it involves no conditioning. It corresponds to a density factorization

\[
f_{A\cup B}(x_A, x_B) = f_A(x_A)f_B(x_B),
\]

which should be recognizable as a familiar independence statement, as we saw in Chapter 2.

Suppose that a random vector \( X \) satisfies a list of conditional independence statements. What other constraints must the same random vector also satisfy? Here we do not assume that we know the density function of \( X \) (in which case, we could simply test all conditional independence constraints), rather, we want to know which implications hold regardless of the distribution. Finding such implications is, in general, a challenging problem. It can depend on the type of random variables under consideration (for instance, an implication might be true for all jointly normal random variables but fail for discrete random variables). In general, it is known that it is impossible to find a finite set of axioms from which all conditional independence relations can be deduced \([Stu92]\). On the other hand, there are a number of easy conditional independence implications which follow directly from the definitions and which are often called the **conditional independence axioms** of conditional independence inference rules.

**Proposition 4.1.4.** Let \( A, B, C, D \subseteq [m] \) be pairwise disjoint subsets. Then

(i) **(symmetry)** \( X_A \perp \!\!\!\!\!\perp X_B | X_C \implies X_B \perp \!\!\!\!\!\perp X_A | X_C \)

(ii) **(decomposition)** \( X_A \perp \!\!\!\!\!\perp X_{B \cup D} | X_C \implies X_A \perp \!\!\!\!\!\perp X_B | X_C \)

(iii) **(weak union)** \( X_A \perp \!\!\!\!\!\perp X_{B \cup D} | X_C \implies X_A \perp \!\!\!\!\!\perp X_B | X_{C \cup D} \)

(iv) **(contraction)** \( X_A \perp \!\!\!\!\!\perp X_B | X_{C \cup D} \) and \( X_A \perp \!\!\!\!\!\perp X_D | X_C \implies X_A \perp \!\!\!\!\!\perp X_{B \cup D} | X_C \)
**Proof.** The proofs of the symmetry axiom follows directly from the commutativity of multiplication. For decomposition axiom, suppose that the CI statement \( X_A \perp X_{B \cup D} \mid X_C \) holds. This is equivalent to the factorization of densities

\[
(4.1.1) \quad f_{A \cup B \cup C \mid D}(x_A, x_B, x_D \mid x_C) = f_{A \mid C}(x_A \mid x_C) \cdot f_{B \cup D \mid C}(x_B, x_D \mid x_C).
\]

Marginalizing this expression over \( X_D \) (that is, integrating both sides of the equation over \( X_D \)) produces the definition of the conditional independence statement \( X_A \perp X_B \mid X_C \) (since \( f_{A \mid C}(x_A \mid x_C) \) will factor out of the integral). Similarly, for the weak union axiom, dividing through \((4.1.1)\) by \( f_{D \mid C}(x_D \mid x_C) \) (i.e., conditioning on \( X_D \)) produces the desired conclusion.

For the proof of the contraction axiom, let \( x_C \) be such that \( f_C(x_C) > 0 \). By \( X_A \perp X_B \mid X_{C \cup D} \), we have that

\[
f_{A \cup B \cup C \cup D}(x_A, x_B, x_C, x_D) = f_{A \mid C}(x_A \mid x_C) \cdot f_{B \mid C \cup D}(x_B \mid x_C, x_D).
\]

Multiplying by \( f_{C \cup D}(x_C, x_D) \) we deduce that

\[
f_{A \cup B \cup C \cup D}(x_A, x_B, x_C, x_D) = f_{A \cup C \mid D}(x_A, x_C, x_D) \cdot f_{B \mid C \cup D}(x_B \mid x_C, x_D).
\]

Dividing by \( f_C(x_C) > 0 \) we obtain

\[
f_{A \cup B \cup C \mid D}(x_A, x_B, x_D \mid x_C) = f_{A \mid D}(x_A, x_D \mid x_C) \cdot f_{B \mid C \cup D}(x_B \mid x_C, x_D).
\]

Applying the conditional independence statement \( X_A \perp X_D \mid X_C \), we deduce

\[
f_{A \cup B \cup C \mid D}(x_A, x_B, x_D \mid x_C) = f_{A \mid C}(x_A \mid x_C) f_{D \mid C}(x_D \mid x_C) f_{B \mid C \cup D}(x_B \mid x_C, x_D)
\]

\[
= f_{A \mid C}(x_A \mid x_C) \cdot f_{B \mid D \mid C}(x_B, x_D \mid x_C),
\]

which means that \( X_A \perp X_{B \cup D} \mid X_C \). \( \square \)

In addition to the four basic conditional independence axioms of Proposition 4.1.4, there is a further fifth “axiom”, which, however, does not hold for every probability distribution but only in special cases.

**Proposition 4.1.5** (Intersection axiom). Suppose that \( f(x) > 0 \) for all \( x \). Then

\[
X_A \perp X_B \mid X_{C \cup D} \text{ and } X_A \perp X_C \mid X_{B \cup D} \implies X_A \perp X_{B \cup C} \mid X_D.
\]

**Proof.** The first and second conditional independence statements imply

\[
(4.1.2) \quad f_{A \cup B \mid C \cup D}(x_A, x_B \mid x_C, x_D) = f_{A \mid C \cup D}(x_A \mid x_C, x_D) f_{B \mid C \cup D}(x_B \mid x_C, x_D),
\]

\[
(4.1.3) \quad f_{A \cup C \mid B \cup D}(x_A, x_C \mid x_B, x_D) = f_{A \mid B \cup D}(x_A \mid x_B, x_D) f_{C \mid B \cup D}(x_C \mid x_B, x_D).
\]
Multiplying (4.1.2) by \( f_{C \cup D}(x_C, x_D) \) and (4.1.3) by \( f_{B \cup D}(x_B, x_D) \), we obtain that

\[
(4.1.4) \quad f_{A \cup B \cup C \cup D}(x_A, x_B, x_C, x_D) = f_{A|C \cup D}(x_A|x_C, x_D)f_{B \cup C \cup D}(x_B, x_C, x_D),
\]

\[
(4.1.5) \quad f_{A \cup B \cup C \cup D}(x_A, x_B, x_C, x_D) = f_{A|B \cup D}(x_A|x_B, x_D)f_{B \cup C \cup D}(x_B, x_C, x_D).
\]

Equating (4.1.4) and (4.1.5) and dividing by \( f_{B \cup C \cup D}(x_B, x_C, x_D) \) (which is allowable since \( f(x) > 0 \)) we deduce that

\[
f_{A|C \cup D}(x_A|x_C, x_D) = f_{A|B \cup D}(x_A|x_B, x_D).
\]

Since the right hand side of this expression does not depend on \( x_C \), we conclude

\[
f_{A|C \cup D}(x_A|x_C, x_D) = f_{A|D}(x_A|x_D).
\]

Plugging this into (4.1.4) and conditioning on \( X_D \) gives

\[
f_{A \cup B \cup C \cup D}(x_A, x_B, x_C|x_D) = f_{A|D}(x_A|x_D)f_{B \cup C \cup D}(x_B, x_C|x_D)
\]

and implies that \( X_A \perp X_{B \cup C} \mid X_D \). \( \square \)

The condition that \( f(x) > 0 \) for all \( x \) is much stronger than necessary for the intersection property to hold. At worst, we only needed to assume that \( f_{B \cup C \cup D}(x_B, x_C, x_D) > 0 \). However, it is possible to weaken this condition considerably. In the discrete case, it is possible to give a precise characterization of the conditions on the density which guarantee that the intersection property holds. This will be done in Section 4.3, based on work of Fink [Pin11].

Now we focus on the cases where an algebraic perspective is most useful, namely the case of discrete and Gaussian random variables. In both cases, conditional independence constraints on a random variable correspond to algebraic constraints on the distribution.

Discrete conditional independence models. Let \( X = (X_1, \ldots, X_m) \) be a vector of discrete random variables. Returning to the notation used in previous chapters, we let \( [r_j] \) be the set of values taken by \( X_j \). Then \( X \) takes its values in \( \mathcal{R} = \prod_{j=1}^m [r_j] \). For \( A \subseteq [m] \), \( \mathcal{R}_A = \prod_{a \in A}[r_a] \). In this discrete setting, a conditional independence constraint translates into a system of quadratic polynomial equations in the joint probability distribution.

**Proposition 4.1.6.** If \( X \) is a discrete random vector, then the conditional independence statement \( X_A \perp X_B \mid X_C \) holds if and only if

\[
(4.1.6) \quad p_{i_A,i_B,i_C,+} \cdot p_{j_A,j_B,i_C,+} - p_{i_A,j_B,i_C,+} \cdot p_{j_A,i_B,i_C,+} = 0
\]

for all \( i_A, j_A \in \mathcal{R}_A, i_B, j_B \in \mathcal{R}_B, \) and \( i_C \in \mathcal{R}_C \).
The notation $p_{i_A,i_B,i_C,+}$ denotes the probability $P(X_A = i_A, X_B = i_B, X_C = i_C)$. As a polynomial expression in terms of indeterminates $p_i$ where $i \in \mathcal{R}$, this can be written as

$$p_{i_A,i_B,i_C,+} = \sum_{j[m] \setminus A \cup B \cup C \in \mathcal{R}[m] \setminus A \cup B \cup C} p_{i_A,i_B,i_C,j[m] \setminus A \cup B \cup C}.$$

Here we use the usual convention that the string of indices $i$ has been regrouped into the string $(i_A, i_B, i_C, j[m] \setminus A \cup B \cup C)$, for convenience.

**Proof.** By marginalizing, we may assume that $A \cup B \cup C = [m]$. By conditioning, we may assume that $C$ is empty. By aggregating the states indexed by $\mathcal{R}_A$ and $\mathcal{R}_B$ respectively, we can treat this as a conditional independence statement $X_1 \perp X_2$. In this setting, the conditional independence constraints in (4.1.6) are equivalent to saying that all $2 \times 2$ minors of the matrix

$$P = \begin{pmatrix}
p_{11} & p_{12} & \cdots & p_{1r_2} 
p_{21} & p_{22} & \cdots & p_{2r_2} 
\vdots & \vdots & \ddots & \vdots 
p_{r_11} & p_{r_12} & \cdots & p_{r_1r_2}
\end{pmatrix}$$

are zero. Since $P$ is not the zero matrix, this means that $P$ has rank 1. Thus $P = \alpha^T \beta$ for some vectors $\alpha \in \mathbb{R}^{r_1}$ and $\beta \in \mathbb{R}^{r_2}$. These vectors can be taken to be nonnegative vectors, and such that $\|\alpha\|_1 = \|\beta\|_1 = 1$. This implies that $p_{ij} = p_{i+j}p_{i+j}$ for all $i$ and $j$, and hence $X_1 \perp X_2$. Conversely, if $X_1 \perp X_2$, $P$ must be a rank one matrix. □

**Definition 4.1.7.** The conditional independence ideal $I_{A \perp B|C} \subseteq \mathbb{C}[p]$ is generated by all the quadratic polynomials in (4.1.6). The discrete conditional independence model $\mathcal{M}_{A \perp B|C} = V_\Delta(I_{A \perp B|C}) \subseteq \Delta_\mathcal{R}$ is the set of all probability distributions in $\Delta_\mathcal{R}$ satisfying the quadratic polynomial constraints (4.1.6).

In fact, it can be shown that the ideal $I_{A \perp B|C}$ is a prime ideal, which we will prove in Chapter [9]

**Example 4.1.8.** Let $m = 2$, and consider the (ordinary) independence statement $X_1 \perp X_2$. Then

$$I_{1 \perp 2} = \langle p_{i_1j_1}p_{i_2j_2} - p_{i_1j_2}p_{i_2j_1} : i_1, i_2 \in [r_1], j_1, j_2 \in [r_2] \rangle.$$

This is the ideal of 2 minors in the proof of Proposition [4.1.6].

If $m = 3$, and we consider the marginal independence statement $X_1 \perp X_2$, and suppose that $r_3 = 2$, then

$$I_{1 \perp 2} = \langle (p_{i_1j_1} + p_{i_1j_2})p_{i_2j_1} + p_{i_1j_2}p_{i_2j_2} - (p_{i_1j_2} + p_{i_1j_2})p_{i_1j_1} + p_{i_1j_2} : i_1, j_1 \in [r_1], i_2, j_2 \in [r_2] \rangle.$$
4.1. Conditional Independence Models

If \( m = 3 \), and we consider the conditional independence statement \( X_2 \perp \perp X_3 | X_1 \), then

\[
I_2 \perp \perp 3 | 1 = \langle p_{i_1 j_1} p_{i_2 j_2} p_{i_3 j_3} : i_1 \in [r_1], i_2, j_2 \in [r_2], i_3, j_3 \in [r_3] \rangle.
\]

If \( C = \{ A_1 \perp \perp B_1 | C_1, A_2 \perp \perp B_2 | C_2, \ldots \} \) is a set of conditional independence statements, we construct the conditional independence ideal

\[
I_C = \sum_{A \perp \perp B | C \in C} I_{A \perp \perp B | C}
\]

which is generated by all the quadratic polynomials appearing in any of the \( I_{A_i \perp \perp B_i | C_i} \). The model \( M_C := V(\Delta(I_C)) \subseteq \Delta_R \) consists of all probability distributions satisfying all the conditional independence constraints arising from \( C \).

Gaussian conditional independence models. Conditional independence for gaussian random vectors is also an algebraic condition. In particular, the conditional independence statement \( X_A \perp \perp X_B | X_C \) gives a rank condition on the covariance matrix \( \Sigma \). Since rank conditions are algebraic (described by vanishing determinants), the resulting conditional independence models can also be analyzed using algebraic techniques.

**Proposition 4.1.9.** The conditional independence statement \( X_A \perp \perp X_B | X_C \) holds for a multivariate normal random vector \( X \sim N(\mu, \Sigma) \) if and only if the submatrix \( \Sigma_{A \cup B, C \cup C} \) of the covariance matrix \( \Sigma \) has rank \( \#C \).

**Proof.** If \( X \sim N(\mu, \Sigma) \) follows a multivariate normal distribution, then the conditional distribution of \( X_{A \cup B} \) given \( X_C = x_C \) is the multivariate normal distribution

\[
N\left( \mu_{A \cup B} + \Sigma_{A \cup B, C} \Sigma_{C, C}^{-1} (x_C - \mu_C), \Sigma_{A \cup B, A \cup B} - \Sigma_{A \cup B, C} \Sigma_{C, C}^{-1} \Sigma_{C, A \cup B} \right),
\]

by Theorem 2.4.2. The statement \( X_A \perp \perp X_B | X_C \) holds if and only if

\[
(\Sigma_{A \cup B, A \cup B} - \Sigma_{A \cup B, C} \Sigma_{C, C}^{-1} \Sigma_{C, A \cup B})_{A, B} = \Sigma_{A, B} - \Sigma_{A, C} \Sigma_{C, C}^{-1} \Sigma_{C, B} = 0
\]

by Proposition 2.4.4. The matrix \( \Sigma_{A, B} - \Sigma_{A, C} \Sigma_{C, C}^{-1} \Sigma_{C, B} \) is the Schur complement of the matrix

\[
\Sigma_{A \cup C, B \cup C} = \begin{pmatrix} \Sigma_{A, B} & \Sigma_{A, C} \\ \Sigma_{C, B} & \Sigma_{C, C} \end{pmatrix}.
\]

Since \( \Sigma_{C, C} \) is always invertible (it is positive definite), the Schur complement is zero if and only if the matrix \( \Sigma_{A \cup C, B \cup C} \) has rank equal to \( \#C \).

The set of partially symmetric matrices with rank \( \leq k \) is an irreducible variety, defined by the vanishing of all \( (k+1) \times (k+1) \) subdeterminants. The ideal generated by these subdeterminants is a prime ideal \( [\text{Con94}] \). Hence, we obtain nice families of conditional independence ideals.
Definition 4.1.10. Fix pairwise disjoint subsets $A, B, C$ of $[m]$. The Gaussian conditional independence ideal $J_{A \perp B | C}$ is the following ideal in $\mathbb{R}[\sigma_{ij}, 1 \leq i \leq j \leq m]$:

$$J_{A \perp B | C} = \langle (\#C + 1) \times (\#C + 1) \text{ minors of } \Sigma_{A \cup C, B \cup C} \rangle$$

Similarly as with the discrete case, we can take a collection $\mathcal{C}$ of conditional independence constraints, and get a conditional independence ideal

$$J_{\mathcal{C}} = \sum_{A \perp B | C \in \mathcal{C}} J_{A \perp B | C}.$$  

The resulting gaussian conditional independence model is a subset of the cone $PD_m$ of $m \times m$ symmetric positive definite matrices:

$$\mathcal{M}_\mathcal{C} := V(J_{\mathcal{C}}) \cap PD_m.$$  

Our goal in the remains of the chapter is to show how algebra can be used to study conditional independence models, and in particular, conditional independence implications. To illustrate the basic idea (and avoiding any advanced algebra), consider the following example.

Example 4.1.11 (Conditional and Marginal Independence). Let $\mathcal{C} = \{1 \perp 3, 1 \perp 3|2\}$. The gaussian conditional independence ideal $J_{\mathcal{C}}$ is generated by two polynomials

$$J_{\mathcal{C}} = \langle \sigma_{13}, \det \Sigma_{\{1,2\},\{2,3\}} \rangle.$$  

The conditional independence model consists of all covariance matrices $\Sigma \in PD_3$ satisfying

$$\sigma_{13} = 0 \quad \text{and} \quad \sigma_{13}\sigma_{22} - \sigma_{12}\sigma_{23} = 0.$$  

This is equivalent to the system

$$\sigma_{13} = 0 \quad \text{and} \quad \sigma_{12}\sigma_{23} = 0,$$

which splits as the union of two linear spaces:

$$L_1 = \{\Sigma : \sigma_{13} = \sigma_{12} = 0\} \quad L_2 = \{\Sigma : \sigma_{13} = \sigma_{23} = 0\}.$$  

The first component $L_1$ consists of gaussian random vectors satisfying $X_1 \perp (X_2, X_3)$, whereas the second component consists of gaussian random vectors satisfying $X_3 \perp (X_1, X_2)$. It follows that the implication

$$X_1 \perp X_3 | X_2 \quad \text{and} \quad X_1 \perp X_3 \implies X_1 \perp (X_2, X_3) \quad \text{or} \quad (X_1, X_2) \perp X_3,$$

holds for multivariate normal random vectors. \qed
4.2. Primary Decomposition

In Example 4.1.11 in the previous section, we saw the solution set to a system of polynomial equations break up into two simpler pieces. In this section, we discuss the general algebraic concept which generalizes this notion. On the level of varieties, the variety will break up as the union of finitely many irreducible varieties. On the more algebraic level of ideals, an ideal can be written as the intersection of finitely many primary ideals. This representation is called a primary decomposition. Details on primary decomposition, including missing proofs of results in this section can be found in standard texts on algebraic geometry (e.g. [CLO07], [Has07]).

**Definition 4.2.1.** A variety \( V \) is called **reducible** if there are two proper subvarieties \( V_1, V_2 \subsetneq V \) such that \( V = V_1 \cup V_2 \). A variety \( V \) that is not reducible is called **irreducible**. An ideal \( I \subseteq \mathbb{K}[p] \) is prime if there are no two elements \( f_1, f_2 \not\in I \) such that \( f_1 f_2 \in I \).

**Proposition 4.2.2.** A variety \( V \) is irreducible if and only if the corresponding ideal \( I(V) \) is a prime ideal.

**Proof.** Suppose \( V \) is reducible. Since \( V_1 \neq V_2 \), there are polynomials \( f_1 \in I(V_1) \setminus I(V_2) \) and \( f_2 \in I(V_2) \setminus I(V_1) \). Then \( I(V) \) is not prime since \( f_1, f_2 \not\in I(V) = I(V_1 \cup V_2) = I(V_1) \cap I(V_2) \), but \( f_1 f_2 \in I(V) \). Conversely, if \( I(V) \) is not prime, with \( f_1, f_2 \not\in I(V) \) but \( f_1 f_2 \in I(V) \), then \( V = V(I(V) + \langle f_1 \rangle) \cap V(I(V) + \langle f_2 \rangle) \) is a proper decomposition of \( V \). \( \square \)

Irreducible varieties are the basic building block for solution sets of polynomial equations, and every variety has a finite decomposition into irreducibles.

**Proposition 4.2.3.** Every variety \( V \) has a unique decomposition \( V = V_1 \cup \cdots \cup V_k \) into finitely many irreducible varieties \( V_i \), such that no \( V_i \) can be omitted from the decomposition. This decomposition is called the irreducible decomposition of the variety \( V \).

**Proof.** To show existence of such a decomposition, consider the following decomposition “algorithm” for a variety. Suppose at some stage we have a representation \( V = V_1 \cup \cdots \cup V_k \) as the union of varieties. If all the \( V_i \) are irreducible, we have an irreducible decomposition. Suppose, on the other hand, that some component, say \( V_1 \) is reducible, i.e. it has a proper decomposition as \( V_1 = V'_1 \cup V'_2 \). Then we augment the decomposition as \( V = V'_1 \cup V'_2 \cup V_2 \cup \cdots \cup V_k \) and repeat. This algorithm either terminates in finitely many steps with an irreducible decomposition (which can be subsequently made irredundant), or there is an infinite sequence of varieties among those
produced along the way such that

\[ W_1 \supset W_2 \supset \cdots. \]

This, in turn, implies an infinite ascending chain of ideals

\[ \mathcal{I}(W_1) \subset \mathcal{I}(W_2) \subset \cdots, \]

violating the Noetherianity of the polynomial ring. Uniqueness of the decomposition is deduced by comparing two different irreducible decompositions.

By the inclusion reversing property of passing from ideals to varieties, we are naturally led to define an irreducible ideal \( I \) to be one which has no proper decomposition \( I = I_1 \cap I_2 \). The same argument as above shows that every polynomial ideal has a decomposition into irreducible ideals (uniqueness of the decomposition is not guaranteed however). The irreducible decomposition however, is not as useful as another decomposition, the primary decomposition, which we describe now.

**Definition 4.2.4.** An ideal \( Q \) is called primary if for all \( f \) and \( g \) such that \( fg \in Q \), either \( f \in Q \) or \( g^k \in Q \) for some \( k \).

Some basic facts about primary ideals.

**Proposition 4.2.5.**

1. Every irreducible ideal is primary.
2. If \( Q \) is primary, then \( \sqrt{Q} = P \) is a prime ideal, called the associated prime of \( Q \).
3. If \( Q_1 \) and \( Q_2 \) are primary, and \( \sqrt{Q_1} = \sqrt{Q_2} = P \), then \( Q_1 \cap Q_2 \) is also primary, with associated prime \( P \).

**Definition 4.2.6.** Let \( I \subseteq \mathbb{K}[p] \) be an ideal. A primary decomposition of \( I \) is a representation \( I = Q_1 \cap \cdots \cap Q_r \) of \( I \) as the intersection of finitely primary ideals. The decomposition is irredundant if no \( Q_i \supseteq \cap_{j \neq i} Q_j \) and all the associated primes \( \sqrt{Q_i} \) are distinct.

By Proposition 4.2.5 part one and the existence of irreducible decompositions of ideals, we see that every ideal \( I \) has a finite irredundant primary decomposition. A primary decomposition is not unique in general, but it does have many uniqueness properties which we outline in the following theorem.

**Theorem 4.2.7.** Let \( I \) be an ideal in a polynomial ring.

1. Then \( I \) has an irredundant primary decomposition \( I = Q_1 \cap \cdots \cap Q_k \)
   such that the prime ideals \( \sqrt{Q_i} \) are all distinct.
4.2. Primary Decomposition

(2) The set of prime ideals \( \text{Ass}(I) := \{ \sqrt{Q_i} : i \in [k] \} \) is uniquely determined by \( I \), and does not depend on the particular irredundant primary decomposition. They are called the associated primes of \( I \).

(3) The minimal elements of \( \text{Ass}(I) \) with respect to inclusion are called minimal primes of \( I \). The primary components \( Q_i \) associated to minimal primes of \( I \) are uniquely determined by \( I \).

(4) The minimal primes of \( I \) are precisely the minimal elements among all prime ideals that contain the ideal \( I \).

(5) Associated primes of \( I \) that are not minimal are called embedded primes. The primary components \( Q_i \) associated to embedded primes of \( I \) are not uniquely determined by \( I \).

(6) \( \sqrt{I} = \cap \sqrt{Q_i} \). If the intersection is taken over the minimal primes of \( I \), this gives a primary (in fact, prime) decomposition of \( \sqrt{I} \).

(7) The decomposition \( V(I) = \cup V(\sqrt{Q_i}) \), where the union is taken over the minimal primes of \( I \) is the irreducible decomposition of the variety \( V(I) \).

Example 4.2.8. We saw at the end of the last section, a simple irreducible decomposition of a variety which corresponds to a primary decomposition of an ideal. In particular:

\[
J_C = \langle \sigma_{13}, \det \Sigma_{\{1,2\},\{2,3\}} \rangle = \langle \sigma_{12}, \sigma_{13} \rangle \cap \langle \sigma_{13}, \sigma_{23} \rangle.
\]

Note that both primary components are prime in this case, in fact, minimal primes, and so everything is uniquely determined.

For an example with embedded primes consider the ideal:

\[
\langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, y \rangle.
\]

Both ideals are primary, the decomposition is irredundant. The associated primes are \( \langle x \rangle \) and \( \langle x, y \rangle \), the first is minimal, and the second is embedded. Furthermore, the decomposition is not unique since,

\[
\langle x^2, xy \rangle = \langle x \rangle \cap \langle x^2, y + cx \rangle
\]

is also a primary decomposition for any \( c \in \mathbb{C} \).

Important operations related to primary decompositions are the ideal quotient and the saturation.

Definition 4.2.9. Let \( I, J \) be ideals in \( \mathbb{K}[p] \). The quotient ideal (or colon ideal) is the ideal

\[
I : J := \{ f \in \mathbb{K}[p] : fg \in I \text{ for all } g \in J \}.
\]

The saturation of \( I \) by \( J \) is the ideal

\[
I : J^\infty := \cup_{k=1}^\infty I : J^k.
\]
If $J = \langle f \rangle$ is a principal ideal, then we use the shorthand $I : f$ to denote $I : \langle f \rangle$ and $I : f^\infty$ to denote $I : \langle f \rangle^\infty$.

**Theorem 4.2.10.** Let $I \subseteq \mathbb{K}[p]$ be an ideal. Then for each prime $P \in \text{Ass}(I)$ there exists a polynomial $f \in \mathbb{K}[p]$ such that $P = I : f$.

For reasonably sized examples, it is possible to compute primary decompositions in computer algebra packages. Such computations can often provide insight in specific examples, and give ideas on how to prove theorems about the decomposition in complicated families.

The best possible case is when the ideal $I$ is a radical ideal. This is because all the information in the primary decomposition is geometric (only the minimal primes come into play). Sometimes, it might be possible to prove directly that an ideal is radical, then use geometric arguments to discover all minimal primes, and thus deduce the prime decomposition of the ideal. For example, the following result on initial ideals can be used in some instances:

**Proposition 4.2.11.** Let $I$ be an ideal and $\prec$ a term order, so that $\text{in}_{\prec}(I)$ is a radical ideal. Then $I$ is radical.

An important and relatively well-understood class of ideals from the standpoint of primary decompositions is the class of binomial ideals. A *binomial* is a polynomial of the form $p^u - \alpha p^v$ where $\alpha \in \mathbb{K}$. An ideal is a binomial ideal if it has a generating set consisting of binomials. Binomial ideals make frequent appearances in algebraic statistics, especially because of their connections to random walks, as discussed in Chapter 9. The primary decomposition of binomial ideals are among the best behaved.

**Theorem 4.2.12.** Let $I$ be a binomial ideal and suppose that $\mathbb{K}$ is an algebraically closed field. Then $I$ has an irredundant primary decomposition such that all primary components are binomial ideals. Furthermore, all associated prime ideals are binomial ideals, as well.

Theorem 4.2.12 was first proved in [ES96], which also includes algorithms for computing the primary decomposition of binomial ideals. However, it remains an active research problem to find better algorithms for binomial primary decomposition, and to actually make those algorithms usable in practice. See [DMM10, Kah10] for recent work on this problem.

In some problems in algebraic statistics, we are only interested in the geometric content of the primary decomposition, and hence, on the minimal primes. In the case of binomials ideals, it is often possible to describe this quite explicitly in terms of lattices.

**Definition 4.2.13.** A *pure difference binomial* is a binomial of the form $p^u - p^v$. A *pure difference binomial ideal* is generated by pure difference
binomials. Let $\mathcal{L} \subseteq \mathbb{Z}^r$ be a lattice. The lattice ideal $I_{\mathcal{L}}$ associated to $\mathcal{L}$ is the ideal

$$\langle p^u - p^v : u - v \in \mathcal{L} \rangle.$$ 

The special case where $\mathcal{L}$ is a saturated lattice (that is $\mathbb{Z}^r / \mathcal{L}$ has no torsion) is called a toric ideal.

Toric ideals and lattice ideals will be elaborated upon in more detail in Chapters 6 and 9. Note that toric ideals are prime over any field. Lattice ideals are usually not prime if the corresponding lattice is not saturated. In the case where $\mathbb{K}$ is an algebraically closed field of characteristic 0 (e.g. $\mathbb{C}$), lattice ideals are always radical, and they have a simple decomposition into prime ideals in terms of the torsion subgroup of $\mathbb{Z}^r / \mathcal{L}$. Because of this property, when we want to find the minimal primes of a pure difference binomial ideal over $\mathbb{C}$, it suffices to look at certain associated lattice ideals (or rather, ideals that are the sum of a lattice ideal and prime monomial ideal). We will call these associated lattice ideals, for simplicity.

Let $B$ be a set of pure difference binomials and $I = \langle B \rangle$. The lattice ideals that contain $I$ and can be associated to $I$ have a restricted form.

Consider the polynomial ring $\mathbb{C}[p] = \mathbb{C}[p_1, \ldots, p_r]$. Let $S \subseteq [r]$. Let $\mathbb{C}[p_S] := \mathbb{C}[p_s : s \in S]$. Form the ideal

$$I_S := \langle p_s : s \in S \rangle + \langle p^u - p^v : p^u - p^v \in B \cap \mathbb{C}[p_{[r] \setminus S}] \rangle : (\prod_{s \in [r] \setminus S} p_s)\infty.$$

We say that $S$ is a candidate set for a minimal associated lattice ideal if for each binomial generator of $I$, $p^u - p^v$ either $p^u - p^v \in \mathbb{C}[p_{[r] \setminus S}]$ or there are $s, s' \in S$ such that $p_s | p^u$ and $p_{s'} | p^v$. Note that the ideal

$$\langle p^u - p^v \in B \cap \mathbb{C}[p_{[r] \setminus S}] \rangle : (\prod_{s \in [r] \setminus S} p_s)\infty$$

is equal to the lattice ideal $I_{\mathcal{L}}$ for the lattice $\mathcal{L} = \mathbb{Z}\{u - v : p^u - p^v \in B \cap \mathbb{C}[p_{[r] \setminus S}]\}$.

**Proposition 4.2.14.** Every minimal associated lattice ideal of the pure difference binomial ideal $I$ has the form $I_S$ for a candidate set $S$. In particular, every minimal prime of $I$ is the minimal prime of one of the ideals $I_S$, for some $S$.

Note that the candidate condition is precisely the condition that guarantees that $I \subseteq I_S$. The minimal associated lattice ideals are just the minimal elements among the candidate associated lattice ideals. Hence, solving the geometric problem of finding irreducible components is a combinatorial problem about when certain lattice ideals contain others (plus the general problem of decomposing lattice ideals).
Example 4.2.15. Let $I$ be the pure difference binomial ideal

$$I = \langle p_{11}p_{22} - p_{12}p_{21}, p_{12}p_{23} - p_{13}p_{22} \rangle.$$ 

The candidate sets of variables must consist of sets of variables that intersect both the leading and trailing term of any binomial in which it has variables in common. The possible candidate sets for $I$ are:

$\emptyset, \{p_{11}, p_{21}\}, \{p_{12}, p_{22}\}, \{p_{13}, p_{23}\}, \{p_{11}, p_{12}, p_{13}\}, \{p_{21}, p_{22}, p_{23}\}$

and any set that can be obtained from these by taking unions. The candidate ideal $I_\emptyset$ is equal to

$$I : (p_{11} \cdots p_{23})^\infty = \langle p_{11}p_{22} - p_{12}p_{21}, p_{12}p_{23} - p_{13}p_{22}, p_{11}p_{23} - p_{13}p_{21} \rangle.$$ 

The candidate ideal $I_{\{p_{12}, p_{22}\}}$ is the monomial ideal

$$I_{\{p_{12}, p_{22}\}} = \langle p_{12}, p_{22} \rangle.$$ 

The ideal $I_{\{p_{11}, p_{21}\}}$ is the ideal

$$I_{\{p_{11}, p_{21}\}} = \langle p_{11}, p_{21}, p_{12}p_{23} - p_{13}p_{22} \rangle.$$ 

Note, however, that $I_\emptyset \subseteq I_{\{p_{11}, p_{21}\}}$, so $I_{\{p_{11}, p_{21}\}}$ is not a minimal prime of $I$. In fact,

$$I = I_\emptyset \cap I_{\{p_{12}, p_{22}\}} = \langle p_{11}p_{22} - p_{12}p_{21}, p_{12}p_{23} - p_{13}p_{22}, p_{11}p_{23} - p_{13}p_{21} \rangle \cap \langle p_{12}, p_{22} \rangle$$

is an irredundant primary decomposition of $I$, showing that all of the other candidate sets are superfluous.

The variety of a lattice ideal $I_L$ in the interior of the positive orthant $\mathbb{R}_{>0}^r$ is easy to describe. It consists of all points $p \in \mathbb{R}_{>0}^r$, such that $(\log p)^T u = 0$ for all $u \in L$. Hence, Proposition 4.2.14 says that the variety of a pure difference binomial ideal in the probability simplex $\Delta_{r-1}$ is the union of exponential families (see Chapter 6).

4.3. Primary Decomposition of CI Ideals

In this section, we compute primary decompositions of the conditional independence ideals $I_C$ and $J_C$ and use them to study conditional independence implications. First we illustrate the idea with some small examples, explaining how these examples can be computed in some computational algebra software. Then we show a number of case studies where theoretical descriptions of the primary decompositions (or information about the primary decomposition, without actually obtaining the entire decomposition) can be used to study conditional independence implications. We try to exploit the binomial structure of these conditional independence ideals whenever possible.
4.3. Primary Decomposition of CI Ideals

We begin with two basic examples that illustrates some of the subtleties that arise.

**Example 4.3.1** (Gaussian Contraction Axiom). Let \( C = \{1 \perp 2 | 3, 2 \perp 3\} \). By the contraction axiom these two statements imply that \( 2 \perp \{1, 3\} \). Let us consider this in the Gaussian case. We have

\[
\mathcal{J}_C = \langle \det \Sigma_{\{1,3\},\{2,3\}}, \sigma_{23} \rangle = \langle \sigma_{12}\sigma_{33} - \sigma_{13}\sigma_{23}, \sigma_{23} \rangle = \langle \sigma_{12}, \sigma_{23} \rangle \cap \langle \sigma_{33}, \sigma_{23} \rangle.
\]

In particular, the variety defined by the ideal \( \mathcal{J}_C \) has two components. However, only one of these components is interesting from the probabilistic standpoint. Indeed, the second component \( V(\langle \sigma_{33}, \sigma_{23} \rangle) \) does not intersect the cone of positive definite matrices. It is the first component which contains the conclusion of the contraction axiom and which is relevant from a probabilistic standpoint.

**Example 4.3.2** (Binary Contraction Axiom). Let \( C = \{1 \perp 2 | 3, 2 \perp 3\} \). By the contraction axiom these two statements imply that \( 2 \perp \{1, 3\} \). Let us consider this in the case of binary random variables. We have

\[
\mathcal{I}_C = \langle p_{111}p_{221} - p_{121}p_{211}, p_{112}p_{222} - p_{122}p_{212},
(p_{111} + p_{211})(p_{122} + p_{222}) - (p_{112} + p_{212})(p_{121} + p_{221}) \rangle.
\]

The following code computes the primary decomposition of this example in Singular:

```plaintext
ring R = 0,(p111,p112,p121,p122,p211,p212,p221,p222),dp;
ideal I =
p111*p221 - p121*p211, p112*p222 - p122*p212,
(p111 + p211)*(p122 + p222) - (p112 + p212)*(p121 + p221);
LIB "primdec.lib";
primdecGTZ(I);
```

The computation reveals that the conditional independence ideal \( \mathcal{I}_C \) is radical with three prime components:

\[
\mathcal{I}_C = \mathcal{I}_{2 \perp \{1,3\}} \cap \langle p_{112}p_{222} - p_{122}p_{212}, p_{111} + p_{211}, p_{121} + p_{221} \rangle \cap \langle p_{111}p_{221} - p_{121}p_{211}, p_{112} + p_{222}, p_{112} + p_{212} \rangle.
\]

Note that while the last two components do intersect the probability simplex, their intersection with the probability simplex is contained within the first components intersection with the probability simplex. Indeed, since
all probabilities are nonnegative, the requirement that, say \( p_{111} + p_{211} = 0 \), forces both \( p_{111} = 0 \) and \( p_{211} = 0 \). Hence, the primary decomposition verifies the conditional independence implication.

A complete analysis of the ideal of the discrete contraction axiom was carried out in [GSS05]. In both of the preceding examples it is relatively easy to derive these conditional independence implications directly, without using algebra. The point of the examples is familiarity with the idea of using primary decomposition. The conditional independence implications and their proofs become significantly more complicated once we move to more involved examples in the following subsections.

4.3.1. Failure of the Intersection Axiom. Here we follow Section 6.6 of [DSS09] and [Pin11] to analyze the failure of the intersection axiom for discrete random variables. Looked at another way, we give the strongest possible conditions based solely on the zero pattern in the distribution which imply the conclusion of the intersection axiom.

In the discrete case, it suffices to analyze the intersection axiom in the special case where we consider the two conditional independence statements \( X_1 \perp \perp X_2 | X_3 \) and \( X_1 \perp \perp X_3 | X_2 \). The traditional statement of the intersection axiom in this case is that if the density \( f(x_1, x_2, x_3) \) is positive then also \( X_1 \perp \perp (X_2, X_3) \) holds. As mentioned after the proof of Proposition 4.1.5, the proof actually only requires that the marginal density \( f_{(2,3)}(x_2, x_3) \) is positive. This can, in fact, be further weakened.

To state the strongest possible version, we associate to a density function \( f(x_1, x_2, x_3) \) a graph, \( G_f \). The graph \( G_f \) has a vertex for every \((i_2, i_3) \in [r_2] \times [r_3]\) such that \( f_{(2,3)}(x_2, x_3) > 0 \). A pair of vertices \((i_2, i_3)\) and \((j_2, j_3)\) is connected by an edge if either \( i_2 = j_2 \) or \( i_3 = j_3 \).

**Theorem 4.3.3.** Let \( X \) be a discrete random variable with density \( f \), satisfying the conditional independence constraints \( X_1 \perp \perp X_2 | X_3 \) and \( X_1 \perp \perp X_3 | X_2 \). If \( G_f \) is a connected graph, then the conditional independence constraint \( X_1 \perp \perp (X_2, X_3) \) also holds.

On the other hand, let \( H \) be any graph with vertex set in \([r_2] \times [r_3]\), and with connectivity between vertices as described above and such that \( H \) is disconnected. Then there is a discrete random vector \( X \) with density function \( f \) such that \( G_f = H \), \( X \) satisfies \( X_1 \perp \perp X_2 | X_3 \) and \( X_1 \perp \perp X_3 | X_2 \), but does not satisfy \( X_1 \perp \perp (X_2, X_3) \).

To prove Theorem 4.3.3, we compute the primary decomposition of the conditional independence ideal \( I_c = I_{1 \perp 2|3} + I_{1 \perp 3|2} \), and analyze the components of the ideal. Note that both conditional independence statements \( 1 \perp 2|3 \) and \( 1 \perp 3|2 \) translate to rank conditions on the \( r_1 \times (r_2 r_3) \) flattened
4.3. Primary Decomposition of CI Ideals

matrix

\[
P = \begin{pmatrix}
p_{111} & p_{112} & \cdots & p_{1r_2r_3} \\
p_{211} & p_{212} & \cdots & p_{2r_2r_3} \\
\vdots & \vdots & \ddots & \vdots \\
p_{r_11} & p_{r_12} & \cdots & p_{r_1r_2r_3}
\end{pmatrix}.
\]

Columns in the flattening are indexed by pairs \((i_2, i_3) \in [r_2] \times [r_3]\). In particular, the CI statement \(1 \perp 2 \mid 3\) says that pairs of columns with indices \((i_2, i_3)\) and \((j_2, i_3)\) are linearly dependent. The CI statement \(1 \perp 3 \mid 2\) says that pairs of columns with indices \((i_2, i_3)\) and \((i_2, j_3)\) are linearly dependent. The conclusion of the intersection axiom is that any pair of columns is linearly dependent, in other words, the matrix \(P\) has rank 1.

Now we explain the construction of the primary components, which can also be interpreted as imposing rank conditions on subsets of columns of the matrix \(P\). Let \(A = A_1 | \cdots | A_l\) be an ordered partition of \([r_2]\) and \(B = B_1 | \cdots | B_l\) be an ordered partition of \([r_3]\) with the same number of parts as \(A\). We assume that none of the \(A_k\) or \(B_k\) are empty. Form an ideal \(I_{A,B}\) with the following generators:

\[p_{i_1i_2i_3}p_{j_1j_2j_3} - p_{i_1j_2i_3}p_{j_1i_2j_3}\text{ for all } k \in [l], i_2, j_2 \in A_k \text{ and } i_3, j_3 \in B_k\]

\[p_{i_1i_2i_3}\text{ for all } k_1, k_2 \in [l] \text{ with } k_1 \neq k_2, \text{ } i_2 \in A_{k_1}, j_2 \in B_{k_2}.
\]

**Theorem 4.3.4.** Let \(I_C = I_{1 \perp 2 \mid 3} + I_{1 \perp 3 \mid 2}\) be the conditional independence ideal of the intersection axiom. Then

\[I_C = \cap_{A,B} I_{A,B}\]

where the intersection runs over all partitions \(A\) and \(B\) with the same number of components (but of arbitrary size). This decomposition is an irredundant primary decomposition of \(I_C\) after removing the redundancy arising from the permutation symmetry (simultaneously permuting the parts of \(A\) and \(B\)).

Theorem 4.3.4 is proven in [Fin11]. We will give a proof of the geometric version of the theorem, that is, show that the ideals \(I_{A,B}\) give all minimal primes of \(I_C\). To achieve this, we exploit to special features of this particular problem.

**Proof.** Since both the conditional independence statements \(X_1 \perp X_2 \mid X_3\) and \(X_1 \perp X_3 \mid X_2\) are saturated (that is, they involve all three random variables), the ideal \(I_C\) is binomial ideal. Second, the special structure of the conditional independence statements in this particular problem allow us to focus on interpreting the conditional independence statements as rank conditions on submatrices of one particular matrix.
Consider the flattened matrix
\[
P = \begin{pmatrix}
p_{111} & p_{112} & \cdots & p_{1r_2r_3} \\
p_{211} & p_{212} & \cdots & p_{2r_2r_3} \\
\vdots & \vdots & \ddots & \vdots \\
p_{r_11} & p_{r_12} & \cdots & p_{r_1r_2r_3}
\end{pmatrix},
\]
whose rows are indexed by \( i_1 \in [r_1] \) and whose columns are indexed by tuples \((i_2, i_3) \in [r_2] \times [r_3] \). The conditional independence statement \( X_1 \perp \! \! \! \perp X_2 | X_3 \) says that the \( r_3 \) submatrices of \( P \) of size \( r_1 \times r_2 \) of the form \((p_{i_1i_2j})_{i_1 \in [r_1], i_2 \in [r_2]} \) have rank 1. The conditional independence statement \( X_1 \perp \! \! \! \perp X_3 | X_2 \) says that the \( r_2 \) submatrices of \( P \) of size \( r_1 \times r_3 \) of the form \((p_{i_1j_3})_{i_1 \in [r_1], j_3 \in [r_3]} \) have rank 1.

The conditional independence constraint \( X_1 \perp \! \! \! \perp (X_2, X_3) \) says that the matrix \( P \) has rank 1. Each of the components \( I_{A,B} \) says that certain columns of \( P \) are zero, while other submatrices have rank 1. We prove now that if a point \( P \in V(I_C) \) then it must belong to one of \( V(I_{A,B}) \) for some pair of partitions \( A \) and \( B \).

Construct a graph \( G_P \) as follows. The vertices of \( G_P \) consists of all pairs \((i_2, i_3)\) such that not all \( p_{i_1i_2i_3} \) are zero. A pair of vertices \((i_2, i_3)\) and \((j_2, j_3)\) will form an edge if \( i_2 = j_2 \) or \( i_3 = j_3 \). Let \( G_1, \ldots, G_k \) be the connected components of \( G_P \). For \( l = 1, \ldots, k \) let \( A_l = \{i_2 : (i_2, i_3) \in V(G_l) \text{ for some } i_3 \} \) and \( B_l = \{i_3 : (i_2, i_3) \in V(G_l) \text{ for some } i_2 \} \). If there is some \( i_2 \in [r_2] \) which does not appear in any \( A_l \), add it to \( A_1 \), and similarly, if there is some \( i_3 \in [r_3] \) which does not appear in any \( B_l \) add it to \( B_1 \). Clearly \( A_1 | \cdots | A_k \) and \( B_1 | \cdots | B_k \) are partitions of \([r_2]\) and \([r_3]\) respectively, of the same size. We claim that \( P \in V(I_{A,B}) \).

It is not difficult to see that \( I_C \subseteq I_{A,B} \), and that each ideal \( I_{A,B} \) is prime. Finally, for two different partitions \( A, B \) and \( A', B' \), which do not different by a simultaneous permutation of the partition blocks we do not have \( I_{A,B} \subseteq I_{A',B'} \). These facts together prove that the varieties \( \cup V(I_{A,B}) = V(I_C) \) is an irredundant irreducible decomposition.

From the geometric version of Theorem 4.3.4 we deduce Theorem 4.3.3.

**Proof of Theorem 4.3.3.** Suppose that \( P \in V(I_C) \) and that the associated graph \( G_P \) is connected. This implies, by the argument in the proof of Theorem 4.3.4 that the flattened matrix \( P \) has rank 1. Hence \( P \in V(I_{[r_2],[r_3]}) \). The component \( V(I_{[r_2],[r_3]}) \) is the component where the flattening has rank 1, and hence \( I_{[r_2],[r_3]} = I_{1\perp \{2,3\}} \).

On the other hand, let \( H \) be a disconnected, induced subgraph of the complete bipartite graph \( K_{r_2,r_3} \). This induces a pair of partitions \( A, B \) of \([r_2]\) and \([r_3]\) (adding indices that do not appear in any of the vertices of \( H \).
to any part of $A$ and $B$, respectively). Since $H$ is disconnected, $A$ and $B$ will each have at least 2 parts. The resulting component $V(I_{A,B})$ contains distributions which have graph $H$. Furthermore, by the rank conditions induced by the $I_{A,B}$ only require that the matrix $P$ have rank 1 on submatrices with column indices given by $A_i, B_i$ pairs. Hence, we can construct elements in $P \in V_{\Delta}(I_{A,B})$ such that $\text{rank} \text{Flat}_{1[23]}(P) = \min(r_1, c(H))$ where $c(H)$ is the number of components of $H$. In particular, such a $P$ is not in $V(I_{1 \perp \{2,3\}})$. \hfill $\square$

4.3.2. Pairwise Marginal Independence. In this section, we study the pairwise conditional independence model for three random variables, that is, three dimensional discrete random vectors satisfying the conditional independence constraints $X_1 \perp X_2$, $X_1 \perp X_3$, and $X_2 \perp X_3$. This example and generalizations of it were studied by Kirkup [Kir07] from an algebraic perspective. In the standard presentation of this conditional independence ideal, it is not a binomial ideal. However, a simple change of coordinates reveals that in a new coordinate system it is binomial, and that new coordinate system can be exploited to get at the probability distributions that come from the model. The same change of coordinates will also work for many other marginal independence models.

We introduce a linear change of coordinates on $\mathbb{R}^R \to \mathbb{R}^R$ as follows. Instead of indexing coordinates by tuples in $[r_1] \times [r_2] \times [r_3]$, we use the set with the same cardinality

$$[r_1 - 1] \cup \{+\} \times [r_2 - 1] \cup \{+\} \times [r_3 - 1] \cup \{+\}.$$ 

So the new coordinates on $\mathbb{R}^R$ looks like $p_{+++}$ and $p_{i_1+i_3}$. The plus denotes marginalization, and this is how the map between coordinates is defined:

\[
\begin{align*}
p_{+++} & := \sum_{j_1 \in [r_1], j_2 \in [r_2], j_3 \in [r_3]} p_{j_1 j_2 j_3} & p_{+++} & := \sum_{j_1 \in [r_1], j_2 \in [r_2], j_3 \in [r_3]} p_{j_1 j_2 j_3} \\
p_{i_1 i_2 +} & := \sum_{j_1 \in [r_1], j_2 \in [r_2], j_3 \in [r_3]} p_{j_1 j_2 i_3} & p_{i_1 i_2 +} & := \sum_{j_2 \in [r_2], j_3 \in [r_3]} p_{i_1 j_2 j_3} \\
p_{i_1 i_2 i_3} & := \sum_{j_1 \in [r_1], j_2 \in [r_2], j_3 \in [r_3]} p_{i_1 j_1 i_2 j_3} & p_{i_1 i_2 i_3} & := \sum_{j_2 \in [r_2], j_3 \in [r_3]} p_{i_1 j_2 i_3}
\end{align*}
\]

where $i_1 \in [r_1 - 1]$, $i_2 \in [r_2 - 1]$, $i_3 \in [r_3 - 1]$. This transformation is square and also in triangular form, hence it is invertible (essentially via Möbius inversion).

In the new coordinate system, any marginal independence statement can be generated by binomial equations. For example, the independence
statement $X_1 \perp X_2$ is equivalent to the matrix

\[
\begin{pmatrix}
p_{1+} & p_{12+} & \cdots & p_{1r_1-1+} & p_{1++} \\
p_{21+} & p_{22+} & \cdots & p_{2r_2-1+} & p_{2++} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
p_{r_1-1+} & p_{r_1-12+} & \cdots & p_{r_1-1r_2-1+} & p_{r_1-1++} \\
p_{+1+} & p_{+2+} & \cdots & p_{+r_2-1+} & p_{+++}
\end{pmatrix}
\]

having rank 1. This follows because the matrix whose rank we usually ask to have rank 1 in the marginal independence statement is related to this one via elementary row and column operations, which preserve rank.

In the new coordinate system, the ideal $I_C$ is binomial. It is:

\[
I_C = \langle p_{i_1j_1}p_{i_2j_2} - p_{i_1j_2}p_{i_1j_2}, \quad p_{i_1i_3p_{j_1j_2} - p_{i_3j_2}p_{i_3j_2}}; \quad i_1, j_1 \in [r_1 - 1] \cup \{+\}, \quad i_2, j_2 \in [r_2 - 1] \cup \{+\}, \quad i_3, j_3 \in [r_3 - 1] \cup \{+\}\rangle.
\]

The following Macaulay 2 code computes the primary decomposition of this ideal in the case where $r_1 = r_2 = r_3 = 2$.

```macaulay2
R = QQ[p000,p001,p010,p011,p100,p101,p110,p111];
I = ideal(p000*p011 - p001*p010,
p000*p101 - p001*p100,
p000*p110 - p010*p100);
primaryDecomposition I
```

Note that 0 takes the place of the symbol “+” in the Macaulay 2 code. We see that in this case of binary random variables, $I_C$ has primary decomposition consisting of four ideals:

\[
I_C = \langle p_{++1}p_{1+} + p_{++1}p_{11+}, p_{+11}p_{++1} - p_{++1}p_{11+}, p_{+1}p_{++} - p_{++}p_{1+1}, p_{++}p_{+1+} - p_{++}p_{+11} \rangle \\
\cap \langle p_{++1}, p_{++1}, p_{++} \rangle \quad \cap \langle p_{+1+}, p_{1++}, p_{+++} \rangle \\
\cap \langle p_{1++}, p_{++1}, p_{+++} \rangle
\]

Note that the three linear components each contain $p_{+++}$ as a generator. Since we are only interested in solutions that intersect the probability simplex, the three linear components do not contribute to our understanding of this conditional independence model. This computation for binary variables suggests the following theorem.

**Theorem 4.3.5.** Let $C = \{1 \perp 2, 1 \perp 3, 2 \perp 3\}$ be the set of all pairwise marginal independencies for three discrete random variables. Then the conditional independence ideal $I_C$ has exactly one component that intersects the probability simplex nontrivially.
The probability distributions in that unique component consist of all distributions which can be written as a sum of a rank 1 3-way tensor plus a three way tensor with all zero 2-way margins.

**Proof.** The ideal $I_C$ homogeneous, so we could consider it as defining a projective variety. To this end, it makes sense to investigate that variety on its affine coordinate charts. In particular, we consider the chart where $p_{+++} = 1$. After adding this condition, we arrive at the ideal

$$J = \langle p_{i_1i_2} - p_{i_1++}p_{i_2++}, p_{i_1+i_3} - p_{i_1++}p_{+++i_3}, p_{++i_3} - p_{i_2}p_{i_3}, i_1 \in [r_1 - 1], i_2 \in [r_2 - 1], i_3 \in [r_3 - 1] \rangle.$$

This ideal is prime, since it has an initial ideal which is linear and hence prime (for example, take any lexicographic order that makes any indeterminate with one + bigger than any indeterminate with two +’s). This implies that besides the prime component $J^h$, (the homogenization of $J$ with respect to the indeterminate $p_{+++}$) every other minimal prime of $I_C$ contains $p_{+++}$. Since $p_{+++} = 1$ for probability distributions, there is only one component which intersects the probability simplex nontrivially.

The description of $J$ also gives us a parametrization of this component after homogenization. It is given parametrically as

$$p_{+++} = t; p_{i_1++} = \theta_{i_1}^{(1)} t; p_{++i_2} = \theta_{i_2}^{(2)} t; p_{+++i_3} = \theta_{i_3}^{(3)} t;$$

$$p_{i_1i_2} = \theta_{i_1}^{(1)} \theta_{i_2}^{(2)} t; p_{i_1+i_3} = \theta_{i_1}^{(1)} \theta_{i_3}^{(3)} t; p_{++i_3} = \theta_{i_3}^{(3)} t; p_{i_1+i_2+i_3} = \theta_{i_1i_2i_3}^{(123)},$$

where $i_1 \in [r_1 - 1], i_2 \in [r_2 - 1], i_3 \in [r_3 - 1]$. Note that we can modify the parametrization to have

$$p_{i_1i_2i_3} = \theta_{i_1}^{(1)} \theta_{i_2}^{(2)} \theta_{i_3}^{(3)} t + \theta_{i_1i_2i_3}^{(123)}$$

without changing the image of the parametrization. This latter variation on the parametrization realizes the second paragraph of the theorem, as we can break the parametrization into the sum of two parts. The first part, with

$$p_{i_1i_2i_3} = \theta_{i_1}^{(1)} \theta_{i_2}^{(2)} \theta_{i_3}^{(3)} t$$

realizes the rank one tensors. The second part, with

$$p_{i_1i_2i_3} = \begin{cases} 
\theta_{i_1i_2i_3}^{(123)} & i_1 \in [r_1 - 1], i_2 \in [r_2 - 1], i_3 \in [r_3 - 1], \\
0 & \text{otherwise}
\end{cases}$$

gives the parametrization of 3-way arrays with all margins equal to zero. \qed
4.3.3. No Finite Excluded Minors for Gaussian Independence. Here we consider an example of conditional independence ideals for Gaussian random variables. This family of examples shows that there is no finite list of excluded minors for Gaussian conditional independence implications. Furthermore, as above, the example ideals are all binomial ideals, and so the techniques for analyzing binomial primary decomposition described above work here as well. This example comes from the paper [Su09].

Consider this cyclic set of conditional independence statements:

\[
X_1 \perp \perp X_2 | X_3, \ldots, X_{n-1} \perp \perp X_n | X_1, X_n \perp \perp X_1 | X_2.
\]

We will show that for Gaussian random variables these statements imply the marginal independent statements:

\[
X_1 \perp \perp X_2, \ldots, X_{n-1} \perp \perp X_n, X_n \perp \perp X_1.
\]

Indeed the conditional independence ideal for the first CI statement is the binomial ideal:

\[
J_C = \langle \sigma_{12} \sigma_{33} - \sigma_{13} \sigma_{23}, \ldots, \sigma_{1n} \sigma_{22} - \sigma_{2n} \sigma_{12}, \ldots \rangle.
\]

The ideal \(J_C\) is a pure difference binomial ideal, so its minimal associated lattice ideals have a prescribed form given by Proposition [4.2.14]. The complete description is given by the following result.

**Theorem 4.3.6.** Assume \( n \geq 4 \) and let \( C = \{ 1 \perp 2|3, 2 \perp 3|4, \ldots, n \perp 1|2 \} \). Then the Gaussian CI ideal \( J_C \) has exactly two minimal primes which are

\[
\langle \sigma_{12}, \sigma_{23}, \ldots, \sigma_{n-1,n}, \sigma_{n1} \rangle
\]

and the toric component

\[
I_0 = J_C : \prod \sigma_{ij}^\infty.
\]

The irreducible component \( V(I_0) \) does not intersect the positive definite cone. Hence, for jointly normal random variables

\[
X_1 \perp X_2 | X_3, \ldots, X_{n-1} \perp X_n | X_1, X_n \perp X_1 | X_2 \implies X_1 \perp X_2, \ldots, X_{n-1} \perp X_n, X_n \perp X_1.
\]

**Proof.** The ideal \( J_C \) involves polynomials only in the variables \( \sigma_{ii}, \sigma_{i,i+1} \) and \( \sigma_{i,i+2} \), for \( i \in [n] \) (with indices considered modulo \( n \)). Note that the variable of the type \( \sigma_{ii} \) and \( \sigma_{i,i+2} \) each only appear in one of the binomial generators of \( J_C \). The results of [HS00] imply that those variables could not appear as variables of a minimal associated lattice ideal. To get a viable candidate set of variables among the remaining variables, we must take the entire remaining set \( \{ \sigma_{i,i+1} : i \in [n] \} \). This gives the ideal \( \langle \sigma_{12}, \sigma_{23}, \ldots, \sigma_{n-1,n}, \sigma_{n1} \rangle \). The empty set is always a valid candidate set, and this produces the ideal
4.4. Exercises

$I_\emptyset$ from the statement of the theorem. The fact that $V(I_\emptyset)$ does not intersect the positive definite cone (proven below), and that the other component does, and that $V(I_\emptyset)$ contains points with all nonzero entries, while the other component does not, ensures that these two components do not contain each other.

To see that the component does not intersect the positive definite cone, we will show that $I_\emptyset$ contains the polynomial

$$f = \prod_i \sigma_{ii} - \prod_i \sigma_{i,i+2}.$$  

For a positive definite matrix, we have for each $i$ that $\sigma_{ii} \sigma_{i+2,i+2} > \sigma_{i,i+2}^2$, which implies that $f > 0$ for any positive definite matrix. Now, the polynomial obtained by multiplying the leading and trailing terms of each of the generators of $J_C$, belongs to $J_C$, which is the polynomial

$$g = \prod_i \sigma_{i,i+1} \sigma_{i,i+2} - \prod_i \sigma_{i,i+1} \sigma_{i,i+2}.$$  

The polynomial $g$ is divisible by $\prod_i \sigma_{i,i+1}$, and hence $f = g/\prod_i \sigma_{i,i+1}$ is in $I_\emptyset = J_C : \prod i \sigma_{i,j}^\infty$.  

The resulting conditional independence implication follows since the linear ideal $\langle \sigma_{12}, \sigma_{23}, \ldots, \sigma_{n-1,n}, \sigma_{n1} \rangle$ is the CI ideal for $D = \{1 \perp \perp 2, \ldots, n \perp \perp 1\}$.  

Note that by carefully choosing a term order, we can arrange to have the binomial generators of $J_C$ with squarefree and relatively prime initial terms. This implies that $J_C$ is radical and hence equal to the intersection of the two primes from Theorem 4.3.6.

The statement that heads the section, that there are no finite list of excluded minors follows from Exercise 4.8 below, which shows that no subset of the given CI statements imply any of the marginal constraints $i \perp \perp i + 1$.

4.4. Exercises

Exercise 4.1. The conditional independence implication

$$A \perp B | c \cup D \quad \text{and} \quad A \perp B | D \quad \Rightarrow \quad A \perp B \cup c | D \quad \text{or} \quad A \cup c \perp B | D$$  

is called the gaussoid axiom, where $c$ denotes a singleton.

(1) Show that if $X$ is a jointly normal random variable, it satisfies the gaussoid axiom.

(2) Show that if $X$ is discrete with finitely many states, then $X$ satisfies the special case of the gaussoid axiom with, $D = \emptyset$ and $r_c = 2$.  


(3) Show that in the discrete case if we eliminate either the condition \( D = \emptyset \) or \( r_c = 2 \) we have distributions that do not satisfy the gaussoid axiom.

**Exercise 4.2.**

1. Show that every prime ideal is radical.
2. Show that the radical of a primary ideal is prime.
3. True or False: If \( \sqrt{Q} \) is a prime ideal, then \( Q \) is primary?

**Exercise 4.3.** Show that if \( I \) is a radical ideal every ideal in its primary decomposition is prime, and this decomposition is unique.

**Exercise 4.4.** For four binary random variables, consider the conditional independence model \( C = \{1 \perp \perp 3 \mid \{2, 4\}, 2 \perp \perp 4 \mid \{1, 3\} \} \). Compute the primary decomposition of \( I_C \) and describe the components.

**Exercise 4.5.** Let \( C = \{A \perp B \mid C, B \perp C\} \) be the set of conditional independence statements from the contraction axiom. Determine the primary decomposition of the Gaussian conditional independence ideal \( J_C \) and use it do deduce the conclusion of the contraction axiom in this case.

**Exercise 4.6.** In the marginal independence model \( C = \{1 \perp 2, 1 \perp 3, 2 \perp 3\} \) from Theorem 4.3.5 find the generators of the ideal of the unique component of \( I_C \) that intersects the probability simplex.

**Exercise 4.7.** Consider the marginal independence model for 4 binary random variables \( C = \{1 \perp 2, 2 \perp 3, 3 \perp 4, 1 \perp 4\} \).

1. Compute the primary decomposition of \( I_C \).
2. Show that there is exactly one component of \( V(I_C) \) that intersects the probability simplex.
3. Give a parametrization of that component.

**Exercise 4.8.** For jointly normal random variables, consider the conditional independence model

\[
C = \{1 \perp 2 \mid 3, 2 \perp 3 \mid 4, \ldots, n - 1 \perp n \mid 1\}.
\]

1. Show that \( J_C \) is a binomial ideal.
2. Show that \( J_C \) is a radical ideal (Hint: show that the given binomial generators are a Gröbner basis with squarefree initial terms and then use Proposition 4.2.11).
3. Show that \( J_C \) is prime by analyzing the candidate primes of Proposition 4.2.14.
Statistics Primer

Probability primarily concerns random variables and studying what happens to those random variables under various transformations or when repeated measurements are made. Implicit in the study is the fact that the underlying probability distribution is fixed and known (or described implicitly) and we want to infer properties of that distribution.

Statistics in large part turns this picture around. We have a collection of data, which are assumed to be random samples from some underlying, but unknown, probability distribution. We would like to develop methods to infer properties of that distribution from the data. Furthermore, we would like to perform hypothesis tests, that is, determine whether or not the data is likely to have been generated from a certain family of distributions, and measure how confident we are in that assessment.

Statistics is a rich subject and we only briefly touch on many topics in that area. Our focus for much of the book will be on frequentist methods of statistics, which focus on the large sample behavior of statistical estimators. We also discuss Bayesian methods in Section 5.5, where statistical inference is concerned with how data can be used to update our prior beliefs about an unknown parameter. Algebraic methods for Bayesian statistics will recur at a few points in the book.

5.1. Statistical Models

Much of statistics is carried out with respect to statistical models. A statistical model is just a family of probability distributions. Often these models are parametric. In this section, we give the basic definitions of statistical models and give a number of important examples.
Definition 5.1.1. A statistical model $\mathcal{M}$ is a collection of probability distributions or density functions. A parametric statistical model $\mathcal{M}_\Theta$ is a mapping from a finite dimensional parameter space $\Theta \subseteq \mathbb{R}^d$ to a space of probability distributions or density functions, i.e.

$$p_\bullet : \Theta \rightarrow \mathcal{M}_\Theta, \quad \theta \mapsto p_\theta.$$  

The model is the image of the map $p_\bullet$, $\mathcal{M}_\Theta = \{p_\theta : \theta \in \Theta\}$.

A statistical model is called identifiable if the mapping $p_\bullet$ is one-to-one; that is, $p_{\theta_1} = p_{\theta_2}$ implies that $\theta_1 = \theta_2$. We will return to discussions of identifiability in Chapter 16.

We have already seen examples of statistical models in the previous chapters, which we remind the reader of, and put into context here.

Example 5.1.2 (Binomial Random Variable). Let $X$ be a discrete random variable with $r + 1$ states, labeled $0, 1, \ldots, r$. Let $\Theta = [0, 1]$ and for $\theta \in \Theta$ consider the probability distribution

$$P_\theta(X = i) = \binom{r}{i} \theta^i (1 - \theta)^{r-i}$$

which is the distribution of a binomial random variable with $r$ samples and parameter $\theta$. The binomial random variable model $\mathcal{M}_\Theta$ consists of all the probability distribution that arise this way. It sits as a subset of the probability simplex $\Delta_r$.

Example 5.1.3 (Multivariable Normal Random Vector). Let $X \in \mathbb{R}^m$ be an $m$-dimensional real random vector. Let $\Theta = \mathbb{R}^m \times PD_m$, where $PD_m$ is the cone of symmetric $m \times m$ positive definite matrices. For $\theta = (\mu, \Sigma) \in \Theta$ let

$$p_\theta(x) = \frac{1}{(2\pi)^{n/2}|\Sigma|^{1/2}} \exp \left( -\frac{1}{2} (x - \mu)^T \Sigma^{-1} (x - \mu) \right)$$

be the density of a jointly normal random variable with mean vector $\mu$ and covariance matrix $\Sigma$. The model $\mathcal{M}_\Theta$ consists of all such density functions for an $m$-dimensional real random vector.

Statistical models with infinite dimensional parameter spaces are called nonparametric or semiparametric depending on the context. Note that this does not necessarily mean that we are considering a statistical model which does not have a parametrization, as so-called nonparametric models might still have nice parametrizations. On the other hand, models which are defined via constraints on probability distributions or densities we will refer to as implicit statistical models. Note, however, that in the statistics literature such models defined by implicit constraints on a finite dimensional parameter space are still called parametric models. We have already seen examples of implicit statistical models when looking at independence constraints.
5.1. Statistical Models

**Example 5.1.4** (Independent Random Variables). Let $X_1$ and $X_2$ be two discrete random variables with state spaces $[r_1]$ and $[r_2]$ respectively, with $\mathcal{R} = [r_1] \times [r_2]$. The model of independence $\mathcal{M}_{X_1 \perp \perp X_2}$ consists of all distributions $p \in \Delta_{\mathcal{R}}$ such that

$$P(X_1 = i_1, X_2 = i_2) = P(X_1 = i_1)P(X_2 = i_2)$$

for all $i_1 \in [r_1]$ and $i_2 \in [r_2]$. Thus, the model of independence is an implicit statistical model. As discussed in Section 4.1, this model consists of all joint distribution matrices which are rank 1 matrices. From that description we can also realize this as a parametric statistical model. Indeed, let $\Theta = \Delta_{r_1 - 1} \times \Delta_{r_2 - 1}$, and given $\theta = (\alpha, \beta) \in \Theta$, define the probability distribution

$$p_\theta(X_1 = i_1, X_2 = i_2) = \alpha_{i_1} \beta_{i_2}. \quad \square$$

Our main example of implicit statistical model in this book comes from looking at conditional independence constraints. If $\mathcal{C} = \{A_1 \perp \perp B_1 | C_1, A_2 \perp \perp B_2 | C_2, \ldots\}$ is a collection of conditional independence statements, for each fixed set of states $r_1, r_2, \ldots, r_m$ we get a discrete conditional independence model

$$\mathcal{M}_C = V(I_{A_1 \perp \perp B_1 | C_1} + I_{A_2 \perp \perp B_2 | C_2} + \cdots) \cap \Delta_{\mathcal{R}}$$

which is an implicit statistical model. Similarly, we get a gaussian conditional independence model

$$\mathcal{M}_C = V(J_{A_1 \perp \perp B_1 | C_1} + J_{A_2 \perp \perp B_2 | C_2} + \cdots) \cap PD_m.$$

An important concept in the study of statistical models is the notion of sufficiency of a statistic. Sufficient statistics explain the way that the state of a variable enters into the calculation of the probability of that state in a model, and the interaction of the state of the random variable with the parameters.

**Definition 5.1.5.** A **statistic** is a function from the state space of a random variable to some other set. For a parametric statistical model $\mathcal{M}_\Theta$, a statistic $T$ is **sufficient** for the model if

$$P(X = x | T(X) = t, \theta) = P(X = x | T(X) = t).$$

Equivalently, the joint distribution $p_\theta(x)$ should factorize as

$$p_\theta(x) = f(x)g(T(x), \theta)$$

where $f$ is a function that does not depend on $\theta$. A statistic $T$ is **minimal sufficient** if every other sufficient statistic is a function of $T$.

Examples of sufficiency will appear in the next section as we discuss different types of data.
5.2. Types of Data

Statistical models are used to analyze data. If we believe our data follows a distribution that belongs to the model, we would like to estimate the model parameters from the data and use the resulting quantities to make some conclusions about the underlying process that generated the data. Alternately, we might not be sure whether or not a given model is a good explanation of the data. To this end, we would perform a hypothesis test, to decide whether or not the model is a good fit. Before we can talk about any of these statistical settings, however, we need to discuss what we mean by data, and, in some sense, different types of models. In particular, natural classes of data generating procedures include, independent identically distributed data, exchangeable data, and time-series and spatial data. The techniques from algebraic statistics that can be applied depend on what was the underlying data generation assumption.

The most common type of data generation we will encounter in this book is the case of independent identically distributed data. In this setting, we assume that we have \( n \) sample data \( D = X^{(1)}, X^{(2)}, \ldots, X^{(n)} \), each distributed identically and independently like the distribution \( p_\theta(X) \), for some distribution \( p_\theta \) in our model. If our random variables are discrete, the probability of observing the particular sequence of data, given \( \theta \) is

\[
p_\theta(D) = \prod_{i=1}^{n} p_\theta(X^{(i)}).
\]

For continuous distributions, the density function is represented similarly in product form. Note that in the discrete case, where our random variable has state space \([r]\), we can compute the vector of counts \( u \in \mathbb{N}^r \), defined by

\[ u_j = \#\{i : X^{(i)} = j\} \]

in which case

\[
p_\theta(D) = \prod_{j=1}^{r} p_\theta(j)^{u_j}
\]

so that the vector of counts gives sufficient statistics for a model under the i.i.d. assumption. Note that for discrete random variables, the vector of counts \( u \) is a summary of the data from which it is possible to compute the probability of observing the particular sequence \( i_1, \ldots, i_n \). When working with such models and discussing data for such models, we usually immediately pass to the vector of counts as our data for such models.

A second type of assumption that arises in Bayesian statistics is known as exchangeable random variables. Discrete random variables \( X^{(1)}, \ldots, X^{(n)} \)
are exchangeable if and only if
\[ P(X_1 = i_1, \ldots, X_n = i_n) = P(X_1 = i_{\sigma(1)}, \ldots, X_n = i_{\sigma(n)}) \]
for any permutation \( \sigma \) of the index set \([n]\). For continuous random variables, we require the same permutation condition on the density function. Note that independent identically distributed random variables are exchangeable, but the reverse is not true. For example, sampling balls from an urn without replacement gives a distribution on sequences of balls that is exchangeable but not i.i.d. Although sampling without replacement is a common sampling mechanism, we will typically assume i.i.d. sampling in most contexts. We will discuss exchangeable random variables again in Section ?? where Definetti’s theorem is discussed.

The first two data types we have discussed have the property that the order that the data arrives does not matter in terms of the joint distribution of all the data. Only the vector of counts is important in both i.i.d. and exchangeable random variables. A third type of data to consider is when the order of the variables does matter. This type of data typical arises in the context of time series data, or spatial data.

A typical example of a time series model, where the resulting order of the observations matters, is a Markov chain (see Chapter ??). In a Markov chain, we have a sequence of random variables \(X_1, \ldots, X_n\) with the same state space \([r]\) such that
\[ P(X_j = i_j | X_{j-1} = i_{j-1}, \ldots, X_1 = i_1) = P(X_j = i_j | X_{j-1} = i_{j-1}) \]
for \(j = 2, \ldots, n, i_1, \ldots, i_n \in [r]^n\), Note that by applying Bayes rule and using the first condition of being a Markov chain, we see that the joint probability factorizes as
\[ P(X_1 = i_1, \ldots, X_n = i_n) = P(X_1 = i_1)P(X_2 = i_2 | X_1 = i_1) \cdots P(X_n = i_n | X_{n-1} = i_{n-1}). \]

The further assumption of homogeneity requires that
\[ P(X_j = i' | X_{j-1} = i) = P(X_2 = i' | X_1 = i) \]
for all \(j = 3, \ldots, n\) and \(i', i \in [r]\). From this we see that the sufficient statistics for a Markov chain model are \(X_1\) and the table of counts \(u\) such that
\[ u_{i'i} = \#\{j : X_j = i', X_{j-1} = i\}. \]
Note that \(u\) counts the number of each type of transition that occurred in the sequences \(X_1, X_2, \ldots, X_n\).

For i.i.d. samples, we typically observe many replicates from the same underlying model. When use a time series or spatial model, the usual way data arrives as a single sample from that models, whose length or size might
not be a priori specified. For these models to be useful in practice, we need them to be specified with a not very large set of parameters, so that as the data grows (i.e. as the sequence gets longer) we have a hope of being able to estimate the parameters.

5.3. Parameter Estimation

Given a parametric statistical model and some data, a typical problem in statistics is to estimate some of, or all of, the parameters of the model based on the data. At this point we do not necessarily assume that the model accurately models the data. The problem of testing whether or not a model actually fits the data is the subject of the next section, on hypothesis testing.

Ideally, we would like a procedure which, as more and more data arrives, if the underlying distribution that generated the data comes from the model, the parameter estimate converges to the true underlying parameter. Such an estimator is called a consistent estimator.

**Definition 5.3.1.** Let $M_\Theta$ be a parametric statistical model with parameter space $\Theta$. A *parameter* of a statistical model is a function $s : \Theta \to \mathbb{R}$. An *estimator* of $s$, is a function from the data space $D$ to $\mathbb{R}$, $\hat{s} : D \to \mathbb{R}$. The estimator $\hat{s}$ is *consistent* if $\hat{s} \xrightarrow{p} s$ as the sample size tends to infinity.

Among the simplest examples of estimators are the plug-in estimators. As the name suggests, a plug-in estimator is obtained by plugging in values obtained from the data to estimate parameters.

**Example 5.3.2.** As a simple example, consider the case of binomial random variable, with $r + 1$ states, $0, 1, \ldots, r$. The model consists of all distributions of the form

$$\left\{ \left( \theta^r, \frac{r}{1} \theta^{r-1}(1-\theta), \ldots, (1-\theta)^r \right) : \theta \in [0, 1] \right\}.$$

Under i.i.d. sampling, data consists of $n$ repeated draws $X(1), \ldots, X(n)$ from an underlying distribution $p_\theta$ in this model. The data is summarized by a vector of counts $u = (u_0, \ldots, u_r)$, where $u_i = \#\{ j : X(j) = i \}$. We would like to estimate the parameter $\theta$ from the data of counts $u$. The value $p_\theta(0) = \theta^r$, hence, if we had a consistent estimator of $p_\theta(0)$, we could obtain a plug-in estimate for $\theta$ by extracting the $r$-th root. For example, the formula

$$\sqrt[n]{\frac{1}{n} \sum_{i=1}^{n} 1_{X(i)=0}} = \sqrt[\frac{u_0}{n}]$$

gives a consistent plug-in estimator of the parameter $\theta$. \qed
Intuitively, the plug-in estimator from Example 5.3.2 is unlikely to be a very useful estimator, since it only uses very little information from the data to obtain an estimate of the parameter \( \theta \). When choosing a consistent plug-in estimator, we would generally like to use one whose variance rapidly tends to zero as \( n \to \infty \). The estimator from Example 5.3.2 has high variance and so is an inefficient estimator of the parameter \( \theta \).

Among the many possible estimators of a parameter, one of the most frequently used is the maximum likelihood estimator (MLE). The MLE is one of the most commonly used estimators in practice, both for its intuitive appeal, and for useful theoretical properties associated with it. In particular, it is usually a consistent estimator of the parameters and with certain smoothness assumptions on the model, it is asymptotically normally distributed. We will return to these properties in Chapter 7.

**Definition 5.3.3.** Let \( D \) be data from some model with parameter space \( \Theta \). The likelihood function

\[
L(\theta|D) := p_\theta(D)
\]

in the case of discrete data and

\[
L(\theta|D) := f_\theta(D)
\]

in the case of continuous data. Here \( p_\theta(D) \) is the probability of observing the data given the parameter \( \theta \) in the discrete case, and \( f_\theta(D) \) is the density function evaluated at the data in the continuous case. The maximum likelihood estimate (MLE) \( \hat{\theta} \) is maximizer of the likelihood function:

\[
\hat{\theta} = \arg \max_{\theta \in \Theta} L(\theta|D).
\]

Note that we consider the likelihood function as a function of \( \theta \) with the data \( D \) fixed. This contrasts the interpretation of the probability distribution where the parameter is considered fixed and the random variable is the unknown (random) quantity.

In the case of i.i.d. sampling, so \( D = X^{(1)}, \ldots, X^{(n)} \), the likelihood function factorizes as

\[
L(\theta|D) = L(\theta|X^{(1)}, \ldots, X^{(n)}) = \prod_{i=1}^{n} L(\theta|X^{(i)}).
\]

In the case of discrete data, this likelihood function is thus only a function of the vector of counts \( u \), so that

\[
L(\theta|X^{(1)}, \ldots, X^{(n)}) = \prod_j p_\theta(j)^{u_j}.
\]
In the common setting in which we treat the vector of counts itself as the data, we need to multiply this quantity by an appropriate multinomial coefficient

\[ L(\theta|u) = \left(\begin{array}{c} n \\ u \end{array}\right) \prod_j p_\theta(j)^{u_j}, \]

which does not change the maximum likelihood estimate but will change the value of the likelihood function when evaluated at the maximizer.

It is common to replace the likelihood function with the log-likelihood function, which is defined as

\[ \ell(\theta|D) = \log L(\theta|D). \]

In the case of i.i.d. data, this has the advantage of turning a product into a sum. Since the logarithm is a monotone function both the likelihood and log-likelihood have the same maximizer, which is the maximum likelihood estimate.

**Example 5.3.4 (Maximum Likelihood of Binomial Random Variable).** Consider the model of a binomial random variable with \( r \) trials. The probability \( p_\theta(i) = \binom{r}{i} \theta^i (1 - \theta)^{r-i} \). Given a vector of counts \( u \), the log-likelihood function is

\[
\ell(\theta, u) = C + \sum_{i=0}^{r} u_i \log(\theta^i (1 - \theta)^{r-i})
\]

\[ = C + \sum_{i=0}^{r} (iu_i \log \theta + (r - i)u_i \log (1 - \theta)), \]

where \( C \) is a constant involving logarithms of binomial coefficients but does not depend on the parameter \( \theta \). To calculate the maximum likelihood estimate, we differentiate the log-likelihood function with respect to \( \theta \) and set it equal to zero, arriving at:

\[
\frac{\sum_{i=0}^{r} iu_i}{\theta} - \frac{\sum_{i=0}^{r} (r - i)u_i}{1 - \theta} = 0.
\]

Hence, the maximum likelihood estimator, \( \hat{\theta} \) is given by

\[
\hat{\theta} = \frac{\sum_{i=0}^{r} iu_i}{rn}. \quad \Box
\]

The gradient of the log-likelihood function is called the score function. Since the gradient of a function is zero at a global maximum of a differentiable function, the equations obtained by setting the score function to zero are called the score equations or the critical equations. In many cases, these equations are algebraic and the algebraic nature of the equations will be explored in later chapters.
5.3. Parameter Estimation

For some of the most standard statistical models, there are well-known closed formulas for the maximum likelihood estimates of parameters.

**Proposition 5.3.5.** For a multivariate normal random variable, the maximum likelihood estimates for the mean and covariance matrix are:

$$
\hat{\mu} = \frac{1}{n} \sum_{i=1}^{n} X^{(i)} , \quad \hat{\Sigma} = \frac{1}{n} (X^{(i)} - \hat{\mu})(X^{(i)} - \hat{\mu})^{T} .
$$

**Proof.** The log-likelihood function has the form

$$
\log(\mu, \Sigma | D) = -\frac{1}{2} n \left( m \log(2\pi) + \log |\Sigma| + (X^{(i)} - \mu)^{T} \Sigma^{-1} (X^{(i)} - \mu) \right) .
$$

The trace trick is useful for rewriting this log-likelihood as

$$
\log(\mu, \Sigma | D) = -\frac{1}{2} \left( nm \log(2\pi) + n \log |\Sigma| + \text{tr}\left( \sum_{i=1}^{n} ((X^{(i)} - \mu)(X^{(i)} - \mu)^{T})\Sigma^{-1} \right) \right) .
$$

Differentiating with respect to $\mu$ and setting equal to zero yields the equation

$$
-\frac{1}{2} \sum_{i=1}^{n} \Sigma^{-1} (X^{(i)} - \mu) = 0 .
$$

From this we deduce that $\hat{\mu} = \frac{1}{n} \sum_{i=1}^{n} X^{(i)}$, the sample mean.

To find the maximum likelihood estimate for the covariance matrix we substitute $K = \Sigma^{-1}$ and differentiate the log-likelihood with respect to an entry of $K$. One makes use of the classical adjoint formula for the inverse of a matrix to see that

$$
\frac{\partial}{\partial k_{ij}} \log |K| = (1 + \delta_{ij})\sigma_{ij}
$$

where $\delta_{ij}$ is the Dirac delta function. Similarly,

$$
\frac{\partial}{\partial k_{ij}} \text{tr}\left( \sum_{i=1}^{n} ((X^{(i)} - \mu)(X^{(i)} - \mu)^{T})K \right) = n(1 + \delta_{ij})s_{ij}
$$

where $S = \frac{1}{n} (\sum_{i=1}^{n} ((X^{(i)} - \mu)(X^{(i)} - \mu)^{T})$ is the sample covariance matrix. Putting these pieces together with our solution that the maximum likelihood estimate of $\mu$ is $\hat{\mu}$ gives that $\hat{\Sigma} = \frac{1}{n} (X^{(i)} - \hat{\mu})(X^{(i)} - \hat{\mu})^{T}$. □

**Proposition 5.3.6.** Let $\mathcal{M}_{1\perp\perp 2}$ be the model of independence of two discrete random variables, with $r_1$ and $r_2$ states respectively. Let $u \in \mathbb{N}^{r_1 \times r_2}$ be the table of counts for this model obtained from i.i.d. samples from the model. Let $u_{i1+} = \sum_{i} u_{i12}$ and $u_{+i2} = \sum_{i} u_{i1i2}$ be the table marginals, and $n =
The sample size. Then the maximum likelihood estimate for a distribution \( p \in \mathcal{M}_{1 \perp 2} \) given the data \( u \) is

\[
\hat{p}_{i_1 i_2} = \frac{u_{i_1 +} + u_{i_2 +}}{n^2}.
\]

**Proof.** A distribution \( p \in \Delta_R \) belongs to the independence model if and only if we can write \( p_{i_1 i_2} = \alpha_{i_1} \beta_{i_2} \) for some \( \alpha \in \Delta_{r_1 - 1} \) and \( \beta \in \Delta_{r_2 - 1} \). We solve the likelihood equations in terms of \( \alpha \) and \( \beta \) and use them to find \( \hat{p} \). Given a table of counts \( u \), the log-likelihood function for a discrete random variable has the form

\[
\ell(\alpha, \beta|u) = \sum_{i_1, i_2 \in \mathcal{R}} u_{i_1 i_2} \log p_{i_1 i_2} \\
= \sum_{i_1, i_2 \in \mathcal{R}} u_{i_1 i_2} \log \alpha_{i_1} \beta_{i_2} \\
= \sum_{i_1 \in [r_1]} u_{i_1 +} \log \alpha_{i_1} + \sum_{i_2 \in [r_2]} u_{i_2 +} \log \beta_{i_2}.
\]

From the last line, we see that we have two separate optimization problems that are independent of each other: maximizing with respect to \( \alpha \) and maximizing with respect to \( \beta \). Remembering that \( \alpha_{r_1} = 1 - \sum_{i_1 = 1}^{r_1 - 1} \alpha_{i_1} \) and computing partial derivatives to optimize shows that \( \hat{\alpha}_{i_1} = \frac{u_{i_1 +}}{n} \). Similarly, \( \hat{\beta}_{i_2} = \frac{u_{i_2 +}}{n} \).

Unlike the three preceding examples, most statistical models do not possess closed form expressions for their maximum likelihood estimates. The algebraic geometry of solving the critical equations will be discussed in later chapters, as will some numerical hill-climbing methods for approximating solutions.

### 5.4. Hypothesis Testing

A hypothesis test is a procedure given data for deciding whether or not a statistical hypothesis might be true. Typically, statistical hypotheses are phrased in terms of statistical models: for example, does the unknown distribution, about which we have collected i.i.d. samples, belong to a given model, or not. Hypothesis testing necessitates the introduction of \( p \)-values which gives us methods to reject our null hypotheses. Note that statisticians are conservative so we rarely say that we accept the null hypothesis after performing a hypothesis test, only that the test has not provided evidence against a particular hypothesis.

As a simple example of a hypothesis test, suppose we have two random variables \( X \) and \( Y \) on the real line, and we suspect that they might be the same distribution. Hence the **null hypothesis** \( H_0 \) is that \( X = Y \) and the
alternative hypothesis $H_a$ is that $X \neq Y$. This is stated as saying we are testing:

$$H_0 : X = Y \text{ vs. } H_a : X \neq Y.$$  

We collect samples $X^{(1)}, \ldots, X^{(n_1)}$ and $Y^{(1)}, \ldots, Y^{(n_2)}$. If $X = Y$ then these two sampled distributions should behave similarly, in particular, they should have the same mean. Of course, the sampling means

$$\bar{\mu}_1 = \frac{1}{n_1} \sum_{i=1}^{n_1} X^{(i)}, \quad \bar{\mu}_2 = \frac{1}{n_2} \sum_{i=1}^{n_2} Y^{(i)}$$

will not be exactly equal, and so we need a way to measure that these are close to each other up to the error induced by sampling.

The following permutation test (also called an exact test) gives a method, free from any distributional assumptions on the variables $X$ and $Y$, to test the null hypothesis versus the alternative hypothesis:

For the given data $X^{(1)}, \ldots, X^{(n_1)}$ and $Y^{(1)}, \ldots, Y^{(n_2)}$ calculate the absolute difference of means $\bar{d} = |\bar{\mu}_1 - \bar{\mu}_2|$. Now, group all of these samples together into one large set of samples $Z_1, \ldots, Z_{n_1+n_2}$. For each partition $A|B$ of $[n_1 + n_2]$ into a set $A$ of size $n_1$ and a set $B$ of size $n_2$, we compute the difference of sample means

$$d(A, B) = |\frac{1}{n_1} \sum_{a \in A} Z_a - \frac{1}{n_2} \sum_{b \in B} Z_b|.$$  

If $d(A, B)$ is smaller than $\bar{d}$ for most partitions $A|B$, we are likely to conclude that $X \neq Y$, since the test seems to indicate that the sample means are farther apart, more than would be expected to sampling error.

Of course, the crucial word “most” in the last sentence needs clarification. The proportion of partitions $A|B$ such that $d(A, B) > \bar{d}$ is called the $p$-value of the permutation test. A large $p$-value indicates that the permutation test provides no evidence against the null hypothesis, whereas a small $p$-value provides evidence against the null hypothesis. Fixing a level $\alpha$, if the $p$-value is less than $\alpha$ we reject the null hypothesis at level $\alpha$. Otherwise, we are unable to reject the null hypothesis. Tradition in statistics sets the usual rejection level at $\alpha = .05$.

We will discuss a number of other hypothesis tests throughout the book, including the likelihood ratio test and Fisher’s exact test. In each case, we must define the $p$-value in a way that is appropriate to the given test. Most generally, when testing a specific hypothesis, we have a test statistic $T$ which we evaluate on the data, which evaluates to zero if the data exactly fits the null hypothesis $H_0$, and which increases moving away from the null hypothesis. The $p$-value is then the probability (under an appropriately chosen distribution) that the test statistic has a larger value than the given
observed value. In the case of permutation test, we calculate the probability that a random partition of the data has differences of means above the value calculated from the data.

A final remark about hypothesis testing is that we rarely calculate the \( p \)-value exactly. Even in the permutation test, it is not possible to give a closed form formula for the \( p \)-value nor is it possible for large sample sizes to compute the sum over all partitions \( A|B \). In that case, we can randomly sample partitions to approximate the \( p \)-value. In other contexts (e.g. the likelihood ratio test), a standard strategy is to assume that the sample size tends to infinity. In this case, it is possible to derive the asymptotic distribution of the test statistic. For smooth models, those asymptotic distributions are familiar distributions of probability theory like the chi-square distribution, and this allows us to compute asymptotic \( p \)-values.

5.5. Bayesian Statistics

Likelihood inference, hypothesis tests, and \( p \)-values are all standard tools from frequentist statistics. Frequentist statistics is typically concerned with the long term behavior of estimators, how they behave as more and more data comes in for analyzing a problem. In frequentist statistics approaches to parametric statistics models, it is assumed that there is a true underlying parameter vector, and we seek to find information about that parameter by collecting data.

A complementary approach in statistics is called Bayesian statistics. In Bayesian statistics, the point of collecting data is to update our beliefs about unknown parameters. Typically we have prior beliefs about the parameters, represented by a prior distribution \( \pi \) on the parameter space \( \Theta \). Data \( D \) allows us to compute an update on the distribution on \( \Theta \) which gives us the posterior distribution. The posterior distribution is computed via the formula

\[
p(\theta|D) = \frac{p(D|\theta)\pi(\theta)}{\int_{\theta} p(D|\theta)\pi(\theta)}.
\]

Note that the quantity in the denominator \( \int_{\theta} p(D|\theta)\pi(\theta) \) is the probability of the data, and is called the marginal likelihood integral. This application of Bayes theorem in the calculation of the posterior distribution is the reason for referring to these methods as Bayesian.

As with many statistical methods, the main difficulty in using Bayesian methods in practice are computational. There are usually no closed form for the posterior distribution and they must be approximated, often using Monte Carlo algorithms. Similarly, the marginal likelihood is usually not easy to calculate and must itself be approximated.
Bayesian methods produce a distribution over the parameter space, our posterior belief about the parameter. In some situations, it is useful or necessary to compute a point estimate of the parameter. A natural choice is the maximum a posteriori estimate or MAP estimate. This is simply the $\theta$ the maximizes the posterior distribution.

**Definition 5.5.1.** Let $\mathcal{M}_\Theta$ be a parametric statistical model, $\pi$ a prior distribution over $\Theta$, $D$ a collection of data, and $p(\theta|D)$ the posterior distribution of $\theta$ given the data. The maximum a posteriori estimator of $\theta$, (MAP) is

$$\hat{\theta} = \arg \max_{\theta \in \Theta} p(\theta|D).$$

Note the similarity of the definition of the MAP estimate to the MLE. These estimates can be vastly different depending on the underlying prior distribution, though increasing amounts of data usually (as one would hope) eliminates the dependence on the prior in the limit.

**Example 5.5.2.** Consider let $X$ be a discrete random variable with $r$ states. We will consider a natural prior distribution, the Dirichlet distribution, which is commonly used in models with discrete random variables.

Let $\alpha \in \mathbb{R}_{>0}^r$ be a nonnegative real parameter vector. A random variable $\in \Delta_{r-1}$ has Dirichlet distribution with parameter $\alpha$, (denoted $X \sim \text{Dir}(\alpha)$) if the density function $f_\alpha(x) \propto \prod_{i=1}^r x_i^{\alpha_i - 1}$. The proportionality constant $B(\alpha)$ is the multivariate beta function

$$B(\alpha) = \frac{\prod_{i=1}^r \Gamma(\alpha_i)}{\Gamma(\alpha_1 + \cdots + \alpha_r)}.$$

If $\alpha_i > 1$ for all $i$, then Dirichlet distribution has peak (both mean and mode) at $\alpha/\|\alpha\|_1$, and the peak becomes narrower for larger values of $\|\alpha\|_1$. As a prior distribution for the multinomial distribution, the Dirichlet distribution gives concentration around the mode $\alpha/\|\alpha\|_1$ with $\|\alpha\|_1$ giving a measure of certainty about the mode.

Now suppose we receive $n$ i.i.d. samples from a random variable $Y$ with $[r]$ states. We record this by the vector of counts $u$. Given a sample size $n$, the conditional distribution of $u$ given $X$ is multinomial, so the joint density of $u$ and $X$ is

$$f(x, u) = B(\alpha) \prod_{i=1}^r x_i^{\alpha_i - 1} \times \binom{n}{u} \prod_{i=1}^r x_i^{u_i}.$$

Whatever the marginal distribution of $u$ is, we see that the conditional density of $X$ given $u$ is

$$f(x|u) \propto \prod_{i=1}^r x_i^{u_i+\alpha_i-1}.$$
That is, the posterior distribution of the parameter given the data \( u \) is a Dirichlet distribution with parameter \( \alpha + u \). So the maximum a posterior estimate of the parameter given the data \( u \) is the vector \( (u + \alpha)/\|u + \alpha\|_1 \).

Now suppose that there is some true underlying distribution \( p \) which generates the samples. As the sample size \( n \) gets large, the law of large numbers shows that \( u/n \) will converge to \( p \). Since \( \alpha \) was some a priori fixed value, this will imply that \( (u + \alpha)/\|u + \alpha\|_1 \) also converges to \( p \) as \( n \) goes to infinity. Hence, regardless of what particular \( \alpha \) we chose at the start of our analysis, eventually we end up with a good estimate of the true underlying parameter \( p \).

An interesting fact about this example is that the posterior distribution has the same functional form as the prior distribution. This does not always happen, but happens here because the Dirichlet distribution is the conjugate prior to the multinomial distribution. □

Bayesian and frequentist statistics are sometimes seen as being at odds with each other. We do not propose to “take sides” in the present work, rather seeing them both as useful methods which make sense for different situations, and, from the standpoint of algebraic statistics, both are rich with connections to algebraic geometry. Bayesian approaches make sense when we wish to incorporate our prior beliefs about parameters into our analysis of data. Frequentist perspectives make sense when we have lots of data arriving and we can analyze asymptotic properties of estimators. We will see specific discussion of Bayesian methods in the chapters on singular learning theory and parametric inference.

5.6. Exercises

Exercise 5.1. An exponential random variable \( X \) with parameter \( \lambda \) has density function

\[
f_{\lambda}(x) = \begin{cases} \lambda \exp(-\lambda x) & x > 0 \\ 0 & \text{otherwise} \end{cases}
\]

Let \( X^{(1)}, \ldots, X^{(n)} \) be i.i.d. exponential random variables. What is the maximum likelihood estimate of \( \lambda \)?

Exercise 5.2. Consider the two lists of, respectively, 15 and 12 real numbers.

\[
A = \{1.04, -0.12, 0.22, 0.08, -0.06, -0.11, 0.06, 1.06, -1.73, -0.58, 0.67, 0.06, 1.10, -0.93, 0.34\}
\]

\[
B = \{3.36, 1.00, 1.15, -0.57, 0.84, 0.18, 0.28, 0.52, 2.44, -4.22, 2.95, -1.83\}
\]
The elements of $A$ are i.i.d. samples from a probability distributions $p$ and the elements of $B$ are i.i.d. samples from a probability distribution $q$. Do you think $p = q$? Formulate and apply a hypothesis test, and calculate $p$-values.
In this chapter we introduce exponential families. This class of statistical models plays an important role in modern statistics because it provides a broad framework for describing statistical models. The most commonly studied families of probability distributions are exponential families, including the families of jointly normal random variables, the exponential, Poisson, and multinomial models. We will see a large number of statistical models that are naturally interpreted as submodels of regular exponential families. The way in which the model is a submodel is in two ways, first, that the parameter of the model sit as a subset of the parameter space, and that the sufficient statistics of the exponential family then maps the data into the cone of sufficient statistics of the larger exponential families. This allows the mathematical analysis of many interesting and complicated statistical models beyond the regular exponential families.

The statistical literature has largely focused on the case where those submodels of exponential families are given by smooth submanifolds of the parameter space. These are known as curved exponential families in the literature. We focus here on the situation where the submodel is a (not-necessarily smooth) semi-algebraic subset of the natural parameter space of the exponential family which are called algebraic exponential families. Semi-algebraic sets are the most fundamental objects of real algebraic geometry and we will review their definitions and properties in Section 6.4. Algebraic exponential families will play a major role throughout the remainder of the text.

Besides being a useful framework for generalizing and unifying families of statistical models for broad analysis, the class of exponential families also
satisfies useful properties that make them pleasant to work with in statistical analyses. For example, all regular exponential families have concave likelihood functions which means implies that hill-climbing approaches can be used to find the maximum likelihood estimates given data (see Section 7.2). These models also have nice conjugate prior distributions, which make them convenient to use in Bayesian analysis.

### 6.1. Regular Exponential Families

Consider a sample space $\mathcal{X}$ with $\sigma$-algebra $\mathcal{A}$ on which is defined a $\sigma$-finite measure $\nu$. Let $T : \mathcal{X} \to \mathbb{R}^k$ be a statistic, i.e., a measurable map, and $h(x) : \mathcal{X} \to \mathbb{R}_{>0}$ a measurable function. Define the natural parameter space

$$N = \left\{ \eta \in \mathbb{R}^k : \int_{\mathcal{X}} h(x) \cdot e^{\eta^T T(x)} d\nu(x) < \infty \right\}.$$ 

For $\eta \in N$, we can define a probability density $p_\eta$ on $\mathcal{X}$ as

$$p_\eta(x) = h(x) e^{\eta^T T(x)-\phi(\eta)},$$

where

$$\phi(\eta) = \log \int_{\mathcal{X}} h(x) e^{\eta^T T(x)} d\nu(x).$$

Let $P_\eta$ be the probability measure on $(\mathcal{X}, \mathcal{A})$ that has $\nu$-density $p_\eta$. Define $\nu^T = \nu \circ T^{-1}$ to be the measure that the statistic $T$ induces on the Borel $\sigma$-algebra of $\mathbb{R}^k$. The support of $\nu^T$ is the intersection of all closed sets $A \subseteq \mathbb{R}^k$ that satisfy $\nu^T(\mathbb{R}^k \setminus A) = 0$. The function $\phi(\eta)$ can be interpreted as the logarithm of the Laplace transform of $\nu^T$. Recall that the affine dimension of $A \subseteq \mathbb{R}^k$ is the dimension of the linear space spanned by all differences $x - y$ of two vectors $x, y \in A$.

**Definition 6.1.1.** Let $k$ be a positive integer. The probability distributions $(P_\eta : \eta \in N)$ form a regular exponential family of order $k$ if $N$ is an open set in $\mathbb{R}^k$ and the affine dimension of the support of $\nu^T$ is equal to $k$. The statistic $T(x)$ that induces the regular exponential family is called a canonical sufficient statistic.

The order of a regular exponential family is unique and if the same family is represented using two different canonical sufficient statistics then those two statistics are non-singular affine transforms of each other [Bro86 Thm. 1.9].

Regular exponential families comprising families of discrete distributions, have been the subject of much of the work on algebraic statistics.
Example 6.1.2 (Discrete data). Let the sample space $\mathcal{X}$ be the set of integers $[r]$. Let $\nu$ be the counting measure on $\mathcal{X}$, i.e., the measure $\nu(A)$ of $A \subseteq \mathcal{X}$ is equal to the cardinality of $A$. Consider the statistic $T : \mathcal{X} \to \mathbb{R}^{r-1}$

$$T(x) = (1_{\{1\}}(x), \ldots, 1_{\{r-1\}}(x))^t,$$

whose zero-one components indicate which value in $\mathcal{X}$ the argument $x$ is equal to. In particular, when $x = r$, $T(x)$ is the zero vector. Let $h(x) = 1$ for all $x \in [r]$. The induced measure $\nu^T$ is a measure on the Borel $\sigma$-algebra of $\mathbb{R}^{r-1}$ with support equal to the $r$ vectors in $\{0, 1\}^{r-1}$ that have at most one non-zero component. The differences of these $r$ vectors include all canonical basis vectors of $\mathbb{R}^{r-1}$. Hence, the affine dimension of the support of $\nu^T$ is equal to $r - 1$.

It holds for all $\eta \in \mathbb{R}^{r-1}$ that

$$\phi(\eta) = \log \int_{\mathcal{X}} e^{\eta^T(x)} d\nu(x) = \log \left(1 + \sum_{x=1}^{r-1} e^{\eta_x}\right) < \infty.$$ 

Hence, the natural parameter space $N$ is equal to all of $\mathbb{R}^{r-1}$ and in particular is open. The $\nu$-density $p_\eta$ is a probability vector in $\mathbb{R}^r$. The components $p_\eta(x)$ for $1 \leq x \leq r - 1$ are positive and given by

$$p_\eta(x) = \frac{e^{\eta_x}}{1 + \sum_{x=1}^{r-1} e^{\eta_x}}.$$

The last component of $p_\eta$ is also positive and equals

$$p_\eta(r) = 1 - \sum_{x=1}^{r-1} p_\eta(x) = \frac{1}{1 + \sum_{x=1}^{r-1} e^{\eta_x}}.$$

The family of induced probability distribution $(P_\eta : \eta \in \mathbb{R}^{r-1})$ is a regular exponential family of order $r - 1$. The interpretation of the natural parameters $\eta_x$ is one of log odds because $p_\eta$ is equal to a given positive probability vector $(p_1, \ldots, p_r)$ if and only if $\eta_x = \log(p_x/p_m)$ for $x = 1, \ldots, r-1$. This establishes a correspondence between the natural parameter space $N = \mathbb{R}^{r-1}$ and the interior of the $r - 1$ dimensional probability simplex $\Delta_{r-1}$. □

The other distributional framework that has seen application of algebraic geometry is that of multivariate normal distributions.

Example 6.1.3 (Normal distribution). Let the sample space $\mathcal{X}$ be Euclidean space $\mathbb{R}^m$ equipped with its Borel $\sigma$-algebra and Lebesgue measure $\nu$. Consider the statistic $T : \mathcal{X} \to \mathbb{R}^m \times \mathbb{R}^{m(m+1)/2}$ given by

$$T(x) = (x_1, \ldots, x_m, -x_1^2/2, \ldots, -x_m^2/2, -x_1 x_2, \ldots, -x_{m-1} x_m)^t.$$
The polynomial functions that form the components of \( T(x) \) are linearly independent and thus the support of \( \nu^T \) has the full affine dimension \( m + m(m + 1)/2 \). Let \( h(x) = 1 \) for all \( x \in \mathbb{R}^m \).

If \( \eta \in \mathbb{R}^m \times \mathbb{R}^{m(m+1)/2} \), then write \( \eta[m] \in \mathbb{R}^m \) for the vector of the first \( p \) components \( \eta_i, 1 \leq i \leq m \). Similarly, write \( \eta[m \times m] \) for the symmetric \( m \times m \)-matrix formed from the last \( m(m + 1)/2 \) components \( \eta_{ij}, 1 \leq i \leq j \leq m \). The function \( x \mapsto e^{\eta^T T(x)} \) is \( \nu \)-integrable if and only if \( \eta[m \times m] \) is positive definite. Hence, the natural parameter space \( N \) is equal to the Cartesian product of \( \mathbb{R}^m \) and the cone of positive definite \( m \times m \)-matrices. If \( \eta \) is in the open set \( N \), then

\[
\phi(\eta) = -\frac{1}{2} \left( \log \det(\eta[m \times m]) - \eta[m] \eta[m \times m] \eta[m] - m \log(2\pi) \right).
\]

The Lebesgue densities \( p_\eta \) can be written as

\[
(6.1.1) \quad p_\eta(x) = \frac{1}{\sqrt{(2\pi)^m \det(\eta[m \times m]^{-1})}} \times \\
\exp \left\{ \eta[m] x - \text{tr}(\eta[m \times m] xx^t)/2 - \eta[m] \eta[m \times m] \eta[m]/2 \right\}.
\]

Here we again use the trace trick, since \( xx^t \eta[m \times m] x = \text{tr}(\eta[m \times m] xx^t)/2 \) allows us to express the quadratic form in \( x \) has a dot product between \( \eta[m \times m] \) and the vector of sufficient statistics. Setting \( \Sigma = \eta[m \times m]^{-1} \) and \( \mu = \eta[m \times m] \eta[m] \), we find that

\[
p_\eta(x) = \frac{1}{\sqrt{(2\pi)^m \det(\Sigma)}} \exp \left\{ -\frac{1}{2} (x - \mu)^t \Sigma^{-1}(x - \mu) \right\}
\]

is the density of the multivariate normal distribution \( \mathcal{N}_m(\mu, \Sigma) \). Hence, the family of all multivariate normal distributions on \( \mathbb{R}^m \) with positive definite covariance matrix is a regular exponential family of order \( m + \binom{m}{2} \). □

In some circumstances it is useful to consider the closure of an exponential family in a suitable representation. This occurs most commonly in the case of discrete exponential families, where we saw that the representation of the multinomial model gives the interior of the probability simplex. Taking the closure yields the entire probability simplex. The set of all distributions which lie in the closure of a regular exponential family is called an extended exponential family. The extended exponential family might involve probability distributions that do not possess densities. For example, in the Gaussian case the closure operation yields covariance matrices that are positive semidefinite, but singular. These yield probability distributions that are supported on lower dimensional linear spaces, and hence do not have densities.
6.2. Discrete Regular Exponential Families

Our goal in this chapter is to describe statistical models which naturally can be interpreted as submodels of exponential families through their natural parameter spaces or transformed versions of those parameter spaces. Before moving to the general setup of algebraic exponential families in Section 6.5, we focus here on the special case where the submodel is itself a regular exponential family. Such a submodel is realized as a linear subspace of the natural parameter space. In the case of discrete random variables, this leads to the study of toric varieties. In the case of Gaussian random variables, this yields inverse linear spaces.

In this section we explore regular exponential families for discrete random variables with a finite number of states, and how they are related to objects in algebra. Since \( \mathcal{X} \) is assumed to be discrete with state space \( \mathcal{X} = \{r\} \), there are a number of simplifications that can be made to the representation of the regular exponential family from the presentation in the previous section. First of all, the statistic \( T(x) \) gives a measurable map from \( \{r\} \) to \( \mathbb{R}^k \). This amounts to associating a vector \( T(x) =: a_x \) to each \( x \in \{r\} \). Similarly, the measurable function \( h : \{r\} \to \mathbb{R}_{>0} \) merely associates a nonnegative real number to each \( x \in \{r\} \). Any nonnegative function is measurable in this setting. The Laplace transform \( \int_{\mathcal{X}} h(x) e^{\eta^T T(x)} d\nu \) is the sum

\[
Z(\eta) = \sum_{x \in \{r\}} h(x) e^{\eta^T T(x)}.
\]

Now we look at the individual elements of the product. Let us call the vector \( T(x) = a_x \), written explicitly as \( a_x = (a_{1x}, \ldots, a_{kx})^t \). Similarly, the vector \( \eta = (\eta_1, \ldots, \eta_k)^t \). We define \( \theta_i = \exp(\eta_i) \). For a notational simplicity, we denote \( h(x) = h_x \) so that \( h = (h_1, \ldots, h_r) \) is a vector in \( \mathbb{R}_{>0}^k \). This means that

\[
p_{\eta}(x) = h(x) e^{\eta^T T(x)} - \phi(\eta)
\]

could also be rewritten as

\[
p_{\theta}(x) = \frac{1}{Z(\theta)} h_x \prod_j \theta_j^{a_{jx}},
\]

where

\[
Z(\theta) = \sum_{x \in \{r\}} h_x \prod_j \theta_j^{a_{jx}}.
\]

In particular, if the \( a_{jx} \) are integers for all \( j \) and \( x \), then the discrete exponential family is a parametrized family of probability distribution, where the parametrizing functions are rational functions.
A third and equivalent representation of the model in this discrete setting arises by asking to determine whether a given probability distribution \( p \in \text{int}(\Delta_{r-1}) \) belongs to the discrete exponential family associated to \( A = (a_{ij})_{j \in [k], x \in [r]} \in \mathbb{Z}^{k \times r} \) and \( h \in \mathbb{R}^r_>0 \). Indeed, taking the logarithm of the exponential family representation, in which case we arrive at
\[
\log p_\eta(x) = \log h(x) + \eta^T(x) - \phi(\eta)
\]
or equivalently
\[
\log p_\theta(x) = \log(h(x)) + \log(\theta)^\top A - \log Z(\theta).
\]
If we make the assumption, which we will do throughout, that the matrix \( A \) contains the vector \( 1 = (1, 1, \ldots, 1) \) in its rowspan, then this is equivalent to requiring that \( \log p \) belong to the affine space \( \log(h) + \text{rowspan}(A) \). For this reason, discrete exponential families are also called log-affine models.

**Definition 6.2.1.** Let \( A \in \mathbb{Z}^{k \times r} \) be a matrix of integers such that \( 1 \in \text{rowspan}(A) \) and let \( h \in \mathbb{R}^r_>0 \). The log-affine model associated to these data is the set of probability distribution
\[
\mathcal{M}_{A,h} := \{ p \in \text{int}(\Delta_{r-1}) : \log p \in \log(h) + \text{rowspan}(A) \}.
\]
If \( h = 1 \) then \( \mathcal{M}_A = \mathcal{M}_{A,1} \) is called a log-linear model.

In addition to the names exponential families and log-linear models, this class of model is also known in the algebraic statistics community as a toric model. This comes from their relation to toric varieties, as we now explain.

**Definition 6.2.2.** Let \( h \in \mathbb{R}^r_>0 \) be a vector of nonnegative numbers and \( A = (a_{ij}) \in \mathbb{Z}^{k \times r} \) a \( k \times r \) matrix of integers and suppose that \( 1 \in \text{rowspan}(A) \). The monomial map associated to this data is the rational map
\[
\phi^{A,h} : \mathbb{R}^k \to \mathbb{R}^r, \quad \phi^{A,h}_j(\theta) = h_j \prod_i \theta_i^{a_{ij}}.
\]
Note that in the definition of the rational map \( \phi^{A,h} \) we have removed the normalizing constant \( Z(\theta) \) from this representation. This has the effect of homogenizing the parametrization so that we can compute the homogeneous vanishing ideal of the model.

**Definition 6.2.3.** Let \( h \in \mathbb{R}^r_>0 \) be a vector of nonnegative numbers and \( A = (a_{ij}) \in \mathbb{Z}^{k \times r} \) a \( k \times r \) matrix. The ideal
\[
I_{A,h} := I(\phi^{A,h}(\mathbb{R}^k)) \subseteq \mathbb{R}[p]
\]
is called the toric ideal associated to the pair \( A \) and \( h \). In the special case that \( h = 1 \) we denote this as \( I_A := I_{A,1} \).
Note that generators for the toric ideal $I_{A,h}$ are easily obtained from generators of the toric ideal $I_A$, by globally making the substitution $p_j \rightarrow p_j / h_j$. Hence, it is sufficient to focus on the case of the toric ideal $I_A$. These ideals turn out to be binomial ideals.

**Proposition 6.2.4.** Let $A \in \mathbb{Z}^{k \times r}$ be a $k \times r$ matrix of integers. Then the toric ideal $I_A$ is a binomial ideal and

$$I_A = \langle p^u - p^v : u, v \in \mathbb{N}^r \text{ and } Au = Av \rangle.$$

If $1 \in \text{rowspan}(A)$ then $I_A$ is homogeneous.

**Proof.** First of all, it is clear that any binomial $p^u - p^v$ such that $Au = Av$ is in the toric ideal $I_A$. To show that $I_A$ is generated by all these binomials, we will show something stronger: in fact, these binomials span the ideal $I_A$ as a vector space. Indeed, let $f(p) \in I_A$ and $c_w p^w$ any monomial appearing in $f$ with nonzero coefficient. For any choice of $\theta$, we must have $f(\phi^A(\theta)) = 0$. This means, that $f(\phi^A(\theta)) = 0$ as a polynomial in $\theta$. Plugging in $\phi^A(\theta)$ into the monomial $c_w p^w$ yields $c_w \theta^{Au}$. For this to cancel, there must be some other monomial $c_v p^v$ such that plugging in $\phi^A(\theta)$ yields the same monomial (with possibly different coefficient) $c_v \theta^{Au}$, so $Au = Av$. Forming the new polynomial $f - c_w(p^u - p^v)$ yields a polynomial with fewer terms. The result is then achieved by induction on the number of terms.

To see that $I_A$ is homogeneous, note that $1 \in \text{rowspan}(A)$ forces that $Au = Av$ implies that $1u = 1v$. Thus all of the generating binomials $p^u - p^v \in I_A$ are homogeneous. \qed

Note that the toric ideals are also lattice ideals, as introduced in Chapter 4. Indeed, $I_A = I_L$ where $L$ is the lattice $L = \ker \mathbb{Z} A$. Note further that if $h = 1$, then the ideal generators can always be chosen to be binomials whose coefficients are $\pm 1$, so the coefficient field of the ring does not matter.

**Example 6.2.5.** Let $A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}$. The toric ideal $I_A$ is the vanishing ideal of the parametrization

$$p_1 = \theta_2^3, \quad p_2 = \theta_1 \theta_2^2, \quad p_3 = \theta_1^2 \theta_2, \quad p_4 = \theta_1^3.$$

The toric ideal is generated by three quadratic binomials

$$I_A = \langle p_1 p_3 - p_2^2, p_1 p_4 - p_2 p_3, p_2 p_4 - p_3^2 \rangle.$$ 

For example, the first binomial $p_1 p_3 - p_2^2$ is $p^u - p^v$ where $u = (1, 0, 1, 0)^T$ and $v = (0, 2, 0, 0)^T$. One checks that $Au = Av$ in this case. The sufficient statistics of this model, obtained from the vector of counts $u$, is the vector $Au$.

Note that if we take $h = (1, 3, 3, 1)$, then $I_{A,h}$ gives the vanishing ideal of the model of a binomial random variable with three trials.
Example 6.2.6. Any time we have a variety parametrized by a monomial functions of parameters the vanishing ideal is a toric ideal. For example, consider the parametrization

\[ p_{ij} = \alpha_i \beta_j \]

where \( i \in [r_1], j \in [r_2] \) and \( \alpha_i \) and \( \beta_j \) are independent parameters. This is, of course, the (homogeneous) parametrization of two discrete independent random variables. The matrix \( A \) representing the toric ideal is a \((r_1 + r_2) \times (r_1 r_2)\) matrix, with one row for each parameter and one column for each state of the pair of random variables. The \( ij\)-th column of \( A \), yielding the exponent vector for \( p_{ij} = \alpha_j \beta_j \) is the vector \( e_i \oplus e'_j \), where \( e_i \) denotes the \( i\)th standard unit vector in \( \mathbb{R}^{r_1} \) and \( e'_j \) denotes the \( j\)th standard unit vector in \( \mathbb{R}^{r_2} \). For example, for \( r_1 = 3 \) and \( r_2 = 4 \), we get the matrix

\[
\begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}
\]

Note that the matrix \( A \) acts as a linear operator that computes the row and column sums of the \( r_1 \times r_2 \) array \( u \). The toric ideal \( I_A \) is generated by all binomials \( p^u - p^v \) such that \( u, v \) have the same sufficient statistics under the model. This means that the arrays \( u \) and \( v \) have the same row and column sums. Note that \( I_A = I_{1 \perp 2} \), so we already know that \( I_A \) is generated by the \( 2 \times 2 \) minors of a generic matrix

\[ I_A = \langle p_{ij_1} p_{i_2 j_2} - p_{i_1 j_2} p_{i_2 j_1} : i_1, i_2 \in [r_1], j_1, j_2 \in [r_2] \rangle. \]

Example 6.2.7. Let \( A \) be the \( 6 \times 8 \) matrix

\[
A = \begin{pmatrix}
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}
\]

The following Singular code computes a Gröbner basis for the toric ideal \( I_A \).

```singular
ing ring r = 0, (p1,p2,p3,p4,p5,p6,p7,p8),dp;
ing intmat A[6][8] = 1,1,1,1,0,0,0,0, \\
0,0,0,0,1,1,1,1, \\
1,1,0,0,1,1,0,0, \\
0,0,1,1,0,0,1,1, \\
0,1,1,0,0,1,1, \\
1,1,0,0,1,1,0,0, \\
0,0,1,1,0,0,1,1, \\
```
6.3. Gaussian Regular Exponential Families

The ideal $I_A$ has nine homogeneous quadratic generators,

$$\langle p_6p_7 - p_5p_8, \ldots, p_2p_3 - p_1p_4 \rangle.$$

Renaming the variables, $p_{111}, \ldots, p_{222}$, we see that the ideal $I_A$ is equal to the conditional independence ideal $I_C$ of complete independence of three binary random variables, that is, with

$$C = \{1 \Join \{2, 3\}, 2 \Join \{1, 3\}, 3 \Join \{1, 2\}\}.$$

\[ \square \]

6.3. Gaussian Regular Exponential Families

Here we describe the regular exponential families that arise as subfamilies of the regular multivariate Gaussian statistical models. Here we should choose a statistic $T(x)$ that maps $x \in \mathbb{R}^m$ to a vector of degree 2 polynomials in $x$ with no constant term. Equivalently, such a model is obtained by taking a linear subspace of the natural parameter space of the model.

In principle, we could consider any set of the form $L \cap (\mathbb{R}^m \times PD_m)$ where $L$ is a linear space in the natural parameter space of pairs $(\Sigma^{-1}\mu, \Sigma^{-1})$ of transformed mean vectors and concentration matrices. The most commonly occurring case in applications is where the linear space $L$ is actually a direct product $L = L_1 \times L_2$ with $L_1 \subseteq \mathbb{R}^m$ and $L_2 \subseteq \mathbb{R}^{(m+1)m/2}$. Often $L_1$ is either $\{0\}$ or $\mathbb{R}^m$. For the purposes of investigating the vanishing ideal of such a model, this assumption means that the vanishing ideal breaks into the ideal sum of two pieces, a part corresponding to $L_1$ and a part corresponding to $L_2$.

When we want to consider the vanishing ideal of such a model we consider it in the ring

$$\mathbb{R}[\mu, \sigma] := \mathbb{R}[\mu_i, \sigma_{ij}, i \leq j, i, j \in [m]].$$
6. Exponential Families

We will restrict to the case that either $L_1 = 0$ or $L_1 = \mathbb{R}^m$. In the first case, the vanishing ideal of such an gaussian exponential family has the form

$$\langle \mu_1, \ldots, \mu_m \rangle + I_2$$

where $I_2$ is an ideal in $\mathbb{R}[\sigma]$. In the second case, the vanishing ideal is generated by polynomials in $\mathbb{R}[\sigma]$. In either case, we can focus on the vanishing ideal of associated to the linear space $L_2$.

Note that the model of a regular exponential subfamily is a linear space in the inverse of the covariance matrix. This leads to the following definition.

**Definition 6.3.1.** Let $L \subseteq \mathbb{R}^{(m+1)m/2}$ be a linear space such that $L \cap PD_m$ is nonempty. The *inverse linear space* $L^{-1}$ is the set of positive definite matrices

$$L^{-1} = \{ K^{-1} : K \in L \cap PD_m \}.$$

Note that the map $L \to L^{-1}$ that takes a matrix and returns its inverse is a rational map (using the adjoint formula for the inverse of a matrix). This means that exponential families in the Gaussian case have interesting ideals in $\mathbb{R}[\sigma]$.

An important example, that we will see again later, concerns the case where $L$ is a coordinate subspace (with no zero entries on the diagonal to ensure the existence of positive definite matrices).

**Proposition 6.3.2.** If $K$ is a concentration matrix for a Gaussian random variable, a zero entry $k_{ij} = 0$ is equivalent to a conditional independence statement $i \perp \perp j | \{i,j\}$.

**Proof.** Let $C = [m] \setminus \{i,j\}$. From the adjoint formula for the inverse of a matrix, we see that $k_{ij} = (-1)^{i+j} \det \Sigma_{j\cup C, i\cup C} / \det \Sigma$. So $k_{ij} = 0$ if and only if $\det \Sigma_{j\cup C, i\cup C} = 0$. This is equivalent to the conditional independence statement $i \perp \perp j | [m] \setminus \{i,j\}$ by Proposition 4.1.9. \qed

Hence, a linear space obtained by setting many of the concentration parameters equal to zero gives a more complicated conditional independence model, where every conditional independence statement is a saturated conditional independence statement (every random variable is involved). Such conditional independence ideals might not be prime in general. However, the linear space $L$ in the concentration coordinates is clearly irreducible, and this can allow us to parametrize the main component of interest.

**Example 6.3.3.** Consider the Gaussian regular exponential family for $m = 3$ random variables described by the linear space of concentration matrices

$$L = \{ K \in PD_3 : k_{12} = 0, k_{13} = 0 \}.$$
This corresponds to the conditional independence statements $1 \perp 2 | \{3\}$ and $1 \perp 3 | 2$. The intersection axiom implies that $1 \perp \{2, 3\}$ in this case, though this is not immediately clear from the gaussian conditional independence ideal

$$J_C = \langle \sigma_{12}\sigma_{33} - \sigma_{13}\sigma_{23}, \sigma_{13}\sigma_{22} - \sigma_{12}\sigma_{23} \rangle.$$

which does not contain any linear polynomials. One could use a computer algebra system to compute the primary decomposition. Alternately, we can use the parametrization of the model to compute this decomposition. Here is an example of the parametrization computation in Macaulay2.

```plaintext
R = QQ[k11,k22,k23,k33,s11,s12,s13,s22,s23,s33,
         MonomialOrder => Eliminate 4];
K = matrix{{k11,0,0},{0,k22, k23},{0,k23,k33}};
S = matrix{{s11,s12,s13},{s12,s22,s23},{s13,s23,s33}};
Eye = matrix{{1,0,0},{0,1,0},{0,0,1}};
I = ideal( flatten(K*S -Eye));
J = ideal selectInSubring(1, gens gb I)

In this case, the resulting ideal $J$ is generated by the polynomials $\sigma_{12}$ and $\sigma_{13}$ realizing the conditional independence statement $1 \perp \{2, 3\}$. □
```

We will return to examples such as this when we discuss Graphical Models in Chapter 13. More complex examples need not have the property that the vanishing ideal of the inverse linear space is generated by determinantal constraints associated with conditional independence statements.

6.4. Real Algebraic Geometry

Our eventual goal in this chapter is to introduce algebraic exponential families. To do this requires the language of real algebraic geometry. The difference between algebraic geometry over the reals versus the algebraic geometry over algebraically closed fields (which has primarily been discussed thus far), is that the real numbers are ordered and this allows for inequalities. These inequalities are an important part of the study, even if one is only interested in zero sets of polynomials and maps between zero sets. Over the complex numbers, the topological closure of the image of a rational variety under a rational map is a rational variety. But over the reals, the topological closure of the image of a real variety under a rational map need not be a real algebraic variety. For instance the projection of the real variety $V(F)(p_1^2 + p_2^2 - 1)$ to the $p_1$ axis is the interval $[-1, 1]$ which is not a real variety. Hence, the theory of real algebraic geometry requires more complicated objects than merely varieties, which are the semialgebraic sets.
Definition 6.4.1. Let $\mathcal{F}, \mathcal{G} \subseteq \mathbb{R}[p]$ be finite sets of polynomials. The basic semialgebraic set defined by $\mathcal{F}$ and $\mathcal{G}$ is the set

$$\{a \in \mathbb{R}^k : f(a) = 0 \text{ for all } f \in \mathcal{F} \text{ and } g(a) > 0 \text{ for all } g \in \mathcal{G}\}.$$ 

A semialgebraic set is any set that can be written as a finite union of basic semialgebraic sets. In the case where $\mathcal{G} = \emptyset$ the resulting basic semialgebraic set is called a real algebraic variety.

Example 6.4.2. The interior of the probability simplex is a basic semialgebraic set with $\mathcal{F} = \{p_i - 1 \mid i \in [r]\}$ and $\mathcal{G} = \{p_i \mid i \in [r]\}$. The probability simplex $\Delta_{r-1}$ is a semialgebraic set, obtained as the union of $2^r - 1$ basic semialgebraic sets which are the relative interiors of the faces of $\Delta_{r-1}$.

In general, $\mathcal{F}$ and $\mathcal{G}$ are finite sets of polynomials, a set of the form

$$\{a \in \mathbb{R}^k : f(a) = 0 \text{ for all } f \in \mathcal{F} \text{ and } g(a) \geq 0 \text{ for all } g \in \mathcal{G}\}$$

will be a semialgebraic set that is not basic. An important example of this type of semialgebraic set is a polyhedron, in which both sets $\mathcal{F}$ and $\mathcal{G}$ consist of linear polynomials. Note that if we are interested only in closed semialgebraic sets, it is not sufficient to only consider semialgebraic sets of this type, as the following example illustrates.

Example 6.4.3. Let $\Theta = D \cup R$ be the union of the disk $D = \{p \in \mathbb{R}^2 : p_1^2 + p_2^2 \leq 1\}$ and the rectangle $R = \{p \in \mathbb{R}^2 : 0 \leq p_1 \leq 1, -1 \leq p_2 \leq 1\}$. This semialgebraic set cannot be written as a set of the form $\{p \in \mathbb{R}^2 : f \geq 0 \text{ for all } f \in \mathcal{F}\}$ for a finite set of polynomials $\mathcal{F}$. Indeed, since a half of the circle $p_1^2 + p_2^2 = 1$ forms part of the boundary of $\Theta$, the polynomial $f = 1 - p_1^2 - p_2^2$ would need to appear in the set $\mathcal{F}$. But not every point in $\Theta$ satisfies $f \geq 0$. □

Most of the models in algebraic statistics arise from taking a parameter space $\Theta$ which is a polyhedron and the model will be the image of $\Theta$ under a rational map. As we will see, such sets are always semialgebraic sets.

Theorem 6.4.4 (Tarski-Seidenberg). Let $\Theta \subseteq \mathbb{R}^{k+1}$ be a semialgebraic set, and let $\pi : \mathbb{R}^{k+1} \to \mathbb{R}^k$ be a coordinate projection. Then $\pi(\Theta) \subseteq \mathbb{R}^k$ is also a semialgebraic set.

The Tarski-Seidenberg theorem is the basis of useful results in real algebraic geometry. In particular, by constructing the graph of a rational map and repeatedly applying the Tarski-Seidenberg theorem, we deduce:

Theorem 6.4.5. Let $\phi : \mathbb{R}^{k_1} \to \mathbb{R}^{k_2}$ be a rational map and $\Theta \subseteq \mathbb{R}^{k_1}$ be a semialgebraic set. Then the image of $\Theta$ under $\phi$

$$\phi(\Theta) := \{\phi(\theta) : \theta \in \Theta \text{ and } \phi(\theta) \text{ is defined}\}$$

is a semialgebraic subset of $\mathbb{R}^{k_2}$. 

Proof. Let $\Gamma_\phi := \{ (\theta, \phi(\theta)) : \theta \in \Theta \}$ be the graph of $\phi$. Since $\phi$ is given by rational functions $\phi_i = f_i/g_i$ this is a semialgebraic set (which comes from taking the semialgebraic set representation of $\Theta$ and adding the constraints that $y_i g_i(\theta) - f_i(\theta) = 0$, and then intersecting with the semialgebraic set $\prod g_i(\theta) \neq 0$). The image $\phi(\Theta)$ is the coordinate projection of the graph $\Gamma_\phi$. □

When we move on to likelihood inference for algebraic exponential families, we will see one nice property of semialgebraic sets is that they have well-defined tangent cones at points, which have the same dimension as the semialgebraic set at that point.

Definition 6.4.6. The tangent cone $TC_{\theta_0}(\Theta)$ of the semialgebraic set $\Theta \subseteq \mathbb{R}^k$ at the point $\theta_0 \in \Theta$ is the set of limits of sequences $\alpha \cdot (\theta_n - \theta_0)$ where $\alpha$ are positive reals and $\theta_n \in \Theta$ converge to $\theta_0$. The elements of the tangent cone are called tangent vectors. We say $\theta_0$ is a smooth point of $\Theta$ if $TC_{\theta_0}(\Theta)$ is a linear space.

The tangent cone is a closed set, and it is indeed a cone, that is multiplying a tangent vector by an arbitrary nonnegative real number yields another tangent vector. Decomposing a semialgebraic set into simpler semialgebraic sets can be useful for determining the tangent cone at a point. For instance, if $\Theta = \Theta_1 \cup \Theta_2$ and $\theta_0 = \Theta_1 \cap \Theta_2$ then $TC_{\theta_0}(\Theta) = TC_{\theta_0}(\Theta_1) \cup TC_{\theta_0}(\Theta_2)$. If, on the other hand, $\theta \in \Theta_1 \setminus \Theta_2$ then $TC_{\theta_0}(\Theta) = TC_{\theta_0}(\Theta_1)$.

Over other fields and working solely with varieties, it is natural to give a definition of the tangent cone based purely on algebraic considerations. Here is a standard definition over algebraically closed fields. To make this precise, let $f$ be a polynomial and expand this as a sum of homogeneous pieces $f = f_i + f_{i+1} + \cdots$ where $f_i$ is the smallest degree piece that appears in this polynomial. Let $\min(f) = f_i$, the homogeneous piece of lowest order.

Definition 6.4.7. Let $\mathbb{K}$ be an algebraically closed field, and $I \subseteq \mathbb{K}[p]$ an ideal. Suppose that the origin is in the affine variety $V(I)$. Then the algebraic tangent cone is defined to be $TC_0(V(I)) = V(\min(I))$ where $\min(I) := \langle \min(f) : f \in I \rangle$.

The definition of the tangent cone given also makes sense for a variety defined over the complex numbers. Over the complex numbers, the tangent cone at a point can be computed directly using Gröbner bases. The idea is a generalization of the following observation: let $f \in I(\Theta)$ and $\theta_0 \in \Theta$. Expand $f$ as a power series around the point $\theta_0$. Then the lowest order term of $f$ in this expansion vanishes on the tangent cone $TC_{\theta_0}(\Theta)$. 

Example 6.4.8. Consider the polynomial \( f = p_2^2 - p_1^3(p_1 + 1) \). The variety \( V(f) \) is the nodal cubic. The polynomial \( \min(f) = p_2^2 - p_1^3 \), from which we see that the tangent cone at the origin of \( V(f) \) is the union of two lines.

To compute the ideal \( \min(I) \) and hence, the tangent cone, requires the use of Gröbner bases.

**Proposition 6.4.9.** Let \( I \subseteq \mathbb{K}[p] \) an ideal. Let \( I^h \subseteq \mathbb{K}[p_0, p] \) be the homogenization of \( I \) with respect to the linear polynomial \( p_0 \). Let \( \prec \) be an elimination order that eliminates \( p_0 \), and let \( \mathcal{G} \) be a Gröbner basis for \( I^h \) with respect to \( \prec \). Then
\[
\min(I) = \langle \min(g(1,p)) : g \in \mathcal{G} \rangle.
\]

To compute the tangent cone at a general point \( \theta \), use Proposition 6.4.9 after first shifting the desired point of interest to the origin.

Example 6.4.10. Consider the monomial parametrization \( \phi^A \) given by the matrix
\[
A = \begin{pmatrix}
1 & 1 & 1 \\
0 & 2 & 3 \\
1 & 1 & 1
\end{pmatrix}.
\]
The point \((1,0,0,0)\) is on the variety \( V_A \) and is a singular point. The following Macaulay2 code computes the tangent cone at this point.

```plaintext
S = QQ[t1,t2];
R = QQ[p1,p2,p3,p4];
f = map(S,R,{t1, t1*t2^2, t1*t2^3,t1*t2^4});
g = map(R,R,{p1+1, p2,p3,p4});
h = map(R,R,{p1-1, p2,p3,p4});
I = kernel f
Ishift = g(I)
T = tangentCone Ishift
Itangentcone = h(T)
```
The maps \( g \) and \( h \) were involved in shifting \((1,0,0,0)\) to the origin. The resulting ideal is \( \langle p_1^2, p_4 \rangle \). So the tangent cone is a two-dimensional plane but with multiplicity 2.

Note that the algebraic tangent cone computation over the complex numbers only provides some information about the real tangent cone. Indeed, if \( \Theta \subseteq \mathbb{R}^k \) is a semialgebraic set, \( I(\Theta) \) its vanishing ideal, and \( 0 \in \Theta \), then the real algebraic variety \( V(\min(I(\Theta))) \) contains the tangent cone \( TC_0(\Theta) \) but need not be equal to it in general.

Example 6.4.11. Let \( f = p_2^2 - p_1^3 \), and \( V(f) \) be the cuspidal cubic in the plane. Then \( \min(f) = p_2^2 \) and hence the complex tangent cone is the \( p_1 \)-axis. On the other hand, every point in \( V(\Re(f)) \) satisfies, \( p_1 \geq 0 \), and hence the real
6.5. Algebraic Exponential Families

tangent cone satisfies this restriction as well. Thus, the tangent cone of the
cuspidal cubic at the origin is the nonnegative part of the $p_1$-axis.

Generalizing Example 6.4.11, we can gain information about the tangent
cone of semialgebraic sets at more general points, by looking at the polynomials
that are nonnegative at the given points.

**Proposition 6.4.12.** Let $\Theta$ be a semialgebraic set, suppose $0 \in \Theta$ and
let $f \in \mathbb{R}[p]$ be a polynomial such that $f(\theta) \geq 0$ for all $\theta \in \Theta$. Then
$\min(f)(\theta) \geq 0$ for all $\theta \in TC_0(\Theta)$.

6.5. Algebraic Exponential Families

Now that we have the basic notions of real algebraic geometry in place, we
can discuss algebraic exponential families.

**Definition 6.5.1.** Let $(P_\eta : \eta \in N)$ be a regular exponential family of order
$k$. The subfamily induced by the set $M \subseteq N$ is an algebraic exponential
family if there exists an open set $\bar{\mathcal{N}} \subseteq \mathbb{R}^k$, a diffeomorphism $g : N \to \bar{\mathcal{N}}$,
and a semi-algebraic set $A \subseteq \mathbb{R}^k$ such that $M = g^{-1}(A \cap \bar{\mathcal{N}})$.

The notion of an algebraic exponential family is quite broad and covers
nearly all of the statistical models we will consider in this book. The two
most common examples we will encounter concern the discrete and multi-
variate Gaussian random variables.

**Example 6.5.2 (Discrete Random Variables).** Let $\bar{\mathcal{N}} = \text{int}(\Delta_{k-1})$ and
consider the diffeomorphism

$$\eta \mapsto (\exp(\eta_1), \ldots, \exp(\eta_k))/\sum_{i=1}^{k} \exp(\eta_i)$$

where $\eta_k = 1 - \eta_1 - \cdots - \eta_{k-1}$. This shows that every semialgebraic subset of
the interior of the probability simplex is an algebraic exponential family. $\Box$

The example of the discrete random variable shows that we cannot take
only rational functions $g$ in the definition, we might need a more complicated
diffeomorphism when introducing an algebraic exponential family. Note that
it can be useful and worthwhile to also take the closure of the set $\bar{\mathcal{N}}$ and the
model $M \subseteq \bar{\mathcal{N}}$. The reason for considering open sets here is for applications
to likelihood ratio tests in Chapter 7 but it is not needed in many other
settings.

**Example 6.5.3 (Gaussian Random Variables).** Let $\mathcal{N} = \mathbb{R}^m \times PD_m$
the cone of positive definite matrices, and consider the diffeomorphism

$$\mathbb{R}^m \times PD_m \to \mathbb{R}^m \times PD_m, (\eta, K) \mapsto (K^{-1}\eta, K^{-1})$$.
This shows that any semialgebraic subset of $\mathbb{R}^m \times PD_m$ of mean and covariance matrices yields an algebraic exponential family. Note that since the map $K \mapsto K^{-1}$ is a rational map, we could have semialgebraic subsets of mean and concentration matrices: the Tarski-Seidenberg theorem guarantees that semialgebraic sets in one regime are also semialgebraic in the other.

The need for considering semialgebraic sets as statistical models is clear as soon as we begin studying hidden variable models, a theme that will recur throughout the text. An important example is the case of mixture models, which we will address in more detail later on. For example, the mixture of binomial random variables, Example 3.2.10, yields the semialgebraic set in $\Delta_2$ consisting of all distributions satisfying the polynomial constraint $4p_0p_2 - p_1^2 \geq 0$.

**Example 6.5.4 (Factor Analysis).** The factor analysis model $F_{m,s}$ is the family of multivariate normal distributions $N_m(\mu, \Sigma)$ on $\mathbb{R}^m$ whose mean vector $\mu$ is an arbitrary vector in $\mathbb{R}^m$ and whose covariance matrix lies in the set

$$F_{m,s} = \{ \Omega + \Lambda \Lambda^T \in PD_m : \Omega > 0 \text{ diagonal}, \Lambda \in \mathbb{R}^{m \times s} \}.$$ 

Here the notation $A > 0$ means that $A$ is a positive definite. Note that $F_{m,s}$ is a semialgebraic set since it is the image of the semialgebraic set $\mathbb{R}_{>0}^m \times \mathbb{R}^{m \times s}$ under a rational map. Hence, the factor analysis model is an algebraic statistical model. It is not, in general, of the form $PD_m \cap V(I)$ for any ideal $I$. In particular, the semialgebraic structure really matters for this model.

As an example, consider the case of $m = 3, s = 1$, a 1-factor model with three covariates. In this case, the model consists of all $3 \times 3$ covariance matrices of the form

$$\Sigma = \Omega + \Lambda \Lambda^T = \begin{pmatrix} \omega_{11} + \lambda_1^2 & \lambda_1 \lambda_2 & \lambda_1 \lambda_3 \\ \lambda_1 \lambda_2 & \omega_{22} + \lambda_2^2 & \lambda_2 \lambda_3 \\ \lambda_1 \lambda_3 & \lambda_2 \lambda_3 & \omega_{33} + \lambda_3^2 \end{pmatrix},$$

where $\omega_{11}, \omega_{22}, \omega_{33} > 0$ and $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{R}$.

Since this model has six parameters and is inside of six dimensional space, we suspect, and a computation verifies, that there are no polynomials that vanish on the model. That is, $I(F_{3,1}) = \langle 0 \rangle$. On the other hand, not every $\Sigma \in PD_3$ belongs to $F_{3,1}$, since, for example, it is easy to see that $\Sigma \in F_{3,1}$ must satisfy $\sigma_{12} \sigma_{13} \sigma_{23} \geq 0$. In addition, it is not possible that exactly one of the entries $\sigma_{12}, \sigma_{13}, \sigma_{23}$ is zero, since such a zero would force one the $\lambda_i$ to be equal to 0, which would introduce further zeros in $\Sigma$. Finally,
if \( \sigma_{jk} \neq 0 \), then we have the formula
\[
\omega_{ii} = \sigma_{ii} - \frac{\sigma_{ij}\sigma_{ik}}{\sigma_{jk}}
\]
which must be positive. Multiplying through by the \( \sigma_{jk}^2 \) we deduce the inequality
\[
\sigma_{jk}(\sigma_{ii}\sigma_{jk} - \sigma_{ij}\sigma_{ik}) \geq 0.
\]
It can be shown that these conditions characterize the covariance matrices in \( F_{3,1} \).

6.6. Exercises

Exercise 6.1. Show that the family of Poisson random variables, that is, the discrete random variable with state space \( X = \mathbb{N} \) and with probability distribution given by
\[
P_\lambda(X = i) = \frac{\lambda^i}{k!} \exp(-\lambda),
\]
is a regular exponential family. What is the natural parameter space?

Exercise 6.2. Consider the vector \( h = (1, 1, 1, 2, 2, 2) \) and the matrix
\[
A = \begin{pmatrix}
2 & 0 & 0 & 1 & 1 & 0 \\
0 & 2 & 0 & 1 & 0 & 1 \\
0 & 0 & 2 & 0 & 1 & 1
\end{pmatrix}.
\]

(1) Compute generators for the toric ideals \( I_A \) and \( I_{A,h} \).

(2) What familiar statistical model is the discrete exponential family \( \mathcal{M}_{A,h} \)?

Exercise 6.3. Consider the monomial parametrization
\[
p_{ijk} = \alpha_{ij}\beta_{ik}\gamma_{jk}
\]
for \( i \in [r_1] \), \( j \in [r_2] \), and \( k \in [r_3] \). Describe the matrix \( A \) associated to this monomial parametrization. How does \( A \) act as a linear transformation on 3-way arrays? Compute the vanishing ideal \( I_A \) for \( r_1 = r_2 = r_3 = 3 \).

Exercise 6.4. Consider the linear space \( L \) of \( 4 \times 4 \) symmetric matrices defined by
\[
L = \{ K \in \mathbb{R}^{10} : k_{11} + k_{12} + k_{13} = k_{23} + k_{34} = 0 \}.
\]
Determine generators of the vanishing ideal \( I(L^{-1}) \subseteq \mathbb{R}[\sigma] \).

Exercise 6.5. The convex hull of a set \( S \subseteq \mathbb{R}^k \) is the smallest convex set that contains \( S \). It denoted \( \text{conv}(S) \) and is equal to
\[
\text{conv}(S) = \{ \sum_{i=0}^{k} \lambda_i s_i : s_i \in S \text{ and } \lambda \in \Delta_k \}.
\]
(1) Show that the convex hull of a semialgebraic set is a semialgebraic set.

(2) Give an example of a real algebraic curve in the plane (that is a set of the form \( C = V(f) \subseteq \mathbb{R}^2 \)) such that the \( \text{conv}(S) \) is not the closure of a basic semialgebraic set.

**Exercise 6.6.** Characterize as completely as possible the semialgebraic set \( F_{m,1} \subseteq PD_m \) of positive definite covariance matrices for the 1-factor models. In particular, give necessary and sufficient conditions on a positive definite matrix \( \Sigma \) which imply that \( \Sigma \in F_{m,1} \).
Likelihood Inference

This chapter is concerned with an in-depth treatment of maximum likelihood estimation from an algebraic perspective. In many situations, the maximum likelihood estimate is one of the critical points of the score equations. If those equations are rational, techniques from computational algebra can be used to find the maximum likelihood estimate, among the real and complex solutions of the score equations. An important observation is that the number of critical points of rational score equations is constant for generic data. This number is called the ML-degree of the model.

Section 7.1 concerns the maximum likelihood degree for discrete and gaussian algebraic exponential families, which always have rational score equations. When parametrized statistical models are not identifiable, direct methods for solving the score equations in the parameters encounter difficulties, with many extraneous and repeated critical points. One strategy to speed up and simplify computations is to work with statistical models in implicit form. In the second half of Section 7.1, we explain how to carry out the algebraic solution of the maximum likelihood equations in implicit form using Lagrange multipliers.

The fact that the ML-degree is greater than one in many models means that there is usually no closed-form expression for the maximum likelihood estimate and that hill climbing algorithms for finding the maximum likelihood estimate can potentially get stuck. In Section 7.2, we illustrate algorithms for computing maximum likelihood estimates in exponential families and other models where the ML-degree can be bigger than 1, but there is still a unique local maximum of the likelihood function. Such models, which usually have concave likelihood functions, appear frequently in practice and specialized algorithms can be used to find their MLEs.
The ML-degree of a statistical model is an invariant of that model. It is natural to ask for a geometric explanation of this invariant. This connection is explained in Section 7.3. In particular, the beautiful classification of models with ML-degree one (that is, models that have rational formulas for their maximum likelihood estimates) is given. This is based on work of Huh [Huh13, Huh14].

Section 7.4 concerns the asymptotic behavior of the likelihood ratio test statistic. At a smooth point, the likelihood ratio test statistic asymptotically approaches a chi-square distribution, which is the basis for p-value calculations in many hypothesis tests. However, many statistical models are not smooth, and the geometry of the singularities informs the way that the asymptotic p-value should be corrected at a singular point.

7.1. Algebraic Solution of the Score Equations

Let $\mathcal{M}_\Theta$ be a parametric statistical model with $\Theta \subset \mathbb{R}^d$ an open full dimensional parameter set. Let $D$ be data and let $\ell(\theta|D)$ be the log-likelihood function.

Definition 7.1.1. The score equations of the model $\mathcal{M}_\Theta$ are the equations obtained by setting the gradient of the log-likelihood function to zero:

$$\frac{\partial}{\partial \theta_i} \ell(\theta|D) = 0, \quad i = 1, \ldots, d.$$ 

The point of this chapter is to understand the algebraic structure of this system of equations, one of whose solutions is the maximum likelihood estimate of the parameters given the data $D$. Note that because we take an open parameter space, the maximum likelihood estimate might not exist (e.g. if there is a sequence of model points approaching the boundary with increasing log-likelihood value).

First of all, we restrict our attention to algebraic exponential families, with i.i.d. data. In this section we assume that the statistical model is parametrized and we restrict to the discrete and gaussian case, as these are situations where the score equations are always rational, giving a well-defined notion of maximum likelihood degree.

First we consider statistical models in the probability simplex $\Delta_{r-1}$, which are parametrized by a full dimensional subset $\Theta \subseteq \mathbb{R}^d$ and such that the map $p: \Theta \to \Delta_{r-1}$ is a rational map. Under the assumption of i.i.d. data, we collect a sequence of samples $X^{(1)}, \ldots, X^{(n)}$ such that each $X^{(i)} \sim p$ for some unknown distribution $p$. This data is summarized by the vector of counts $u \in \mathbb{N}^r$, given by $u_j = \#\{i : X^{(i)} = j\}$. The log-likelihood function
of the model in this case becomes
\[ \ell(\theta|u) = \sum_{j=1}^{r} u_j \log p_j(\theta) \]
in which case the score equations are the rational equations
\[ \sum_{j=1}^{r} \frac{u_j}{p_j} \frac{\partial p_j}{\partial \theta_i} (\theta) = 0, \quad i = 1, \ldots, d. \]  

**Theorem 7.1.2.** Let \( M_\Theta \subseteq \Delta_{r-1} \) be a statistical model. For generic data, the number of solutions to the score equations (7.1.1) is independent of \( u \).

In algebraic geometry, the term *generic* means that the condition holds except possibly on a proper algebraic subvariety. This requires a word of comment since \( u \in \mathbb{N}^r \), and \( \mathbb{N}^r \) is not an algebraic variety. The score equations make sense for any \( u \in \mathbb{C}^r \). In the statement of Theorem 7.1.2 “generic” refers to a condition that holds off a proper subvariety of \( \mathbb{C}^r \). Since no proper subvariety of \( \mathbb{C}^r \) contains all of \( \mathbb{N}^r \), we have a condition that holds for generic data vectors \( u \).

**Proof.** To get a generic statement, it suffices to work in the coefficient field \( \mathbb{C}(u) := \mathbb{C}(u_1, \ldots, u_r) \). This allows us to multiply and divide by arbitrary polynomials in \( u_1, \ldots, u_r \), and the nongeneric set will be the unions of the zero sets of all of those functions.

Write \( p_j(\theta) = \frac{f_j(\theta)}{g_j(\theta)} \). To this end, consider the ideal
\[ J = \left( \prod_{j=1}^{r} f_j g_j \right) \left( \sum_{j=1}^{r} \frac{u_j}{p_j} \frac{\partial p_j}{\partial \theta_i} (\theta) \right) : \left( \prod_{j=1}^{r} f_j g_j \right)^\infty. \]

Multiplying the score equations through by \( \prod_{j=1}^{r} f_j g_j \) yields a set of polynomial equations. This follows since,
\[ \frac{\partial}{\partial \theta_i} \log \frac{f_j}{g_j} = \frac{1}{f_j} \frac{\partial f_j}{\partial \theta_i} - \frac{1}{g_j} \frac{\partial g_j}{\partial \theta_i} \]
so all the denominators are cleared. However, after clearing denominators, we might have introduced extraneous solutions, which lie where some of the \( f_j \) or \( g_j \) are zero. These are removed by computing the saturation by the product \( \prod_{j=1}^{r} f_j g_j \) (see Definition 7.1.4).

The resulting ideal \( J \in \mathbb{C}(u)[\theta] \) has zero set consisting of all solutions to the score equations, considered as elements of \( \overline{\mathbb{C}(u)^d} \), (where \( \overline{\mathbb{C}(u)} \) denotes the algebraic closure of \( \mathbb{C}(u) \)). This number is equal to the degree of the ideal \( J \), if it is a zero dimensional ideal, and infinity if \( J \) has dimension greater than zero. \( \square \)
Definition 7.1.3. The number of solutions to the score equations \((7.1.1)\) for generic \(u\) is called the maximum likelihood degree (ML-degree) of the parametric discrete statistical model \(p: \Theta \to \Delta_{r-1}\).

In the proof of Theorem \(7.1.2\) the operation of saturation was used to remove extraneous components.

Definition 7.1.4. Let \(I, J \subseteq \mathbb{K}[p_1, \ldots, p_r]\) be ideals. The quotient ideal or colon ideal is the ideal
\[
I : J = \langle g : g \cdot J \subseteq I \rangle.
\]
The saturation of \(I\) with respect to \(J\) is the ideal,
\[
I : J^\infty = \bigcup_{k=1}^\infty I : J^k
\]
Note that if \(J = \langle f \rangle\) is a principal ideal, then we use the shorthand \(I : f = I : \langle f \rangle\) and \(I : f^\infty = I : \langle f \rangle^\infty\). The geometric content of the saturation is that \(V(I : J^\infty) = V(I) \setminus V(J)\), that is, the saturation removes all the components of \(V(I)\) contained in \(V(J)\). When computing solutions to the score equations, we need to remove the extraneous components that arise from clearing denominators.

Example 7.1.5 (Random censoring). We consider families of discrete random variables that arise from randomly censoring exponential random variables. This example describes a special case of a censored continuous time conjunctive Bayesian network; see [BS09] for more details and derivations.

A random variable \(T\) is exponentially distributed with rate parameter \(\lambda > 0\) if it has the (Lebesgue) density function
\[
f(t) = \lambda \exp(-\lambda t) \cdot 1_{\{t \geq 0\}}, \quad t \in \mathbb{R}.
\]
Let \(T_1, T_2, T_s\) be independent exponentially distributed random variables with rate parameters \(\lambda_1, \lambda_2, \lambda_s\), respectively. Suppose that instead of observing the times \(T_1, T_2, T_s\) directly, we can only observe for \(i \in \{1, 2\}\), whether \(T_i\) occurs before or after \(T_s\). In other words, we observe a discrete random variable with the four states \(\emptyset, \{1\}, \{2\}\) and \(\{1, 2\}\), which are the elements \(i \in \{1, 2\}\) such that \(T_i \leq T_s\). This induces a rational map \(g\) from the parameter space \((0, \infty)^3\) into the probability simplex \(\Delta_3\). The coordinates of \(g\) are the functions
\[
\begin{align*}
g_{\emptyset}(\lambda_1, \lambda_2, \lambda_s) &= \frac{\lambda_s}{\lambda_1 + \lambda_2 + \lambda_s} \\
g_{\{1\}}(\lambda_1, \lambda_2, \lambda_s) &= \frac{\lambda_1}{\lambda_1 + \lambda_2 + \lambda_s} \cdot \frac{\lambda_s}{\lambda_2 + \lambda_s} \\
g_{\{2\}}(\lambda_1, \lambda_2, \lambda_s) &= \frac{\lambda_2}{\lambda_1 + \lambda_2 + \lambda_s} \cdot \frac{\lambda_s}{\lambda_1 + \lambda_s}
\end{align*}
\]
7.1. Algebraic Solution of the Score Equations

g_{1,2}(\lambda_1, \lambda_2, \lambda_s) = \frac{\lambda_1}{\lambda_1 + \lambda_s} \cdot \frac{\lambda_2}{\lambda_2 + \lambda_s} \cdot \frac{\lambda_1 + \lambda_2 + 2\lambda_s}{\lambda_1 + \lambda_2 + \lambda_s},

where \( g_\emptyset(\lambda) \) is the probability that \( T_1 > T_s \) and \( T_2 > T_s \), and so on. Given counts \( u_0, u_1, u_2, \) and \( u_{12} \), the log-likelihood function is

\[ \ell(\lambda) = (u_1 + u_{12}) \log \lambda_1 + (u_2 + u_{12}) \log \lambda_2 + (u_0 + u_1 + u_2) \log \lambda_s + u_{12} \log(\lambda_1 + \lambda_2 + 2\lambda_s) - (u_2 + u_{12}) \log(\lambda_1 + \lambda_s) - (u_1 + u_{12}) \log(\lambda_2 + \lambda_s) - (u_0 + u_1 + u_2 + u_{12}) \log(\lambda_1 + \lambda_2 + \lambda_s). \]

Since the parametrization involves rational functions of degree zero, we can set \( \lambda_s = 1 \), and then solve the likelihood equations in \( \lambda_1 \) and \( \lambda_2 \). These likelihood equations are

\[ \frac{u_1 + u_{12}}{\lambda_1} + \frac{u_{12}}{\lambda_1 + \lambda_2 + 2} - \frac{u_2 + u_{12}}{\lambda_1 + 1} - \frac{u_0 + u_1 + u_2 + u_{12}}{\lambda_1 + \lambda_2 + 1} = 0 \]
\[ \frac{u_2 + u_{12}}{\lambda_2} + \frac{u_{12}}{\lambda_1 + \lambda_2 + 2} - \frac{u_1 + u_{12}}{\lambda_2 + 1} - \frac{u_0 + u_1 + u_2 + u_{12}}{\lambda_1 + \lambda_2 + 1} = 0. \]

In this case, clearing denominators always introduces three extraneous solutions \((\lambda_1, \lambda_2) = (-1, -1), (0, -1), (-1, 0)\). The following code for the software Singular exemplifies how to compute all solutions to the equations with the denominators cleared, and how to remove the extraneous solutions via the command sat. The particular counts used for illustration are specified in the third line.

LIB "solve.lib";
ring R = 0,(l1,l2),dp;
int u0 = 3; int u1 = 5; int u2 = 7; int u12 = 11;
ideal I = (u1+u12)*(l1+l2+2)*(l1+1)*(l1+l2+1) +
(u12)*l1*(l1+1)*(l1+l2+1) -
(u2+u12)*l1*(l1+1)*(l1+l2+1) -
(u0+u1+u2+u12)*l1*(l1+1),
ideal J = sat(I,K)[1];
solve(J);

In particular, there are three solutions to the likelihood equations, and the ML-degree of this model is 3. In general, the maximum likelihood estimate of \( \lambda_2 \) is a root of the cubic polynomial

\[ f(\lambda_2) = (u_0 + 2u_1)(u_1 - u_2)\lambda_2^3 \]
This polynomial was computed using a variation of the above code, working over the field \( \mathbb{Q}(u_0, u_1, u_2, u_{12}) \) that can be defined in Singular by
\[
\text{ring } R = (0, u_0, u_1, u_2, u_{12}), (11, 12), dp;
\]
The leading coefficient reveals that the degree of \( f(\lambda_2) \) is three for all non-zero vectors of counts \( u \) away from the hyperplane defined by \( u_1 = u_2 \). □

In addition to the algebraic models for discrete random variables, the score equations are also rational for algebraic exponential families arising as submodels of the parameter space of the general multivariate normal model. Here we have parameter space \( \Theta \subseteq \mathbb{R}^m \times PD_m \) which gives a family of probability densities
\[
P_\Theta = \{ \mathcal{N}(\mu, \Sigma) : (\mu, \Sigma) \in \Theta \}.
\]
Given data, \( X^{(1)}, \ldots, X^{(n)} \), the minimal sufficient statistics for the saturated gaussian model are
\[
\hat{\mu} = \bar{X} = \frac{1}{n} \sum_{i=1}^{n} X^{(i)} \quad \text{and} \quad \hat{\Sigma} = S = \frac{1}{n} \sum_{i=1}^{n} (X^{(i)} - \bar{X})(X^{(i)} - \bar{X})^T.
\]
Since \( \bar{X} \) and \( S \) are minimal sufficient statistics for the saturated model, they are sufficient statistics for any submodel, and we can rewrite the log-likelihood for any gaussian model in terms of these quantities. Indeed, the log-likelihood function becomes:
\[
(7.1.2) \quad \ell(\mu, \Sigma | \bar{X}, S) = -\frac{n}{2} \log \det \Sigma - \frac{n}{2} \text{tr}(S \Sigma^{-1}) - \frac{n}{2} (\bar{X} - \mu)^T \Sigma^{-1} (\bar{X} - \mu).
\]

Two special cases are especially worthy of attention, and where the maximum-likelihood estimation problem reduces to a simpler problem.

**Proposition 7.1.6.** Let \( \Theta = \Theta_1 \times \text{Id}_m \subseteq \mathbb{R}^m \times PD_m \) be the parameter space for a gaussian statistical model. Then the maximum likelihood estimation for \( \Theta \) is equivalent to the least-squares point on \( \Theta_1 \).

**Proof.** Since \( \Sigma = \text{Id}_m \), the first two terms in the likelihood function are fixed, and we must maximize
\[
-\frac{n}{2} (\bar{X} - \mu)^T \text{Id}_m^{-1} (\bar{X} - \mu)
\]
which is equivalent to minimizing \( \| \bar{X} - \mu \|^2_2 \) over \( \Theta_1 \). □
7.1. Algebraic Solution of the Score Equations

In the mathematical optimization literature, the number of critical points of the critical equations to the least squares closest point on a variety is called the Euclidean distance degree \[ \text{DHtO}^{+16} \]. Hence the ML-degree of a gaussian model with identity covariance matrix, and where the means lie on a prescribed variety is the same as the ED-degree of that variety.

**Example 7.1.7.** Let \( \Theta_1 = \{(t^2, t^3) : t \in \mathbb{R} \} \), consisting of the points on a cuspidal cubic curve. Given the observed mean vector \( \bar{X} \) we wish to compute the maximum likelihood estimate for \( \mu \in \Theta_1 \). The relevant part of the likelihood function has the form

\[
(\bar{X}_1 - t^2)^2 + (\bar{X}_2 - t^3)^2.
\]

Differentiating with respect to \( t \) yields the quintic equation

\[
t(2\bar{X}_1 + 3\bar{X}_2 t - 2t^2 - 3t^4) = 0.
\]

Note that this degree 5 equation always has the origin \( t = 0 \) as a solution, and the degree 4 factor is irreducible. In this case, although this equation has degree 5, we still say that the maximum likelihood degree is 4, since finding the critical point only involves an algebraic function of degree 4 in general. On the other hand, note that if \( \bar{X} \) lies to the left of the curve:

\[
V(2x + 32x^2 + 128x^3 + y^2 + 72xy^2 + 27y^4),
\]

the MLE will be the origin. The curve \( V(y^2 - x^3) \) and the discriminantal curve that separates the regions where the optimum is on the smooth locus and the singular point at the origin are illustrated in Figure 7.1.1.
We see in the previous example an important issue regarding maximum likelihood estimation: singular points matter, and for a large region of data space, the MLE might be forced to lie on a lower dimensional stratum of the model. These sorts of issues can also arise when considering closed parameter spaces with boundary. The maximum likelihood estimate might lie on the boundary for a large region of the data space.

**Example 7.1.8.** Let $\Theta_1 = \{(t^2 - 1, t(t^2 - 1)) : t \in \mathbb{R}\}$, consisting of points on a nodal cubic. Note that the node arises when $t = \pm 1$. Given the observed mean vector $\bar{X}$ we wish to compute the maximum likelihood estimate for $\mu \in \Theta_1$. The relevant part of the likelihood function has the form

$$(\bar{X}_1 - (t^2 - 1))^2 + (\bar{X}_2 - (t^3 - t))^2.$$ 

Differentiating with respect to $t$ yields the irreducible quintic equation

$$-\bar{X}_2 + (2\bar{X}_1 + 1)t + 2\bar{X}_2t^2 + 2t^3 - 3t^5 = 0.$$ 

In this case, the ML-degree is five. While both this and the previous are parametrized by cubics, the ML-degree drops in the cuspidal because of the nature of the singularity there.

**Proposition 7.1.9.** Let $\Theta = \mathbb{R}^m \times \Theta_1 \subseteq \mathbb{R}^m \times PD_m$ be the parameter space for a gaussian statistical model. Then the maximum likelihood estimation problem gives $\mu = \bar{X}$, and reduces to maximizing

$$\ell(\Sigma) = -\frac{n}{2} \log \det \Sigma - \frac{n}{2} \text{tr}(S\Sigma^{-1}).$$

**Proof.** Since $\Sigma$ is positive semidefinite, the expression

$$-\frac{n}{2}(\bar{X} - \mu)^T \Sigma^{-1} (\bar{X} - \mu)$$

in the likelihood function is always $\leq 0$, and equal to zero if and only if $(\bar{X} - \mu) = 0$. Since we are trying to maximize the likelihood function, choosing $\mu = \bar{X}$ makes this term as large as possible and does not effect the other terms of the likelihood function. \qed

A similar result holds in the case of centered gaussian models, that is models where the mean is constrained to be zero.

**Proposition 7.1.10.** Let $\Theta = \{0\} \times \Theta_1 \subseteq \mathbb{R}^m \times PD_m$ be the parameter space for a centered gaussian statistical model. Then the maximum likelihood estimation problem gives $\mu = \bar{X}$, and reduces to maximizing

$$\ell(\Sigma) = -\frac{n}{2} \log \det \Sigma - \frac{n}{2} \text{tr}(S\Sigma^{-1})$$

where $S = \sum_{i=1}^n (X^{(i)}(X^{(i)})^T$ is the centered sample covariance matrix.
Example 7.1.11. Consider the gaussian statistical model $\Theta = \mathbb{R}^m \times \Theta_1$ where

$$\Theta_1 = \{ \Sigma \in PD_4 : \sigma_{12} = \sigma_{21} = 0, \sigma_{34} = \sigma_{43} = 0 \}.$$ 

This model is a gaussian independence model with the two marginal independence constraints $X_1 \perp \perp X_2$ and $X_3 \perp \perp X_4$. Since the likelihood function involves both $\log \det \Sigma$ and $\Sigma^{-1}$, we will need to multiply all equations through by $(\det \Sigma)^2$ to clear denominators, which introduces extraneous solutions. In this example, there is a six dimensional variety of extraneous solutions. Saturating with respect to this determinant removes that space of extraneous solutions to reveal 17 solutions to the score equations. The following code in Macaulay2 shows that there are 17 solutions for a particular realization of the sample covariance matrix $S$.

```
R = QQ[s11,s13,s14,s22,s23,s24,s33,s44];
D = matrix{{19, 3, 5, 7}, {3 ,23,11,13},
          {5 ,11,31,-1}, {7 ,13,-1,37}};
S = matrix{{s11,0 ,s13,s14}, {0 ,s22,s23,s24},
          {s13,s23,s33,0 },{s14,s24,0 ,s44}};
W = matrix{{0,0,0,1},{0,0,-1,0},{0,1,0,0},{-1,0,0,0}};
adj = W*exteriorPower(3,S)*W;
L = trace(D*adj);
f = det S;
J = ideal apply(flatten entries vars R,
               i -> f*diff(i,f) - f*diff(i,L) + diff(i,f)*L);
K = saturate(J,ideal(f));
dim J, dim K, degree K
```

Further study of maximum likelihood estimation in gaussian marginal independence models that generalize this example appear in [DR08]. In particular, a characterization of when these models have ML-degree 1 can be given.

Many statistical models are given implicitly, for instance, conditional independence models. To solve the score equations in such models, we must use an appropriate version of Lagrange multipliers which is compatible with the algebraic structure of the models and clearing denominators. This structure was worked out in detail by Hoşten, Khetan, and Sturmfels [HKS05], and is useful not only for models that are intrinsically implicit, but also for parametric models since they can be implicitized. The implicit representation is also useful for discussing geometric properties of the ML-degree, which we elaborate on in Section 7.3.

Suppose we have a statistical model for discrete random variables given in implicit form via the homogeneous prime ideal $I \subseteq \mathbb{R}[p]$. That is, our
model is of the form \( V(I) \cap \Delta_{r-1} \). For fixed data vector \( u \in \mathbb{N}^r \), maximum likelihood estimation amounts to maximizing the degree zero rational function

\[
L(p|u) = \frac{p_1^{u_1} \cdots p_r^{u_r}}{(p_1 + \cdots + p_r)^n}
\]

over the projective variety \( V(I) \subseteq \mathbb{P}^{r-1} \), where \( n \) is the sample size. Of course, on the model \( V(I) \cap \Delta_{r-1} \), the denominator is identically equal to one, but we need to include it so that we can perform our calculations with respect to the homogeneous ideal \( I \).

Let \( f = (f_1, \ldots, f_k)^T \) be a collection of generators of the ideal \( I \) written as a vector. The theory of Lagrange multipliers tells us that a local maximizer of the log-likelihood function will be a critical point of the Lagrangian:

\[
L(p, \lambda) = \ell(p, u) + \lambda^T f
\]

where \( \lambda = (\lambda_1, \ldots, \lambda_k)^T \) is the vector of Lagrange multipliers. The critical equations of the Lagrangian are

\[
u_i - \frac{n}{p_1 + \cdots + p_r} + \lambda^T \frac{\partial f}{\partial p_i} = 0, \quad i = 1, \ldots, r
\]

\[
f_j(p) = 0, \quad j = 1, \ldots, k.
\]

These conditions can be restated as follows:

**Proposition 7.1.12.** A vector \( p \in V(I) \setminus V(p_1 \cdots p_r(p_1 + \cdots + p_r)) \) is a critical point of the Lagrangian if and only if the data vector \( u \) lies in the row span of the augmented Jacobian matrix of \( f \).

The augmented Jacobian matrix of \( f \) is the matrix

\[
J(p) = \begin{pmatrix}
p_1 \frac{\partial f_1}{\partial p_1} & p_2 \frac{\partial f_1}{\partial p_1} & \cdots & p_r \frac{\partial f_1}{\partial p_1} \\
p_1 \frac{\partial f_2}{\partial p_1} & p_2 \frac{\partial f_2}{\partial p_1} & \cdots & p_r \frac{\partial f_2}{\partial p_1} \\
p_1 \frac{\partial f_k}{\partial p_1} & p_2 \frac{\partial f_k}{\partial p_1} & \cdots & p_r \frac{\partial f_k}{\partial p_1} \\
\vdots & \vdots & \ddots & \vdots \\
p_1 \frac{\partial f_1}{\partial p_r} & p_2 \frac{\partial f_1}{\partial p_r} & \cdots & p_r \frac{\partial f_1}{\partial p_r} \\
p_1 \frac{\partial f_2}{\partial p_r} & p_2 \frac{\partial f_2}{\partial p_r} & \cdots & p_r \frac{\partial f_2}{\partial p_r} \\
\vdots & \vdots & \ddots & \vdots \\
p_1 \frac{\partial f_k}{\partial p_r} & p_2 \frac{\partial f_k}{\partial p_r} & \cdots & p_r \frac{\partial f_k}{\partial p_r}
\end{pmatrix}
\]

Proposition 7.1.12 can be used to develop algorithms for computing the maximum likelihood estimates in implicit models. Here is an algorithm taken from [HKS05] which can be used to compute solutions to the score equations for implicit models.

**Algorithm 7.1.13.** Input: A homogeneous prime ideal \( P = \langle f_1, \ldots, f_k \rangle \subseteq \mathbb{R}[p_1, \ldots, p_r] \) and a data vector \( u \in \mathbb{N}^r \).

Output: The likelihood ideal \( I_u \) for the model \( V(P) \cap \Delta_{r-1} \).

Step 1: Compute \( c = \text{codim}(P) \) and let \( Q \) be the ideal generated by the \( c+1 \) minors of the Jacobian matrix \( \frac{\partial f_i}{\partial p_j} \).
Step 2: Compute the kernel of $J(p)$ over the coordinate ring $\mathbb{R}[V] := \mathbb{R}[p_1, \ldots, p_r]/P$. This kernel is a submodule, $M$, of $\mathbb{R}[V]^r$.

Step 3: Let $I'_u$ be the ideal in $\mathbb{R}[V]$ generated by the polynomials $\sum_{i=1}^r u_i \phi_i$ running over all the generators $(\phi_1, \ldots, \phi_r)$ for the module $M$.

Step 4: The likelihood ideal $I_u$ equals

$$I_u = I'_u : (p_1 \cdots p_r (p_1 + \cdots + p_r)Q)^\infty.$$ 

Example 7.1.14. Here we illustrate Algorithm 7.1.13 on the random censoring model from Example 7.1.5. Algorithms for implicitization from Chapter 3 can be used to show that the homogeneous vanishing ideal is

$$P = \langle 2p_0p_1p_2 + p_1^2p_2 + p_1p_2^2 - p_0^2p_12 + p_1p_2p_12 \rangle \subseteq \mathbb{R}[p_0, p_1, p_2, p_12].$$

We solve the score equations in the implicit case using the following code in Singular.

```
LIB solve.lib;
ring R = 0, (p0, p1, p2, p12), dp;
ideal P = 2*p0*p1*p2 + p1^2*p2 + p1*p2^2 - p0^2*p12 + p1*p2*p12;
matrix u[1][4] = 4,2, 11, 15;
matrix J = jacob(sum(maxideal(1)) + P) * diag(maxideal(1));
matrix I = diag(P, nrows(J));
module M = modulo(J,I);
ideal Iprime = u * M;
int c = nvars(R) - dim(groebner(P));
ideal Isat = sat(Iprime, minor(J, c+1))[1];
ideal IP = Isat, sum(maxideal(1))-1;
solve(IP);
```

The computation shows that there are three solutions to the score equations so this model has maximum likelihood degree 3, which agrees with our earlier computations in the parametric setting.

7.2. Concave Likelihood Functions

Solving the score equations is a fundamental problem of computational statistics. Numerical strategies have been developed for finding solutions to the score equations, which are generally heuristic in nature. That is, algorithms for finding the maximum likelihood estimate might not be guaranteed to return the maximum likelihood estimate, but at least converge to a local maximum, or critical point, of the likelihood function. In special cases, in particular for exponential families and for discrete linear models, the likelihood function is concave and such hill-climbing algorithms converge to the maximum-likelihood estimate.
Definition 7.2.1. A set $S \subseteq \mathbb{R}^d$ is convex if it is closed and for all $x, y \in S$, $(x + y)/2 \in S$ as well. If $S$ is a convex set, a function $f : S \to \mathbb{R}$ is convex if $f((x + y)/2) \leq (f(x) + f(y))/2$ for all $x, y \in S$. A function $f : S \to \mathbb{R}$ is concave if $f((x + y)/2) \geq (f(x) + f(y))/2$ for all $x, y \in S$.

Proposition 7.2.2. Suppose that $S$ is convex, and $f : S \to \mathbb{R}$ is a concave function. Then the set $U \subseteq S$ where $f$ attains its maximum value is a convex set. If $f$ is strictly concave ($f((x + y)/2) > (f(x) + f(y))/2$ for all $x \neq y \in S$) then $f$ has a unique global maximum, if a maximum exists.

Proof. Suppose that $x, y \in U$ and let $\alpha$ be the maximum value of $f$ on $S$. Then

$$f((x + y)/2) \geq (f(x) + f(y))/2 = (\alpha + \alpha)/2 = \alpha \geq f((x + y)/2).$$

This shows that the set of maximizers is convex. A strict inequality leads to a contradiction if there are two maximizers. □

Definition 7.2.3. Let $f_1(\theta), \ldots, f_r(\theta)$ be nonzero linear polynomials in $\theta$ such that $\sum_{i=1}^r f_i(\theta) = 1$. Let $\Theta \subseteq \mathbb{R}^d$ be the set such that $f_i(\theta) > 0$ for all $\theta \in \Theta$, and suppose that dim $\Theta = d$. The model $M = f(\Theta) \subseteq \Delta_r$ is called a discrete linear model.

Note that in [PS05], the discrete linear models were called linear models. We choose not to use that name because “linear model” usually refers to models for continuous random variables where the random variables are related to each other by linear relations.

Proposition 7.2.4. Let $M$ be a discrete linear model. Then the likelihood function $\ell(\theta|u)$ is concave. The set

$$\Theta' = \{\theta : f_i(\theta) > 0 \text{ for all } i \text{ such that } u_i > 0\}$$

is bounded if and only if the likelihood function has a unique local maximum in $\Theta'$.

Proof. Any linear function is concave, and the logarithm of a concave function is concave. The sum of concave functions is concave. This implies that the log-likelihood function

$$\ell(\theta|u) = \sum_{i=1}^d u_i \log f_i(\theta)$$

is a concave function over the region $\Theta'$. If $\Theta'$ is unbounded, by choosing a point $\theta_0 \in \Theta'$ and a direction $\nu$ such that the ray $\{\theta_0 + t\nu : t \geq 0\}$ is contained in $\Theta'$, we see that $\ell(\theta_0 + t\nu|u)$ increases without bound as $t \to \infty$. Otherwise, if $\Theta'$ is bounded, $\ell$ is strictly concave on $\Theta'$, so there is a unique local maximum on $\Theta'$. □
Note that if all \( u_i > 0 \), then our assumption that \( \sum_i f_i = 1 \) guarantees that \( \Theta \) is bounded, so a maximum likelihood estimate always exists. A similar argument as the proof of Proposition 7.2.4 shows that, for \( u \) with \( u_i > 0 \) for all \( i \), the likelihood function \( L(\theta|u) \) has a real critical point on each bounded region of the arrangement complement

\[
\mathcal{H}(f) = \{ \theta \in \mathbb{R}^d : \prod_{i=1}^r f_i(\theta) \neq 0 \}.
\]

Remarkably, this trivial lower bound on the maximum likelihood degree is tight.

**Theorem 7.2.5. [Var95]** The maximum likelihood degree of the discrete linear model parametrized by \( f_1, \ldots, f_r \) equals the number of regions in the arrangement complement \( \mathcal{H}(f) \).

**Example 7.2.6.** A typical situation where discrete linear models arise is when considering mixture distributions of known distributions. For example, consider the three probability distributions

\[
P_1 = \left( \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4} \right), \quad P_2 = \left( \frac{2}{5}, \frac{2}{5}, 0, \frac{2}{5} \right), \quad P_3 = \left( \frac{2}{3}, \frac{1}{6}, \frac{1}{6}, 0 \right),
\]

and consider the statistical model \( \mathcal{M} \subseteq \Delta_4 \) that arises from taking all possible mixtures of these three distributions. This will consist of all distributions of the form

\[
\theta_1(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}) + \theta_2(\frac{2}{5}, \frac{2}{5}, 0, \frac{2}{5}) + (1 - \theta_1 - \theta_2)(\frac{2}{3}, \frac{1}{6}, \frac{1}{6}, 0)
\]

with \( 0 \leq \theta_1, 0 \leq \theta_2, \) and \( \theta_1 + \theta_2 \leq 1 \). This is a subset of a discrete linear model, with linear parametrizing functions given by

\[
f_1(\theta_1, \theta_2) = \frac{2}{3} - \frac{5}{12} \theta_1 - \frac{7}{15} \theta_2, \quad f_2(\theta_1, \theta_2) = \frac{1}{6} + \frac{1}{12} \theta_1 + \frac{7}{30} \theta_2,
\]

\[
f_3(\theta_1, \theta_2) = \frac{1}{6} + \frac{1}{12} \theta_1 - \frac{1}{6} \theta_2, \quad f_4(\theta_1, \theta_2) = \frac{1}{4} \theta_1 + \frac{2}{5} \theta_2.
\]

Figure 7.2.1 displays the configuration of lines given by the zero sets of each of the polynomials, \( f_1, \ldots, f_4 \). The gray triangle \( T \) denotes the region of \( \theta \) space corresponding to viable parameters from the standpoint of the mixture model.

The polyhedral region containing \( T \), is the region \( \Delta \) on which the parameters are defined. Note that the likelihood function will have a unique maximum in \( T \), since \( \ell \) will be convex on \( T \). Furthermore, Figure 7.2.1 has three bounded regions so the maximum likelihood degree of the model is three. However, the MLE will only be a degree three function of the data if the maximum likelihood estimate lies in the interior of \( T \). When the maximum likelihood estimate lies on the boundary of \( T \), the MLE is a degree one function of the data. \( \square \)
A second situation where the log-likelihood function is concave and there is a direct iterative procedure to compute the maximum likelihood estimate is for canonical exponential families. A standard algorithm for computing the maximum likelihood estimate in this case is called iterative proportional fitting (also iterative proportional scaling is used).

To prove that the likelihood function is concave for canonical exponential families uses some basic properties of these models.

**Proposition 7.2.7.** Let $\mathcal{M}$ be a canonical exponential family with sufficient statistics $T(x)$ and natural parameter $\eta$, with density $p_\eta(x) = h(x) \exp(\eta T(x) - \phi(\eta))$. Then

$$\frac{\partial}{\partial \eta_i} \phi(\eta) = E_{\eta}[T_i(X)] \quad \text{and} \quad \frac{\partial^2}{\partial \eta_i \eta_j} \phi(\eta) = \text{Cov}_{\eta}[T_i(X), T_j(X)].$$

**Proof.** Recall that $\phi(\eta) = \log \int_{x \in \mathcal{X}} h(x) \exp(\eta T(x)) dx$. Differentiating with respect to $\eta_i$ yields

$$\frac{\partial}{\partial \eta_i} \phi(\eta) = \frac{\int_{x \in \mathcal{X}} T_i(x) h(x) \exp(\eta T(x)) dx}{\int_{x \in \mathcal{X}} h(x) \exp(\eta T(x)) dx} = E_{\eta}[T_i(X)].$$

Let $Z(\eta) = \int_{x \in \mathcal{X}} h(x) \exp(\eta T(x)) dx$. Differentiating this expression again with respect to $\eta_j$ and using the quotient rule for derivatives yields

$$\frac{\partial^2}{\partial \eta_i \eta_j} \phi(\eta) =$$
7.2. Concave Likelihood Functions

\[ \frac{\int_{x \in X} T_i(x)T_j(x)h(x) \exp(\eta T(x))dx}{Z(\eta)} - \frac{\left(\frac{\partial}{\partial \eta} Z(\eta)\right)\left(\frac{\partial}{\partial \eta} Z(\eta)\right)}{Z(\eta)^2} \]

\[ = E_{\eta}[T_i(X)T_j(X)] - E_{\eta}[T_i(X)]E_{\eta}[T_j(X)] \]

\[ = \text{Cov}_{\eta}[T_i(X), T_j(X)]. \] □

From Proposition 7.2.7 we can easily see that the likelihood function of a canonical exponential family must be concave.

**Corollary 7.2.8.** Let \( \mathcal{M} \) be a canonical exponential family with sufficient statistics \( T(x) \) and natural parameter \( \eta \), with density \( p_{\eta}(x) = h(x) \exp(\eta T(x) - \phi(\eta)) \). Then the likelihood function is convex. Furthermore the maximum likelihood estimate, if it exists, is the solution to the equation

\[ (7.2.1) \quad T(x) = E_{\eta}[T(X)] \]

where \( x \) denotes the data vector.

**Proof.** We compute the log-likelihood given the data \( x \), \( \ell(\eta|x) = \log h(x) + \eta T(x) - \phi(\eta) \). Differentiating with respect to \( \eta_i \) and setting equal to zero yields the score equation \( T_i(x) = E_{\eta}[T_i(X)] \), from which the formula for the maximum likelihood estimate \( T(x) = E_{\eta}[T(X)] \) follows. Computing second partial derivatives and using Proposition 7.2.7 we see that the matrix of second partials is negative the covariance matrix of the vector \( T(X) \). This Hessian matrix is thus negative definite, which implies the log-likelihood function is concave. □

We explain what this expression means for discrete and gaussian exponential families and the resulting algebraic expressions of the score equations in implicit and explicit form. This is summarized in the next two corollaries. Then we explain the iterative proportional fitting algorithm for these models.

**Corollary 7.2.9.** Let \( A \in \mathbb{Z}^{k \times r} \) such that \( 1 \in \text{rowspan}(A) \), let \( h \in \mathbb{R}_{>0}^r \), and let \( u \) be the vector of counts from \( n \) i.i.d. samples. Then the maximum likelihood estimate in the log-linear model \( \mathcal{M}_{A,h} \) given the data \( u \) is the unique solution, if it exists, to the equations:

\[ Au = nAp \quad \text{and} \quad p \in \mathcal{M}_{A,h}. \]

**Proof.** The sufficient statistics of the data \( u \) is \( Au \). Given a distribution \( p \in \mathcal{M}_{A,h} \) and a sample of size \( n \), the expected value of the sufficient statistics is \( nAp \). Thus, the result follows from Equation 7.2.1. □

The proof of the analogous result for gaussian exponential families is similar and left to the reader.
Corollary 7.2.10. Let $L$ be a linear space in $\mathbb{R}^{m(m+1)/2}$ such that $L \cap PD_m$ is not empty, and let $\mathbb{R}^m \times M_{L^{-1}}$ be the corresponding parameter space of the canonical gaussian exponential family. Let $X^{(1)}, \ldots, X^{(n)} \in \mathbb{R}^m$ be i.i.d. samples and let $\bar{X}$ and $S$ be the corresponding sample mean and sample covariance matrix. Then the maximum likelihood estimate for $(\mu, \Sigma) \in \mathbb{R}^m \times M_{L^{-1}}$ is $(\hat{X}, \hat{S})$ where $\hat{S}$ is the unique solution, if it exists, to the equations

$$\pi(S) = \pi(\hat{S}) \quad \text{and} \quad \hat{S} \in M_{L^{-1}}$$

where $\pi$ denotes the orthogonal projection onto $L$.

Here we explain how to use the iterative proportional fitting algorithm to compute maximum likelihood estimates for discrete exponential families $M_{A,h}$. The basic idea of the method is as follows. We initially with any positive distribution $p \in M_{A,h}$. This $p$ is probably not the maximum likelihood estimate, in particular it does not satisfy $Ap = A\frac{u}{n}$. To make $p$ fit the data more closely we rescale the distribution by values related to this failure of the matching of the sufficient statistics to get a new distribution that is closer to having the correct sufficient statistics. We suppose that $A$ has the property that all column have the same sum $a$.

Algorithm 7.2.11 (Iterative Proportional Scaling). Input: The matrix $A \in \mathbb{N}^{k \times r}$, a vector $h \in \mathbb{R}^r > 0$, a vector of counts $u \in \mathbb{N}^r$ and a tolerance $\epsilon > 0$.

Output: Maximum likelihood estimate $\hat{p} \in M_{A,h}$ given data $u$.

Step 1: Initialize a distribution $p \in M_{A,h}$. For example, take $p_i = h_i/(\sum_j h_j)$.

Step 2: While $\|Ap - A\frac{u}{n}\| > \epsilon$ do:

For all $i \in [r]$ set $p_i := p_i \cdot \left(\frac{\phi_{A,h}(Au/n)}{\phi_i(Ap)}\right)^{1/a}$

Step 3: Output $\hat{p} = p$.

The proof of convergence of iterative proportional scaling for discrete exponential families is due to Darroch and Ratcliff [DR72]. It is also possible to derive similar algorithms for canonical exponential families that are not discrete.

7.3. Geometry of the ML-Degree

The ML-degree of a discrete statistical model has a beautiful geometric interpretation as a topological Euler characteristic. Furthermore, it is possible to characterize those models which have ML-degree one. These are both results of June Huh [Huh13, Huh14], which we survey in this section. These results are best stated for models that are defined implicitly.

Definition 7.3.1. The algebraic torus is the set $(\mathbb{K}^*)^r$. A very affine variety is a set of the form $V \cap (\mathbb{K}^*)^r$ where $V$ is a variety.
Here we consider a slight variation of the maximum likelihood estimation problem, in particular, for each $u \in \mathbb{N}^r$ the optimization problem

$$\max p_1^{u_1} \cdots p_r^{u_r} \text{ subject to } p \in V$$

where $V$ is an arbitrary (real) very affine variety. The maximum likelihood degree is the number of critical points of the likelihood function $\ell(p|u)$ over $V$.

**Theorem 7.3.2** ([Huh13]). Let $V \subseteq (\mathbb{C}^*)^r$ be a very affine variety of dimension $d$. If $V$ is smooth then the ML-degree of $V$ is $(-1)^d \chi(V)$, where $\chi(V)$ denotes the topological Euler characteristic.

As we have seen in our discussion of algebraic exponential families many statistical models are not smooth. Note, however, that Theorem 7.3.2 only requires smoothness away from the coordinate hyperplanes, and so this theorem applies to any discrete exponential family.

**Example 7.3.3.** Consider the statistical model of independence for two binary random variables. As a variety, this is given by the equations

$$V(p_{11} + p_{12} + p_{21} + p_{22} - 1, p_{11}p_{22} - p_{12}p_{21}).$$

As a very affine variety this is isomorphic to $(\mathbb{C}^* - \{-1\})^2$. To see this note that this very affine variety can be parametrized via the map $\phi : (\mathbb{C}^*)^2 \rightarrow (\mathbb{C}^*)^4$

$$(\alpha, \beta) \mapsto \left(\frac{\alpha}{1 + \alpha}, \frac{\beta}{1 + \beta}, \frac{1}{1 + \alpha}, \frac{1}{1 + \beta}, \frac{1}{1 + \alpha + \beta}, \frac{1}{1 + \beta + \alpha} \right)$$

which is undefined when $\alpha$ or $\beta$ are $-1$. Note that $\mathbb{C}^* - \{-1\}$ is a sphere minus three points, and has Euler characteristic $-1$. Thus, the ML-degree is $(-1)^2 \times (-1)^2 = 1$.

As we have seen, most statistical models do not have ML-degree one. When a model does have ML-degree one, we immediately see that that model must be (part of) a unirational variety, since the map from data to maximum likelihood estimate will be a rational function that parametrizes the model. Huh [Huh14] has shown that the form of the resulting parametrization is extremely restricted.

**Theorem 7.3.4.** The following are equivalent conditions on a very affine variety.

1. $V \subseteq (\mathbb{C}^*)^r$ has ML-degree 1.
2. There is a vector $h = (h_1, \ldots, h_r) \in (\mathbb{C}^*)^r$ an integral matrix $B \in \mathbb{Z}^{n \times r}$ with all columns sums equal to zero, and a map $\psi : (\mathbb{C})^r \rightarrow \mathbb{C}^n$
\[(\mathbb{C}^*)^r\]

\[\Psi_k(u_1, \ldots, u_r) = h_k \cdot \prod_{i=1}^{n} \left( \sum_{j=1}^{r} b_{ij} u_j \right)^{b_{ik}}\]

such that \(\Psi\) maps dominantly onto \(V\).

The map \(\Psi\) above which parametrizes any variety of ML-degree one is called the Horn uniformization. This shows that the varieties with ML-degree one are precisely the \(A\)-discriminants (see [GKZ94]).

Example 7.3.5. Let

\[B = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -2 & -2 & -2 & -2 \end{pmatrix}\]

and \(h = (4, 4, 4, 4)\).

Then

\[\Psi_{ij}(u_{11}, u_{12}, u_{21}, u_{22}) = \frac{(u_{11} + u_{12})(u_{1j} + u_{2j})}{(u_{11} + u_{12} + u_{21} + u_{22})^2}.\]

In particular, the Horn uniformization parametrizes the model of independence of two discrete random variables.

7.4. Likelihood Ratio Tests

After we have computed the maximum likelihood estimate of the model parameters given data, a natural next step is to try to address the question of how well the model fits the data. A standard approach to this problem is based on the likelihood ratio test. We typically have two models \(M_0 \subseteq M_1\), we compute the maximum likelihood estimate in each model and compare the evaluation of the likelihood function at these estimates. If the ratio of likelihood scores is larger than one would expect by chance, we reject the smaller model. Theoretical study of this process involves understanding the asymptotic distribution of the likelihood ratio test statistic, and algebraic geometry enters the picture because the asymptotic distribution of the likelihood ratio test statistic changes at singular points of the models. Our presentation follows that of [Drt09b], which contains extensive details and examples.

Let \(M_\Theta = \{P_\theta : \theta \in \Theta\}\) be a statistical model where \(\Theta \subseteq \mathbb{R}^k\) is the parameter space which we assume is open and has dimension \(k\). Consider a submodel \(M_{\Theta_0} \subseteq M_\Theta\) obtained by considering a subset of the parameter space \(\Theta_0 \subseteq \Theta\). We obtain independent random samples \(X^{(1)}, \ldots, X^{(n)}\) which
we assume are distributed according to some distribution $P_{\theta} \in \mathcal{M}_\Theta$. We would like to test the hypothesis:

$$H_0 : \theta \in \Theta_0 \quad \text{versus} \quad H_1 : \theta \in \Theta \setminus \Theta_0.$$  

The likelihood ratio test is one method for performing this hypothesis test. We assume that the distributions in $\mathcal{M}_\Theta$ have densities $p_{\theta}(x)$ with respect to a fixed measure on the sample space. Thus the log-likelihood function of the model $\mathcal{M}_\Theta$ has the form

$$\ell_n(\theta) = \sum_{i=1}^n \log p_{\theta}(X^{(i)}).$$

**Definition 7.4.1.** Let likelihood ratio statistic for the hypothesis test (7.4.1) is

$$\lambda_n = 2 \left( \sup_{\theta \in \Theta} \ell_n(\theta) - \sup_{\theta \in \Theta_0} \ell_n(\theta) \right).$$

Since $\Theta_0 \subseteq \Theta$, $\lambda_n \geq 0$. The likelihood ratio test assesses whether $\lambda_n$ is too large for what one would expect if $\theta \in \Theta_0$, and rejects the null hypothesis if that is the case. Our goal is the try to understand what “too large” means. Note that we here explicitly express the dependence of the log-likelihood function and the likelihood ratio statistic on the sample size, $n$, because we will often need to understand this expression as $n$ goes to infinity. To evaluate $\lambda_n$ requires computing maximum likelihood estimates in $\mathcal{M}_\Theta$ and $\mathcal{M}_{\Theta_0}$ which can be achieved using methods from previous sections of this chapter.

We illustrate the main idea, we will first focus on a very special case: models of gaussian random variables with restricted mean parameter. In particular let $\Theta = \mathbb{R}^m$ and let the model $\mathcal{M}_\Theta$ be the family of normal distributions

$$\{N(\mu, I) : \mu \in \mathbb{R}^m\}$$

where $I$ is the $m \times m$ identity matrix. Let $\bar{X}$ denote the sample mean of $X^{(1)}, \ldots, X^{(n)}$. Evaluating (7.1.2) with $\Sigma = I$ gives the log-likelihood function

$$\ell_n(\mu) = -\frac{n}{2} \| \bar{X} - \mu \|_2^2 - \frac{1}{2} \sum_{i=1}^n \| X^{(i)} - \bar{X} \|_2^2$$

so that the likelihood ratio statistic becomes

$$\lambda_n = n \cdot \inf_{\mu \in \Theta_0} \| \bar{X} - \mu \|_2^2.$$  

So, maximum likelihood estimation in this case is amounts to computing the least squares closest point in the model $\Theta_0$ (see Proposition 7.1.6) and the likelihood ratio statistic is the squared Euclidean distance to $\Theta_0$, scaled by the sample size $n$. 

To know when to reject the null hypothesis via the likelihood ratio test, we need to understand when \( \lambda_n \) is large assuming the data was generated from a \( \mu_0 \in \Theta_0 \). In particular, we must understand what probability distribution \( \lambda_n \) has. To do this, we rewrite

\[
\lambda_n = \inf_{\mu \in \Theta_0} \| \sqrt{n}(\bar{X} - \mu) - \sqrt{n}(\mu - \mu_0) \|^2.
\]

Thinking about \( \lambda_n \) as a random variable, since \( X^{(1)}, \ldots, X^{(n)} \) have a \( \mathcal{N}(\mu_0, I) \) distribution, the term \( \sqrt{n}(\bar{X} - \mu_0) \) is distributed as a standard normal random variable \( Z \sim \mathcal{N}(0, I) \). So we can rewrite the likelihood ratio statistic as a random variable as

\[
\lambda_n = \inf_{h \in \sqrt{n}(\Theta_0 - \mu_0)} \| Z - h \|^2.
\]

In the special case where \( \Theta_0 \) is a linear space, we have an exact characterization of this distribution regardless of \( n \).

**Proposition 7.4.2.** Let \( \Theta_0 \subseteq \Theta = \mathbb{R}^m \) be a linear space of dimension \( d \), and \( \mu_0 \in \Theta_0 \), and consider the hypothesis test (7.4.1) for the models

\[
\mathcal{M}_{\Theta_0} \subseteq \mathcal{M}_\Theta = \{ \mathcal{N}(\mu, I) : \mu \in \mathbb{R}^m \}.
\]

Then the likelihood ratio statistics \( \lambda_n \) has a \( \chi^2_{m-d} \)-distribution.

**Proof.** If \( \Theta_0 \) is a linear space then \( L = \sqrt{n}(\Theta_0 - \mu_0) \) is a linear space passing through the origin. As \( Z \sim \mathcal{N}(0, I) \) is rotationally invariant, we can assume that \( L \) is a coordinate subspace where the first \( d \) coordinates are nonzero. The squared distance between a point \( Z = (Z_1, \ldots, Z_m) \) and \( L \) is \( \sum_{i=d+1}^m Z_i^2 \) which has a \( \chi^2_{m-d} \)-distribution by definition. \( \square \)

This leads to an explicit p-value calculation for the likelihood ratio test in the case that \( \Theta_0 \subseteq \mathbb{R}^m \) is a linear space of dimension \( d \). Namely we should reject the null hypothesis at level \( \alpha \) if

\[
P(\chi^2_{m-d} \geq \lambda_{obs}) \leq \alpha.
\]

Here \( \lambda_{obs} \) denotes the observed value of \( \lambda_n \) obtained from a specific data set.

If \( \Theta_0 \), is not a linear space, the set \( \sqrt{n}(\Theta_0 - \mu_0) \) will not be a fixed set, and hence the distribution of \( \lambda_n \) will change as a function of \( n \). To deal with this problem, we assume we have a large sample size and take the limit as \( n \to \infty \). If \( \mu_0 \in \Theta_0 \), as \( n \to \infty \), the limiting object \( \lim_{n \to \infty} \sqrt{n}(\Theta_0 - \mu_0) \) is the tangent cone of \( \Theta_0 \) at \( \mu_0 \), \( TC_{\mu_0}(\Theta_0) \). In other words:

**Proposition 7.4.3.** Let \( \Theta_0 \subseteq \Theta = \mathbb{R}^m \), and \( \mu_0 \in \Theta_0 \). Then as \( n \to \infty \),

\[
\lambda_n \xrightarrow{D} \inf_{h \in TC_{\mu_0}(\Theta_0)} \| Z - h \|^2
\]
where $Z \sim \mathcal{N}(0, I)$. That is, the limiting distribution of $\lambda_n$ is the distribution of a standard normal random variable to the tangent cone of $\Theta_0$ at $\mu_0$.

Suppose that we remain in the case of Gaussian models with $\Theta_0 \subseteq \Theta = \mathbb{R}^m$ a smooth manifold of dimension $d$. Each tangent cone $TC_{\mu_0}(\Theta_0)$ is a linear space of dimension $d$. From Proposition 7.4.3 we deduce that, regardless of what the true underlying parameter $\mu_0 \in \Theta_0$ is, the limiting distribution of $\lambda_n$ as $n \to \infty$ is a $\chi^2_{m-d}$ distribution. This leads to the asymptotic likelihood ratio test for smooth models: namely, take the asymptotic/approximate p-value

$$p = \lim_{n \to \infty} P(\lambda_n \geq \lambda_{\text{obs}}) = P(\chi^2_{m-d} \geq \lambda_{\text{obs}})$$

and reject at level $\alpha$ is this is less than $\alpha$. Such a limit can be used for any model that is a smooth submodel of a regular exponential family, and using this asymptotic approximation to a smooth model is usually what statisticians refer to when they talk about using a likelihood ratio test. Of course, as we have seen in previous chapters, statistical models need not be smooth manifolds. The distribution of the distance from a standard normal to the tangent cone will usually not be a chi-square distribution in this case.

**Example 7.4.4.** Let $\Theta_0 \subseteq \mathbb{R}^2$ be the cuspidal cubic curve

$$\Theta_0 = \{(\mu_1, \mu_2) \in \mathbb{R}^2 : \mu_2^2 = \mu_1^3\}$$

see Example 7.1.7 and Figure ???. The only singularity of $\Theta_0$ is that the origin, $\mu_0 = (0, 0)$, and the tangent cone is the ray:

$$TC_{(0,0)}(\Theta_0) = \{(\mu_1, 0) : \mu_1 \geq 0\}.$$

Taking $Z \sim \mathcal{N}(0, Id)$, we see that the squared Euclidean distance from $Z$ to $TC_{(0,0)}(\Theta_0)$ is either $Z_2^2$ if $Z_1 \geq 0$, or is $Z_1^2 + Z_2^2$ if $Z_1 \leq 0$. Since $P(Z_1 \leq 0) = P(Z_1 \geq 0) = \frac{1}{2}$ it follows that $\lambda_n$ converges to a mixture of chi-square distributions:

$$\lambda_n \xrightarrow{D} \frac{1}{2} \chi^2_1 + \frac{1}{2} \chi^2_2.$$

Since $P(\chi^2_1 \geq t) < P(\chi^2_2 \geq t)$ for all $\alpha > 0$, we see that if the true parameter $\mu_0$ were the origin, a typical asymptotic p-value computation based on the $\chi^2_1$ distribution would yield a p-value that is too small.

**Example 7.4.5.** On the other hand, if $\Theta_0 \subseteq \mathbb{R}^2$ is the nodal cubic curve

$$\Theta_0 = \{(\mu_1, \mu_2) \in \mathbb{R}^2 : \mu_2^2 = \mu_1^3 + \mu_1^2\}$$

then $\mu_0 = (0, 0)$ is still the only singular point and the tangent cone is

$$TC_{(0,0)}(\Theta_0) = \{(\mu_1, \mu_2) \in \mathbb{R}^2 : \mu_2^2 = \mu_1^2\}.$$
This tangent cone is the union of two perpendicular lines that cross at the origin. After applying a rotation, we can treat these two lines as the coordinate axes. If $Z \sim N(0, I)$ the squared Euclidean distance to the closest coordinate axis is $\min(Z_1^2, Z_2^2)$. In other words,

$$\lambda_n = D \min(\chi_1^2, \chi_1^2).$$

Since the $P(\min(Z_1^2, Z_2^2) < t) < P(\min(Z_1^2 < t)$ for all $t$, we see that an asymptotic $p$-value that was approximated using just the $\chi_1^2$ distribution would be too large.

In Examples 7.4.4 and 7.4.5 we saw relatively clean expressions for the limiting distribution that arise in the likelihood ratio test. In general these limiting distributions need not have simple closed expressions. For example, replacing Example 7.4.5 with the nodal cubic

$$\Theta_0 = \{ (\mu_1, \mu_2) \in \mathbb{R}^2 : \mu_2^2 = \mu_1^3 + 2\mu_1 \}$$

yields a similar singularity but the limiting distribution does not have a simple expression as the minimum of 2 $\chi_1^2$ distributions. In general, one probably needs to run simulations to compute $p$-values.

So far we have only discussed very special models that arise as submodels of $\mathbb{R}^m$ as a restricted set of possible mean vectors for multivariate normal distribution, with identity as the covariance matrix. But the same general principles apply to arbitrary statistical models that are semialgebraic submodels of regular exponential families.

**Definition 7.4.6.** Let $M_\Theta$ be a statistical model where $\Theta \subseteq \mathbb{R}^k$, and the $\theta \in \Theta$. The *Fisher-information matrix* $I(\theta)$ is the $k \times k$ matrix with entries

$$I(\theta)_{ij} = \mathbb{E} \left[ \left( \frac{\partial}{\partial \theta_i} \log p_\theta(X) \right) \left( \frac{\partial}{\partial \theta_j} \log p_\theta(X) \right) \right].$$

The expectation is calculated assuming that $X \sim P_\theta$.

Note that the Fisher information will always be a symmetric positive semi-definite matrix, so $I(\theta)$ always has a matrix square root.

**Theorem 7.4.7.** Suppose that the model $M_\Theta$ is a regular exponential family with parameter space $\Theta \subseteq \mathbb{R}^k$ and lest $\Theta_0$ be a semi-algebraic subset of $\Theta$. If the true parameter $\theta_0$ is in $\Theta_0$ and $n \to \infty$, then the likelihood ratio statistic converges in distribution to the distribution of the squared Euclidean distance

$$\min_{h \in TC_{\theta_0}(\Theta_0)} \|Z - I(\theta_0)^{1/2} h\|_2^2$$

between $Z \sim N(0, I)$ and the linearly transformed tangent cone $I(\theta_0)^{1/2} TC_{\theta_0}(\Theta_0)$. Here $I(\theta_0)^{1/2}$ can be any matrix square root of $I(\theta_0)$. 
Given the difficulties that can arise when models have singularities, it is natural to wonder what we should actually do when attempting to use the likelihood ratio tests with real data. In practice we do not know whether or not the true parameter \( \theta_0 \) belongs to \( \Theta_0 \) nor whether or not \( \theta_0 \) is a singular point of \( \Theta_0 \). So we do not know which distribution we should use when deciding to calculate a \( p \)-value, since we do not know the true value of \( \theta \).

Perhaps the most conservative choice is to use all the singularity information from the model \( \Theta_0 \) to produce a range of \( p \)-values and use this range to make some decision on whether to reject the null hypothesis.

7.5. Exercises

Exercise 7.1. (1) Show that for any ideals \( I \) and \( J \), there exists a \( k_0 \) such that for all \( k \geq k_0 \), \( I : J^k = I : J^{k_0} \).

(2) Show that \( V(I : J^\infty) = V(I) \setminus V(J) \).

Exercise 7.2. Maximum likelihood estimation induces a map from the probability simplex, into the parameters. In Example 7.2.6 that function \( ML : \Delta_4 \to T \) is sometimes an algebraic function of degree 3, and sometimes an algebraic function of degree 1, depending on which face of \( T \) the function \( ML \) maps to. Determine the decomposition of \( \Delta_4 \) induced by the \( ML \) map in this case.

Exercise 7.3. Consider the log-linear model given by the following parametrization \( p_{ijkl} = \alpha_{ij}\beta_{jk}\gamma_{kl} \) for four discrete random variables each with two states.

(1) Show that this model has \( ML \)-degree one.

(2) Realize this model via a Horn uniformization.

Exercise 7.4. Calculate the Fisher information matrix when \( \Theta = \Delta_{k-1} \) is the probability simplex for a discrete random variable with \( k \) states.

Exercise 7.5. Let \( \Theta_0 = \{(\mu_1, \mu_2) \in \mathbb{R}^2 : \mu_2^2 = \mu_1^3 + 2\mu_2^2 \} \subseteq \mathbb{R}^2 \) and consider the statistical model \( \mathcal{M}_{\Theta_0} = \{N(\mu, I) : \mu \in \Theta_0 \} \). Consider the ten data points \( X^{(1)}, \ldots, X^{(10)} \) which are the columns of the following \( 2 \times 10 \) matrix:

\[
\begin{pmatrix}
-0.709 & -0.755 & -1.374 & -0.678 & 0.349 & 0.361 & 0.228 & -0.435 & 1.353 & -0.987 \\
1.284 & 0.223 & 0.202 & -0.289 & 0.274 & -0.950 & -0.347 & -0.822 & -0.627 & 0.674
\end{pmatrix}
\]

Use the conservative likelihood ratio test outlined at the end of Section 7.4 to decide if this data set was generated from a point on the model.
The Cone of Sufficient Statistics

For a fixed exponential family $\mathcal{M}$, the set of all sufficient statistics of (unnormalized, real) data that can arise forms a convex cone. For discrete exponential families this is a convex polyhedral cone, and for Gaussian exponential families it is a cone inside the cone of positive semidefinite matrices. We introduce and study these cones in this section. This will also provide us with the introduction to convex and polyhedral geometry, whose study will also play an important role in other chapters in this book. The question of when there exists a maximum likelihood estimate for an exponential family is also related and will be discussed.

8.1. Polyhedral Geometry

In this section we review various notions from convex and polyhedral geometry. Most of the main results are stated without proof, and can be found, for instance, in [Zie95] or [Tho06]. Recall the definition of a convex set from Chapter 7.

**Definition 8.1.1.** A set $S \subseteq \mathbb{R}^d$ is called convex if for all $p^1, p^2 \in S$ and all $\lambda \in [0, 1] \subseteq \mathbb{R}$, $\lambda p^1 + (1 - \lambda)p^2 \in S$.

Any linear or affine space is convex. Let $a \in \mathbb{R}^d$ and $b \in \mathbb{R}$. The set $H = \{p \in \mathbb{R}^d : a^T p \leq b\}$ is called a half-space, and is an important example of a convex set. Note that we include $a = \mathbf{0}$ so that $\mathbb{R}^d$ and $\emptyset$ are both examples of half-spaces. The intersection of any collection of convex sets is convex.
The cone of sufficient statistics

Definition 8.1.2. For an arbitrary set $S \subseteq \mathbb{R}^d$ the convex hull of $S$, denoted $\text{conv}(S)$, is the smallest convex set that contains $S$.

The convex hull of a set $S$ is well-defined since it can be explicitly taken to be the intersection of all convex sets that contain $S$. These definitions are illustrated in Figure 8.1.1.

Definition 8.1.3. A set $P \subseteq \mathbb{R}^d$ that is the intersection of finitely many half-spaces is called a polyhedron. A bounded polyhedron is called a polytope.

The dimension of a polyhedron $P$ is defined to be the dimension of the smallest affine space containing it, and is denoted $\dim P$.

Example 8.1.4. The set of points

$$C_d := \{ p \in \mathbb{R}^d : 0 \leq p_i \leq 1 \text{ for all } i \}$$

is a polytope called the standard $d$-dimensional hypercube. The set of points

$$\Delta_{d-1} := \{ p \in \mathbb{R}^d : 0 \leq p_i, \sum_{i=1}^d p_i = 1 \}$$

is the standard $(d-1)$-dimensional simplex, often called the probability simplex up to this point.

Note that any equality constraint $\mathbf{a}^T \mathbf{p} = b$ can be realized as the intersection of the two half-spaces $\mathbf{a}^T \mathbf{p} \leq b$ and $\mathbf{a}^T \mathbf{p} \geq b$. So combinations of finitely many linear inequality and equality constraints yield polyhedra.

Definition 8.1.5. A face of a polyhedron $P$ is a set of the form $\{ p : \mathbf{a}^T \mathbf{p} = b \} \cap P$ where the half-space $H = \{ p : \mathbf{a}^T \mathbf{p} \leq b \}$ contains $P$.

Technically we allow $\mathbf{a}$ to be the zero vector in this definition, so that $P$ and $\emptyset$ are always both faces of $P$. The faces of a polyhedron are themselves polyhedra. The 0-dimensional faces are called vertices, the 1-dimensional faces are called edges. If $\dim P = d$, then the $d-1$ dimensional faces are
called facets. For example, the $d$-dimensional cube $C_d$ has $2d$ facets, and $2^d$ vertices. The $d-1$-dimensional simplex has \( \binom{d}{i} \) $(i-1)$-dimensional faces for each $i$. Note that the empty set is considered a $-1$-dimensional face.

Every polyhedron has finitely many faces. This follows from the fact that every face must be obtained by taking a subset of the half-space defining inequalities of $P$ and making some of them equalities. So if $P$ has $m$ facets, it has at most $2^m$ faces. This upper bound on the number of faces is attained only for the simplex. Usually, there are many fewer faces than $2^m$.

**Definition 8.1.6.** Two polyhedra $P \subseteq \mathbb{R}^d$ and $Q \in \mathbb{R}^e$ are **affinely isomorphic** if there is an affine transformation $\phi : \mathbb{R}^d \to \mathbb{R}^e$ such that $\phi(P) = Q$, and an affine transformation $\psi : \mathbb{R}^e \to \mathbb{R}^d$ such that $\psi(Q) = P$. The polyhedra $P$ and $Q$ are **combinatorially equivalent** if there is a bijection between the faces of $P$ and the faces of $Q$ which preserves the incidences between faces.

Note that any polytope combinatorially equivalent to the standard simplex is affinely isomorphic to the standard simplex. On the other hand, a polytope combinatorially equivalent to the standard cube need not be affinely isomorphic to it.

The definition of polyhedra we have given so far is in terms of half-spaces. Such a polyhedron is sometimes called an $\mathcal{H}$-polyhedron (the $\mathcal{H}$ for “half-space”). Polyhedra can also be described in a dual approach called a $\mathcal{V}$-polyhedron (the $\mathcal{V}$ for vertex). In the special case of polytopes, the $\mathcal{V}$-description is easy to state.

**Theorem 8.1.7.** The convex hull of any finite set is a polytope. Every polytope is equal to the convex hull of its set of vertices.

To explain the generalization of this result to arbitrary polyhedra, we need a few more definitions.

**Definition 8.1.8.** A **polyhedral cone** $C$ is a set of the form

$$C = \{ p \in \mathbb{R}^d : Ap \leq 0 \}$$

where $A \in \mathbb{R}^{k \times d}$ is a matrix. For two vectors, $p, q \in \mathbb{R}^k$, $p \leq q$ means that the inequality holds for all coordinates.

Equivalently, a polyhedral cone is a polyhedron where all the defining half-spaces pass through the origin. Because of this, a polyhedral cone can have at most one vertex, namely, the origin. In the case where the polyhedral cone $C$ does have the origin as a vertex, it is called a **pointed cone**. A cone being pointed is equivalent to it not containing any lines.
Definition 8.1.9. Let $V = \{v_1, \ldots, v_k\} \subseteq \mathbb{R}^d$ be a finite set of vectors. The set

$$\text{cone}(V) = \{\lambda_1 v_1 + \cdots + \lambda_k v_k : \lambda_1, \ldots, \lambda_k \geq 0\}$$

is the cone generated by $V$.

Definition 8.1.9 gives the $V$-description of a polyhedral cone.

Definition 8.1.10. Let $S, T \subseteq \mathbb{R}^d$ be two sets. The Minkowski sum is the set $S + T = \{p + q : p \in S \text{ and } q \in T\}$.

Note that if $S$ and $T$ are convex sets, then so is the Minkowski sum, $S + T$. In general, a $V$-polyhedron is a set that can be expressed in the form: $\text{conv}(V_1) + \text{cone}(V_2)$ for two finite sets $V_1$ and $V_2 \subset \mathbb{R}^d$. The main theorem relating $\mathcal{H}$-polyhedra and $V$-polyhedra is the following.

Theorem 8.1.11. Every $\mathcal{H}$-polyhedron is a $V$-polyhedron, and every $V$-polyhedron is a $\mathcal{H}$-polyhedron. For every polyhedron $P$, if $P = C + Q$ where $C$ is a cone and $Q$ is a polytope, then $C$ is uniquely determined by $P$ and is called the recession cone of $P$. If the polyhedron $P$ contains no lines, $Q$ can be taken to be the convex hull of the set of vertices of $P$.

A proof of Theorem 8.1.11 is a standard result in polyhedral geometry and can be found, for instance in [Zie95]. For a pointed polyhedral cone $C$, there is a unique minimal set of vectors (up to scaling) $V$ such that $\text{cone}(V) = C$. The set $V$ are called the extreme rays of $C$.

Example 8.1.12. Let $P$ be the polyhedron

$$P = \{(x, y) \in \mathbb{R}^2 : x \geq 0, y \geq 1, x + y \geq 2\}.$$ 

Then $P = \text{cone}(V) + \text{conv}(W)$ where

$$V = \{(1, 0), (0, 1)\} \quad \text{and} \quad W = \{(1, 1), (0, 2)\}.$$ 

8.2. Discrete Exponential Families

Polyhedral geometry arises when studying exponential families since for a discrete exponential family, the set of all sufficient statistics for all (unnormalized nonnegative real) data is a polyhedral cone, the cone of sufficient statistics.

Recall the setup from Section 6.2. Let $A \in \mathbb{Z}^{k \times r}$ will $1 \in \text{rowspan}(A)$. Let $\mathcal{M}_A$ be the regular exponential family defined by $A$. Let $X^{(1)}, \ldots, X^{(n)}$ be i.i.d. samples from a distribution $p \in \mathcal{M}_A$. The probability that $X^{(i)} = j$ only depends on the parameter vector $\theta$ through the vector $a_j$. 


8.2. Discrete Exponential Families

Indeed, let $u \in \mathbb{N}^r$ be the vector of counts, $u_j = \#\{i : X^{(i)} = j\}$. Then in the discrete log-linear model $M_A$ we have

$$p_\theta(X^{(1)} = j_1, \ldots, X^{(n)} = j_n) = \frac{1}{Z(\theta)^n} \prod_{i=1}^n \theta^{a_{ji}} = \frac{1}{Z(\theta)^n} \theta^{Au}.$$ 

Since the probability only depends on the vector of sufficient statistics $Au$, it makes sense to study the set of all such vectors of sufficient statistics, over all possible data sets. This is the affine semigroup

$$\mathbb{N}A := \{Au : u \in \mathbb{N}^r\}.$$ 

This is a complicated discrete object, which we will discuss in more detail later. As a first approximation, we can instead study the polyhedral cone

$$\text{cone}(A) := \{Au : u \in \mathbb{R}^r_{\geq 0}\}.$$ 

One reason for studying the polyhedral cone $\text{cone}(A)$ is because of its connection to maximum likelihood estimation as explained in the following theorem.

**Theorem 8.2.1.** Let $A \in \mathbb{Z}^{k \times r}$ be the integer matrix with $1 \in \text{rowspace}(A)$ let $h \in \mathbb{R}^r_{\geq 0}$, and let $M_{A,h}$ be the corresponding regular exponential family. Let $u \in \mathbb{N}^r$ be the vector of counts for i.i.d. data. Then a maximum likelihood estimate of parameters given the data $u$ exists in the model $M_{A,h}$ if and only if $b = Au$ lies in the relative interior of $\text{cone}(A)$.

**Proof.** According to Corollary 7.2.9, the maximum likelihood estimate, if it exists, is the solution to the equation system

$$A \frac{u}{n} = Ap \quad \text{and} \quad p \in M_{A,h}.$$ 

By the nature of the log-linear model $M_{A,h}$ every distribution $p \in M_{A,h}$ must have all coordinates of $p$ positive. If such a $p$ exists then $A \frac{u}{n} = Ap$ could not lie on the boundary of $\text{cone}(A)$ because it is a positive combination of the columns of $A$.

On the other hand, suppose that $b = Au$ lies in the relative interior of $\text{cone}(A)$. Then there is a positive real vector $v$ such that $b = Av$. By the property of the sufficient statistics, maximizing the likelihood $\prod_{i=1}^r p_{i}^{v_i}$ over $p \in M_{A,h}$ is equivalent to maximizing the likelihood $\prod_{i=1}^r p_{i}^{v_i}$ over $p \in M_{A,h}$. Since all coordinates of $v_i$ are positive, this ensures that $\prod_{i=1}^r p_{i}^{v_i} = 0$ for any $p \in M_{A,h}$ that has a zero coordinate. On the other hand, $\prod_{i=1}^r p_{i}^{v_i} > 0$ for any $p \in M_{A,h}$. Since the likelihood function is convex, and is zero on the boundary, it must have a maximum in $M_{A,h}$. \qed
The condition of Theorem 8.2.1 can be checked using linear programming and the following proposition.

**Proposition 8.2.2.** Suppose that $A \in \mathbb{Z}^{d \times r}$ satisfies $1 \in \text{rowspace}(A)$. Let $u$ be a vector of counts, and let $b = Au$ be the vector of sufficient statistics, and let

$$Q(b) = \{ c \in \mathbb{R}^d : cA \leq \frac{1}{n} cb \}.$$ 

Then $b$ is in the relative interior of $\text{cone}(A)$ if and only if $Q(u)$ is equal to the orthogonal complement of $\text{span}(A)$.

In practice, checking the condition of Proposition 8.2.2 might involve studying the geometry of a polytope with exponentially many inequalities, for example if $r$ has exponential size. In many instances, if the model has some underlying combinatorial structure, it might be possible to set up an equivalent system using significantly smaller numbers of variables to decide whether or not $b$ lies in the relative interior of $\text{cone}(A)$. See [EFRS06].

A more direct, but also expensive, approach to deciding the existence of maximum likelihood estimates is to simply list all facet defining inequalities of the cone $\text{cone}(A)$. The point $b$ lies in the relative interior of $\text{cone}(A)$ if and only if none of the facet defining inequalities are tight.

A second interesting problem concerning the cone of sufficient statistics for a discrete exponential family concerns the integer points inside that cone. After all, each data vector $u$ is a vector of counts, so the vectors of sufficient statistics $Au$ is also an integral vector. The set of all possible sufficient statistics vectors is a semigroup denoted

$$\mathbb{N}A := \{ Au : u \in \mathbb{N}^r \}.$$ 

Similarly let $ZA := \{ Au : u \in \mathbb{Z}^r \}$ denote the lattice spanned by the columns of $A$. Note that $\mathbb{N}A \subseteq ZA \cap \text{cone}(A)$ but in general the containment might be strict.

**Example 8.2.3.** Let $A = \begin{pmatrix} 0 & 1 & 3 \\ 1 & 1 & 1 \end{pmatrix}$. Then the vector $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$ belongs to $ZA \cap \text{cone}(A)$ but is not in the semigroup $\mathbb{N}A$. Figure 8.2 shows the semigroup and the facets of $\text{cone}(A)$.

**Definition 8.2.4.** The semigroup $\mathbb{N}A$ is called saturated if $\mathbb{N}A = ZA \cap \text{cone}(A)$. Alternate terminology is that the matrix $A$ is normal. Elements of $(ZA \cap \text{cone}(A)) \setminus \mathbb{N}A$ are called holes.
In Example 8.2.3, the matrix $A$ is nonnormal, and $\binom{2}{1}$ is a hole. In fact, the set of all holes for this semigroup are the points of the form $\binom{3t-1}{t}$ with $t = 1, 2, 3, \ldots$.

Here we illustrate these ideas on a family of examples, the binary graph models, or heterogeneous Ising models. Let $G = (V, E)$ be an undirected graph with vertex set $V$ and edge set $E$. We create a matrix $A_G$ with $\#V + \#E + 1$ rows and $2^{\#V}$ columns as follows. Let $\#V = m$. The columns are indexed by elements of $\{0, 1\}^m$. For each such string $\epsilon = (\epsilon_1, \ldots, \epsilon_m)$ we form the vector

$$a_\epsilon = (1, \epsilon_1, \ldots, \epsilon_m) \oplus (\epsilon_i \epsilon_j)_{ij \in E} \in \mathbb{Z}^{1+m+\#E}$$

and let $A_G$ be the matrix which these vectors as its columns.

The corresponding log-linear model gives distributions for $m$ binary random variables of the form

$$P_\theta(X_1 = x_1, \ldots, X_m = x_m) = \frac{1}{Z(\theta)} \prod_{i=1}^{m} \theta_{x_i}^{x_i} \prod_{ij \in E} \theta_{ij}^{x_i x_j}$$

where $\theta = (\theta_i)_{i \in [m]}, (\theta_{ij})_{ij \in E} \in \mathbb{R}^{m+\#E}$.

The cone of sufficient statistics for this model is $\text{cone}(A_G)$ a $1+m+\#E$ dimensional polyhedral cone with $2^m$ extreme rays $a_\epsilon$. The coordinates on $\mathbb{R}^{1+m+\#E}$ are indexed by $\{\emptyset\} \cup V \cup E$, and we denote them by $p_\emptyset$, $p_i$ and $p_{ij}$, respectively.
Example 8.2.5. Let $G$ be the graph with 3 vertices and two edges $E = \{12, 23\}$. The matrix $A_G$ is a $6 \times 8$ matrix:

$$A_G = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

For example, the 7th column is $a_{(1,1,0)}$. The cone $A_G$ is described by 8 facet-defining inequalities:

$$p_{12} \geq 0, \ p_{23} \geq 0, \ p_1 \geq p_{12}, \ p_2 \geq p_{12}, \ p_2 \geq p_{23}, \ p_3 \geq p_{23},$$

$$p_{12} - p_1 - p_2 + p_0 \geq 0, \ p_{23} - p_2 - p_3 + p_0 \geq 0.$$

The cone $cone(A_G)$ is closely related to the polytope $conv(A_G)$, which is a well-studied object in optimization. It is known as the correlation polytope or moment polytope. The correlation polytope is also affinely isomorphic, via an appropriate change of coordinates, to the cut polytope. See [DL97] for extensive background on correlation and cut polytopes. Cut polytopes and the connection to correlation polytopes are discussed in Section 19.1. The interpretation and the name correlation polytope come from the following proposition.

Proposition 8.2.6. Let $P \in \Delta_{2^m-1}$ be a probability distribution for $m$ binary random variables $X_1, \ldots, X_m \in \{0, 1\}$. Let $G = ([m], E)$ be an undirected graph. Let $p = A_G P$, whose coordinates are indexed by the set $\{\emptyset\} \cup V \cup E$. Then $p_0 = 1$, $p_i = \mathbb{E}[X_i]$ and $p_{ij} = \mathbb{E}[X_iX_j]$.

Proof. We calculate the entries of $p$. For $P \in \Delta_{2^m-1}$ and $\epsilon \in \{0, 1\}^m$, let $P_\epsilon$ denote the probability $P_\epsilon = P(X_1 = \epsilon_1, \ldots, X_m = \epsilon_m)$. Then

$$p_0 = \sum_{\epsilon \in \{0, 1\}^m} a_{\emptyset, \epsilon} P_\epsilon = \sum_{\epsilon \in \{0, 1\}^m} 1 \cdot P_\epsilon = 1$$

$$p_i = \sum_{\epsilon \in \{0, 1\}^m} a_{i, \epsilon} P_\epsilon = \sum_{\epsilon \in \{0, 1\}^m} \epsilon_i P_\epsilon = \mathbb{E}[X_i]$$

$$p_{ij} = \sum_{\epsilon \in \{0, 1\}^m} a_{ij, \epsilon} P_\epsilon = \sum_{\epsilon \in \{0, 1\}^m} \epsilon_i \epsilon_j P_\epsilon = \mathbb{E}[X_iX_j].$$

To this end, inequality constraints on the cone of sufficient statistics $cone(A_G)$ can be used to check consistency of a given set of lower-order moments of a distribution. Indeed, a potential vector of moments $p \in \mathbb{R}^{1+m+\#E}$ is actually the vector of moments of some probability distribution if and only
if \( p_\emptyset = 1 \) and \( p \in \text{cone}(A_G) \). Inequality constraints can also be used to produce bounds on moments given some collection of other moments, as will be illustrated in Chapter 10. To do either of these things in practice requires explicit knowledge of the combinatorial structure of the facet-defining inequalities of \( \text{cone}(A_G) \). It seems unlikely that there is a simple, compact description of the facet-defining inequalities of \( \text{cone}(A_G) \) for all graphs \( G \). However, there are some classes of graphs for which the description is known. From the moment description, we always have the following valid inequalities on \( \text{cone}(A_G) \):

\[
(8.2.1) \quad p_{ij} \geq 0, \quad p_i \geq p_{ij}, \quad p_j \geq p_{ij}, \quad p_\emptyset + p_{ij} \geq p_i + p_j \text{ for all } ij \in E.
\]

Moreover, those inequalities always define facets of \( \text{cone}(A_G) \). Cycles in \( G \) impose further facet defining inequalities on \( \text{cone}(A_G) \).

**Definition 8.2.7.**

- A sequence of vertices \( v_0, v_1, \ldots, v_k \) in a graph \( G \) is a *cycle* if \( v_0 = v_k \), there are no other repeated vertices in the sequence, and \( v_i v_{i+1} \) is an edge in the \( G \).
- Given a subset \( K \subseteq V \) of the vertices of \( G = (V, E) \), the *induced subgraph* \( G_K \) is the graph with vertex set \( K \) and edge set \( E_K = \{ij : i, j \in K \text{ and } ij \in E\} \).
- A cycle in a graph \( G \) is induced if the induced subgraph on the vertex set of the cycle consists of exactly the edges in the cycle.

**Proposition 8.2.8.** Let \( G \) be a graph, \( C \) be any induced cycle of \( G \), and \( O \) a subset of the edges of \( C \) of odd cardinality. Then

\[
\sum_{jk \in O} p_{jk} - \sum_{jk \in C \setminus O} p_{jk} - \sum_{j \in V(O)} p_j + \sum_{j \in V(C \setminus O)} p_j + \frac{\#O - 1}{2} p_\emptyset \geq 0
\]

is a valid inequality for the cone \( \text{cone}(A_G) \) and is facet-defining.

The proof of Proposition 8.2.8 will be postponed until Chapter 19 where it will be more easy to state in the language of cut polytopes.

**Theorem 8.2.9.** [BM86] The cone of sufficient statistics \( \text{cone}(A_G) \) is defined by the inequalities from Equation 8.2.1 if and only if \( G \) is a forest. The cone of sufficient statistics \( \text{cone}(A_G) \) is defined by the inequalities from Equation 8.2.1 plus the cycle inequalities of Proposition 8.2.8 from every induced cycle if and only if \( G \) is free of \( K_4 \) minors.

The problem of studying the integral points in \( \text{cone}(A_G) \) can be made into a more interesting/relevant/practical problem if we allow ourselves to change the matrix to one that has the same row span. Changing the matrix but leaving the row span the same does not change the resulting log-linear model, nor does it change the geometry of the cone of sufficient statistics,
but the new coordinates that arise might change our interpretation of the sufficient statistics. To this end, for each such string \( \epsilon = (\epsilon_1, \ldots, \epsilon_m) \in \{0,1\}^m \) we form the vector
\[
c_\epsilon = (\epsilon_i \epsilon_j, (1-\epsilon_i)\epsilon_j, \epsilon_i (1-\epsilon_j), (1-\epsilon_i)(1-\epsilon_j))_{ij \in E} \in \mathbb{Z}^{4\#E},
\]
and let \( C_G \) be the \( 4\#E \times 2^m \) matrix consisting of the \( c_\epsilon \) as column vectors. Note that for a vector of counts \( u \), the vector \( C_G u \) consists of all of the marginal counts for pairs of random variables \((X_i, X_j)\) such that \( ij \) is an edge in \( G \). The matrices \( A_G \) and \( C_G \) have the same integral row span and hence they are either both normal or both not normal. Characterizing the semigroup \( N_{A_G} \) can be used to determine which collections of integer marginals could have come from a \( 2^m \) integer contingency table. If the semigroup \( N_{A_G} \) is normal then one only needs to check that it lies in the lattice \( \mathbb{Z}A_G \) and lies in the cone cone\((A_G)\).

The characterization of the normal binary graph models is the content of the following theorem.

**Theorem 8.2.10.** \([\text{Ohs10}, \text{Su10}]\) The semigroup \( N_{A_G} \) is saturated if and only if \( G \) is free of \( K_4 \) minors.

### 8.3. Gaussian Exponential Families

For exponential families besides the discrete exponential families, the cone of sufficient statistics is still convex but usually not polyhedral. To study such cones requires more general tools from convex geometry. For Gaussian exponential families the cones under consideration have natural interpretations as cones related to the cone of positive semidefinite matrices.

Let \( PD_m \) denote the cone of \( m \times m \) symmetric positive definite matrices, and \( PSD_m \) the cone of \( m \times m \) symmetric positive semidefinite matrices. For any two real symmetric matrices \( A, B \), let \( A \succeq B \) mean that \( A - B \in PSD_m \) and \( A \succ B \) that \( A - B \in PD_m \). So \( A \succeq 0 \) means that \( A \) is a positive semidefinite matrix.

Let \( L \subseteq \mathbb{R}^{m(m+1)/2} \) be a linear space such that \( L \cap PD_m \) is nonempty, which determines a Gaussian exponential family of covariance matrices via the set \( L^{-1} = \{K^{-1} : K \in L \cap PD_m\} \). Given data \( X^{(1)}, \ldots, X^{(n)} \), the sufficient statistics \( T(X) \) of this model take the sample covariance matrix \( S \) and map it via orthogonal projection onto \( L \). The sample covariance matrix is, in principle, any positive semidefinite matrix and \( T \) is a linear map, so \( T(PSD_m) \) is the cone of sufficient statistics. Following \([\text{SU10}]\), we denote this set by \( \mathcal{C}_L \).

The cone of sufficient statistics for a Gaussian exponential family is usually not a polyhedral cone. However, since \( PSD_m \) is a semialgebraic set
and the orthogonal projection map $T$ is a linear function, the image $C_L$ is also a semialgebraic set, though it need not be a closed basic semialgebraic set.

We illustrate the basic ideas with coordinate subspaces. Let $G = (V, E)$ be a graph. Let

$$L(G) = \{ K \in \mathbb{R}^{m(m+1)/2} : K_{ij} = 0, \text{ if } i \neq j \text{ and } ij \notin E \}.$$  

The resulting model $\mathcal{M}_G$ consisting of gaussian random variables whose covariance matrices belong to the inverse linear space $L(G)^{-1}$ is called a concentration graph model, or gaussian graphical model for an undirected graph. The sufficient statistic map is the map

$$T : \mathbb{R}^{m(m+1)/2} \rightarrow \mathbb{R}^V \oplus \mathbb{R}^E, \quad T(S) = (s_{ii})_{i \in V} \oplus (s_{ij})_{ij \in E}$$

that extracts the diagonal elements of $S$ and the off-diagonal elements corresponding to edges in the graph $G$. To describe the image of $T$ amounts to solving the following problem:

**Problem 8.3.1.** Given a graph $G$ and a partially observed symmetric matrix $T(S)$, determine whether or not there exists a $S' \in \text{PSD}_m$ such that $T(S') = T(S)$.

There are some obvious necessary conditions.

**Proposition 8.3.2.** Let $G = (V, E)$ be a graph and let $K \subseteq V$ be a set of vertices such that $G_K$ is a complete subgraph. Then if there exists an $S' \in \text{PSD}_m$ such that $T(S') = T(S)$, it must be that $S_{K,K}$ is a positive semidefinite matrix.

Proposition 8.3.2 rarely gives a necessary and sufficient condition. This holds if and only if $G$ satisfies strong conditions, which we describe now.

**Definition 8.3.3.** A graph $G$ is chordal if on every cycle $v_0, v_1, \ldots, v_k = v_0$ in $G$ of length $k \geq 4$, there is a pair of vertices $v_i, v_j$ with $i - j \neq -1, 0, 1 \text{ mod } k$ such that $v_i v_j \in E(G)$.

A variety definition of chordal graph is that every induced cycle is a three cycle. Chordal graphs play an important role in the theory of graphical models and hence in algebraic statistics. Their study originates in graph theory and they play a major role in the theory of graph minors. There are a number of different ways to describe these graphs besides the definition above. A second description is in terms of graph decompositions.

**Definition 8.3.4.** Say that a graph $G = (V, E)$ has a reducible decomposition into induced subgraph $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ if

1. $G_i = G_{V_i}, i = 1, 2$
The Cone of Sufficient Statistics

Figure 8.3.1. A chordal graph and its decomposition into maximal cliques.

\( G_{V_1 \cap V_2} \) is a complete subgraph of \( G \), and
\( G = G_1 \cup G_2 \).

A graph with a reducible decomposition is reducible. A graph is decomposable if it is either a complete graph or it is reducible and both \( G_1 \) and \( G_2 \) are decomposable.

Reducible graphs are obtained from two graphs by gluing along a common clique. A decomposable graph can be obtained by a succession of gluing operations, starting with a collection of complete graphs. Chordal graphs are related to decomposable graphs by the following:

**Theorem 8.3.5.** [Dir61] A graph is chordal if and only if it is decomposable.

Figure 8.3 shows an example of a chordal graph and its decomposition into maximal cliques.

Say that a symmetric matrix \( S \) satisfies the clique condition with respect to the graph \( G \) if all the determinants \( |S_{K,K}| \) are nonnegative for \( K \) a clique of \( G \). Proposition 8.3.2 implies that if there exists a \( S' \in PSD_m \) such that \( T(S) = T(S') \) then \( S \) must satisfy the clique condition with respect to \( G \). This can be turned around for chordal graphs.

**Theorem 8.3.6.** [GJdSW84] If \( G \) is a chordal graph then a symmetric matrix \( S \) satisfies the clique condition with respect to \( G \) if and only if there exists an \( S' \in PSD_m \) such that \( T(S) = T(S') \).

**Proof.** Let \( G \) be a chordal graph. By Theorem 8.3.5 and induction, we can assume that the graph \( G \) consists of two cliques \( A \cup B \) and \( B \cup C \) meeting at a common subclique \( B \), and that \( A \cup B \cup C = [m] \). To start with, we will assume that \( T(S) \) is a partially positive definite matrix (i.e., all cliques have positive determinant). Our partial matrix has the following form

\[
T(S) = \begin{pmatrix}
S_{A,A} & S_{A,B} & X \\
S_{B,A} & S_{B,B} & S_{B,C} \\
X^T & S_{C,B} & S_{C,C}
\end{pmatrix}
\]
8.3. Gaussian Exponential Families

where $X$ is the unknown matrix that we are trying to fill in. We claim we can take $X = S_{A,B}S_{B,B}^{-1}S_{B,C}$ to get a positive definite matrix. Indeed, let $S'$ be the resulting matrix with this fill-in. Let $U$ be the upper triangular matrix

$$U = \begin{pmatrix} I & -S_{A,B}S_{B,B}^{-1} & 0 \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix}.$$  

Then

$$US'U^T = \begin{pmatrix} S_{A,A} - S_{A,B}S_{B,B}^{-1}S_{B,A} & 0 & 0 \\ 0 & S_{B,B} & S_{B,C} \\ 0 & S_{C,B} & S_{C,C} \end{pmatrix}.$$  

Note that $S_{A,A} - S_{A,B}S_{B,B}^{-1}S_{B,A}$ is positive definite since it is the Schur complement of the positive definite matrix $S_{A,B,A,B}$. This means that $US'U^T$ is positive definite, so $S'$ must have been positive definite.

Now suppose that $T(S)$ satisfies that clique property. Because the clique property is determined by nonnegativity of finitely many matrix inequalities, the set of partial matrices satisfying the clique property is a closed set. The interior consists of all the partial positive definite matrices. Let $T(S_1), T(S_2), \ldots$ be a sequence of partial positive definite matrices converging to $T(S)$, with $S_1, S_2, \ldots$ the positive definite matrices guaranteed to exist by the first part of our proof. Since $T(S)$ extracts the diagonal entries of $S$, this implies that the diagonal entries of all the $S_1, S_2, \ldots$ are bounded by some constant. By positive definiteness, this implies that all the entries of the $S_1, S_2, \ldots$ are bounded. Hence, by the Bolzano-Weierstrass Theorem, there exists a subsequence $S_{i1}, S_{i2}, \ldots$, converging to some positive semidefinite matrix $S'$. This matrix satisfied $T(S') = T(S)$. \hfill $\square$

On the other hand, as soon as $G$ contains an induced cycle without a chord, there are other conditions that must be satisfied to guarantee that there is a positive semidefinite matrix completion.

**Example 8.3.7.** Let $G$ be the four cycle $C_4$, with edges $\{12, 23, 34, 14\}$, and consider the partial matrix

$$T(S) = A = \begin{pmatrix} 1 & a & x & -a \\ a & 1 & a & y \\ x & a & 1 & a \\ -a & y & a & 1 \end{pmatrix}.$$  

Here $a \in [-1, 1]$ is a given parameter value and $x$ and $y$ are the unknown values. The problem is to determine if there are values of $x$ and $y$ that make the matrix positive semidefinite. We consider what happens as $a$ varies. Note that every $1 \times 1$ and $2 \times 2$ principal submatrix of $A$ using observed
values is positive semidefinite for any choice of \( a \in [-1, 1] \). On the other hand, when we require that

\[
|A_{\{1,2,3\},\{1,2,3\}}| = -(x + 1 - 2a^2)(x - 1) \geq 0
\]

we deduce that \( x \in [2a^2 - 1, 1] \). On the other hand the condition

\[
|A_{\{1,3,4\},\{1,3,4\}}| = -(x - 1 + 2a^2)(x + 1) \geq 0
\]

forces that \( x \in [-1, -1 - 2a^2] \). So if \( a > \frac{1}{\sqrt{2}} \) there are no values of \( x \) and \( y \) that complete the matrix to a positive semidefinite matrix.

For cycles of arbitrary length, there is a general structural result characterizing the partial matrices that can be completed to positive semidefinite matrices.

**Theorem 8.3.8.** [BJT93, Buh93] Let \( T(S) \) be a partial matrix associated to the \( m \)-cycle graph \( C_m \) with edges \( \{12, 23, \ldots, m1\} \). This partial matrix can be completed to a positive definite matrix if and only if

1. All \( s_{ii} > 0 \),
2. All \( s_{ii}s_{i+1,i+1} - s_{i,i+1}^2 > 0 \), and
3. Let \( x_i = \arccos\left(\frac{s_{i,i+1}}{\sqrt{s_{ii}s_{i+1,i+1}}}\right) \) then for all \( i, x_i < \sum_{j \neq i} x_j \).

Here we consider the indices modulo \( m \) so \( m + 1 = 1 \).

The conditions of Theorem 8.3.8 involves the \( \arccos \) of functions of entries of partially observed matrix \( T(S) \) and so does not appear to be algebraic. In fact, this condition can actually be rephrased as an algebraic condition. Indeed, the equation that makes up part of the algebraic boundary of the cone of sufficient statistics then comes from making one of the inequalities an equality. In this case, it consists of a single hypersurface obtained from the equation

\[
(8.3.1) \quad \frac{s_{1,2}}{s_{11}s_{22}} = \cos \left( \sum_{i=2}^{n} \arccos\left(\frac{s_{i,i+1}}{\sqrt{s_{ii}s_{i+1,i+1}}}\right) \right)
\]

which can be converted to an algebraic expression using trigonometric identities. In the case that \( m = 3 \), this is just the \( 3 \times 3 \) determinant. The degree of the resulting equation is calculated in [SU10] for small values of \( m \).

Further work studying when these cycle conditions plus the conditions that come from cliques appeared in [BJL96], and the graphs where these conditions suffice to characterize the existence of a positive semidefinite completion have been completely characterized. The boundary of the cone of sufficient statistics was studied in depth for other graphs on small numbers of vertices in [SU10].
As in the discrete case, a second motivation for studying the cone of sufficient statistics is to determine when maximum likelihood estimates exist for given datasets. Here we collect some sample data $X^{(1)}, \ldots, X^{(n)}$, compute a sample mean and sample covariance matrix, and ask when these lie on the boundary of the cone of sufficient statistics, or not. The sample mean does not affect this question (since the mean is constrained to a linear space in such models) and so we will ignore the mean in this discussion. To be precise, we assume that we consider a model of the form $\{0\} \times \Theta$ where $\Theta \subseteq PD_m$ is an inverse linear space. In such a centered Gaussian exponential family, the sample covariance matrix given the data is

$$S = \sum_{i=1}^{n} X^{(i)} (X^{(i)})^T$$

which is generically a positive semidefinite matrix of rank $\min(m, n)$. We want to know when $T(S)$ lies on the boundary of the cone of sufficient statistics. Since our data was generated by a random process on $\mathbb{R}^m$ we can assume that it is generic among positive semidefinite matrices of rank $\min(m, n)$. To lie in the interior of the cone of sufficient statistics is equivalent to the existence of a positive definite matrix $\Sigma$ such that $T(S) = T(\Sigma)$. Clearly if $n \geq m$, then any generic $S$ is of full rank $m$, and positive definite, so we can just take $\Sigma = S$. So the question of existence of maximum likelihood estimates becomes interesting when $n < m$, that is, there are fewer data points $n$ than coordinates $m$ of our random variables. The best case would be that the maximum likelihood estimates exists for generic data sets with a certain number $n$ of data points. This leads to the following definition.

**Definition 8.3.9.** Let $L \subseteq PD_m$ be a linear space with associated inverse linear space $L^{-1}$. Let $T_L$ be the associated projection onto the cone of sufficient statistics. The maximum likelihood threshold of $L$, denoted $\text{mlt}(L)$ is the smallest $n$ such that for all generic positive semidefinite matrices $S \in PSD_m$ of rank $n$, there exists a positive definite matrix $\Sigma \in PD_m$ such that $T_L(S) = T_L(\Sigma)$.

The special case of coordinate subspaces (corresponding to the graphical gaussian models mentioned above) has been the most studied, with partial results appearing in [Buh93, GS14, SU10]. In this case, the notation $\text{mlt}(G)$ is used to represent $\text{mlt}(L_G)$ where $L_G = \{ \Sigma \in PD_m : \sigma_{ij} = 0 \text{ if } i \neq j \text{ and } ij \notin E(G) \}$. Some sample results from this theory:

**Theorem 8.3.10.** [Buh93] Suppose that $G$ is a chordal graph. Then $\text{mlt}(G)$ is the size of the largest clique in $G$. More generally, if $G$ is a graph and $H$ is a chordal graph such that $E(G) \subseteq E(H)$ then $\text{mlt}(G) \leq$ the size of the largest clique in $H$. 
Theorem 8.3.11. [GS14] If $G$ is a planar graph then $\text{mlt}(G) \leq 4$.

8.4. Exercises

Exercise 8.1. Does there exist a probability distribution on three binary random variables such that $\mathbb{E}[X_1] = \mathbb{E}[X_2] = \mathbb{E}[X_3] = 1/2$ and $\mathbb{E}[X_1X_2] = \mathbb{E}[X_1X_3] = \mathbb{E}[X_2X_3] = 1/8$?

Exercise 8.2. (1) Compute the facet defining inequalities of the cone of sufficient statistics for the binary graph model associated to the graph $K_4$. Which inequalities do not come from (8.2.1) or Proposition 8.2.8?

(2) The matrix of the binary graph model $A_{K_4}$ is not normal. Compute the holes of the semigroup.

Exercise 8.3. Let $G$ be the graph with three vertices and three edges $1 - 2, 2 - 3, 1 - 3$. Consider the table of counts $u$ with

- $u_{000} = 7, u_{001} = 3, u_{010} = 0, u_{011} = 6$,
- $u_{100} = 12, u_{101} = 0, u_{110} = 2, u_{111} = 4$.

Does the maximum likelihood estimate exists in the log-linear model $M_{A_G}$ for this graph and this data?

Exercise 8.4. Prove that for a graph $G$ the two matrices $A_G$ and $C_G$ associated to a binary graph model have the same row span.

Exercise 8.5. Prove Proposition 8.3.2.

Exercise 8.6. Find an explicit algebraic representation of the boundary equation (8.3.1) in the case that $m = 4$. What is the degree of the resulting polynomial?

Exercise 8.7. Let $L \subseteq \mathbb{R}^{10}$ be the linear space of concentration matrices of the form:

$$
\begin{pmatrix}
a & c & 0 & d \\
c & b & d & 0 \\
0 & d & a & c \\
d & 0 & c & b
\end{pmatrix}
$$

(1) What are the sufficient statistics of the associated Gaussian exponential family?

(2) Determine the boundary of the cone of sufficient statistical $C_L$.

(3) What is the maximum likelihood threshold of $L$?
Chapter 9

Fisher’s Exact Test

The paper [DS98], widely considered to be the first paper in the algebraic statistics literature, established a connection between toric ideals, on the algebra side, and an important sampling problem related to contingency tables and discrete data. The sampling problem amounts to generating random lattice points from inside of polytopes (with respect to an appropriate distribution), or said more statistically, sampling from the set of all contingency tables with a given set of sufficient statistics. This sampling is used in a Monte Carlo version of Fisher’s exact test.

In this chapter we explain the connection between Fisher’s exact test and toric ideals. Because of their connection to the sampling problem for Fisher’s exact test using Markov chain Monte Carlo algorithms, generating sets of toric ideals are often known as Markov bases. We also introduce the hierarchical log-linear models which are an important general class, related to graphical models studied in more detail in Chapter 13. Beyond Markov bases, we will also discuss Graver bases as another sampling tool when bounds on cell entries are imposed, as well as some other strategies for sampling when Markov bases are too difficult to compute.

9.1. Conditional Inference

Consider a discrete exponential family $\mathcal{M}_{A,h} \subseteq \Delta_{r-1}$ and suppose that we collect data $X^{(1)}, \ldots, X^{(n)} \in [r]$ which are independent and identically distributed according to a distribution $p \in \text{int}(\Delta_{r-1})$. We would like to test the hypothesis

$$H_0 : p \in \mathcal{M}_{A,h} \quad \text{versus} \quad H_1 : p \notin \mathcal{M}_{A,h}.$$
Suppose that the null hypothesis is true: \( p \in \mathcal{M}_{A,h} \). So there is a parameter \( \theta \in \mathbb{R}^k > 0 \) such that \( p_j = Z(\theta)^{-1} h_j \theta^a_j \) for \( j = 1, 2, \ldots, r \). Let \( u \in \mathbb{N}^r \) be the vector of counts or summary contingency table: that is, \( u_j = \# \{ i : X(i) = j \} \) for \( j \in [r] \). Then the probability of observing the table \( u \) given a parameter value \( \theta \) is

\[
L(u|\theta) = \binom{n}{u} h^n \theta^A u Z(\theta)^{-n}
\]

where \( \binom{n}{u} = \frac{n!}{u_1! \cdots u_r!} \) is the multinomial coefficient. Let \( t : \mathbb{N}^r \to \mathbb{R} \) be a “nice” statistic which is zero if and only if \( u/n \in \mathcal{M}_{A,h} \) and increases away from \( \mathcal{M}_{A,h} \). Then we could calculate the \( p \)-value

\[
E_p[1_{t(v) > t(u)}(V)]
\]

where the expected value is taken over all \( v \in \mathbb{N}^r \) such that \( ||v|| = n \), the sample size, sampled with respect to the distribution \( p \). Here \( 1_{t(v) > t(u)}(v) \) is the indicator function of the event that \( t \) is greater than the value of the test statistics on the data point \( u \). The random variable \( V \) is a multinomial random variable sampled with respect to the probability distribution \( p \).

If the \( p \)-value is small, then \( u/n \) is far from a distribution that lies in the model \( \mathcal{M}_{A,h} \) (or, more precisely, the value of the statistic \( t(u) \) was unlikely to be so large if the true distribution belonged to the model). In this case, we reject the null hypothesis.

Of course, it is not possible to actually perform such a test as indicated since it depends on knowing the underlying distribution \( p \), which is unknown and unknowable. If we knew \( p \), we could just test directly whether \( p \in \mathcal{M}_{A,h} \), or not. There are two ways out of this dilemma: asymptotics and conditional inference.

In the asymptotic perspective, we choose a test statistic \( t \) such that as the sample size \( n \to \infty \), the probability density of \( t(v) > t(u) \) converges to a distribution that does not depend on the true underlying distribution \( p \in \mathcal{M}_{A,h} \). The \( p \)-value computation can then be approximated based on this asymptotic assumption.

The usual choice of a test statistic which is made for log-linear models is Pearson’s \( X^2 \) statistic, which is defined as

\[
X_n^2(u) = \sum_{j=1}^{r} \frac{(u_j - \hat{u}_j)^2}{\hat{u}_j}
\]

where \( \hat{u} = n \hat{p} \) is the maximum likelihood estimate of counts under the model \( \mathcal{M}_{A,h} \). Note that \( \hat{p} \) can be computed using iterative proportional scaling when there are no exact formulas for it, as described in Chapter 7. A
key results about the limiting distribution of Pearson’s $X^2$ statistics is the following proposition, whose proof can be found, for example, in [Agr90] Section 12.3.3.

**Proposition 9.1.1.** If the joint distribution of $X$ is given by a distribution $p \in M_{A,h}$, then

\[
\lim_{n \to \infty} P(X^2(V) \geq t) = P(\chi^2_{df} \geq t) \text{ for all } t \geq 0,
\]

where $df = r - 1 - \dim M_{A,h}$ is the codimension or number of degrees of freedom of the model. In other words, for a distribution lying in the model, the Pearson $X^2$ statistic converges to a chi-square distribution with $df$ degrees of freedom.

The following example illustrates the application of the asymptotic $p$-value calculation.

**Example 9.1.2.** Consider the following data from [EGG89] which categorizes 132 schizophrenic hospital patients based on the length of hospital stay (in year $Y$) and the frequency $X$ with which they were visited by relatives:

<table>
<thead>
<tr>
<th>Visitors status</th>
<th>$2 \leq Y &lt; 10$</th>
<th>$10 \leq Y &lt; 20$</th>
<th>$20 \leq Y$</th>
<th>Totals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visited regularly</td>
<td>43</td>
<td>16</td>
<td>3</td>
<td>62</td>
</tr>
<tr>
<td>Visited rarely</td>
<td>6</td>
<td>11</td>
<td>10</td>
<td>27</td>
</tr>
<tr>
<td>Visited never</td>
<td>9</td>
<td>18</td>
<td>16</td>
<td>43</td>
</tr>
<tr>
<td>Totals</td>
<td>58</td>
<td>45</td>
<td>29</td>
<td>132</td>
</tr>
</tbody>
</table>

The most basic hypothesis one could test for this data is whether or not $X$ and $Y$ are independent. The maximum likelihood estimate for the data under the independence model is

\[
\begin{pmatrix}
27.2424 & 21.1364 & 13.6212 \\
11.8636 & 9.20455 & 5.93182 \\
18.8939 & 14.6591 & 9.44697
\end{pmatrix}
\]

The value of Pearson’s $X^2$-statistic at the data table $u$ is $X^2(u) = 32.3913$. The model of independence $M_{X \perp \perp Y}$ is four dimensional inside the probability simplex $\Delta_8$, so this model has $df = 4$. The probability that a $\chi^2(4)$ random variable is greater than $X^2(u) = 35.17109$ is approximately $4.2842 \times 10^{-7}$. This asymptotic $p$-value is very small, in which case the asymptotic test tells us we should reject the null hypothesis of independence. The following code performs the asymptotic test in R

```r
tab <- as.table(matrix(c(43, 16, 3, 6, 11, 10, 9, 18, 16), nrow = 3, byrow = TRUE))
```
```r
dimnames(tab) <- list(X = c("X1","X2","X3"), Y = c("Y1","Y2","Y3"))
tab
MASS::loglm(~ X + Y, data = tab) # asymptotic test
```

A similar strategy is based on the likelihood ratio test, where we use the \(G\)-statistic, instead of the \(X^2\)-statistic. The \(G\)-statistic is defined by:

\[
G(u) = 2 \sum_{j=1}^{r} u_j (\log u_j - \log \hat{u}_j).
\]

As with the \(X^2\)-statistic, the \(G\) statistic converges to a chi-square distribution with \(df = r - 1 - \dim \mathcal{M}_{A,h}\) degrees of freedom, which follows from results in Section 7.4 since \(\mathcal{M}_{A,h}\) is smooth everywhere.

Appealing to an asymptotic distribution is natural when viewing a statistical problem through the lens of probability theory. On the other hand, in most cases the sample size is quite small, and in particular we do not have \(n \to \infty\). The typical rule of thumb that has been used in these problems if “most” entries of \(u\) are greater than 5, then the asymptotics are reasonably accurate. However, since many large contingency tables are sparse, and data is rare and expensive to obtain, this suggests that other strategies besides the asymptotic might be appropriate. Thus we are posed the question: Is there any other way to eliminate the dependence of the non-asymptotic \(p\)-value on the unknown parameter values \(\theta\)? This leads to the framework of conditional inference.

The conditional inference framework is based on the following observation. Let

\[
\mathcal{F}(u) = \{ v \in \mathbb{N}^r : Av = Au \}
\]

denote the fiber of the table \(u\) with respect to the the sufficient statistic \(A\). The conditional likelihood function \(L(v|v \in \mathcal{F}(u), \theta)\) does not depend on the unknown parameter \(\theta\). Indeed, this likelihood function is

\[
L(v|v \in \mathcal{F}(u), \theta) = \frac{\binom{n}{v} \theta^Av Z(\theta)^{-n}}{\sum_{v \in \mathcal{F}(u)} \binom{n}{v} \theta^Av Z(\theta)^{-n}}
\]

and since \(Av = Au\) for all \(v \in \mathcal{F}(u)\), all the terms involving \(\theta\) drop out and we are left with

\[
L(v|v \in \mathcal{F}(u), \theta) = L(u|v \in \mathcal{F}(u)) = \frac{\binom{n}{v}}{\sum_{v \in \mathcal{F}(u)} \binom{n}{v} h^v}.
\]

The resulting distribution on the fiber \(\mathcal{F}(u)\) where \(P(v) \propto \binom{n}{v} h^v\) is called the generalized hypergeometric distribution. Thus, conditional inference provides us with a means for computing a \(p\)-value that does not depend on the
unknown parameter $\theta$. However, we are left with computing or approximating the sum

$$\frac{1}{\#\mathcal{F}(u)} \sum_{v \in \mathcal{F}(u)} 1_{t(v) \geq t(u)} L(u|v \in \mathcal{F}(u)).$$

In addition to Pearson’s $X^2$-statistic and the $G$-statistic, another choice is the sum up the probabilities of all the tables in the fiber which have a lower hypergeometric probability than the observed table. Thus we have a $p$-value measuring the probability that the given table was more likely to occur than a random table in the fiber.

**Example 9.1.3.** We now apply the Fisher’s exact test to the data from Example 9.1.2. In this case, the fiber consists of 258909 $3 \times 3$ tables. For each of these tables, we determine in the $X^2$ statistic is greater than that of the data table, and sum of the probabilities of all such tables. The resulting $p$-value is $3.18356 \times 10^{-7}$, which is on the same order of magnitude as the $p$-value for the asymptotic test. Both tests suggest that we should reject the null hypothesis.

In the previous example, all the cell entries are greater than 5, so the asymptotics and Fisher’s exact test give similar results. Fisher’s exact test is mainly of interested in the situation where the table is sparse, with small cell entries. Even in this case, the fibers $\mathcal{F}(u)$ are enormous and impossible to enumerate. Furthermore, it is unlikely that there exists any analytic expression for (9.1.1). So the usual strategy is to approximate the exact test $p$-value by randomly generating samples from $\mathcal{F}(u)$ with respect to the generalized hypergeometric distribution. This suggests the following problem, which will occupy us for the majority of this chapter.

**Problem 9.1.4.** Generate random samples from the fiber $\mathcal{F}(u)$ with respect to the generalized hypergeometric distribution $P(v) \propto \binom{n}{v} h^v$.

### 9.2. Markov Bases

As discussed in the previous section, to perform Fisher’s exact test we must generate random samples from the fiber $\mathcal{F}(u)$ with respect to the generalized hypergeometric distribution. Markov bases provide a tool for generating such random samples, which can be applied to any distribution on $\mathcal{F}(u)$, and we focus on that general version of the problem. The problem of generating random tables from fibers with respect to other distributions besides the generalized hypergeometric distribution has other applications in statistics. For example, the Diaconis-Efron test [DE85] requires samples from the uniform distribution on the fiber $\mathcal{F}(u)$. In Bayesian statistics as part of a
larger posterior distribution calculation, we might be required to generate random samples from essentially arbitrary distributions on $\mathcal{F}(u)$.

**Definition 9.2.1.** Let $A \in \mathbb{Z}^{k \times r}$. Let $\ker \mathbb{Z} A = \{ v \in \mathbb{Z}^r : Av = 0 \}$ be the integer kernel of $A$. A finite set $B \subseteq \ker \mathbb{Z} A$ is called a Markov basis if for all $u \in \mathbb{N}^n$ and $u' \in \mathcal{F}(u)$, there is a sequence $v_1, \ldots, v_L \in B$ such that

$$u' = u + \sum_{k=1}^L v_k \quad \text{and} \quad u + \sum_{k=1}^l v_k \geq 0 \text{ for all } l = 1, \ldots, L.$$  

The elements of the Markov basis are called moves.

An alternate description of a Markov basis is via a graph on the fiber. To the fiber $\mathcal{F}(u)$ and the set of moves $B \subseteq \ker \mathbb{Z} A$ we make a graph $\mathcal{F}(u)_B$ as follows. The vertices of $\mathcal{F}(u)_B$ are the elements of $\mathcal{F}(u)$. Two elements $v, v' \in \mathcal{F}(u)$ are connected by an edge if $v - v' \in B$ or $v' - v \in B$. To say that $B$ is a Markov basis for $A$ is equivalent to saying that the graph $\mathcal{F}(u)_B$ is connected for all $u$.

We will discuss the existence and computation of Markov bases later in this section, and in Section 9.3 the construction of Markov bases in the important case of hierarchical models. The import of Markov bases is that they can be used to generate random samples from a distribution on $\mathcal{F}(u)$ using the Metropolis-Hastings algorithm.

**Algorithm 9.2.2** (Metropolis-Hastings).

**Input:** A contingency table $u \in \mathbb{N}^r$, a Markov basis $B$ for the model $\mathcal{M}_A$, and a probability distribution $p$ on $\mathcal{F}(u)$ which gives nonzero probability to every $u' \in \mathcal{F}(u)$.

**Output:** A sequence of tables $u_n \in \mathcal{F}(u)$.

**Step 1:** Initialize $u_1 = u$.

**Step 2:** For $t = 1, 2, \ldots$ repeat the following steps:

(i) Select uniformly at random a move $v_t \in B$.

(ii) If $\min(u_t + v_t) < 0$, then set $u_{t+1} = u_t$, else set

$$u_{t+1} = \begin{cases} u_t + v_t & \text{with probability } q \\ u_t & \text{with probability } 1 - q \end{cases},$$

where

$$q = \min \left\{ 1, \frac{p(u_t + v_t)}{p(u_t)} \right\}.$$ 

**Step 3:** Output the sequence $u_t$.

**Theorem 9.2.3.** The output sequence of tables $u_t$ from Algorithm 9.2.2 is an aperiodic, reversible, and irreducible Markov chain that has stationary distribution equal to the distribution $p$ on $\mathcal{F}(u)$.
A proof of this theorem can be found, for example, in [DS98, Lemma 2.1] or [RC99, Chapter 6]. The consequence of Theorem 9.2.3 is that if we let the Markov chain in the Metropolis-Hastings algorithm run long enough, then we can draw samples from the distribution \( p \) on \( F(u) \), and hence use those samples to approximate the p-value from (9.1.1). It remains a major unsolved research problem to determine bounds on the time until a sample that is drawn is close to the desired distribution. This time is called the mixing time of the Markov chain (see [LPW09] for an in-depth treatment). Even in the case of attempting to sample from the uniform distribution on the fiber \( F(u) \), the mixing time remains unknown (but see [Win16] for related results). In practice it is possible to increase the connectivity by using integer multiples or linear combinations of the moves \( v \in B \).

One important feature of the Metropolis-Hastings algorithm is that it is not necessary to be able to compute exactly the probability of the particular table \( p(u) \), one need only know this probability distribution up to the normalization constant. Indeed, the only place in the Metropolis-Hastings algorithm where the probability distribution \( p \) appears is in the calculation of \( q \), and the normalizing constant drops out of the ratio \( p(u_t + v_t)/p(u_t) \).

This makes the application of the algorithm for the generalized hypergeometric distribution feasible, since the nonnormalized version \( p(u) \propto \binom{n}{u} h^u \) is tractable. Similarly for the uniform distribution, the normalizing constant is the cardinality of the fiber \( F(u) \), but the Metropolis-Hastings algorithm does not require us to know this difficult-to-obtain quantity.

**Example 9.2.4** (Metropolis-Hastings for the Uniform Distribution). Note that for the uniform distribution, the quantity \( p(u_t + v_t)/p(u_t) \) is always equal to one. Hence, provided that \( \min(u_t + v_t) \geq 0 \), we always move to \( u_t + v_t \).

Markov bases are fundamentally connected to computational algebra via toric ideals. Recall, that the toric ideal \( I_A \) associated to the integer matrix \( A \), is the vanishing ideal of the monomial parametrization \( \phi^A \). By Proposition 6.2.4

\[
I_A = \langle p^u - p^{u'} : u, u' \in \mathbb{N}^r \text{ and } Au = Au' \rangle
\]

so the toric ideal \( I_A \) gives an encoding of the integer lattice \( \ker_Z A \). In particular, if we are given a vector \( v \in \ker_Z A \), we can write \( v = v^+ - v^- \) where the coordinates of \( v^+ \) and \( v^- \) are given by \( v^+_j = \max(v_j, 0) \) and \( v^-_j = -\max(-v_j, 0) \). To the vector \( v \), we associate the binomial \( p^{v^+} - p^{v^-} \in I_A \). Conversely, if \( p^u - p^{u'} \in I_A \), then \( u - u' \in \ker_Z A \). The following theorem of Diaconis and Sturmfels [DS98] connects the toric ideal \( I_A \) to Markov bases.
Theorem 9.2.5 (Fundamental Theorem of Markov Bases). A subset $B \subseteq \ker Z A$ is a Markov basis for $A$ if and only if the corresponding set of binomials $\{p^{v^+} - p^{v^-} : v \in B\}$ is a generating set for the toric ideal $I_A$.

Proof. ($\Rightarrow$) Let $B$ be a Markov basis for $A$. We will show that the set of binomials $B = \{p^{v^+} - p^{v^-} : v \in B\}$ is a generating set of $I_A$. According to Proposition 6.2.4, it suffices to show that any binomial $p^u - p^{u'} \in I_A$ is in the ideal generated by the binomials in $B$. Since $Au = Au'$ and $B$ is a Markov basis, there is a sequence of moves $v_1, \ldots, v_L \in B$ such that

$$u' = u + \sum_{k=1}^L v_k \quad \text{and} \quad u + \sum_{k=1}^l v_k \geq 0 \quad \text{for all} \quad l = 1, \ldots, L.$$ 

This implies that

$$p^{u'} = p^u + \sum_{k=1}^L p^{u+v_1+\cdots+v_{k-1}-v_k^-} (p^{v_k^+} - p^{v_k^-})$$

and each of the exponent vectors

$$u + v_1 + \cdots + v_{k-1} - v_k^-$$

is nonnegative. Thus, $p^u - p^{u'}$ is in the ideal generated by $B$.

($\Leftarrow$) Conversely, suppose that $B$ is a binomial generating set for the ideal $I_A$. Then any $p^u - p^{u'} \in I_A$ has an expression as

$$p^u - p^{u'} = \sum_{k=1}^L p^{m_k} (p^{v_k^+} - p^{v_k^-}).$$

This sum can be arranged in such a way that $p^{m_k} p^{v_k^+} = p^u$ and each successive pair of terms $p^{m_k} p^{v_k^-} = p^{m_{k+1}} p^{v_{k+1}^+}$. This forces $p^{m_L} p^{v_L^-} = p^{u'}$, and implies that

$$u = u' + \sum_{k=1}^L v_k \quad \text{and} \quad u' + \sum_{k=1}^l v_k \geq 0 \quad \text{for all} \quad l = 1, \ldots, L.$$ 

Thus, $B$ is a Markov basis for $A$. \qed

Because of the Fundamental Theorem of Markov Bases, a binomial generating set of a toric ideal is often called a Markov basis. One immediate consequence of Theorem 9.2.5 is that Markov bases exist; that is, for any $A$, there exists a finite set of moves $B \subset \ker Z A$ which connects all the fibers $F(u)$. This follows from the Fundamental Theorem of Markov Bases plus the Hilbert Basis Theorem, since the ideal $I_A$ must have a finite generating set consisting of binomials. A second consequence of Theorem 9.2.5 is a
method for computing Markov bases: since $I_A$ is the homogeneous vanishing ideal of the discrete exponential family $\mathcal{M}_A$, we can compute a binomial generating set using implicitization via Gröbner basis calculation. In fact, the special combinatorial nature of toric ideals yields sophisticated lattice-based algorithms for computing generating sets and Gröbner bases of toric ideals. These algorithms are implemented in the software 4ti2 [HH03]. 4ti2 can be run as a stand-alone program, as part of the lattice point package LattE [BBDL+15], or run from inside Macaulay2 as the following example illustrates.

**Example 9.2.6.** Consider the matrix

$$
A = \begin{pmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
\end{pmatrix}
$$

Letting $u = (u_{11}, u_{12}, u_{13}, u_{21}, u_{22}, u_{23}, u_{31}, u_{32}, u_{33})^T$, we see that $Au = (u_{1+}, u_{2+}, u_{3+}, u_{+1}, u_{+2}, u_{+3})^T$ is the vector of sufficient statistics of the independence model for two discrete random variables with 3 states. We compute the Markov basis in Macaulay2 using the following code:

```plaintext
loadPackage "FourTiTwo"
A = matrix{
  {1,1,1,0,0,0,0,0,0},
  {0,0,0,1,1,1,0,0,0},
  {0,0,0,0,0,0,1,1,1},
  {1,0,0,1,0,0,1,0,0},
  {0,1,0,0,1,0,0,1,0},
  {0,0,1,0,0,1,0,0,1},
};

toricMarkov A
```

which produces the output:

```
004 = |
0 0 0 0 1 -1 0 -1 1 |
0 0 0 1 -1 0 -1 1 0 |
0 0 0 1 0 -1 -1 0 1 |
0 1 -1 0 -1 1 0 0 0 |
0 1 -1 0 0 0 -1 1 1 |
1 -1 0 -1 1 0 0 0 0 |
1 -1 0 0 0 0 -1 1 0 |
1 0 -1 -1 0 1 0 0 0 |
1 0 -1 0 0 0 -1 0 1 |
```
oo4: Matrix ZZ <--- ZZ

The rows of this output matrix are the elements of the Markov basis. Written as $3 \times 3$ contingency tables, these are:

$$
\begin{pmatrix}
0 & 0 & 0 \\
0 & 1 & -1 \\
0 & -1 & 1 \\
\end{pmatrix},
\begin{pmatrix}
0 & 0 & 0 \\
1 & -1 & 0 \\
-1 & 1 & 0 \\
\end{pmatrix}, \ldots,
\begin{pmatrix}
1 & 0 & -1 \\
0 & 0 & 0 \\
-1 & 0 & 1 \\
\end{pmatrix}.
$$

According to Theorem 9.2.5, these tables convert to binomials which are a generating set for $I_A$:

$$
p_{22}p_{33} - p_{23}p_{32}, \quad p_{21}p_{32} - p_{22}p_{31}, \quad \ldots, \quad p_{11}p_{33} - p_{13}p_{31}.
$$

Another consequence of Theorem 9.2.5 is that it gives us a useful combinatorial procedure to construct a generating set of a toric ideal. That is, to prove that a given set of binomials is a generating set of a toric ideal $I_A$ we can show that every fiber $F(u)$ is connected by the corresponding set of moves.

**Theorem 9.2.7.** Let $e_1, \ldots, e_{r_1}$ and $e'_1, \ldots, e'_{r_2}$ denote the standard unit vectors in $\mathbb{R}^{r_1}$ and $\mathbb{R}^{r_2}$, respectively. Let $A$ be the matrix whose columns are the $r_1r_2$ vectors $e_i \oplus e'_j$ with $i_1 \in [r_1]$ and $i_2 \in [r_2]$. So $A : \mathbb{Z}^{r_1 \times r_2} \to \mathbb{Z}^{r_1} \oplus \mathbb{Z}^{r_2}$ represents the linear transformation that computes the row and column sums of and $r_1 \times r_2$ tables. Let

$$
\mathcal{B}_{r_1r_2} := \{ e_{i_1j_1} + e_{i_2j_2} - e_{i_1j_2} - e_{i_2j_1} : i_1, j_1 \in [r_1], i_2, j_2 \in [r_2] \}
$$

where $e_{11}, \ldots, e_{r_1r_2}$ denote the standard unit vectors in $\mathbb{R}^{r_1 \times r_2}$. Then $\mathcal{B}_{r_1r_2}$ is a Markov basis for $A$.

**Proof.** Let $u \neq v$ be two non-negative integral tables that have the same row and column sums. It suffices to show that there is an element $b \in \mathcal{B}_{r_1r_2}$, such that $u + b \geq 0$ and $\|u - v\|_1 > \|u + b - v\|_1$, because this implies that we can use elements of $\mathcal{B}_{r_1r_2}$ to bring points in the same fiber closer to one another. Since $u$ and $v$ are not equal and $Au = Av$, there is at least one positive entry in $u - v$. Without loss of generality, we may suppose $u_{11} - v_{11} > 0$. Since $u - v \in \ker_Z A$, there is an entry in the first row of $u - v$ that is negative, say $u_{12} - v_{12} < 0$. By a similar argument $u_{22} - v_{22} > 0$. But this implies that we can take $b = e_{12} + e_{21} - e_{11} - e_{22}$ which attains $\|u - v\|_1 > \|u + b - v\|_1$ and $u + b \geq 0$ as desired. \Box

Note that the Markov basis in Theorem 9.2.7 is a minimal Markov basis, that is, no move can be omitted to obtain a set that satisfies the Markov basis property. Indeed, if, for example, the move $e_{11} + e_{22} - e_{12} - e_{21}$ is
omitted, then the fiber
\[ F(e_{11} + e_{22}) = \{ e_{11} + e_{22}, e_{12} + e_{21} \} \]
cannot be connected by any of the remaining moves of \( B_{r_1r_2} \).

Theorem 9.2.7 on Markov bases of two-way contingency tables allows us to fill in a missing detail from our discussions on conditional independence from Chapter 4.

Corollary 9.2.8. The homogeneous vanishing ideal of the independence model on two discrete random variables is the prime toric ideal
\[ I_{X \perp \perp Y} = \langle p_{i_1i_2}p_{j_1j_2} - p_{i_1j_2}p_{j_1i_2} : i_1, j_1 \in [r_1], i_2, j_2 \in [r_2] \rangle. \]

Proof. Discrete random variables \( X \) and \( Y \) are independent if and only if
\[ P(X = i, Y = j) = P(X = i)P(Y = j) \]
for all \( i \) and \( j \). Treating the marginal probability distributions as parameters we can express this as
\[ P(X = i, Y = j) = \frac{1}{Z} \alpha_i \beta_j \]
where \( Z \) is a normalizing constant. Hence, the model of independence is a discrete exponential family. The sufficient statistics of that family are the row and column sums of a table \( u \in \mathbb{N}^{r_1 \times r_2} \). Since the coefficient vector \( h = 1 \), the vector of ones, we see that the homogeneous vanishing ideal of \( \mathcal{M}_{X \perp \perp Y} \) is the toric ideal associated to the matrix \( A \) from Theorem 9.2.7.

Each of the moves in the Markov basis \( B_{r_1r_2} \)
\[ e_{i_1i_2} + e_{j_1j_2} - e_{i_1j_2} - e_{j_1i_2} \]
translates into a binomial
\[ p_{i_1i_2}p_{j_1j_2} - p_{i_1j_2}p_{j_1i_2}. \]
The fundamental theorem of Markov bases says that these binomials generate the toric ideal. \( \square \)

Example 9.2.9. Example of a contingency table and performing test of independence using Markov bases.

As a second example in this section, we consider the model of Hardy-Weinberg equilibrium, which represents a famous use of the exact test and Monte Carlo computations from the paper of Guo and Thompson [GT92]. The Hardy-Weinberg model is a model for a discrete random variable \( X \) whose states are unordered pairs \( ij \) with \( i, j \in [r] \). The probability distribution of \( X \) is given by
\[ P(X = ij) = \begin{cases} 2\theta_i \theta_j & i \neq j \\ \theta_i^2 & i = j \end{cases} \]
The Hardy-Weinberg distribution is the result of taking two independent draws from a multinomial distribution with parameter $\theta = (\theta_1, \ldots, \theta_r)$. This special instance of a multinomial model has a special name because of its applications in biology. Suppose that a gene has $r$ alleles (i.e. different versions). In a diploid species, each organism has two copies of each chromosome and hence two copies of each gene. The genotype of each organism is, hence, an unordered pair of elements from $[r]$. If the population is well-mixed and there is no positive or negative selection against any combinations of alleles, the population frequencies will be in Hardy-Weinberg equilibrium, since the probability of a genotype will just be the product of the probabilities of each allele times a multinomial coefficient. Hardy-Weinberg equilibrium was postulated in [2]. To test whether a given data set is consistent with the model of Hardy-Weinberg equilibrium, we need to perform an exact test.

In particular, consider the following data set from Guo and Thompson [GT92] of genotype frequencies in Rhesus data, which we display as an upper triangular matrix:

<table>
<thead>
<tr>
<th></th>
<th>1236</th>
<th>120</th>
<th>18</th>
<th>982</th>
<th>32</th>
<th>2582</th>
<th>6</th>
<th>2</th>
<th>115</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>0</td>
<td>55</td>
<td>1</td>
<td>132</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>7</td>
<td>0</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>249</td>
<td>12</td>
<td>1162</td>
<td>4</td>
<td>0</td>
<td>53</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>29</td>
<td>0</td>
<td>1</td>
<td>149</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1312</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In spite of the large sample size in this example, asymptotic approximations appear unwise since there are so many small entries in the table, and it is also relatively sparse.

In general, data for the model of Hardy-Weinberg equilibrium is a upper triangular data table $u = (u_{ij})$ such that $1 \leq i \leq j \leq r$. The sufficient statistics for this model are the sums for each $i$

$$\sum_{j=1}^{i} u_{ji} + \sum_{j=i}^{r} u_{ij}$$

which gives the number of times that the allele $i$ appears in the population. Note that we count the diagonal entry $u_{ii}$ twice. Writing this out in matrix
form for $r = 4$ yields the matrix:
\[
\begin{pmatrix}
2 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 2 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
\end{pmatrix}.
\]

**Theorem 9.2.10.** The Markov basis for the model of Hardy-Weinberg equilibrium consists of the following family of moves
\[
B_r = \{ e_{ij} + e_{kl} - e_{ik} - e_{jl} : i, j, k, l \in [r] \}
\]

In the theorem, we use the convention that $e_{ij} = e_{ji}$. Note that this set of moves includes moves like $e_{ii} + e_{jj} - 2e_{ij}$ so that this is an example of a Markov basis that does not consist only of moves whose coefficients are $1, -1, 0$. Applying the fundamental theorem of Markov bases, we can also state Theorem 9.2.10 in the language of toric ideals. That is, translating the moves in $B_r$ into binomials, we also have the following equivalent representation.

**Theorem 9.2.11.** The homogeneous vanishing ideal of the model of Hardy-Weinberg equilibrium is the ideal generated by $2 \times 2$ minors of the symmetric matrix:
\[
\begin{pmatrix}
2p_{11} & p_{12} & p_{13} & \cdots & p_{1r} \\
p_{12} & 2p_{22} & p_{23} & \cdots & p_{2r} \\
p_{13} & p_{23} & 2p_{33} & \cdots & p_{3r} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
p_{1r} & p_{2r} & p_{3r} & \cdots & 2p_{rr}
\end{pmatrix}.
\]

### 9.3. Markov Bases for Hierarchical Models

Among the most important discrete exponential families are the hierarchical log-linear models. These statistical models are for collections of random variables, and a simplicial complex is used to encode interaction factors among the random variables. The sufficient statistics of a hierarchical model are also easily interpretable as lower-dimensional margins of a contingency table. Hierarchical models are, thus, a broad generalization of the independence model whose Markov basis we have seen in Theorem 9.2.7. However, it is usually not straightforward to describe their Markov bases and significant effort has been put towards developing theoretical tools for describing Markov bases for these models.

**Definition 9.3.1.** For a set $S$, let $2^S$ denote its power set, that is the set of all of its subsets. A *simplicial complex* with ground set $S$ is a set $\Gamma \subseteq 2^S$
such that if $F \in \Gamma$ and $F' \subseteq F$ then $F' \in \Gamma$. The elements of $\Gamma$ are called the \textit{faces} of $\Gamma$ and the inclusion maximal faces are the \textit{facets} of $\Gamma$.

Note Definition 9.3.1 is more properly called called an abstract simplicial complex. This abstract simplicial complex has a geometric realization where a face $F \in \Gamma$ with $i + 1$ elements yields an $i$-dimensional simplex in the geometric realization. To describe a simplicial complex we need only list its facets. We will use the bracket notation from the theory of hierarchical log-linear models [Chr97]. For instance, $\Gamma = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$.

The geometric realization of $\Gamma$ is the boundary of a triangle.

Hierarchical models are log-linear models, so they can be described as $\mathcal{M}_A$ for a suitable matrix $A$ associated to the simplicial complex $\Gamma$. However, it is usually easiest to describe this model first by giving their monomial parametrization, and then recovering the associated matrix. Both descriptions are heavy on notation.

We use the following convention for writing subindices. If $i = (i_1, \ldots, i_m) \in \mathcal{R}$ and $F = \{f_1, f_2, \ldots, \} \subseteq [m]$ then $i_F = (i_{f_1}, i_{f_2}, \ldots)$. For each subset $F \subseteq [m]$, the random vector $X_F = (X_f)_{f \in F}$ has the state space $\mathcal{R}_F = \prod_{f \in F} [r_f]$.

**Definition 9.3.2.** Let $\Gamma \subseteq 2^{[m]}$ be a simplicial complex and let $r_1, \ldots, r_m \in \mathbb{N}$. For each facet $F \in \Gamma$, we introduce a set of $\#\mathcal{R}_F$ positive parameters $\theta_{i_F}^{(F)}$. The \textit{hierarchical log-linear model} associated with $\Gamma$ is the set of all probability distributions

\begin{equation}
\mathcal{M}_\Gamma = \left\{ p \in \Delta_{\mathcal{R} - 1} : p_i = \frac{1}{Z(\theta)} \prod_{f \in \text{facet}(\Gamma)} \theta_{i_f}^{(F)} \text{ for all } i \in \mathcal{R} \right\},
\end{equation}

where $Z(\theta)$ is the normalizing constant (or partition function)

\[ Z(\theta) = \sum_{i \in \mathcal{R}} \prod_{F \in \text{facet}(\Gamma)} \theta_{i_F}^{(F)}. \]

In the parameters $\theta_{i_F}^{(F)}$ are sometimes called potential functions, especially when hierarchical models are used in their relationship to graphical models.

**Example 9.3.3** (Independence). Let $\Gamma = [1][2]$. Then the hierarchical model consists of all positive probability matrices $(p_{i_1 i_2})$

\[ p_{i_1 i_2} = \frac{1}{Z(\theta)} \theta_{i_1}^{(1)} \theta_{i_2}^{(2)} \]
9.3. Markov Bases for Hierarchical Models

where \( \theta^{(j)} \in (0, \infty)^{r_j}, j = 1, 2 \). That is, the model consists of all positive rank one matrices. It is the positive part of the model of independence \( \mathcal{M}_{X \perp \perp Y} \), or in algebraic geometric language, the positive part of the Segre variety. The normalizing constant in this case is

\[
Z(\theta) = \sum_{i_1=1}^{r_1} \sum_{i_2=1}^{r_2} \theta_{i_1} \theta_{i_2}.
\]

In this case, the partition function factorizes as

\[
Z(\theta) = \left( \sum_{i_1=1}^{r_1} \theta_{i_1} \right) \left( \sum_{i_2=1}^{r_2} \theta_{i_2} \right).
\]

Complete factorization of the partition function as in this example is a rare phenomenon. \( \square \)

Example 9.3.4 (No 3-way interaction). Let \( \Gamma = [12][13][23] \) be the boundary of a triangle. The hierarchical model \( \mathcal{M}_\Gamma \) consists of all \( r_1 \times r_2 \times r_3 \) tables \( (p_{i_1 i_2 i_3}) \) with

\[
p_{i_1 i_2 i_3} = \frac{1}{Z(\theta)} \theta^{(12)}_{i_1 i_2} \theta^{(13)}_{i_1 i_3} \theta^{(23)}_{i_2 i_3},
\]

for some positive real tables \( \theta^{(12)} \in (0, \infty)^{r_1 \times r_2}, \theta^{(13)} \in (0, \infty)^{r_1 \times r_3}, \) and \( \theta^{(23)} \in (0, \infty)^{r_2 \times r_3} \). Unlike the case of the model of independence, this important statistical model does not have a correspondence with any classically studied algebraic variety. In the case of binary random variables, its implicit representation is the equation

\[
p_{111} p_{122} p_{212} p_{221} = p_{112} p_{121} p_{211} p_{222}.
\]

That is, the log-linear model consists of all positive probability distributions that satisfy this quartic equation. \( \square \)

Example 9.3.5 (Something more general). Let \( \Gamma = [12][23][345] \). The hierarchical model \( \mathcal{M}_\Gamma \) consists of all \( r_1 \times r_2 \times r_3 \times r_4 \times r_5 \) probability tensors \( (p_{i_1 i_2 i_3 i_4 i_5}) \) with

\[
p_{i_1 i_2 i_3 i_4 i_5} = \frac{1}{Z(\theta)} \theta^{(12)}_{i_1 i_2} \theta^{(23)}_{i_2 i_3} \theta^{(345)}_{i_3 i_4 i_5},
\]

for some positive real tables \( \theta^{(12)} \in (0, \infty)^{r_1 \times r_2}, \theta^{(23)} \in (0, \infty)^{r_2 \times r_3}, \) and \( \theta^{(345)} \in (0, \infty)^{r_3 \times r_4 \times r_5} \). These tables of parameters represent the potential functions. \( \square \)

To begin to understand the Markov bases of hierarchical models, we must come to terms with the 0/1 matrices \( A_\Gamma \) that realize these models in the form \( \mathcal{M}_{A_\Gamma} \). In particular, we must determine what linear transformation the matrix \( A_\Gamma \) represents. Let \( u \in \mathbb{N}^R \) be an \( r_1 \times \cdots \times r_m \) contingency table. For any subset \( F = \{ f_1, f_2, \ldots \} \subseteq [m] \), let \( u|_F \) be the \( r_{f_1} \times r_{f_2} \times \cdots \) marginal
table such that \((u_F)_i = \sum_{j \in R_{\{m\}\setminus F}} u_{i,F,j}\). The table \(u_F\) is called the \(F\)-marginal of \(u\).

**Example 9.3.6.** Let \(u\) be the \(2 \times 2 \times 3\) table

\[
\begin{array}{ccc}
  u_{111} & u_{112} & u_{113} \\
  u_{121} & u_{122} & u_{123} \\
  u_{211} & u_{212} & u_{213} \\
  u_{221} & u_{222} & u_{223}
\end{array}
= \begin{array}{ccc}
  4 & 6 & 0 \\
  3 & 0 & 12 \\
  5 & 4 & 1 \\
  17 & 0 & 3
\end{array}
\]

The marginal \(u|_{23}\) is the \(2 \times 3\) table

\[
\begin{array}{ccc}
  (u|_{23})_{11} & (u|_{23})_{12} & (u|_{23})_{13} \\
  (u|_{23})_{21} & (u|_{23})_{22} & (u|_{23})_{23}
\end{array}
= \begin{array}{ccc}
  9 & 10 & 1 \\
  20 & 0 & 15
\end{array}
\]

and the table \(u|_{1}\) is the vector \(\begin{pmatrix} 25 \\ 30 \end{pmatrix}\).

**Proposition 9.3.7.** Let \(\Gamma = [F_1][F_2] \cdots\). The matrix \(A_\Gamma\) represents the linear transformation

\[u \mapsto (u|_{F_1}, u|_{F_2}, \ldots),\]

and the \(\Gamma\)-marginals are minimal sufficient statistics of the hierarchical model \(M_\Gamma\).

**Proof.** We can read off the matrix \(A_\Gamma\) from the parametrization. In the parametrization, the rows of \(A_\Gamma\) correspond to parameters, and the columns correspond to states of the random variables. The rows come in blocks that correspond to the facets \(F\) of \(\Gamma\). Each block has cardinality \(#R_F\). Hence, the rows of \(A_\Gamma\) are indexed by pairs \((F,i_F)\) where \(F\) is a facet of \(\Gamma\) and \(i_F \in R_F\). The columns of \(A_\Gamma\) are indexed by all elements of \(R\). The entry in \(A_\Gamma\) for row index \((F,i_F)\) and column index \(j \in R\) equals 1 if \(j_F = i_F\) and equals zero otherwise. This description follows by reading the parametrization from \([9.3.1]\) down the column of \(A_\Gamma\) that corresponds to \(p_j\). The description of minimal sufficient statistics as marginals comes from reading this description across the rows of \(A_\Gamma\), where the block corresponding to \(F\), yields the \(F\)-marginal \(u|_F\). \(\square\)

**Example 9.3.8.** Returning to our examples above, for \(\Gamma = [1][2]\) corresponding to the model of independence, the minimal sufficient statistics are the row and column sums of \(u \in \mathbb{N}^{r_1 \times r_2}\). That is

\[A_{[1][2]}u = (u_{1}, u_{2}).\]

Above, we abbreviated these row and column sums by \(u_{+}\) and \(u_{+-}\), respectively.

For the model of no 3-way interaction, with \(\Gamma = [12][13][23]\), the minimal sufficient statistics consist of all 2-way margins of the three way table \(u\). That is

\[A_{[12][13][23]}u = (u_{12}, u_{13}, u_{23}).\]
and $A_{[12][13][23]}$ is a matrix with $r_1 r_2 + r_1 r_3 + r_2 r_3$ rows and $r_1 r_2 r_3$ columns.

As far as explicitly writing down the matrix $A_{\Gamma}$, this can be accomplished in a uniform way by assuming that the rows and columns are ordered lexicographically.

**Example 9.3.9.** Let $\Gamma = [12][14][23]$ and $r_1 = r_2 = r_3 = r_4 = 2$. Then $A_{\Gamma}$ is the matrix

\[
\begin{pmatrix}
1111 & 1112 & 1121 & 1211 & 1122 & 1212 & 1221 & 2111 & 2112 & 2121 & 2211 & 2212 & 2221 & 2212 & 2222 \\
11& 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
12& 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
21& 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
22& 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1-1& 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1-2& 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2-1& 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
2-2& 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
-11& 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
-12& 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-21& 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
-22& 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
\end{pmatrix}
\]

where the rows correspond to ordering the facets of $\Gamma$ in the order listed above and using the lexicographic ordering $11 > 12 > 21 > 22$ within each facet. For example, the tenth row of $A_{\Gamma}$, whose label is $1 \cdot 2$, tells us we are looking at the $12$ entry of the $14$ margin.

To perform the asymptotic tests with the hierarchical models, we need to know the dimension of these models, from which we can compute the degrees of freedom (i.e. the codimension). For a proof of this formula see [HS02, Cor 2.7].

**Proposition 9.3.10.** Let $\Gamma$ be a simplicial complex on $[m]$, and $r_1, \ldots, r_m \in \mathbb{N}$. The rank of the matrix $A_{\Gamma}$ associated to these parameters is

\[
\sum_{F \in \Gamma} \prod_{f \in F} (r_f - 1)
\]

where the sum runs over all faces of $\Gamma$. The dimension of the associated hierarchical model $\mathcal{M}_{\Gamma}$ is one less than the rank of $A_{\Gamma}$.

One of the big challenges in the study of Markov bases of hierarchical models is to find descriptions of the Markov bases as the simplicial complex $\Gamma$ and the numbers of states of the random variables vary. When it is not possible to give an explicit description of the Markov basis (that is, a list
of all types of moves needed in the Markov basis), we might still hope to
provide structural or asymptotic information about the types of moves that
could arise. In the remainder of this section, we describe some results of this
type.

For a simplicial complex $\Gamma$, let $G(\Gamma) = \bigcup_{F \in \Gamma} F$ denote the ground set of
$\Gamma$.

**Definition 9.3.11.** A simplicial complex $\Gamma$ is reducible, with reducible de-
composition $(\Gamma_1, S, \Gamma_2)$ and separator $S \subset G(\Gamma)$, if it satisfies $\Gamma = \Gamma_1 \cup \Gamma_2$
and $\Gamma_1 \cap \Gamma_2 = 2^S$. Furthermore, we here assume that neither $\Gamma_1$ nor $\Gamma_2$ is
$2^S$. A simplicial complex is decomposable if it is reducible and $\Gamma_1$ and $\Gamma_2$
are decomposable or simplices (that is, of the form $2^R$ for some $R \subseteq [m]$).

Of the examples we have seen so far, the simplicial complexes $[1][2]$ and
$[12][23][345]$ are decomposable, whereas the simplicial complex $[12][13][23]$ is
not reducible. On the other hand, the complex $\Gamma = [12][13][23][345]$ is re-
ducible but not decomposable, with decomposition $([12][13][23], \{3\}, [345])$.
Also, any complex with only two facets is decomposable.

**Remark 9.3.12.** Comparing Definition 9.3.11 for decomposable complex
and Definition 8.3.4 for a decomposable graph, we see that these notations
are not the same. That is a decomposable graph, when considered as a
simplicial complex is probably not decomposable. To make the two definitions
related, a graph is a decomposable graph if and only if the complex of cliques
of the graph is a decomposable simplicial complex.

For reducible complexes, there is a relatively straightforward procedure
to build the Markov basis for $\Gamma$ from the Markov bases for $\Gamma_1$ and $\Gamma_2$ which
we describe now. To do this, first we introduce tableau notation, which
is a useful unary representation of elements in the lattice $\ker_{\mathbb{Z}} A_\Gamma$, or, of
binomials in the ring $\mathbb{K}[p]$.

To construct the tableau notation for a table $u \in \mathbb{N}^R$ first represent
$u = e_{i_1} + e_{i_2} + \cdots + e_{i_r}$, with each $i_j \in R$. The tableau for $u$ is the array

$$
\begin{array}{c}
 i_1 \\
 i_2 \\
 \vdots \\
 i_r 
\end{array}
$$

Two tableau represent the same table $u$ if and only if they differ by per-
muting rows. Tableau notation also gives a representation for a monomial
$p^u$, and can be used to represent binomials. For an element $u \in \mathbb{Z}^R$, we
write $u = u^+ - u^-$, construct the tableau for each of the nonnegative integer
vectors $u^+$ and $u^-$, and write the formal difference of the resulting tableau.
For instance, the move
\[ e_{i_1i_2} + e_{j_1j_2} - e_{i_1j_2} - e_{i_2j_1} \]
for the independence model translates into the tableau notation
\[
\begin{bmatrix}
i_1 & i_2 \\
j_1 & j_2
\end{bmatrix}
- \begin{bmatrix}
i_1 & j_2 \\
j_1 & i_2
\end{bmatrix}.
\]

In tableau notation, it is easy to compute the marginals of a given table.

**Proposition 9.3.13.** Let \( u \in \mathbb{N}^R \) be a table and \( F \subseteq [m] \), and let \( T \) be the tableau associated to \( u \). Then the tableau for the \( F \)-margin \( u|_F \) is \( T|_F \), obtained from \( T \) by taking the only columns of \( T \) indexed by \( F \).

**Proof.** It suffices to see the statement for a tableau consisting of a single row. This corresponds to a table that is a standard unit vector \( e_i \). Its \( F \)-marginal is precisely the table \( e_i|_F = e_{i_F} \). The index \( i_F = (i_f)_{f \in F} \), which is obtained by taking only the parts of \( i \) indexed by \( F \). \( \square \)

Proposition 9.3.13 allows for us to easily check whether or not two tables \( u \) have the same \( \Gamma \) marginals, equivalently, when an element is in the kernel of \( A_\Gamma \), equivalently, when the corresponding binomial belongs to the toric ideal \( I_{A_\Gamma} \). This is achieved by checking when each of the restricted tableau are the same up to permuting rows.

**Example 9.3.14.** Consider the complex \( \Gamma = [12][13][234] \). Then the following move
\[
\begin{bmatrix}
1 & 1 & 1 & 2 \\
1 & 2 & 2 & 1 \\
2 & 1 & 2 & 2 \\
2 & 2 & 2 & 1
\end{bmatrix}
- \begin{bmatrix}
1 & 1 & 2 & 2 \\
1 & 2 & 1 & 2 \\
2 & 1 & 1 & 2 \\
2 & 2 & 2 & 1
\end{bmatrix}
\]
represented in tableau notation, belongs to \( \text{ker}_{\mathbb{Z}} A_\Gamma \), since for each facet \( F \) of \( \Gamma \), the restriction of the tableaux to the columns indexed by \( F \) represent the same table.

Let \( \Gamma \) be a reducible complex with decomposition \((\Gamma_1,S,\Gamma_2)\). We let \( V_1 = G(\Gamma_1) \setminus S \) and \( V_2 = G(\Gamma_2) \setminus S \), where \( G(\Gamma_i) = \bigcup_{F \in \Gamma_i} F \) is the ground set of \( \Gamma_i \). After renaming the elements of the ground sets, we can assume that \( V_1 = \{1,2,\ldots,m_1\} \), \( S = \{m_1 + 1, \ldots, m_2\} \), and \( V_2 = \{m_2, \ldots, m\} \). With respect to the resulting tripartition \( V_1|S|V_2 \), we can represent the tableau as having three groups of columns, as
\[
\begin{bmatrix}
i_1 & j_1 & k_1 \\
\vdots & \vdots & \vdots \\
i_d & j_d & k_d
\end{bmatrix}
\]
so that, $i_1 \in \mathcal{R}_{V_1}$, \ldots, $k_d \in \mathcal{R}_{V_2}$. Similarly, the tableau involved in representing a move for $A_{\Gamma_1}$ or $A_{\Gamma_2}$ will look like

$$
\begin{bmatrix}
  i_1 & j_1 \\
  \vdots & \vdots \\
  i_d & j_d \\
\end{bmatrix}
- 
\begin{bmatrix}
  j_1 & k_1 \\
  \vdots & \vdots \\
  j_d & k_d \\
\end{bmatrix}
$$

respectively, where the $j_1, \ldots, j_d$ are in $\mathcal{R}_S$.

For a reducible complex $\Gamma$, with decomposition $(\Gamma_1, S, \Gamma_2)$ we first introduce an operation to take moves for $\Gamma_1$ and $\Gamma_2$ to produce moves for $\Gamma$. This is the lifting operation, which we explain now. Let

$$
\begin{bmatrix}
  i_1 & j_1 \\
  \vdots & \vdots \\
  i_d & j_d \\
\end{bmatrix}
- 
\begin{bmatrix}
  i'_1 & j'_1 \\
  \vdots & \vdots \\
  i'_d & j'_d \\
\end{bmatrix}
$$

be a move for $\Gamma_1$. Since $S$ is a face of $\Gamma_1$, we must have that the multisets of $\{j_1, \ldots, j_d\}$ and $\{j'_1, \ldots, j'_d\}$ are the same, by Proposition 9.3.13. Hence, after reordering rows and renaming indices, we can assume this move has the form

(9.3.2) $$
\begin{bmatrix}
  i_1 & j_1 \\
  \vdots & \vdots \\
  i_d & j_d \\
\end{bmatrix}
- 
\begin{bmatrix}
  i'_1 & j_1 \\
  \vdots & \vdots \\
  i'_d & j_d \\
\end{bmatrix}
$$

Now let $k_1, \ldots, k_d \in \mathcal{R}_{V_2}$ and form the move

(9.3.3) $$
\begin{bmatrix}
  i_1 & j_1 & k_1 \\
  \vdots & \vdots & \vdots \\
  i_d & j_d & k_d \\
\end{bmatrix}
- 
\begin{bmatrix}
  i'_1 & j_1 & k_1 \\
  \vdots & \vdots & \vdots \\
  i'_d & j_d & k_d \\
\end{bmatrix}
$$

**Proposition 9.3.15.** Let $\Gamma$ be reducible with decomposition $(\Gamma_1, S, \Gamma_2)$. Consider the move (9.3.2) which belongs to $I_{\Gamma_1}$, and form the move (9.3.3) by applying the lifting procedure above. Then the resulting move (9.3.3) belongs to $I_{\Gamma}$.

**Proof.** Let $T$ and $T'$ be the resulting tableau in (9.3.3). We must show that for any face $F \in \Gamma$, $T|_F = T'|_F$. Since $\Gamma$ is reducible, either $F \in \Gamma_1$ or $F \in \Gamma_2$. In the first case, forming the restriction of $T|_{\mathcal{G}(\Gamma_1)} - T'|_{\mathcal{G}(\Gamma_1)}$ yields the starting move. Since that move belonged to $I_{\Gamma_1}$ we must have $T|_F = T'|_F$. On the other hand if $F \in \Gamma_2$ we already have that $T|_{\mathcal{G}(\Gamma_2)} = T'|_{\mathcal{G}(\Gamma_2)}$ which implies that $T|_F = T'|_F$.

If $\mathcal{F}_1 \subseteq I_{\Gamma_1}$ is a set of moves, then we denote by $\text{Lift}(\mathcal{F}_1)$ the set of all the moves in $I_{\Gamma}$ by applying this procedure, using all possible elements
Proposition 9.3.16. Let $\Gamma$ be a decomposable simplicial complex with two facets $F_1, F_2$ with $S = F_1 \cap F_2$, $V_1 = F_1 \setminus S$, and $V_2 = F_2 \setminus S$. The set of quadratic moves $\text{Quad}(V_1, S, V_2)$ of the form

\begin{equation}
\begin{bmatrix}
i_1 & j & k_1 \\
i_2 & j & k_2 
\end{bmatrix} - \begin{bmatrix}
i_1 & j & k_2 \\
i_2 & j & k_1 
\end{bmatrix}
\end{equation}

form a Markov basis for $I_{\Gamma}$, where $i_1, i_2 \in R_{V_1}$, $j \in R_S$, and $k_1, k_2 \in R_{V_2}$.

Proof. This Markov basis problem reduces to the case of 2-way tables with fixed row and column sums. The details are left to the reader. \qed

The set of quadratic moves $\text{Quad}(V_1, S, V_2)$ associated to a tripartition of the ground set $[m]$, will play an important role in the next Theorem, which gives a description of the Markov bases of reducible hierarchical models in terms of the Markov bases of each of the pieces.

Theorem 9.3.17 (Markov bases of reducible models \cite{DS04, HS02}). Let $\Gamma$ be a reducible simplicial complex with decomposition $(\Gamma_1, S, \Gamma_2)$, and suppose that $F_1$ and $F_2$ are Markov bases for $I_{\Gamma_1}$ and $I_{\Gamma_2}$ respectively. Then

\begin{equation}
G = \text{Lift}(F_1) \cup \text{Lift}(F_2) \cup \text{Quad}(V_1, S, V_2)
\end{equation}

is a Markov basis for $I_{\Gamma}$.

Proof. Let $u$ and $u'$ be two tables belonging to the same fiber with respect to $\Gamma$, and $T$ and $T'$ the corresponding tableaux. We must show that $T$ and $T'$ can be connected using the moves from $G$.

Restricting to the set $|\Gamma_1|$, we know that $T|_{|\Gamma_1|}$ and $T'|_{|\Gamma_1|}$ can be connected using the moves in $F_1$, since $F_1$ is a Markov basis for $\Gamma_1$. Suppose that the move

\[
f = \begin{bmatrix}i_1 & j_1 \\
i_2 & j_2 \\
i_d & j_d \end{bmatrix} - \begin{bmatrix}i_1' & j_1 \\
i_2' & j_2 \\
i_d' & j_d \end{bmatrix}
\]

is to be applied first to $T|_{|\Gamma_1|}$. For it to be possible to apply this move to $T|_{|\Gamma_1|}$, it must be the case that, up to permuting the rows of $T$, the first $d$ rows of $T$ are

\[
\begin{bmatrix}i_1 & j_1 & k_1 \\
i_2 & j_2 & k_2 \\
i_d & j_d & k_d \end{bmatrix}
\]
for some \(k_1, \ldots, k_d\). Hence, we can lift \(f\) to the move
\[
\begin{bmatrix}
i_1 & j_1 & k_1 \\
\vdots & \vdots & \vdots \\
i_d & j_d & k_d
\end{bmatrix}
- \begin{bmatrix}
i'_1 & j_1 & k_1 \\
\vdots & \vdots & \vdots \\
i'_d & j_d & k_d
\end{bmatrix}
\]
in \(\text{Lift}(\mathcal{F}_1)\) which can be applied to \(T\). This same reasoning can be applied to all the moves that are used in sequence to connect \(T|_{\Gamma_1}\) and \(T'|_{\Gamma_1}\). This connect \(T\) with a new tableau \(T''\) which has the property that \(T''|_{\Gamma_1} = T'|_{\Gamma_1}\).

Applying the same reasoning, with respect to \(\Gamma_2\), we can find a set of moves in \(\text{Lift}(\mathcal{F}_2)\) which connect \(T''\) to a new tableau \(T'''\) and such that \(T'''|_{\Gamma_1} = T'|_{\Gamma_1}\). Furthermore, the moves in \(\text{Lift}(\mathcal{F}_2)\) have the property that they do not change the marginal with respect to \(|\Gamma_1|\). Hence \(T'''|_{\Gamma_1} = T'|_{\Gamma_1}\), as well. So \(T''\) and \(T'\) have the same marginals with respect to the simplicial complex whose only facets are \(|\Gamma_1|\) and \(|\Gamma_2|\). By Proposition 9.3.16, \(T''\) and \(T'\) can be connected using the moves in \(\text{Quad}(V_1, S, V_2)\).

Thus, \(\mathcal{G}\) is a Markov basis for \(\Gamma\). □

Using the fact that the Markov basis for the model when \(\Gamma\) is a simplex is just the empty set, and applying induction, one gets a complete description of the Markov bases of decomposable models.

**Corollary 9.3.18** ([Dob03, Tak99]).

If \(\Gamma\) is a decomposable simplicial complex, then the set of moves
\[
\mathcal{B} = \bigcup_{(\Gamma_1, S, \Gamma_2)} \text{Quad}(\Gamma_1, \Gamma_2),
\]
with the union over all reducible decompositions of \(\Gamma\), is a Markov basis for \(A_{\Gamma}\).

**Example 9.3.19.** Consider the four-chain \(\Gamma = [12][23][34]\). This graph has two distinct reducible decompositions with minimal separators, namely \(([12], \{2, 3\}, [34])\) and \(([12][23] , \{3\}, [34])\). Therefore, the Markov basis consists of moves of two types \(\mathcal{D}([12], [23][34])\) and \(\mathcal{D}([12][23], [34])\), which in tableau notation look like:
\[
\begin{bmatrix}
i_1 & j & i_3 & i_4 \\
i'_1 & j' & i'_3 & i'_4
\end{bmatrix}
- \begin{bmatrix}
i_1 & j' & i'_3 & i'_4 \\
i'_1 & j & i_3 & i_4
\end{bmatrix}
\]
and
\[
\begin{bmatrix}
i_1 & i_2 & j & i_4 \\
i'_1 & i'_2 & j' & i'_4
\end{bmatrix}
- \begin{bmatrix}
i_1 & i_2 & j' & i'_4 \\
i'_1 & i'_2 & j & i_4
\end{bmatrix}
\]
Note that the decomposition \(([12][23], \{2, 3\}, [23][34])\) is also a valid reducible decomposition of \(\Gamma\), but it does not produce any new Markov basis elements that were not already accounted for by the other decompositions. □

Theorem 9.3.17 can also be generalized beyond reducible models in some instances using the theory of toric fiber products [Sul07, RS16, EKS14].
9.3. Markov Bases for Hierarchical Models

Theorem 9.3.17 shows that to determine Markov bases of all hierarchical models it suffices to focus on attention on hierarchical models that are not reducible. While there a number of positive results in the literature about the structure of Markov bases in the nonreducible case, a general description is probably impossible, and it is already difficult to describe Markov bases completely in even the simplest nonreducible models.

Example 9.3.20. The simplest nonreducible hierarchical model has simplicial complex $\Gamma = [12][13][23]$. Suppose that $r_1 = r_2 = 3$ and $r_3 = 5$. The Markov basis for this model consists of 2670 moves. Among these are moves that generalize the ones for 2-way tables:

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{vmatrix} - \begin{vmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 2 & 1 & 1 \\ 2 & 2 & 2 \end{vmatrix}$$

but also unfamiliar moves where it is hard to imagine how they generalize to larger tables, for example:

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 5 \\ 1 & 3 & 4 \\ 2 & 1 & 3 \\ 2 & 2 & 1 \\ 2 & 3 & 5 \\ 3 & 1 & 2 \\ 3 & 2 & 4 \\ 3 & 3 & 3 \end{vmatrix} - \begin{vmatrix} 1 & 1 & 2 \\ 1 & 2 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 5 \\ 2 & 1 & 1 \\ 2 & 2 & 5 \\ 2 & 3 & 3 \\ 3 & 1 & 3 \\ 3 & 2 & 2 \\ 3 & 3 & 4 \end{vmatrix}$$

The no-3-way interaction model with $r_1 = r_2 = r_4 = 4$ has 148968 moves in its minimal Markov basis.

One of the remarkable consequences of Corollary 9.3.18 is that the structure of the Markov basis of a decomposable hierarchical log-linear model does not depend on the number of states of the underlying random variables. In particular, regardless of the sizes $r_1, r_2, \ldots, r_m$, the Markov basis for a decomposable model always consists of moves with one-norm equal to four, with a precise and global combinatorial description. The following theorem of De Loera and Onn [DLO06] says that this nice behavior fails, in the worst possible way, already for the simplest non-decomposable model. We fix $\Gamma = [12][13][23]$ and consider $3 \times r_2 \times r_3$ tables, where $r_2, r_3$ can be arbitrary. De Loera and Onn refer to these as slim tables.

**Theorem 9.3.21 (Slim tables).** Let $\Gamma = [12][13][23]$ be the 3-cycle and let $v \in \mathbb{Z}^k$ be any integer vector. Then there exist $r_2, r_3 \in \mathbb{N}$ and a coordinate
projection $\pi : \mathbb{Z}^{3 \times r_2 \times r_3} \rightarrow \mathbb{Z}^k$ such that every minimal Markov basis for $\Gamma$ on $3 \times r_2 \times r_3$ tables contains a vector $u$ such that $\pi(u) = v$.

In particular, Theorem 9.3.21 shows that there is no hope for a general bound on the one-norms of Markov basis elements for non-decomposable models, even for a fixed simplicial complex $\Gamma$. On the other hand, if only one of the table dimensions is allowed to vary, then there is a bounded finite structure to the Markov bases. This theorem was first proven in [HS07b] and generalizes a result in [SS03a].

**Theorem 9.3.22 (Long tables).** Let $\Gamma$ be a simplicial complex and fix $r_2, \ldots, r_m$. There exists a number $b(\Gamma, r_2, \ldots, r_m) < \infty$ such that the one-norms of the elements of any minimal Markov basis for $\Gamma$ on $s \times r_2 \times \cdots \times r_m$ tables are less than or equal to $b(\Gamma, r_2, \ldots, r_m)$. This bound is independent of $s$, which can grow large.

From Corollary 9.3.18 we saw that if $\Gamma$ is decomposable and not a simplex, then $b(\Gamma, r_2, \ldots, r_m) = 4$. One of the first discovered results in the non-decomposable case was $b([12][13][23], 3, 3) = 20$, a result obtained by Aoki and Takemura [AT03]. The most complicated move that appears for $3 \times 3 \times r_3$ tables is the one shown in Example 9.3.20.

In general, it seems a difficult problem to actually compute the values $b(\Gamma, r_2, \ldots, r_m)$, although some recent progress was reported by Hemmecke and Nairn [HN07]. The proof of Theorem 9.3.22 only gives a theoretical upper bound on this quantity, involving other numbers that are also difficult to compute. Further generalizations of these results appear in [HS12].

The Markov basis database [KR14] collects known results about specific Markov bases, including Markov bases of hierarchical models. Further theoretical results on Markov bases for many models, including hierarchical models, can be found in [AHT12].

### 9.4. Graver Bases and Applications

In some contingency table analysis problems, the types of tables that can occur are limited by structural conditions. A typical example is that cell entries are constrained to be in $\{0, 1\}$, or that certain entries are forced to be zero, but other types of cell entry constraints are also commonly occurring. In this case, the notion of Markov basis might need to be changed to take into account these new constraints. One tool that is help in these contexts is the notion of a Graver basis of a matrix $A$, which can simultaneous solve Markov basis problems for all bounded cell entry problems simultaneously.

We start this section with a very general definition of a Markov basis.
Definition 9.4.1. Let $F$ be a collection of finite subsets of $\mathbb{N}^r$. A finite set $B \subseteq \mathbb{Z}^r$ is called a Markov basis for $F$ if for all $F \in F$ and for all $u, u' \in F$, there is a sequence $v_1, \ldots, v_L \in B$ such that

$$u' = u + \sum_{k=1}^L v_k \quad \text{and} \quad u + \sum_{k=1}^L v_k \in F$$

for all $l = 1, \ldots, L$.

The elements of the Markov basis are called moves.

This definition contains our previous definition of Markov basis as a subcase with $F = \{F(u) : u \in \mathbb{N}^r\}$. In this section, we consider more general sets of fibers. Let $L \in \mathbb{N}^r$ and $U \in \mathbb{N}^r$. For a given matrix $A \in \mathbb{Z}^{d \times r}$, and $u \in \mathbb{N}^r$, let the fiber $F(u, L, U)$ be the set

$$F(u, L, U) = \{v \in \mathbb{N}^r : Av = Au \text{ and } L_i \leq v_i \leq U_i \text{ for all } i \in [r]\}.$$

Hence $L$ and $U$ are vectors of lower and upper bound constraints on cell entries. Let $F_A^{\text{bound}}$ be the set of all the fibers $F(u, L, U)$ with $u, L, U \in \mathbb{N}^r$. We will describe the Markov basis for this set of fibers.

Definition 9.4.2. Let $u \in \mathbb{Z}^r$. A conformal decomposition of $u$ is an expression $u = v + w$ where $v, w \in \mathbb{Z}^r \setminus \{0\}$ and $|u_i| = |v_i| + |w_i|$ for all $i \in [r]$. Given a matrix $A \in \mathbb{Z}^{d \times r}$, the Graver basis of $A$, denoted $Gr_A$, is the set of all nonzero $u \in \ker Z A$ such that $u$ does not have a conformal decomposition with $v$ and $w$ in $\ker Z A$.

Conformal decomposition of a vector is also known as a sign consistent decomposition. A simple example showing the structure of a Graver basis concerns the independence model for 2-way tables.

Proposition 9.4.3. Let $\Gamma = [1][2]$ and $r = (r_1, r_2)$ and let $A_{\Gamma,r}$ be the resulting matrix representing the model of independence of two random variables. Let $i = i_1, \ldots, i_k \in [r_1]$ be a sequence of disjoint elements, and $j = j_1, \ldots, j_k \in [r_2]$ be a sequence of disjoint elements. The move

$$f_{i,j} = e_{i_1 j_1} - e_{i_1 j_2} + e_{i_2 j_2} - e_{i_2 j_3} + \cdots + e_{i_k j_k} - e_{i_k j_1}$$

belongs to the Graver basis of $A_{\Gamma,r}$, and the Graver basis of $A_{\Gamma,r}$ consists of all such moves for $k = 2, \ldots, \min(r_1, r_2)$.

Proof. First, suppose that $f_{i,j}$ was not in the Graver basis. Then there are $v, w \in \ker Z A_{\Gamma,r}$ such that $f_{i,j} = v + w$ and this is a conformal decomposition. Since $f_{i,j}$ is a vector with all entries in $\{-1, 0, 1\}$, each of the unit vectors contributing to its definition ends up in either $v$ or $w$. Say that $e_{i_1 j_1}$ appears in $v$. Since $v$ has all row and column sums equal to zero, this forces $-e_{i_1 j_2}$ to appear in $v$ as well. By reasoning through the cyclic structure, we must have $v = f_{i,j}$ and $w = 0$ contradicting that $f_{i,j} = v + w$ is a conformal decomposition. This shows that $f_{i,j}$ is in the Graver basis.
To see that this set of moves is a Graver basis, let \( u \in \ker \mathbb{Z} A_{\Gamma, r} \) assume it is not an \( f_{ij} \) move. After permuting rows and columns, we can assume that \( u_{11} > 0 \). Since the row and column sums of \( u \) are zero, there is some entry in row one that is negative, say \( u_{12} < 0 \). Since the row and column sums of \( u \) are zero, then there is some entry in column two that is positive, say \( u_{22} > 0 \). Now one of two things could happen. If \( u_{21} < 0 \), then \( u = f_{12, 12} + w \) will be a conformal decomposition. If \( u_{21} \geq 0 \), then there is some entry say \( u_{23} \) in the first row that is negative. Repeating this procedure eventually must close off a cycle to obtain \( u = f_{i,j} + w \) as a conformal decomposition. This shows that the set of \( f_{i,j} \) is a Graver basis. □

In general, the Graver basis of a matrix \( A \) is much larger and more complex than a minimal Markov basis of that matrix. The Graver basis of a matrix \( A \) can be computed using tool from computational algebra, and direct algorithms for computing it are available in 4ti2 [HH03], which can be accessed through Macaulay2.

**Example 9.4.4.** Here will illustrate how to compute the Graver basis of of the hierarchical model with \( \Gamma = [12][13][14][234] \) and \( r = (2, 2, 2, 2) \) in Macaulay2.

```plaintext
loadPackage "FourTiTwo"
S = ZZ[x1,x2,x3,x4]
listofmonomials = matrix{{1,x1,x2,x3,x4,x1*x2,x1*x3, x1*x4, x2*x3,x2*x4,x3*x4,x2*x3*x4}};
A = transpose matrix toList apply((0,0,0,0)..(1,1,1,1), 
i -> flatten entries sub(listofmonomials, 
  {x1 => i_0, x2 => i_1, x3=> i_2, x4 => i_3}))
L = toricGraver(A)
```

The output is a \( 20 \times 16 \) matrix whose rows are the elements of the Graver basis up to sign. For example, the first row is the vector:

\[
2 \hspace{0.5em} -1 \hspace{0.5em} -1 \hspace{0.5em} 0 \hspace{0.5em} -1 \hspace{0.5em} 0 \hspace{0.5em} 1 \hspace{0.5em} -2 \hspace{0.5em} 1 \hspace{0.5em} 1 \hspace{0.5em} 0 \hspace{0.5em} 0 \hspace{0.5em} 0 \hspace{0.5em} -1
\]

which can be represented in tableau notation as

\[
\begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 2 & 2 & 2 \\
1 & 2 & 2 & 1 \\
2 & 1 & 2 & 1 \\
2 & 1 & 2 & 1 \\
2 & 2 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & 1 & 1 & 2 \\
1 & 1 & 2 & 1 \\
1 & 2 & 1 & 1 \\
2 & 1 & 1 & 1 \\
2 & 1 & 1 & 1 \\
2 & 2 & 2 & 2
\end{bmatrix}
\]

**Theorem 9.4.5.** Let \( A \in \mathbb{Z}^{d \times r} \). Then the Graver basis of \( A \) is a Markov basis for the set of fibers \( \mathcal{F}_A^{\text{bound}} \).
**Proof.** Let \( u, u' \in \mathcal{F}(u, L, U) \). We must show that \( u \) and \( u' \) can be connected by elements of \( Gr_A \) without leaving \( \mathcal{F}(u, L, U) \). The vector \( u - u' \in \ker Z_A \). It is either a Graver basis element, in which case \( u - u' \) are connected by a Graver basis element, or there is a Graver basis element \( v \) such that
\[
u - u' = v + w \text{ is a conformal decomposition, where } w \in \ker Z_A.
\]
But then \( u - v \in \mathcal{F}(u, L, U) \) since
\[
L_i \leq \min(u_i, u'_i) \leq \max(u_i, u'_i) \leq U_i
\]
for all \( i \in [r] \). Furthermore, \( \|u - u'\|_1 > \|(u - v) - u'\|_1 \) so \( u - v \) and \( u' \) are closer than \( u \) and \( u' \). So by induction, it is possible to connect \( u \) and \( u' \) by a sequence of moves from \( Gr_A \). \( \square \)

In some problems of statistical interest, it is especially interesting to focus only on the case where all lower bounds are zero and all upper bounds are 1, that is, restricting to the case where all elements of the fiber have 0/1 entries. In this case, it is only necessary to determine the Graver basis elements that have 0, \( \pm 1 \) entries. Even so, this set of Graver basis elements might be larger than necessary to connect the resulting fibers. We use \( 0 \) and \( 1 \) to denote the vector or table of all 0’s or 1’s, respectively.

**Theorem 9.4.6.** Let \( \Gamma = [1][2] \) and \( r = (r_1, r_2) \) and let \( A_{\Gamma,r} \) be the resulting matrix representing the model of independence of two random variables. Then the set of moves
\[
\{e_{i_1,j_1} + e_{i_2,j_2} - e_{i_1,j_2} - e_{i_2,j_1} : i_1, i_2 \in [r_1], j_1, j_2 \in [r_2]\}
\]
is a Markov basis that connects the fibers \( \mathcal{F}(u, 0, 1) \) for all \( u \).

**Proof.** We show that these standard moves for the independence model can be used to bring any two elements in the same fiber closer to each other. Let \( u, v \in \mathcal{F}(u, 0, 1) \). First of all, we can assume that \( u \) and \( v \) have no rows in common, otherwise we could delete this row and reduce to a table of a smaller size. We will show that we can apply moves from (9.4.1) to make the first rows of \( u \) and \( v \) the same. After simultaneously permuting columns of \( u \) and \( v \), we can assume that the first rows of each \( (u_1 \) and \( v_1 \), respectively) have the following form:
\[
u_1 = (1 \ 0 \ 0 \ 1) \quad v_1 = (1 \ 0 \ 1 \ 0).
\]
The corresponding blocks of each component are assumed to have the same size. In other words, we have arranged things so that we have first a region where \( u_1 \) and \( v_1 \) completely agree, and then a region where they completely disagree. It suffices to show that we can decrease the length of the region where they completely disagree.

If it were not possible to decrease the region where they disagree then, in particular, we could not apply a single move from (9.4.1) that involves
the first row entries corresponding to the last two blocks. We focus on what
the rest of the matrices $u$ and $v$ look like below those blocks. In particular, $u$ will have the following form after permuting rows:

$$u = \begin{pmatrix}
1 & 0 & 0 & 1 \\
A_1 & A_2 & A_3 & 1 \\
B_1 & B_2 & 0 & B_4
\end{pmatrix}.$$ 

The salient feature here is that if a 1 appeared in any position in the third
block of columns, then in the corresponding row in the fourth block must be
all 1’s, otherwise it would be possible to use a move to decrease the amount
of discrepancy in the first row. Similarly, if there were a 0 in the fourth block
of columns there must be all 0’s in the corresponding row in the third block.
A similar argument shows that there is a (possibly different) permutation
of rows so that $v$ has the following form:

$$v = \begin{pmatrix}
1 & 0 & 1 & 0 \\
C_1 & C_2 & C_3 & 0 \\
D_1 & D_2 & 1 & D_4
\end{pmatrix}.$$ 

Let $a$ and $b$ be the number rows in the corresponding blocks of rows in $u$ and $c$ and $d$ the number of rows in the corresponding blocks of rows in $v$. Since $u$ and $v$ have the same column sums, we deduce the following inequalities

$$1 + d \leq a \quad \text{and} \quad 1 + a \leq d$$

which is clearly a contradiction. Hence, there must be a move that could be
applied that would decrease the discrepancy in the first row. \qed

A common setting in analysis of contingency table data is that some
entries are constrained to be zero. For instance, in the genetic data of the
Hardy-Weinberg model (Theorem 9.2.10) it might be the case that certain
pairs of alleles cannot appear together in an organism because they cause
greatly reduced fitness. These forced zero entries in the contingency table
are called structural zeroes and the Graver basis can be useful in their anal-
ysis. Indeed, in the context of Markov bases for fibers with bounds, this is
equivalent to setting the upper bounds to 0 for certain entries. Hence, hav-
ing the Graver basis for a certain matrix $A$ can be useful for any structural zero problem associated to the corresponding log-linear model \cite{Rap06}.

9.5. Lattice Walks and Primary Decompositions

A Markov basis for a matrix $A$ has the property that it it connects every fiber $\mathcal{F}(u)$. In practical applications, we are usually interested in the connectivity of a specific fiber $\mathcal{F}(u)$. Furthermore, it might not be possible to obtain a Markov basis because it is too big to compute, and there might not exist theoretical results for producing the Markov basis. In this setting, a natural
strategy is to find and use a set of easy to obtain moves $B \subset \ker Z A$ to perform a Markov chain over the fiber $\mathcal{F}(u)$, which a priori may not be connected. Then we hope to understand exactly how much of the fiber $\mathcal{F}(u)$ is connected by $B$, and, in particular, conditions on $u$ that guarantee that the fiber $\mathcal{F}(u)$ is connected. One strategy for addressing this problem is based on primary decomposition of binomial ideals, as introduced in the paper [DES98]. Because the set of moves $B$ does not connect every fiber, these sets are sometimes called Markov subbases.

The strategy for using primary decomposition is based on the following simple generalization of Theorem 9.2.5.

**Theorem 9.5.1.** Let $B \subseteq \ker Z A$ be a subset of the lattice $\ker Z A$ and let $J_B$ be the ideal $J_B = \langle p^v - p^{v'} : v \in B \rangle$. Then $u, u' \in \mathcal{F}(u)$ are in the same connected component of the graph $\mathcal{F}(u)_B$ if and only if $p^u - p^{u'} \in J_B$.

Note that Theorem 9.5.1 immediately implies Theorem 9.2.5 since we require every $u, u' \in \mathcal{F}(u)$ to be in the same connected component to have a Markov basis.

Of course, deciding whether or not $p^u - p^{u'} \in J_B$ is a difficult ideal membership problem in general. The method suggested in [DES98] is to compute a decomposition of the ideal $J_B$, as $J_B = \cap_i I_i$. Then deciding membership in $J_B$ is equivalent to deciding membership in each of the ideals $I_i$. Hopefully, it is easier to decide membership in each of the ideals $I_i$. We illustrate the point with some examples.

**Example 9.5.2 (2 × 3 table).** Consider the problem of connecting 2 × 3 tables with fixed row and column sums. Of course, we know that the set

$$B' = \left\{ \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & -1 \\ -1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix} \right\}$$

forms a Markov basis for the corresponding $A$ via Theorem 9.2.7. But let us consider the connectivity of the random walk that arises from using the first and last two moves in this set. We denote the corresponding set of moves $B$. The resulting ideal is the ideal generated by two binomials:

$$J_B = \langle p_{11}p_{22} - p_{12}p_{21}, p_{12}p_{23} - p_{13}p_{22} \rangle$$

whose primary decomposition is

$$J_B = \langle p_{11}p_{22} - p_{12}p_{21}, p_{12}p_{23} - p_{13}p_{22}, p_{11}p_{23} - p_{13}p_{21} \rangle \cap \langle p_{12}, p_{22} \rangle.$$

We want to use this decomposition to decide when two 2 × 3 tables are connected by the moves of $B$. The first component is the ideal of 2 × 2 minors of a generic 2 × 3 matrix, which is the toric ideal of the independence model, i.e. $J_{B'}$. Of course, a binomial $p^u - p^v \in J_{B'}$ if and only if $u$ and $v$ have the same row and column sums. For a binomial $p^u - p^v$ to belong to
the second component, we must have each of \( p^u \) and \( p^v \) divisible by either \( p_{12} \) or \( p_{22} \). Thus we deduce that \( u \) and \( v \) are connected by the set of moves \( \mathcal{B} \) if and only if

1. \( u \) and \( v \) have the same row and column sums and
2. the sum \( u_{12} + u_{22} = v_{12} + v_{22} > 0 \).

Attempts to generalize this example to arbitrary sets of adjacent minors appear in [DES98, HsS04].

For hierarchical models, there are many natural families of moves which could be used as a starting point to try to employ the strategy for analyzing connectivity based on primary decomposition. In the case where the underlying complex \( \Gamma \) is the set of cliques in a graph \( G \), then the natural choice is the set of degree 2 moves that come from the conditional independence statements implied by the graph. (The connection between conditional independence structures and graphs will be explained in Chapter 13.) A computational study along these lines was undertaken in the paper [KRS14].

9.6. Other Sampling Strategies

In the previous sections we saw Markov Chain MonteCarlo strategies for generating tables from the fibers \( \mathcal{F}(u) \) based on fixed marginal totals. These were based on computing Markov bases or Graver bases or using appropriate Markov subbases which connect many fibers. In this section we describe some alternative strategies for sampling from the fibers \( \mathcal{F}(u) \), which can be useful in certain situations.

The urn scheme is a method for obtaining exact samples from the hypergeometric distribution on 2-way contingency tables with fixed row and column sums, with a natural generalization to decomposable hierarchical models. It can also be applied to speed up the generation of random samples from the hypergeometric distribution on fibers associated to reducible models. Note, however, that if a different distribution on the fiber \( \mathcal{F}(u) \) is required, it does not seem possible to modify the urn scheme to generate samples. For example, even introducing a single structural zero can make it impossible to use the urn scheme to generate samples from the hypergeometric distribution.

The basic urn scheme for two-way tables is described as follows.

**Algorithm 9.6.1 (Urn Scheme for 2-way tables).** Input: A table \( u \in \mathbb{N}^{r_1 \times r_2} \).

Output: A sample \( v \in \mathbb{N}^{r_1 \times r_2} \) from the hypergeometric distribution on \( \mathcal{F}(u) \).
9.6. Other Sampling Strategies

(1) Let \( b_i = \sum_j u_{ij} \), \( c_j = \sum_i u_{ij} \), and \( n = \sum_{i,j} u_{ij} \).

(2) Let \( P \) be a uniformly random permutation matrix of size \( n \times n \).

(3) For each \( i, j \) define

\[
v_{ij} = \sum_{k=b_1+\cdots+b_{i-1}+1}^{b_1+\cdots+b_i} \sum_{l=c_1+\cdots+c_{j-1}+1}^{c_1+\cdots+c_j} P_{kl}
\]

(4) Output \( v \).

In other words, to generate a random table from the hypergeometric distribution on \( \mathcal{F}(u) \), we just need to generate a uniformly random permutation and then bin the rows and columns into groups whose sizes are the row and column sums of \( u \). This is doable, because it is easy to generate uniformly random permutation matrices, by sampling without replacement.

**Proof of correctness of Algorithm 9.6.1.** We need to show that the probability of sampling a table \( v \) is proportional to \( \prod_{ij} v_{ij}! \). To do this, we calculate the number of permutations that lead to a particular table \( v \). This is easily seen to be

\[
\prod_{i=1}^{r_1} \binom{b_i}{v_{i1}, v_{i2}, \ldots, v_{ir_i}} \prod_{j=1}^{r_2} \binom{c_j}{v_{1j}, v_{2j}, \ldots, v_{r_1j}} \prod_{i=1}^{r_1} \prod_{j=1}^{r_2} v_{ij}!
\]

The first product shows the numbers of ways to choose columns for the 1's in the permutation to live, compatible with the \( v_{ij} \), the second product gives the number of ways to choose columns for the permutation, compatible with the \( v_{ij} \), and the \( v_{ij}! \) give the number of permutations on the resulting \( v_{ij} \times v_{ij} \) submatrix. Expanding the multinomial coefficients yields the equivalent expression:

\[
\frac{\prod_{i=1}^{r_1} b_i! \prod_{j=1}^{r_2} c_j!}{\prod_{ij} v_{ij}!}.
\]

Since the vectors \( b \) and \( c \) are constants, this shows that the probability of the table \( v \) is given by the hypergeometric distribution. \( \square \)

For the special case of reducible models, there is a general recursive strategy using the urn scheme that take hypergeometric samples from the pieces of the decomposition and constructs a hypergeometric sample from the entire model.

Let \( \Gamma \) be a reducible simplicial complex with reducible decomposition \((\Gamma_1, S, \Gamma_2)\), and let \( u \) be a table. Let \( V_i = |\Gamma_i| \setminus S \), \( i = 1, 2 \). Let \( u_i = \pi_{\Gamma_i \cup S}(u) \) be the projection onto the random variables appearing in \( \Gamma_i \). Let \( v_i \) be a sample from the hypergeometric distribution on the fiber \( \mathcal{F}_{\Gamma_i}(u_i) \). To generate a hypergeometric sample on \( \mathcal{F}(u) \), do the following.
For each index $i_S \in \mathcal{R}_S$, use the urn scheme on $\#\mathcal{R}_{V_1} \times \#\mathcal{R}_{V_2}$ tables to generate a random hypergeometric table with row indices and column indices equal to

$$(v_1)_{i_{V_1,i_S}}i_{V_1} \in \mathcal{R}_{V_1} \quad \text{and} \quad (v_2)_{i_{V_2,i_S}}i_{V_2} \in \mathcal{R}_{V_2}$$

respectively. For each $i_S$ this produces a table which comes from the hypergeometric distribution and the combination of all of these tables will be a table from the hypergeometric distribution.

**Example 9.6.2.** Let $\Gamma = [12][23][345]$ a decomposable simplicial complex and suppose that $d = (2, 3, 4, 5, 6)$. To generate a random sample from the hypergeometric distribution on the fiber $\mathcal{F}_\Gamma(u)$ for this decomposable model, we proceed as follows. First we restrict to the subcomplex $\Gamma_1 = [12][23]$, and we need to generate hypergeometric samples on the fiber $\mathcal{F}_{\Gamma_1}(u_{123})$. To do this, we must generate samples from the hypergeometric distribution on $d_2 = 3, 2 \times 4$ tables with fixed row and column sums. This leads to a random hypergeometric distributed sample $v$ from $\mathcal{F}_{\Gamma_1}(u_{123})$. Now we proceed to the full model $\Gamma$. To do this, we need to generate $d_3 = 4$ random hypergeometric tables of size $6 \times 30$, using the margins that come from $v$ and $u|_{345}$.

Direct sampling from the underlying distribution of interest on $\mathcal{F}(u)$ is usually not possible. This is the reason for the Markov chain approaches outlined in previous sections. An alternate Markov chain strategy, which was described in [HAT12], is based on simply having a spanning set for the lattice $\ker ZA$ and using that to construct arbitrarily complicated moves and perform a random walk. Let $\mathcal{B} \subseteq \ker ZA$ be a spanning set of $\ker ZA$. Suppose that $\mathcal{B} = \{b_1, \ldots, b_d\}$ has $d$ elements. Let $P$ be a probability distribution on $\mathbb{Z}^d$ that is symmetric about the origin, $P(m) = P(-m)$, and such that every vector in $\mathbb{Z}^d$ has positive probability. To get a random element in $\ker ZA$, take a random draw $m \in \mathbb{Z}^d$ with respect to $P$ and form the vector $\sum_i m_ib_i$. This gives random element of $\ker ZA$, which can then be used to run the Markov chain. The fact that the distribution $P$ is symmetric about the origin guarantees that the resulting Markov chain is irreducible, and then the Metropolis-Hastings algorithm can be employed to generate samples converging to the true distribution.

An alternate strategy for computing approximate samples that does not use Markov chains is sequential importance sampling, which works by building a random table entry by entry. This method does not produce a random table according to the hypergeometric distribution, but then importance weights are used to correct for the fact that we sample from the incorrect distribution. To generate a random table entry by entry requires to know upper and lower bound cell entries given table margins. We discuss this method further in Chapter 10.
9.7. Exercises

Exercise 9.1. For the generalized hypergeometric distribution, write as simple an expression as possible for the fraction \( p(u_t + v_t)/p(u_t) \) that is computed in the Metropolis-Hastings algorithm (i.e. give an expression that involves as few multiplications as possible).

Exercise 9.2. Prove Theorems 9.2.10 and 9.2.11.

Exercise 9.3. Suppose that \( A' \) is a matrix obtained as the subset of columns of the matrix \( A \), indexed by the set of columns \( S \).

1. Show that \( I_{A'} = I_A \cap \mathbb{K}\{p_i : i \in S\} \).
2. Explain how the previous result can be used for Markov basis problems for models with structural zeros.
3. Compute a Markov basis for Hardy-Weinberg equilibrium on seven alleles with structural zeros in all the \((i, i + 1)\) positions.


Exercise 9.5. Let \( \Gamma = [1][2][3] \) and \( r = (2, 2, 2) \) be the model of complete independence for 3 binary random variables, and let \( u \) be the \( 2 \times 2 \times 2 \) table

\[
\begin{pmatrix}
16 & 4 \\
2 & 3
\end{pmatrix}
\begin{pmatrix}
3 & 22 \\
11 & 6
\end{pmatrix}
\]

What is the expected value of the \((1, 1, 1)\) coordinate of \( v \in \mathcal{F}(u) \) selected with respect to the generalized hypergeometric distribution and the uniform distribution?

Exercise 9.6. Perform Fisher’s exact test on the \( 2 \times 2 \times 2 \) table

\[
\begin{pmatrix}
1 & 5 \\
3 & 5
\end{pmatrix}
\begin{pmatrix}
4 & 4 \\
9 & 6
\end{pmatrix}
\]

with respect to the model of complete independence, i.e. where \( \Gamma = [1][2][3] \).

Exercise 9.7. Let \( \Gamma \) be the simplicial complex \( \Gamma = [12][13][234] \) and \( r = (2, 2, 2, 4) \). Use the fact that \( \Gamma \) is reducible to give the Markov basis for \( A_{\Gamma, r} \).

Exercise 9.8. Let \( A \in \mathbb{Z}^{k \times r} \) and let \( \Lambda(A) \) denote the \((r + k) \times 2r\) matrix

\[
\Lambda(A) = \begin{pmatrix} A & 0 \\ I & I \end{pmatrix}
\]

where \( I \) denotes the \( r \times r \) identity matrix. Note that \( u \in \ker_{\mathbb{Z}}(A) \) if and only if \((u, -u) \in \ker_{\mathbb{Z}}(\Lambda(A))\). Show that a set of moves \( \mathcal{B} \in \ker_{\mathbb{Z}}(A) \) is the Graver basis for \( A \) if and only if the set of moves \( \{(u, -u) : u \in \mathcal{B}\} \) is a minimal Markov basis for \( \Lambda(A) \).

Exercise 9.10. Let $\Gamma = [12][23][34][45][15]$ be the five cycle and suppose that $r = (2, 2, 2, 2, 2)$.

1. Describe all the Markov basis elements of $A_{\Gamma,d}$ which have 1-norm 4.

2. Compute the primary decomposition of the ideal generated by the corresponding degree 2 binomials described in the previous part.

3. Use the primary decomposition from the previous part to deduce that if $u$ satisfies $A_{\Gamma,d}u > 0$, then the fiber $\mathcal{F}(u)$ is connected by the moves of 1-norm 4.

Exercise 9.11. Describe an Urn scheme for generating hypergeometric samples for the model of Hardy-Weinberg equilibrium.
Bounds on Cell Entries

In this chapter we consider the problem of computing upper and lower bounds on cell entries in contingency tables given lower dimensional marginal totals. The calculation of lower and upper bounds given constraints is an example of an integer program. There is an established history of developing closed formulas for upper and lower bounds on cell entries given marginal totals, but these typically only apply in special cases. Techniques from computational algebra can be used to set up and solve these integer programs, and certain results on toric ideals and their Gröbner bases can be used to analyze the effectiveness of linear programming relaxations to approximate solutions to the corresponding integer programs. We begin the chapter by motivating the problem of computing bounds with two applications.

10.1. Motivating Applications

In this section, we consider motivating applications for computing upper and lower bounds on cell entries given marginal totals. The first application is to Sequential Importance Sampling, a procedure for generating samples from fibers $\mathcal{F}(u)$ that avoids the difficulty of sampling from the hypergeometric distribution. A second application is to Disclosure Limitation, which concerns whether or not privacy is preserved when making certain data releases of sensitive data.

10.1.1. Sequential Importance Sampling. In Chapter 9 we saw strategies for sampling from the fiber $\mathcal{F}(u)$ to approximate the expected value $\mathbb{E}_p[f(u)]$ where $p$ is the hypergeometric distribution or uniform distribution
and $f$ is an indicator function pertaining to the test statistic of the particular hypothesis test we are using. Since generating direct samples from either the hypergeometric distribution or uniform distribution are both difficult, we might content ourselves with sampling from an easy-to-sample-from distribution $q$ on $\mathcal{F}(u)$, which has the property that the probability of any $v \in \mathcal{F}(u)$ is positive. Then we have

$$\mathbb{E}_q[f(v) \frac{p(v)}{q(v)}] = \sum_{v \in \mathcal{F}(u)} f(v) \frac{p(v)}{q(v)} \cdot q(v) = \sum_{v \in \mathcal{F}(u)} f(v)p(v) = \mathbb{E}_p[f(v)].$$

So to approximate the expected value we are interested in we compute random samples $v^1, \ldots, v^n$ from the distribution $q$ and calculate

$$\frac{1}{n} \sum_{i=1}^{n} f(v^i) \frac{p(v^i)}{q(v^i)}.$$ as an estimator of the expectation. This procedure is called importance sampling and the ratios $\frac{p(v^i)}{q(v^i)}$ are the importance weights.

A further difficulty in applying importance sampling for Fisher’s exact test, is that our target distribution $p$ on $\mathcal{F}(u)$ is the hypergeometric distribution on $\mathcal{F}(u)$ where we cannot even compute the value $p(v)$ for $v \in \mathcal{F}(u)$. This is because we usually only have the formula for $p$ up to the normalizing constant. Indeed, if $p'$ is the unnormalized version of $p$, so that $p(v) = p'(v)/\sum_{w \in \mathcal{F}(u)} p'(w)$, then for $n$ samples $v^1, \ldots, v^n$ according to the distribution $q$ the expression

$$\frac{1}{n} \sum_{i=1}^{n} p'(v^i) / q(v^i),$$

converges to the normalizing constant, hence

$$\left(\sum_{i=1}^{n} f(v^i) \frac{p'(v^i)}{q(v^i)} / \sum_{i=1}^{n} \frac{p'(v^i)}{q(v^i)}\right)$$

converges to the mean of the distribution $p$.

The question remains: how should we choose the distribution $q$? The sequential part of sequential importance sampling relies on the fact that the distribution $p$ is usually over some high dimensional sample space. The strategy is then to compute a distribution $q$ by sequentially filling in each entry of the vector we intend to sample. In the case of sampling from a fiber $\mathcal{F}(u)$, we want to fill in the entries of the vector $v \in \mathcal{F}(u)$, one at a time. To do this, we need to know what the set of all possible first coordinates of all $v \in \mathcal{F}(u)$ are. This can be approximated by computing upper and lower bounds on cell entries.
10.1. Motivating Applications

Example 10.1.1. Consider generating a random $3 \times 3$ nonnegative integer array with fixed row and column sums as indicated in the following table.

<table>
<thead>
<tr>
<th>$v_{11}$</th>
<th>$v_{12}$</th>
<th>$v_{13}$</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_{21}$</td>
<td>$v_{22}$</td>
<td>$v_{23}$</td>
<td>3</td>
</tr>
<tr>
<td>$v_{31}$</td>
<td>$v_{32}$</td>
<td>$v_{33}$</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

We compute upper and lower bounds on entry $v_{11}$ and see that $v_{11} \in \{0, 1, 2, 3\}$. Suppose we choose $v_{11} = 2$, and we want to fill in values for $v_{12}$. We compute upper and lower bounds on $v_{12}$ given that $v_{11} = 2$ and see that $v_{12} \in \{1, 2, 3, 4\}$, and we might choose $v_{12} = 3$. At this point, $v_{13}$ is forced to be 1 by the row sum constraints. We can proceed to the second row by treating this as a random table generation problem for a $2 \times 3$ table. Continuing in this way, we might produce the table

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>1</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

Assuming that when we have a range of values to choose from at each step, we pick them uniformly at random, the probability of selecting the table $v$ above is $\frac{1}{4} \cdot \frac{1}{4} \cdot \frac{1}{2} \cdot \frac{1}{3}$.

A key step in the sequential importance sampling algorithm for contingency tables is the calculation of the upper and lower bounds on cell entries. That is, we need to calculate, for example,

$$\max \text{ / } \min v_{11} \text{ subject to }$$

$$\sum_{j=1}^{r_2} v_{ij} = u_{i+} \text{ for } i \in [r_1], \sum_{i=1}^{r_1} v_{ij} = u_{+j} \text{ for } j \in [r_2] \text{ and } v \in \mathbb{N}^{r_1 \times r_2}.$$

For 2-way tables, such bounds are easy to calculate given the marginal totals.

Proposition 10.1.2. Let $u \in \mathbb{N}^{r_1 \times r_2}$ be a nonnegative integral table. Then for any $v \in \mathcal{F}(u)$ we have

$$\max(0, u_{i+} + u_{+j} - u_{++}) \leq v_{ij} \leq \min(u_{i+}, u_{+j})$$

and these bounds are tight. Furthermore, for every integer $z$ between then upper and lower bounds, there is a table $v \in \mathcal{F}(u)$ such that $v_{ij} = z$.

Proof. Clearly the upper bound is valid, since all entries of the table are nonnegative. To produce a table that achieves the upper bound, we use a procedure that is sometimes referred to as “stepping-stones”. Without loss of generality, we can focus on $v_{11}$. We prove by induction on $r_1$ and
that there is a table whose 11 entry is \( \min(u_{1+}, u_{+1}) \). Suppose that the minimum is attained by the row sum \( u_{1+} \). Set \( v_{11} = u_{1+} \) and \( v_{1j} = 0 \) for all \( j = 2, \ldots, r_2 \). Then we can restrict attention to the bottom \( r_1 - 1 \) rows of the matrix. Updating the column sums by replacing \( u_{+1}' = u_{+1} - u_{1+} \), we arrive at a smaller version of the same problem. Since the row and column sums of the resulting \((r_1 - 1) \times r_2\) matrix are consistent, induction shows that there exists a way to complete \( v \) to a nonnegative integral table satisfying the original row and column sums and with \( v_{11} \) equal to the upper bound. The procedure is called stepping-stones because if you follow it through from the 11 entry down to the bottom produces a sequence of nonnegative entries in the resulting table \( v \).

For the lower bound, we note an alternate interpretation of this formula. Suppose that in a given row \( i \) we were to put the upper bound value \( u_{+k} \) in each entry \( u_{jk} \) for \( k \neq j \). Then this forces

\[
 u_{ij} = u_{i+} - \sum_{k \neq j} u_{+k} = u_{i+} + u_{+j} - u_{++}
\]

which is a lower bound since we made the other entries in the \( i \)th row as large as possible. This lower bound is attainable (and nonnegative) precisely when all the \( u_{+k} \) for \( k \neq j \) are smaller than \( u_{i+} \), which again follows from the stepping-stones procedure. Otherwise the lower bound of 0 is attained by putting some \( u_{ik} = u_{i+} \).

To see that every integer value in between the bounds is attained by some table \( v \) in the fiber, note that the Markov basis for 2-way tables with fixed row and column sums consists only of moves with 0, ±1 entries. Hence in a connected path from a table that attains the upper bound to one that attains the lower bound we eventually see each possible entry between the upper and lower bounds.

Example 10.1.3. We apply the basic strategy described above to the 2-way table from Example 9.1.2. Generating 1000 samples from the proposal distribution generates an approximation to the Fisher’s exact test \( p \)-value of \( 1.51 \times 10^{-7} \).

Note however that this most basic strategy can be problematic in more complicated problems, because it does not put enough probability mass on the small proportion of tables that have high probability under the hypergeometric distribution. For this reason, the SIS strategy has been primarily used to approximate samples from the uniform distribution where that is appropriate. One example application is to use SIS to approximate the cardinality of the fiber \( \mathcal{F}(u) \). Using the arguments above, and taking \( p \) to be
the uniform distribution on $\mathcal{F}(u)$, it is not difficult to see that the estimator
\[
\frac{1}{n} \sum_{i=1}^{n} \frac{1}{q(v^{(i)})}
\]
converges to $|\mathcal{F}(u)|$ as the number of samples $n$ tends to infinity. Using the same 1000 samples above, we estimate $|\mathcal{F}(u)| \approx 2.6 \times 10^5$.

Further details about applications of sequential importance sampling to the analysis of tables appear in [CDHL05] where the focus is on 2-way tables, with special emphasis on 0/1 tables. The paper [CDS06] considers the extensions to higher-order tables under fixed margins, using some of the tools discussed in this chapter.

Computing bounds on cell entries in 2-way tables is especially easy. In general, it is difficult to find general formulas for the bounds on cell entries given marginal totals. We discuss this in more detail in Section 10.5. It remains a problem to compute bounds on tables of larger sizes with respect to more complex marginals, or for more general log-linear models besides hierarchical models. General easy to compute formulas are lacking and usually algorithmic procedures are needed, which we will see in subsequent sections.

10.1.2. Disclosure Limitation. Computing bounds on entries of contingency tables can also be useful in statistical disclosure limitation or other areas of data privacy. Census bureaus and social science researchers often collect data via surveys with a range of questions including various demographic questions, questions about income and job status, health care information, and personal opinions. Often there are sensitive questions mixed in among a great many other innocuous questions.

To assure that the survey respondents give truthful answers, such surveys typically offer guarantees to the participants that individual personal information will not be revealed, that respondent files will not be linked with names, and that the data will only be released in aggregate. In spite of such guarantees from the survey collectors, the summary of data in a cross-classified contingency table together with the knowledge that a particular person participated in the survey can often be enough to identify sensitive details about individuals, especially when those people belong to minority groups.

To illustrate the problem, consider the following hypothetical contingency table cross-classifying a group of mathematics professors at a particular university according to rank (R), gender (G), sexual orientation (SO), income (I), and opinion about university administration (UA). Possible answers for these survey questions are...
• Rank: Assistant Professor, Associate Professor, Full Professor,
• Gender: Male, Female
• Sexual Orientation: Heterosexual, Gay/Lesbian/Bisexual
• Income: <$80K, $80K - 120K, >$120K
• Opinion: Excellent job, Neutral, Terrible job

<table>
<thead>
<tr>
<th>University Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Income</td>
</tr>
<tr>
<td>Rank</td>
</tr>
<tr>
<td>Gender</td>
</tr>
<tr>
<td>Rank</td>
</tr>
<tr>
<td>SO</td>
</tr>
<tr>
<td>Gender</td>
</tr>
<tr>
<td>Rank</td>
</tr>
</tbody>
</table>

The table shows the results of the hypothetical survey of a department of 31 faculty. For example the 1 entry denotes the one female, lesbian, associate professor, in the middle income range, and neutral about the university administration. As should be clear from this example, even with only 5 survey questions, the resulting tables are very sparse, and with many singleton entries. Table observers with access to public information (e.g. a departmental websites, social media, etc.) can combine this information to deduce sensitive information, for example, sexual orientation or the faculty member’s opinion on the administration. Research in disclosure limitation is designed to analyze what data can be released in anonymized form without revealing information about the participants.

If we focus only on the information contained in the table, we should be concerned about any entry that is a 1 or a 2, as these are considered the most sensitive. A 1 means a person is uniquely identified, and a 2 means that two participants can identify each other. One easy to implement strategy to preserve the knowledge of the exact table values in a large table is to only release lower dimensional marginals of the tables with no ones or twos. However, an agency or researcher releasing such information must be sure that this release does not further expose cell entries in the table. A typical question that we how much information about \( u \) can be recovered from the released margins \( A_\Gamma u \), for some particular choice of margins \( \Gamma \)? The most
naive way to assess this is to compute bounds on individual cell entries given the marginal $A_{1:n}$. If the bounds are too narrow and the lower bounds are positive, then they probably reveal too much about the cell entry.

For example, in the table above, the release of all 3-way marginals of the table does not mask the table details at all: in fact, it is possible to recover all table entries given all 3-way margins in this case. If we restrict to just 2-way marginals, then by computing linear programming upper and lower bounds, we are uniquely able to recover one of the table entries namely the position marked by 1. This example show that even releasing quite low dimensional marginals on a 5-way table that is sparse can still reveal table entries that are sensitive.

The issue of privacy from databases is a very active research area, and the problem of computing bounds on entries represents only a tiny part. Perhaps the most widely studied framework is called differential privacy [Dwo06]. A survey of statistical aspects of the disclosure limitation problem is [FS08].

10.2. Integer Programming and Gröbner Bases

To discuss computing bounds in more detail requires some introduction to the theories of integer and linear programming. This is explained in the present section which also makes the connection to Gröbner bases of toric ideals. More background on linear and integer programming can be found in [BT97], and the book [DLHK13], has substantial material on applications of algebra to optimization.

Let $A \in \mathbb{Z}^{k \times r}$, $b \in \mathbb{Z}^k$ and $c \in \mathbb{Q}^r$. The standard form integer program is the optimization problem

\begin{equation}
\text{min } c^T x \text{ subject to } Ax = b \text{ and } x \in \mathbb{N}^r.
\end{equation}

The optimal value of the integer program will be denoted $IP(A,b,c)$. The linear programming relaxation of the integer program is the optimization problem

\begin{equation}
\text{min } c^T x \text{ subject to } Ax = b, x \geq 0 \text{ and } x \in \mathbb{R}^r.
\end{equation}

Its optimal value will be denoted $LP(A,b,c)$. Since the optimization in the linear programming relaxation is over a larger set than in the integer program, $LP(A,b,c) \leq IP(A,b,c)$.

For general $A$, $b$, and $c$, integer programming is an NP-hard problem while linear programming can be solved in polynomial time in the input complexity (e.g. via interior point methods). Since integer programs are difficult to solve in general, there are a range of methods that can be used. Here we discuss methods based on Gröbner bases. In the optimization literature these are closely related to optimization procedures based on test
Recall that \( \mathcal{F}(u) = \{ v \in \mathbb{N}^r : Au = Av \} \) is the fiber in which \( u \) lies. This is the set of feasible points of the integer program (10.2.1). Let \( \mathcal{B} \subseteq \text{ker}_Z A \) be a set of moves and construct the directed graph \( \mathcal{F}(u)_B \) whose vertex set is \( \mathcal{F}(u) \) and with an edge \( v \rightarrow w \) if \( c^T v \geq c^T w \) and \( v - w \in \pm \mathcal{B} \). If this directed fiber graph has been constructed with nice enough properties, we can follow the edges in the graph down to an optimal vertex to find a minimizer.

**Definition 10.2.1.** Let \( A \in \mathbb{Z}^{k \times r} \) and \( c \in \mathbb{Q}^r \). Assume that the vector \( 1 \in \text{rowspace}(A) \) (so that \( \mathcal{F}(u) \) is finite for every \( u \)). A subset \( \mathcal{B} \subseteq \text{ker}_Z A \) is called a Gröbner basis for \( A \) with respect to the cost vector \( c \) if each nonempty fiber \( \mathcal{F}(u)_B \) has a unique sink component. Note that a sink component is a strongly connected subgraph of \( \mathcal{F}(u)_B \) with no outgoing edges. The existence of a single sink component guarantees that the greedy search algorithm terminates at an optimum of the integer program (10.2.1). We use the term Gröbner basis here, which we have already used in the context of computing in polynomial rings previously. There is a close connection.

**Definition 10.2.2.** Let \( c \in \mathbb{Q}^r \). The weight term order \( \prec_c \) on \( \mathbb{K}[p_1, \ldots, p_r] \) is defined by \( p^u \prec_c p^v \) if \( c^T u < c^T v \). The weight of a monomial \( p^u \) is \( c^T u \).

Note that under the weight order, it can happen that two or more monomials all have the same weight. For a polynomial \( f = \sum_{u \in \mathbb{N}^r} c_u p^u \) let \( \text{in}_c(f) \) be the sum of all monomials in \( f \) of the highest weight. As usual, the initial ideal \( \text{in}_c(I) = \langle \text{in}_c(f) : f \in I \rangle \). A weight order is \( \prec_c \) is said to be generic for an ideal \( I \) if \( \text{in}_c(I) \) is a monomial ideal.

**Theorem 10.2.3.** Let \( A \in \mathbb{Z}^{k \times r} \) and \( c \in \mathbb{Q}^r \) and suppose that \( c \) is generic for \( I_A \). Then \( \mathcal{B} \subseteq \text{ker}_Z A \) is a Gröbner basis for \( A \) with respect to \( c \) if and only if the set of binomials \( \{ p^{b^+} - p^{b^-} : b \in \mathcal{B} \} \) is a Gröbner basis for \( I_A \) with respect to the weight order \( \prec_c \).

**Proof.** Let \( p^u \) be a monomial and suppose we apply one single step of polynomial long division with respect to a binomial \( p^{b^+} - p^{b^-} \) in the collection \( \{ p^{b^+} - p^{b^-} : b \in \mathcal{B} \} \) assuming that \( p^{b^+} \) is the leading term. A single step of long division produces the remainder \( p^{u-b} \) which must be closer to optimal than \( p^u \). In the fiber graph \( \mathcal{F}(u)_B \) we should connect \( u \) and \( u - b \) with a directed edge. Since \( \{ p^{b^+} - p^{b^-} : b \in \mathcal{B} \} \) is a Gröbner basis we end this process with a unique end monomial \( p^v \). The point \( v \) must be the unique sink in \( \mathcal{F}(u)_B \), else there is a binomial \( p^v - p^v' \) where neither term is divisible.
by any leading term in \(\{p^b+ - p^b- : b \in B\}\), contradicting the Gröbner basis property.

In particular, using Theorem 10.2.3 tells us exactly how to solve an integer program using Gröbner bases. The normal form of \(p^u\) modulo a Gröbner basis of \(I_A\) with respect to the weight order \(\prec_c\) will be a monomial \(p^v\) that is minimal in the monomial order. This result and the Gröbner basis perspective on integer programming originated in [CT91].

Note that for the optimization problems we consider here associated with computing upper and lower bounds on cell entries, the cost vector \(c\) is a standard unit vector, or its negative. These cost vectors are usually not generic with respect to a toric ideal \(I_A\). However, there are term orders that can be used that will do the same job from the Gröbner basis standpoint.

**Proposition 10.2.4.** Let \(A \in \mathbb{Z}^{k \times r}\) with \(1 \in \text{rowspan}(A)\). Let \(\prec_{\text{lex}}\) be the lexicographic order with \(p_1 \succ_{\text{lex}} p_2 \succ_{\text{lex}} \cdots\) and let \(\prec_{\text{revlex}}\) be the reverse lexicographic order with \(p_1 \prec_{\text{revlex}} p_2 \prec_{\text{revlex}} \cdots\).

1. The normal form of \(p^u\) with respect to the toric ideal \(I_A\) and the term order \(\prec_{\text{lex}}\) is a monomial \(p^v\) where \(v_1\) is minimal among all \(v \in F(u)\).

2. The normal form of \(p^u\) with respect to the toric ideal \(I_A\) and the term order \(\prec_{\text{revlex}}\) is a monomial \(p^v\) where \(v_1\) is maximal among all \(v \in F(u)\).

**Proof.** We prove the result for the lexicographic order, the proof for the reverse lexicographic order being similar. Suppose that \(p^v\) is the normal form of \(p^w\), but \(w \in F(u)\) has smaller first coordinate then \(v\). Then \(p^v - p^w\) is in \(I_A\) and the leading term with respect to the lex order is \(p^v\) since \(v_1 > w_1\). But this contradicts the fact the \(p^v\) was the normal form, and hence not divisible by any leading term of any element of the Gröbner basis.

### 10.3. Quotient Rings and Gröbner Bases

A key feature of Gröbner bases is that they give a well-defined computational strategy for working with quotient rings of polynomial rings modulo ideals. Performing division with respect to a Gröbner basis chooses a distinct coset representative for each coset, namely the normal form under polynomial long-division. In the case of toric ideals, the unique coset representative of a coset of the form \(p^u + I_A\) also gives the solution to the corresponding integer programming problem. Structural information about the set of standard monomials can also give information about how well linear programming relaxations perform, which we discuss in the next section. Computing with
quotient rings also plays an important role in the design of experiments, covered in detail in Chapter 12.

Let \( R \) be a ring, \( I \) an ideal of \( R \), and \( f \in R \). The coset of \( f \) is the set \( f + I := \{ f + g : g \in I \} \). The set of cosets of the ideal \( I \) form a ring with addition and multiplication defined by:

\[
(f + I) + (g + I) = (f + g) + I \quad \text{and} \quad (f + I)(g + I) = fg + I.
\]

The property of being an ideal guarantees that these operations do not depend on which element of the coset is used in the calculation. The set of all cosets under these operations is denoted by \( R/I \) and is called the quotient ring. One way to think about quotients is that the set of elements \( I \) are all being “set to zero”. Or, we can think about the elements in \( I \) as being new relations that we are adding to the defining properties of our ring. The following is a key example of a quotient ring arising from algebraic geometry.

**Proposition 10.3.1.** Let \( V \subseteq \mathbb{K}^n \) be an affine variety. The quotient ring \( \mathbb{K}[p]/I(V) \) is called the coordinate ring of \( V \) and consists of all polynomial functions defined on \( V \).

**Proof.** Two polynomials \( f, g \in \mathbb{K}[p] \) define the same function on \( V \) if and only if \( f - g = 0 \) on \( V \), that is, \( f - g \in I(V) \). But \( f - g \in I(V) \) if and only if \( f + I(V) = g + I(V) \). \( \square \)

At first glance, it might not be obvious how to perform computations using quotient rings. For instance, how can we check whether or not \( f + I = g + I \)? One solution is provided by Gröbner bases.

**Proposition 10.3.2.** Let \( I \subseteq \mathbb{K}[p] \) be an ideal, and \( \mathcal{G} \) a Gröbner basis for \( I \) with respect to a term order \( \prec \) on \( \mathbb{K}[p] \). Two polynomials \( f, g \in \mathbb{K}[p] \) belong to the same coset of \( I \) if and only if \( NF_{\mathcal{G}}(f) = NF_{\mathcal{G}}(g) \).

**Proof.** If \( NF_{\mathcal{G}}(f) = NF_{\mathcal{G}}(g) \) then \( f - g \in I \) (this is true, whether or not \( \mathcal{G} \) is a Gröbner basis). On the other hand, if \( NF_{\mathcal{G}}(f) \neq NF_{\mathcal{G}}(g) \) then

\[
NF_{\mathcal{G}}(f - g) = NF_{\mathcal{G}}(NF_{\mathcal{G}}(f) - NF_{\mathcal{G}}(g)) = NF_{\mathcal{G}}(f) - NF_{\mathcal{G}}(g) \neq 0.
\]

By Theorem 3.3.9, \( f - g \notin I \), so \( f \) and \( g \) are not in the same coset. \( \square \)

**Definition 10.3.3.** Let \( M \) be a monomial ideal. The standard monomials of \( M \) are the monomials \( p^u \in \mathbb{K}[p] \) such that \( p^u \notin M \).

Proposition 10.3.2 guarantees that the normal form can be used as a unique representative as elements of a coset. Note that the only monomials that can appear in the in a normal form \( NF_{\mathcal{G}}(f) \) are the standard monomials of \( \text{in}_\prec(I) \). Clearly, any polynomial whose support is in only the standard monomials of \( \text{in}_\prec(I) \) will be a normal form. This proves:

...
Proposition 10.3.4. For any ideal $I \subseteq \mathbb{K}[p]$, and any monomial order $\prec$, the set of standard monomials of $\text{in}_\prec(I)$ form a $\mathbb{K}$-vector space basis for the quotient ring $\mathbb{K}[p]/I$.

The structure of the set of standard monomials of an initial ideal $\text{in}_\prec(I)$ is particularly interesting in the case of toric ideals, as it relates to integer programming.

Proposition 10.3.5. Let $A \in \mathbb{Z}^{k \times r}$ be an integer matrix and $c \in \mathbb{Q}^r$ be a generic cost vector with respect to the toric ideal $I_A \subseteq \mathbb{K}[p]$. The standard monomials $p^u$ of the initial ideal $\text{in}_c(I_A)$ are the optimal points of all integer programs (10.2.1) for $b \in \mathbb{N}A$.

Proof. If $c$ is generic then the integer program (10.2.1) has a unique solution for each $b \in \mathbb{N}A$. For a fixed $b$ call this optimum $u$. Computing the normal form of any monomial $p^v$ where $v \in \mathcal{F}(u)$ with respect to the Gröbner basis of $I_A$ under the term order $\prec_c$ produces the monomial $p^u$ which is a standard monomial. This shows that every monomial $p^v$ is either in $\text{in}_c(I_A)$ or is optimal. □

Note that for generic $c$, Proposition 10.3.5 gives a bijection between the elements of the semigroup $\mathbb{N}A$ and the standard monomials of $\text{in}_c(I_A)$.

10.4. Linear Programming Relaxations

Integer programming is generally an NP-hard problem so it is unlikely that there is a polynomial time algorithm that solves general integer programs. In the applications in Sections 10.1.1 and 10.1.2, we might be only interested in some bounds we can compute quickly without worrying about whether or not they are tight all the time. In Section 10.5, we explore the possibility of developing general closed formulas for bounds on cell entries. In this section, we focus on a general polynomial time algorithm to get rough bounds, namely the computation of linear programming bounds as an approximation to integer programming bounds.

For given $A$, $b$ and $c$ recall that $\text{IP}(A,b,c)$ is the optimal value of the integer program (10.2.1) and $\text{LP}(A,b,c)$ is the optimal value of the linear program (10.2.2). Linear programs can be solved in polynomial time using interior point methods, so we might hope that perhaps for the bounds problem that arises in the analysis of contingency tables, that $\text{IP}(A,b,c) = \text{LP}(A,b,c)$ for all $b$ for the particular $A$ and $c$ that arise in contingency table problems. There is a precise algebraic way to characterize when this equality happens for all $b$ in the case of generic cost vectors $c$. 
Theorem 10.4.1. Let \( A \in \mathbb{Z}^{k \times r} \) and \( c \in \mathbb{Q}^r \) generic with respect to the toric ideal \( I_A \). Then \( LP(A, b, c) = IP(A, b, c) \) for all \( b \in \mathbb{N}^A \) if and only if \( \text{in}_c(I_A) \) is a squarefree monomial ideal.

**Proof.** Suppose that \( \text{in}_c(I_A) \) is not a squarefree monomial ideal and let \( p^u \) be a minimal generator of \( I_A \) that has some exponent greater than one. We may suppose \( u_1 > 1 \). Since \( p^u \) is a minimal generator of \( \text{in}_c(I_A) \), \( p^{u-e_1} \) is a standard monomial of \( \text{in}_c(I_A) \). In particular, the vector \( u - e_1 \) is optimal for the integer program in its fiber. Now let \( v \in \mathbb{N}^r \) so that \( p^u - p^v \) is in the Gröbner basis of \( I_A \) with respect to \( c \) with \( p^u \) as leading term. Since \( c \) is generic, \( c^T u > c^T v \) which means that \( (u - e_1) - \frac{u_1-1}{u_1}(u - v) \) is a nonnegative vector rational vector which has a better cost than \( u - e_1 \). Hence, \( LP \) does not equal \( IP \) for the corresponding vector \( b = A(u - e_1) \).

Conversely, suppose that \( \text{in}_c(I_A) \) is a squarefree monomial ideal such that \( v \) is LP optimal, \( u \) is IP optimal, and \( c^T v < c^T u \). For this to happen \( v \) must have rational coordinates. Let \( D \) be the least common multiple of the denominators of the nonzero coordinates of \( v \). Consider the linear and integer programs where \( b \) has been replaced by \( Db \). Clearly \( Dv \) is the optimum for the LP since it continues to be a vertex of the corresponding polytope. Since we cleared denominators, it is also an integer vector so is IP optimal. This means that \( Du \) is not IP optimal. So there exists a binomial \( p^w - p^{w'} \) in the Gröbner basis such that \( Du - w + w' \geq 0 \). Since the cost vector is generic, \( Du - w + w' \) is IP feasible and must have improved cost. However, \( w \) is a zero one vector. This forces that \( u \geq w \) coordinatewise. This implies that \( u - w + w' \geq 0 \) as well and since \( c \) is generic, \( u - w + w' \) also has improved cost. This contradicts our assumption that \( u \) was IP optimal. \( \square \)

For the minimization and maximization of a cell entry given marginals the cost vectors \( c \) are not generic. There is an analogous statement to Theorem \[10.4.1\] for the lexicographic and reverse lexicographic term orders.

**Proposition 10.4.2.** Let \( A \in \mathbb{Z}^{k \times r} \) with \( 1 \in \text{rowspan}(A) \). Let \( \prec_{\text{lex}} \) be the lexicographic order with \( p_1 \succ_{\text{lex}} p_2 \succ_{\text{lex}} \cdots \) and let \( \prec_{\text{revlex}} \) be the reverse lexicographic order with \( p_1 \prec_{\text{revlex}} p_2 \prec_{\text{revlex}} \cdots \).

(1) If \( \text{in}_{\text{lex}}(I_A) \) is a squarefree monomial ideal then \( LP(A, b, e_1) = IP(A, b, e_1) \) for all \( b \in \mathbb{N}^A \).

(2) If \( \text{in}_{\text{revlex}}(I_A) \) is a squarefree monomial ideal then \( LP(A, b, -e_1) = IP(A, b, -e_1) \) for all \( b \in \mathbb{N}^A \).

The proof combines the arguments of the proofs of Theorem \[10.4.1\] and Proposition \[10.2.4\] and is left as an exercise. Note that whether or not
Example 10.4.3. Consider the matrix $A_\Gamma$ for $\Gamma = [1][2][3]$ and $r_1 = r_2 = r_3 = 2$. Let $\prec_{\text{lex1}}$ be the lexicographic order with

$$
\begin{align*}
P_{111} &\prec_{\text{lex1}} P_{112} \prec_{\text{lex1}} P_{121} \prec_{\text{lex1}} P_{122} \prec_{\text{lex1}} P_{211} \\
P_{211} &\prec_{\text{lex1}} P_{212} \prec_{\text{lex1}} P_{221} \prec_{\text{lex1}} P_{222}.
\end{align*}
$$

Then $\text{in}_{\text{lex1}}(I_A)$ is a squarefree monomial ideal:

$$
\text{in}_{\text{lex1}}(I_A) = \langle p_{211}p_{222}, p_{121}p_{222}, p_{121}p_{212}, p_{112}p_{222}, p_{112}p_{221}, p_{111}p_{222}, p_{111}p_{221}, p_{111}p_{212}, p_{111}p_{122} \rangle.
$$

On the other hand, with respect to the lexicographic order with

$$
\begin{align*}
P_{111} &\prec_{\text{lex2}} P_{112} \prec_{\text{lex2}} P_{211} \prec_{\text{lex2}} P_{212} \prec_{\text{lex2}} P_{221} \prec_{\text{lex2}} P_{222} \\
P_{112} &\prec_{\text{lex2}} P_{121} \prec_{\text{lex2}} P_{211} \prec_{\text{lex2}} P_{212} \prec_{\text{lex2}} P_{221} \prec_{\text{lex2}} P_{222}
\end{align*}
$$

the initial ideal $\text{in}_{\text{lex2}}(I_{A_\Gamma})$ is not squarefree, since

$$
\text{in}_{\text{lex2}}(I_{A_\Gamma}) = \langle p_{221}p_{112}, p_{212}p_{121}, p_{212}p_{221}, p_{122}p_{211}, p_{122}p_{221}, p_{222}p_{121}, p_{222}p_{212}, p_{111}p_{222}, p_{111}p_{221}, p_{111}p_{122} \rangle.
$$

Although the second Gröbner basis is not revealing about whether or not the linear programming relaxation solves the integer programs (since we consider a nongeneric cost vector), the first Gröbner basis shows that in fact linear programming does solve the integer program in this case. \qed

More generally, for a nongeneric cost vector $c$ and an ideal $I_A$, we can define a refinement of $\prec_c$ to be any term order $\prec$ such that $\text{in}_{\prec}(p^u - p^v) = \text{in}_{\prec_c}(p^u - p^v)$ for all $p^u - p^v \in I_A$ such that $\text{in}_{\prec}(p^u - p^v)$ is a monomial. Proposition 10.4.2 can be generalized to show that if $\prec$ is a refinement of the weight order $\prec_c$ then if $\text{in}_{\prec}(I_A)$ is a squarefree monomial ideal then $LP(A, b, c) = IP(A, b, c)$ for all $b \in NA$.

Example 10.4.3 shows that we might need to investigate many different lexicographic term orders before we find one that gives a squarefree initial ideal. On the other hand, a result of [Sul06] shows that toric ideals that are invariant under a transitive symmetry group on the variables either have every reverse lexicographic initial ideal squarefree or none are, and that this is equivalent to linear programming solving the integer programs for the upper bounds on coordinates problem. Since this symmetry property is satisfied for the toric ideals $I_{A_\Gamma}$ of hierarchical models, one can check for the existence of a squarefree reverse lexicographic initial ideal for these models in a single ordering of the variables.

In general, the problem of classifying which $\Gamma$ and $r = (r_1, \ldots, r_m)$ have $I_{A_\Gamma}$ possessing squarefree lexicographic and/or reverse lexicographic initial
ideal is an interesting open problem. One partial result is the following from [Sul06].

**Theorem 10.4.4.** Let $\Gamma$ be a graph and suppose that $r = 2$, so we consider a binary graph model. Then $I_{A,\Gamma}$ has a squarefree reverse lexicographic initial ideal if and only if $\Gamma$ is free of $K_4$ minors and every induced cycle in $\Gamma$ has length $\leq 4$.

Extending this result to arbitrary simplicial complexes and also to lexicographic term orders is an interesting open problem. Computational results appear in [BS17].

In the other direction, one can ask how large the difference between $IP(A, b, c)$ and $LP(A, b, c)$ can be for these cell entry bound problems, in cases where the linear programming relaxations do not always solve the integer program. A number of negative results are known producing instances with exponential size gaps between the LP relaxations and the true IP bounds for lower bounds [DLO06, Sul05]. These examples for gaps on the lower bounds can often be based on the following observation.

**Proposition 10.4.5.** Let $A \in \mathbb{Z}^{k \times r}$ and suppose that $F(u) = \{u, v\}$ is a two element fiber with $\text{supp}(u) \cap \text{supp}(v) = \emptyset$. Then $p^u - p^v$ belong to any minimal binomial generating of $I_A$ and reduced Gröbner basis of $I_A$. Furthermore, if $u_1 > 1$ then

$$IP(A, A(u - e_1), e_1) - LP(A, A(u - e_1), e_1) = u_1 - 1.$$  

**Proof.** The fact that $p^u - p^v$ is any binomial generating set follows from the Markov basis characterization of generating sets: the move $u - v$ is the only one that can connect this fiber. A similar argument holds for the Gröbner basis statement.

For the statement on gaps, note the $F(u - e_1) = \{u - e_1\}$ consists of a single element, so the minimal value for the first coordinate in the fiber is $u_1 - 1$. However, the nonnegative real table $u - e_1 - \frac{u_1 - 1}{u_1}(u - v)$ has first coordinate zero.  

**Example 10.4.6.** Let $\Gamma = K_5$ be the simplicial complex on [5] whose facets are all pairs of vertices, and let $r = (2, 2, 2, 2, 2)$. Among the generators of the toric ideal $I_{A_{K_5}}$ is the degree 8 binomial

$$p_{00000P00111P00101P01001P10001P11110}^3 - p_{00001P00110P00100P01000P10000P11111}^3.$$  

The corresponding vectors $u, v$ are the only elements of their fiber. Proposition 10.4.5 shows that there is a $b$ such that

$$IP(A_{K_5}, b, e_{00000}) - LP(A_{K_5}, b, e_{00000}) = 2.$$
Hoşten and Sturmfels [HS07a] showed that for any fixed $A$ and $c$, there is always a maximum discrepancy between the integer programming optimum and the linear programming relaxation. That is:

**Theorem 10.4.7.** Fix $A \in \mathbb{Z}^{k \times r}$ and $c \in \mathbb{Q}^r$. Then

$$\max_{b \in \mathbb{N}^A} (IP(A, b, c) - LP(A, b, c)) < \infty.$$ 

The number $\text{gap}(A, c) = \max_{b \in \mathbb{N}^A} (IP(A, b, c) - LP(A, b, c))$ is called the integer programming gap, and exhibits the worst case behavior of the linear programming relaxation. It can be computed via examining the irreducible decomposition of the monomial ideal $\text{in}_c(I_A)$ or a related monomial ideal in the case that $c$ is not generic with respect to $I_A$ [HS07a], as follows.

For an arbitrary $c \in \mathbb{Q}^r$, let $M(A, c)$ be the monomial ideal generated by all monomials $p^u$ such that $u$ is not optimal for the integer program (10.2.1) for $b = Au$. Note that every monomial $p^v \in M(A, c)$ has $v$ nonoptimal since if $u$ is nonoptimal in its fiber and $w$ is optimal in this same fiber, and $p^u | p^v$, then $v$ could not be optimal since $v + (w - u)$ is in the same fiber as $v$ and has a lower weight.

An ideal $I$ is irreducible if it cannot be written nontrivially as $I = J \cap K$ for two larger ideals $J$ and $K$. Each irreducible monomial ideal is generated by powers of the variable, specifically a monomial is irreducible if and only if it has the form

$$I_{u, \tau} = \langle p_i^{u_i+1} : i \in \tau \rangle,$$

where $u \in \mathbb{N}^r$ and $\tau \subseteq [r]$, and $u_i = 0$ if $i \notin \tau$. Every monomial ideal $M$ can be written in a unique minimal way as the intersection of irreducible monomial ideals. This is called the irreducible decomposition of $M$.

To each such irreducible monomial ideal in the irreducible decomposition of $M(A, c)$ we calculate the gap value associated to $c$ and $A$, which is the optimal value of the following linear program:

(10.4.1) $\max c^T u - c^T v$ such that $Av = Au$, and $v_i \geq 0$ for $i \in \tau$.

**Theorem 10.4.8.** [HS07a] The integer programming gap $\text{gap}(A, c)$ equals the maximum gap value over all irreducible components $I_{u, \tau}$ of the monomial ideal $M(A, c)$.

**Example 10.4.9.** Consider the hierarchical model with $\Gamma = [12][13][14][234]$ and $r = (2, 2, 2, 2)$. Consider the nongeneric optimization problem of minimizing the first cell entry in a $2 \times 2 \times 2 \times 2$ contingency table given the $\Gamma$ margins. Hence $c = e_{1111}$. The integer programming gap $\text{gap}(A_{\Gamma}, e_{1111})$ measures the discrepancy between integer programming and linear programming in this case. Note that $A_{\Gamma}$ is not normal in this case, so no initial ideal
of \( I_{A_{n}} \) is squarefree (see Exercise 10.4) and we must do further analysis to determine the value of \( \text{gap}(A_{n}, e_{1111}) \).

Since \( e_{1111} \) is not generic with respect to the matrix \( A_{n} \), \( M(A_{n}, e_{1111}) \) is not an initial ideal of \( I_{A_{n}} \). We can compute the ideal \( M(A_{n}, e_{1111}) \) as follows. First we compute the nonnomial initial ideal \( \text{in}_{e_{1111}}(I_{A_{n}}) \). The ideal \( M(A_{n}, e_{1111}) \) is the ideal generated by all the monomials contained in \( \text{in}_{e_{1111}}(I_{A_{n}}) \). This ideal can be computed using Algorithm 4.4.2 in [SST00], which has been implemented in Macaulay2. The following Macaulay2 code computes the ideal \( M(A_{n}, e_{1111}) \) and its irreducible decomposition:

```plaintext
loadPackage "FourTiTwo"
S = ZZ[x1,x2,x3,x4]
listofmonomials = matrix{{1,x1,x2,x3,x4,x1*x2,x1*x3, x1*x4, x2*x3,x2*x4,x3*x4,x2*x3*x4}};
A = transpose matrix toList apply((0,0,0,0)..(1,1,1,1),
i -> flatten entries sub(listofmonomials,
{x1 => i_0, x2 => i_1, x3=> i_2, x4 => i_3}))
L = toricGraver(A);
R = QQ[p_(1,1,1,1)..p_(2,2,2,2), MonomialOrder => {Weights =>
{1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0}}]
I = ideal gens toBinomial(L, R)
J = ideal leadTerm(1, I)
M = monomialSubideal(J)
K = transpose gens N
L = irreducibleDecomposition M
```

Among the 16 monomial irreducible ideals in the irreducible decomposition of \( M(A_{n}, e_{1111}) \) is the ideal

\[ \langle p_{1222}, p_{2112}, p_{2121}, p_{2211}^{2} \rangle. \]

To compute its gap value amounts to solving the linear program:

\[
\text{max} \quad -v_{1111} \quad \text{subject to} \quad A_{n}v = (A_{n})_{2211}, \quad \text{and} \quad v_{1222}, v_{2112}, v_{2121}, v_{2221} \geq 0.
\]

The solution to this linear program shows that the gap value for this irreducible component is 1/2. Looking at all 16 irreducible components in this case produced one component with gap value 1, which was the largest value. Hence, \( \text{gap}(A_{n}, e_{1111}) = 1. \)

### 10.5. Formulas for Bounds on Cell Entries

The formulas in Proposition 10.1.2 for upper and lower bounds on cell entries of a two-way contingency table given the row and column sums are extremely appealing and it is natural to wonder if there are generalizations of these formulas for larger tables and more complex marginals. For example, in the
10.5. Formulas for Bounds on Cell Entries

In the case of two-way contingency tables none of the Gröbner basis machinery is needed to compute bounds on cell entries and use the SIS procedures, so one might wonder if the Gröbner basis procedure is always needed. In principle there is always a closed formula for the linear programming upper and lower bounds, which can be revealed by the polyhedral geometry of the cone $\mathbb{R}_{\geq 0} A \Gamma$. As we have seen in previous sections, in some cases those LP optima are equal to IP optima, and this can be useful. In most cases, the resulting formula that arises becomes increasingly complicated as the size of the contingency table increases.

We first consider the general integer program:

\[
\text{(10.5.1)} \quad \max x_1 \text{ subject to } Ax = b \text{ and } x \in \mathbb{R}_{\geq 0}^r.
\]

associated with maximizing a coordinate. This optimization problem can be reformulated as follows in terms of the cone $\mathbb{R}_{\geq 0} A$. 

**Proposition 10.5.1.** The linear program [10.5.1] is equivalent to the optimization problem

\[
\text{(10.5.2)} \quad \max z \text{ subject to } b - z A_1 \in \text{cone}(A)
\]

where $A_1$ denotes the first column of $A$.

The proof of Proposition [10.5.1] is straightforward and left to the reader. The application of Proposition [10.5.1] comes from knowing the facet defining inequalities of the cone $\mathbb{R}_{\geq 0} A$. Indeed, suppose that $c^T y \geq 0$ is a valid inequality for cone$(A)$. Then we must have $c^T (b - z A_1) \geq 0$. If $c^T A_1 > 0$ then we deduce that $z \leq c^T b / c^T A_1$. Taking the minimum over all such formulas gives the solution to the linear program [10.5.1]. For example, this can be used to give a simple proof of the upper bound in the case of 2-way tables.

**Example 10.5.2.** Let $\Gamma = [1][2]$ and $r = (r_1, r_2)$, and consider the matrix $A \Gamma$ and the corresponding optimization problem of maximizing the first coordinate of $x_{11}$ subject to the constraints $A \Gamma x = b$, and $x \geq 0$. The cone cone$(A \Gamma) \subseteq \mathbb{R}^{r_1+r_2}$ is given by a simple explicit description

$$
\text{cone}(A \Gamma) = \{(y^{(1)}, y^{(2)}) \in \mathbb{R}^{r_1} \oplus \mathbb{R}^{r_2} : y^{(1)}_i \geq 0 \text{ for all } i \in [r_1], y^{(2)}_i \geq 0 \text{ for all } i \in [r_2], \\
\sum_{i=1}^{r_1} y^{(1)}_i = \sum_{i=1}^{r_2} y^{(2)}_i \}.
$$

The first column vector of $A \Gamma$ is the vector $e_1^{(1)} \oplus e_1^{(2)}$ where $e_1^{(j)}$ denotes the first standard unit vector in $\mathbb{R}^{r_j}$. Of the $r_1 + r_2$ facet defining inequalities $c^T y \geq 0$, of cone$(A \Gamma)$, only two of them satisfy that $c^T A_1 > 0$. These correspond to the inequalities $y^{(1)}_1 \geq 0$ and $y^{(2)}_1 \geq 0$. Now we apply the formula
214 10. Bounds on Cell Entries

\[ z \leq \frac{c^T b}{c^T A_1}. \]

Note that in this context \( b = (u_{1+}, \ldots, u_{r_1+}, u_{1+}, \ldots, u_{r_2+}) \).
So the inequality \( y_1^{(1)} \geq 0 \) implies that \( x_{11} \leq u_{1+} \) and the inequality \( y_1^{(2)} \geq 0 \)
implies that \( x_{11} \leq u_{+1} \). In summary, \( x_{11} \leq \min(u_{1+}, u_{+1}) \).

**Example 10.5.3.** For a more complex example consider the case of the binary graph model from Chapter 8 with \( G = K_3 \), the complete graph on 3 vertices. This is equivalent to the hierarchical model with \( \Gamma = [12][13][23] \) and \( r = (2,2,2) \), but the binary graph representation has the advantage that the matrix \( A_G \) has full row rank, so there is no ambiguity in the choice of the facet defining inequalities.

The facet defining inequalities of the polyhedral cone \( \text{cone}(A_G) \) were given for general \( K_4 \) minor free graphs in Theorem 8.2.9. For the case of the graph \( K_3 \), there are sixteen inequalities in total. These are the twelve basic inequalities:

\[ p_{ij} \geq 0, p_i - p_{ij} \geq 0, p_{ij} + p_0 - p_i - p_j \geq 0 \]

for \( i, j \in \{1,2,3\} \) and four triangle inequalities:

\[
\begin{align*}
    p_{12} - p_{13} - p_{23} + p_3 &\geq 0 \\
    p_{13} - p_{12} - p_{23} + p_2 &\geq 0 \\
    p_{23} - p_{12} - p_{13} + p_1 &\geq 0 \\
    p_0 + p_{12} + p_{13} + p_{23} - p_1 - p_2 - p_3 &\geq 0
\end{align*}
\]

The column vector corresponding to the coordinate \( x_{000} \) is \((1,0,0,0,0,0)^T\). So the bounds we seek are only formulas that come from the inequalities where \( p_0 \) appears with a positive coefficient. From this, we deduce the following upper bound on the coordinate \( x_{111} \):

\[
x_{111} \leq \min(p_0 - p_1 - p_2 + p_{12}, p_0 - p_1 - p_2 + p_{12}, p_0 - p_2 - p_3 + p_{23}, p_0 - p_1 - p_2 - p_3 + p_{12} + p_{13} + p_{23}).
\]

We can also express these formulas in terms of entries in the 2-way marginals alone, those these formulas are not unique. in particular there are many choices for the final formula:

\[
x_{111} \leq \min(u_{11+} + u_{1+1} + u_{11+} + u_{21+} + u_{22+} - u_{+12} - u_{+21}).
\]

For lower bounds we can use a similar idea to find formula, but the relevant cone changes from \( \text{cone}(A) \) to a different cone. Indeed, we need to perform the following minimization:

**Proposition 10.5.4.** The linear program \( \min x : Ax = b, x \geq 0 \), is equivalent to the optimization problem

\[
\min z \text{ subject to } b - z A_1 \in \text{cone}(A'), z \geq 0
\]
10.5. Formulas for Bounds on Cell Entries

where \( A_1 \) denotes the first column of \( A \), and \( A' \) is the matrix obtained from \( A \) by deleting the first column.

From Proposition 10.5.4 we deduce that \( z \geq c^T b c^T A_1 \) for any valid inequality \( c^T y \geq 0 \) for cone(\( A' \)) for which \( c^T A_1 < 0 \). The proof of Proposition 10.5.4 follows because we want to choose the smallest nonnegative value of \( z \) such that \( b - z A_1 \) can be written as a nonnegative combination of the other columns. Note that this is also true for the maximization problem, but we do not need to consider cone(\( A' \)) because we automatically end up in cone(\( A' \)) when performing the maximization (whereas, this is not forced in the minimization, i.e. we can always choose \( z = 0 \), if we worked with cone(\( A \)) in the minimization problem).

The polyhedron cone(\( A' \)) is less well-studied for contingency table problems, but can be worked out in simple examples, and deserves further study.

Example 10.5.5. Let \( \Gamma = [1][2] \) and \( r = (r_1, r_2) \), and consider the matrix \( A_\Gamma \) and the corresponding optimization problem of minimizing the first coordinate of \( x_{11} \) subject to the constraints \( A_\Gamma x = b \), and \( x \geq 0 \). The cone \( \text{cone}(A_\Gamma) \subseteq \mathbb{R}^{r_1+r_2} \) is given by a simple explicit description:

\[
\text{cone}(A_\Gamma) = \{(y^{(1)}, y^{(2)}) \in \mathbb{R}^{r_1} \oplus \mathbb{R}^{r_2} : \\
y_i^{(1)} \geq 0 \text{ for all } i \in [r_1], y_i^{(2)} \geq 0 \text{ for all } i \in [r_2] \\
\sum_{i=2}^{r_1} y_i^{(1)} - y_1^{(2)} \geq 0 \\
\sum_{i=1}^{r_1} y_i^{(1)} = \sum_{i=1}^{r_2} y_i^{(2)} \}. 
\]

The only inequality \( c^T y \geq 0 \) such that \( c^T A_1 < 0 \) is the new inequality, \( \sum_{i=2}^{r_1} y_i^{(1)} - y_1^{(2)} \geq 0 \) from which we deduce that

\[
x_{11} \geq u_{+1} - \sum_{i=2}^{r_1} u_{i+}. 
\]

Note that because cone(\( A_\Gamma' \)) is not full dimensional, there might be many different ways to represent this expression in terms of the marginals. For, instance \( x_{11} \geq u_{+1} + u_{1+} - u_{++} \) is an equivalent inequality known as the Bonferroni bound. Always we will need to take the max of whatever expressions we find and 0.

As we have seen, the decomposable hierarchical models possess similar properties to the case of 2-way contingency tables. This similarity extends to the existence of simple formulas for the upper and lower bounds for the cell entries given the decomposable marginals [DF00].
Theorem 10.5.6. Let $\Gamma$ be a decomposable simplicial complex with facets $F_1, F_2, \ldots, F_k$. Suppose further that these facets are ordered so that for each $j = 2, \ldots, k$, the complex $\Gamma_j$ whose facets are $\{F_1, \ldots, F_{j-1}\}$ is also decomposable and $F_j \cap \Gamma_j$ is a simplex $2S_i$. Let $u \in \mathbb{N}^R$ be a contingency table. Then for each $i \in R$ and $v \in F(u)$,

$$\min \left((u|_{F_1})_{i_{F_1}}, \ldots, (u|_{F_k})_{i_{F_k}}\right) \geq v_i \geq \max \left(\sum_{j=1}^{k} (u|_{F_j})_{i_{F_j}} - \sum_{j=2}^{k} (u|_{S_j})_{i_{S_j}}, 0\right).$$

Furthermore, the upper and lower bounds are tight, in the sense that for each coordinate there exist two tables $v^U, v^L \in F(u)$ achieving the upper and lower bounds, respectively.

The ordering of the facets of $\Gamma$ in Theorem 10.5.6 is called a perfect elimination ordering.

Example 10.5.7. Let $\Gamma = [12|23|24][567]$. A perfect elimination ordering of the facets is given by the ordering that the facets are listed in the complex. The resulting sequence of separators is $S_2 = \{2\}, S_3 = \{2\}, S_4 = \emptyset$. Theorem 10.5.6 gives the following tight upper and lower bounds on the cell entry $v_{1i_12i_23i_34i_45i_56i_67}$ given the marginals $A_\Gamma u$:

$$\min \left((u|_{12})_{i_1{i_2}}, (u|_{23})_{i_2{i_3}}, (u|_{24})_{i_2{i_4}}, (u|_{567})_{i_5{i_6{i_7}}}\right) \geq v_{1i_12i_23i_34i_45i_56i_67} \geq \max \left((u|_{12})_{i_1{i_2}} + (u|_{23})_{i_2{i_3}} + (u|_{24})_{i_2{i_4}} + (u|_{567})_{i_5{i_6{i_7}}} - 2(u|_{2})_{i_2} - u_{10}, 0\right).$$

10.6. Exercises

Exercise 10.1. Let $\Gamma = [1][2][3]$. Find formulas for the upper and lower bounds on $u_{ijk}$ given the $A_\Gamma u = b$ and $u \in \mathbb{N}^{r_1 \times r_2 \times r_3}$. Show that your bounds are tight and that every value in between the upper and lower bounds occurs for some table with the given fixed margins.

Exercise 10.2. Let $A \in \mathbb{N}^{d \times r}$ be an integer matrix and $b \in \mathbb{R}^d$. For each $i$ suppose $L_i^t, U_i^t \in \mathbb{R}^r$ are vectors such that $L_i^t \leq x_i \leq U_i^t$ for all $x \in \mathbb{R}^r$ satisfying $Ax = b, x \geq 0$. That is, $L_i^T$ and $U_i^T$ are valid upper and lower bounds on coordinates of $x$ in the polytope $P(A, b) = \{x \in \mathbb{R}^r : Ax = b, x \geq 0\}$.

Define $L_i^{t+1}$ and $U_i^{t+1}$ as follows:

$$L_i^{t+1} = \max(0, L_i^t, \max_{j:A_{ji} \neq 0} \left(\frac{1}{A_{ji}} \sum_{k \neq i} A_{jk} U_k\right))$$

$$U_i^{t+1} = \min(U_i^t, \min_{j:A_{ji} \neq 0} \left(\frac{1}{A_{ji}} \sum_{k \neq i} A_{jk} L_k\right)).$$
Show that $L^{t+1}$ and $U^{t+1}$ are also valid upper and lower bounds on coordinates of $x$ in the polytope $P(A,b)$, that improve $L^t$ and $U^t$.

Exercise 10.2 is the basis for the shuttle algorithm of Dobra and Fienberg [DF01, Dob02] for computing bounds on cell entries in contingency tables.

**Exercise 10.3.** Prove Proposition 10.4.2

**Exercise 10.4.** Show that if there is a term order such that $\succ_\omega(I_A)$ is a squarefree monomial ideal then $NA$ is a normal semigroup.

**Exercise 10.5.** Let $\Gamma = K_4$ and take $r = (2,2,2,2)$. Show that there is a $b$ such that $IP(A_\Gamma, b, e_{1111}) - LP(A_\Gamma, b, e_{1111}) = 1$.

**Exercise 10.6.** Let $\Gamma = K_4$ and take $r = (2,2,2,2)$. Show that $\text{gap}(A_\Gamma, e_{1111}) = 5/3$.

**Exercise 10.7.** Let $\Gamma = K_4$ and take $r = (2,2,2,2)$. Find an explicit formula for the real upper and lower bounds on the cell entry $x_{1111}$ given the marginal totals akin to the formula we derived in Example 10.5.3.
Chapter 11

Exponential Random Graph Models

In this chapter we study the exponential random graph models, which are statistical models that are frequently used in the study of social networks. While exponential random graph models are a special case of discrete exponential family models, their study presents some subtleties because data sets that arise are of a vastly different nature. For a typical exponential family model, we imagine receiving i.i.d. samples from an underlying distribution in the model. However, for an exponential random graph model, we typically only have a sample size of 1, that is, we observe a single graph and would like to make inferences about the process that generated it. This issue of small sample size presents serious problems about the existence of maximum likelihood estimates, and also means that we cannot use hypothesis tests based on asymptotics. These issues can be addressed via analyzing the polyhedral structure of the set of sufficient statistics, in the first case, and developing tools for performing Fisher’s exact test in the second.

11.1. Basic Setup

Models for random graphs are widely used and are of interest in network science, including the study of social networks. Generally, we create a statistical model for a random graph where the probability of a particular graph depends on some features of the graph. Exponential random graphs models provide a precise way to make to set up a very general family of such models.

Definition 11.1.1. Let $G_m$ denote the set of all undirected simple graphs on $m$ vertices. A graph statistic is a function $t : G_m \to \mathbb{R}$. 219
Examples of graph statistics that are commonly used in this area include: the number of edges in the graph, the number of isomorphic copies of a certain small graph, the degree of a particular vertex, etc.

Definition 11.1.2. Let \( T = (t_1, \ldots, t_k) \) be graph statistics. The exponential random graph model associated to \( T \) is the exponential family where

\[
P(X = G) = \frac{1}{Z(\theta)} \exp(t_1(G)\theta_1 + \cdots + t_k(G)\theta_k)
\]

where \( \theta = (\theta_1, \ldots, \theta_k) \in \mathbb{R}^k \) is a real parameter and \( Z(\theta) \) is the normalizing constant

\[
Z(\theta) = \sum_{G \in G_m} \exp(t_1(G)\theta_1 + \cdots + t_k(G)\theta_k).
\]

Example 11.1.3. The prototypical example of an exponential random graph model is the Erdős-Rényi random graph model. In the language of exponential random graph models, the Erdős-Rényi model has a single parameter \( \theta \), and the corresponding graph statistics \( t(G) \) is the number of edges in \( G \). Setting \( p = \frac{\exp(\theta)}{1 + \exp(\theta)} \) we see that the probability of observing a particular graph \( G \) is

\[
P(X = G) = p^{E(G)}(1 - p)^{(m^2) - |E(G)|}.
\]

An interpretation of this probability is that each edge in the graph is present independently with probability \( p \), which is the usual presentation for the Erdős-Rényi random graph model.

One nice property of this simple one parameter model is that the normalizing constant \( Z(\theta) \) ends up having a simple factorization. Indeed, \( Z(\theta) = (1 + \exp(\theta))^{\binom{m}{2}} \). This makes this exponential random graph model especially easy to work with, since we do not need to actually sum over all graphs to find the probability of a graph. There typically is not such a simple formula for the normalizing constant.

Example 11.1.4. Consider the exponential random graph model with graph statistics \( T = (t_1, t_2) \) where \( t_1(G) \) is the number of edges in \( G \) and \( t_2(G) \) is the number of triangles in \( G \) (that is, the number of triples of vertices \( i, j, k \) such that all of \( ij, ik, jk \) are edges in \( G \)). Although there are \( 2^m(m-1)/2 \) different graphs on \( m \) vertices, there are significantly fewer possible pairs \((t_1(G), t_2(G))\). For example, for \( m = 7 \), there are 2097152 graphs but only 110 different pairs of values of the number of edges and number of triangles. These 110 points and their convex hull is illustrated in Figure 11.1. Note that the fact that the line segment connecting the points \((0, 0)\) and \((21, 35)\) does not contain any other points of the form \((t_1(G), t_2(G))\) implies that the normalizing constant \( Z(G) \) is an irreducible polynomial in the quantities \( \exp(\theta_1) \) and \( \exp(\theta_2) \).
One great difference between using exponential random graph models and the majority of other exponential families we have discussed thus far is that the datasets that are observed do not typically consist of i.i.d. samples from an underlying distribution. Rather, the dataset is simply a single graph (or perhaps, a time series of graphs on the same node set). In this setting, large sample theory does not apply, so hypothesis tests based on asymptotic approximations to test statistics are not appropriate. In particular, hypothesis testing should be performed using Fisher’s exact test.

To perform Fisher’s exact test for an exponential random graph model, we need to sample from the set of all graphs with a given sufficient statistic. As we only have one sample, there is no multinomial coefficient that appears in the likelihood function, so we sample from the uniform distribution on a fiber. For even quite simple models, it is not at all clear how to construct a Markov basis for the sampling problem.

Example 11.1.5. For the model in Example 11.1.4, we would need to sample from the set of graphs with a fixed number of vertices, edges, and triangles. It is unclear what a general strategy for such sampling might be. For instance, suppose we want to sample from the set of graphs with $2m$ vertices, $m^2$ edges, and no triangles. The only such graphs are the complete bipartite graphs with bipartition of vertices into parts of size $m$ and $m$. A move that connects two such graphs will have to involve swapping two vertices between the different parts of the bipartition. This has the effect of changing $2m - 2$ edges. In fact, for this model there is no set of moves that connects fibers that only involves a bounded number of edges. 

\[ \square \]
For most exponential random graph models, sampling from fibers becomes a purely combinatorial undertaking. However, for certain specific exponential random graphs models, more algebraic tools can be employed to design sampling schemes. We will see this in Section 11.2.

One key issue in using the exponential random graph models is estimating their parameters from data. As we discussed in Chapter 8, the maximum likelihood estimates will exist if and only if the observed sufficient statistics lie in the interior of the convex hull of the set of all sufficient statistics. For many exponential graph models, a large proportion of graphs have their sufficient statistics on or near to the boundary of the convex hull, and this presents a problem for inference with these models.

Example 11.1.6. Consider the exponential random graph model from Example 11.1.4, and suppose that we observe a graph $G$ with seven vertices and sufficient statistics $(13, 8)$, that is 13 edges and 8 triangles. Letting $y_1 = \exp(\theta_1)$ and $y_2 = \exp(\theta_2)$, we need to optimize the function $y_1^{13} y_2^8 Z(y_1, y_2)^{-1}$ where $Z(y_1, y_2)$ is the normalizing constant, a polynomial of degree 56 in $y_1$ and $y_2$ with 110 terms. Since this is an exponential family, there is a unique maximum in the positive orthant. This is obtained for $y_1 \approx 2.0396$ and $y_2 \approx 0.8880$. On the other hand, if we observe a graph with 7 vertices 13 edges and only 4 triangles, while this data point is not on the boundary of the convex hull, it is quite close to the boundary, and the computation of maximum likelihood estimates is quite slow to converge, suggesting a limiting value with $y_1$ large and $y_2$ close to zero. These issues about the existence and difficulty of computing maximum likelihood estimates in ERGMs are studied in detail in [RPF13].

11.2. The Beta Model and Variants

In this section, we discuss some widely used exponential random graph models that are based on degrees of vertices. Unlike the simple model that was discussed in Example 11.1.4 in Section 11.1, these models have a number of parameters that increases with the graph size. This makes it especially difficult to talk about asymptotic properties of these models. However, the beta model and its variants also possess certain nice properties that make them easier to analyze and where connections to toric ideals can be made.

Definition 11.2.1. Let $G$ be a graph with vertex set $[m]$. For $i \in [m]$ let $\deg_i(G)$ denote the number of edges of $G$ incident to vertex $i$. This number is called the degree of vertex $i$. The beta model is the exponential random graph model for an $m$ vertex graph whose sufficient statistics are $(\deg_1(G), \ldots, \deg_m(G))$. 
Among the nice properties of the beta model are that its normalizing constant is simple to compute.

**Proposition 11.2.2.** The normalizing constant for the beta model is

\[ Z(\theta) = \prod_{1 \leq i < j \leq m} (1 + \exp(\theta_i + \theta_j)). \]

**Proof.** For each pair \(i, j\), the corresponding edge is either in the graph, or not in the graph. If it is in the graph, it contributes +1 to \(\text{deg}_i(G)\) and \(\text{deg}_j(G)\). If it is not in the graph, the degree remains unchanged. This explains the two terms in the product for each pair \(1 \leq i < j \leq m\). \(\square\)

An integer vector \(d = (d_1, \ldots, d_m)\) is called a **degree sequence** if it is the sequence of vertex degrees of some graph on \(m\) vertices. The polytope of all sufficient statistics of the beta model consists of the convex hull of all degree sequence vectors. These possible degree sequences are characterized by the Erdős-Gallai theorem [EG60].

**Theorem 11.2.3.** A sequence of nonnegative integers \((d_1, \ldots, d_m)\) with \(d_1 \geq d_2 \geq \cdots \geq d_m\) is the degree sequence of a simple graph if and only if \(d_1 + \cdots + d_m\) is even and for all \(k = 1, \ldots, m\),

\[ \sum_{i=1}^{k} d_i \leq k(k - 1) + \sum_{i=k+1}^{m} \min(d_i, k). \]

A closely related model to the beta model is the Rasch model, which can be seen in various guises. The closest relation to the beta model follows from taking the beta model restricted to bipartite graphs with a fixed bipartition of the vertices. There is also a simple description of which vectors are actually possible as sufficient statistics vectors in this model, provided by the Gale-Ryser theorem [Gal57, Rys57].

**Theorem 11.2.4.** A pair of nonnegative integer sequences \((d_1, \ldots, d_m)\), \((e_1, \ldots, e_{m'})\) with \(d_1 \geq d_2 \geq \cdots \geq d_m\) and \(e_1 \geq \cdots \geq e_m\) is a pair of degree sequences of a bipartite graph if and only if \(\sum_{i=1}^{m} d_i = \sum_{i=1}^{m'} e_i\) and for \(k = 1, \ldots, m\),

\[ \sum_{i=1}^{k} d_i \leq \sum_{i=1}^{m'} \min(e_i, k). \]

Each simple bipartite graph with bipartition of the vertex set with \(m\) and \(m'\) vertices respectively, naturally corresponds to an \(m \times m'\) table of zeros and ones. Fixing the vertex degrees is equivalent to fixing the row and columns sums of that matrix. Hence, the fiber of bipartite graphs with fixed vertex degrees can be connected using moves that involve changing only two edges at a time, if we apply Theorem 9.4.6.
It is also possible to give a simple description of a Markov basis that will allow for a random walk on the fiber $F(G)$ consisting of the set of arbitrary graphs which have the same degree sequence as the given graph $G$, using a similar argument as Theorem 9.4.6.

**Proposition 11.2.5.** Consider the beta model and let $G$ be a graph with degree sequence $(d_1, \ldots, d_m)$. The fiber $F(G)$ consisting of all graphs with degree sequence $(d_1, \ldots, d_m)$ can be connected by local moves which replace the pair of edges in the graph $ij, kl$ with the pair of edges $ik, jl$ provided that neither of these edges already appeared in the graph.

We do not provide a proof of Proposition 11.2.5 but it follows the basic outline of the proof of Theorem 9.4.6.

The polyhedral descriptions of the set of degree sequences for simple graphs and bipartite graphs obtained in the Erdős-Gallai theorem and the Gale-Ryser theorem allow to easily check whether a given degree sequence lies on the boundary of the polytope of all degree sequences. Another use for these theorems is that they can be used in the development of sequential importance sampling machinery for approximately generating samples from the corresponding fibers. These strategies are described in [BD10] and [CDHL05] for graphs and bipartite graphs, respectively. We describe the basic idea of this procedure here for bipartite graphs, phrased in the language of sampling 0/1 matrices.

The basic sequential importance sampling scheme described in Section 10.1.1 involves filling entries in a contingency table one at a time, and computing bounds at each step. For sampling 0/1 matrices with fixed row and column sums, [CDHL05] advocates sampling each column one at a time (that is, filling a whole column in one step). Let the row sums and columns sums be $(d_1, \ldots, d_m)$ and $(e_1, \ldots, e_m^r)$ respectively. To choose a possible column with column sum $e_1$, amounts to choosing a 0/1 vector in $\mathbb{N}_m$. There are ${m} \choose {e_1}$ possible 0/1 vectors to choose. The most naive algorithm would be to simply pick such a vector uniformly at random to fill in the column, then update the row sums accordingly. One can check for rejection after each step using the Gale-Ryser theorem (i.e. check if the updated row and column sums are actually the row and columns sums of a 0/1 matrix). According to [CDHL05] this is not a very effective strategy because, intuitively, if a row sum is large the corresponding entry in that row should be 1 with higher probability than if the row sum were small. To remedy this problem, [CDHL05] proposes using the conditional Poisson distribution to sample columns. For $i = 1, \ldots, m$ let $p_i = \frac{d_i}{d_1 + \cdots + d_m}$ let $Z_i$ be a Bernoulli random variable with parameter $p_i$. The conditional Poisson distribution is the distribution of $(Z_1, \ldots, Z_m)$ conditional on $Z_1 + \cdots + Z_m = \frac{e_1}{d_1 + \cdots + d_m}$.
11.2. The Beta Model and Variants

It is not difficult to check that

\[
P(Z = z | Z_1 + \cdots + Z_m = e_{m'}) \propto \prod_{i=1}^{m} \left( \frac{p_i}{1 - p_i} \right)^{z_i}
\]

which ensures that rows with large row sums are more likely to have a 1 put in the corresponding position. \textbf{[CDHL05]} reports significantly improved performance under this sampling strategy. Further performance improvements can be obtained by making better use of the Gale-Ryser theorem beyond forcing rejections. For instance, analysis with the Gale-Ryser theorem can identify positions that must be 0 or must be 1, or regions that must contain a large number of 1s. These observations can lead to adjustments in how the conditional Poisson distribution is modified and further improvements. Similar strategies can also be employed for sampling graphs with fixed degree sequences as explained in \textbf{[BD10]}.

The beta model has a number of generalizations that involve either expanding the class of combinatorial structures considered or allowing more complicated graph interactions. For example, \textbf{[SSR+14]} generalizes the beta model to allow not just pairwise connections but connections of arbitrary size. This results in a hypergraph version of the beta model.

A widely used generalization of the beta model in social network analysis is the $p_1$-model \textbf{[HL81]}. This model essentially allows for different types of edge interactions between pairs of vertices. Between a pair of vertices $i, j$ there might be no edge, a directed edge from $i$ to $j$, a directed edge from $j$ to $i$, or a bidirected edge between $i$ and $j$. In the social network setting, this might be seen as having one user follow another on a social networking platform, so also both of the pair could follow each other. The full $p_1$ model has $2\binom{m}{2} + 2m - 1$ parameters which are for each pair $\lambda_{ij}$, and $\rho_{ij}$, a parameter $\theta$, and $\alpha_i$ and $\beta_j$. It is typically represented in log-linear form by looking at the log of the probability of the different types of edges appearing, via the following equations:

\[
\begin{align*}
\log p_{ij}(0, 0) &= \lambda_{ij} \\
\log p_{ij}(1, 0) &= \lambda_{ij} + \alpha_i + \beta_j + \theta \\
\log p_{ij}(0, 1) &= \lambda_{ij} + \alpha_j + \beta_i + \theta \\
\log p_{ij}(1, 1) &= \lambda_{ij} + \alpha_i + \beta_j + \alpha_j + \beta_i + 2\theta + \rho_{ij}
\end{align*}
\]

These quantities are interpreted as follows: $p_{ij}(0, 0)$ is the probability of no edge between $i$ and $j$, $p_{ij}(1, 0)$ is the probability of a directed edge from $i$ to $j$, $p_{ij}(0, 1)$ is the probability of a directed edge from $j$ to $i$, and $p_{ij}(1, 1)$ is the probability of a bidirected edge between $i$ and $j$. The parameter $\alpha_i$ is an effect local to $i$ measuring its strength of sending outgoing edges and similarly $\beta_j$ is an effect local to $j$ measuring its strength of receiving incoming
edges. The parameter $\theta$ is an intensity of the appearance of any edge (so that the bidirected edge could be considered a double edge). The parameter $\rho_{ij}$ is an intensity factor for reciprocation between $i$ and $j$. The parameters $\lambda_{ij}$ are essentially normalizing constants that are present to ensure that
\[ p_{ij}(0,0) + p_{ij}(1,0) + p_{ij}(0,1) + p_{ij}(1,1) = 1 \]
for each $i,j$ pair. Note that to avoid over-parametrization of the model, we can assume that $\sum \alpha_i = 0$ and $\sum \beta_j = 0$.

Submodels of the $p_1$-model are studied based on reducing the degrees of freedom in the $\rho_{ij}$ parameters. These possible submodels are:

- $\rho_{ij} = 0$, i.e. no reciprocation effect.
- $\rho_{ij} = \rho$, i.e. constant reciprocation effect.
- $\rho_{ij} = \rho + \rho_i + \rho_j$, vertex dependent reciprocation effect.

It is worth thinking through the sufficient statistics of these various models, to try to understand what the fibers of the models look like and how this affects the problem of developing a scheme for sampling from the corresponding fibers. Common to all the models is the requirement that each pair of vertices has exactly one type of interaction. The $\alpha_i$ and $\beta_j$ terms say that we want to look at graphs that have the same outdegree and indegree at each vertex (where a bidirected edge contributes both out and in at each vertex). If we were to set both $\theta$ and $\rho_{ij}$ to zero this would correspond to a directed analogue of the beta model. The $\theta$ parameter says that the total number of edges appearing in the graph should be constant, where the bidirected edge is counted as two edges. Adding the constant reciprocation effect $\rho$ says that the total number of bidirected edges in the graph should remain constant. Lastly, adding the vertex dependent reciprocation terms says that the vertex degrees in the subgraph of bidirected edge should be fixed.

Describing methods to sample from these fibers of the $p_1$ model seems a difficult problem in general. An initial study of the Markov bases and geometry of the marginal polytopes for these models appears in [FPR11], and a more detailed study appears in [PRF10]. For the model without reciprocation, it is possible to give a straightforward description of a Markov basis, closely related to the problem of sampling 0/1 matrices with fixed row and column sums that we have discussed previously. Without reciprocation, each bidirected edge $i \rightarrow j$ can be thought of as the pair of directed edges $i \rightarrow j$ and $j \rightarrow i$. Then to distinguish in and out degrees, we convert this to a bipartite graph on twice as many vertices, $\{u_1, \ldots, u_m\}$ and $\{v_1, \ldots, v_m\}$. We include an edge $u_i - v_j$ in this new undirected graph if there is a directed edge $i \rightarrow j$ in the original graph. Since we do not allow loops $i \rightarrow i$, we must exclude the possibility of edges $u_i - v_i$ for all $i$. In the usual
way, we can translate a bipartite graph into a 0/1 incidence matrix. Our condition on not allowing edges $u_i - v_i$ for all $i$ forces that this matrix has all zeroes on the diagonal. The condition on fixing indegrees and outdegrees in the original graph translates to fixing vertex degrees in the bipartite graph, which amounts to fixing row and column sums in the 0/1 matrix. In summary:

**Proposition 11.2.6.** Sampling from the fiber of graphs in the $p_1$ model with no reciprocation effect is equivalent to sampling 0/1 $m \times m$ matrices with zeroes on the diagonal and fixed row and column sums.

From the Graver basis for 2-way tables under the independence model, we deduce immediately a Markov basis for sampling from the the fibers in the $p_1$ model without reciprocation. This will come from moves that come from even cycles in the bipartite graph (see Proposition 9.4.3). In fact, it is possible to connect these fibers using a smaller set of moves, as explained in Exercise 11.3.

It seems a difficult problem to give a general description of the Markov basis or Graver basis for the $p_1$ model with other conditions on the reciprocation parameters $\rho_{ij}$. On the level of our 0/1 matrices, the corresponding sufficient statistics do not correspond to linear constraints on the matrix. Two options for dealing with this problem are to directly use the corresponding linear constraints as implied by the exponential family representation, or use nonlinear constraints (which is potentially complicated for setting up sampling schemes).

To illustrate the ideas, consider the constant reciprocation effect, with $\rho_{ij} = \rho$. The corresponding sufficient statistic is the number of bidirected edges in the graph. In terms of our $m \times m$ 0/1 matrix $X = (x_{ij})_{i,j \in [m]}$, the number of reciprocal pairs is

$$\sum_{1 \leq i < j \leq m} x_{ij}x_{ji}.$$  

This quadratic constraint can be converted into linear constraints by lifting into higher dimensions using the geometry of the cut polytope. See [DL97] for the general approach and [XS14] for an application in algebraic statistics. However, it is not clear in general how to sample from the set of graphs which have this complicated mixture of constraints.

### 11.3. Models from Subgraphs Statistics

In this section, we discuss some generalizations of Example 11.1.4, where all of the statistics being considered are subgraph statistics. The geometry of the resulting polytopes of all sufficient statistics have interesting connections to problems in real algebraic geometry.
Definition 11.3.1. Let $H$ and $G$ be graphs. The subgraph count statistic $t_H(G)$ counts the number of isomorphic copies of the graph $H$ in $G$. Suppose that $G$ has $m$ vertices. The normalized subgraph count statistic or subgraph density is $\bar{t}_H(G) = \frac{t_H(G)}{t_H(K_m)}$.

Note that in the subgraph count statistic we are counting the number of isomorphic copies of a graph in $H$ in $G$. There might be many such copies on the same set of vertices. For instance, the graph $K_4 \setminus e$ is a subgraph 6 times in the graph $K_4$.

Definition 11.3.2. Let $\mathcal{H} = \{H_1, \ldots, H_k\}$ be a collection of graphs. The exponential random graph model associated to $\mathcal{H}$ is the exponential family on the set of graphs of a fixed size where the vector of sufficient statistics is $(\bar{t}_{H_1}(G), \ldots, \bar{t}_{H_k}(G))$.

One advantage of working with the normalized graph count statistics is that the normalization guarantees that $\bar{t}_H(G) \in [0, 1]$ regardless of the size of the graph $G$. This makes it easier to compare the density of the two graphs of different sizes.

Definition 11.3.3. Let $\mathcal{H} = \{H_1, \ldots, H_k\}$ be a collection of graphs. The polytope of subgraph statistics defined by $\mathcal{H}$, denoted $P_{\mathcal{H}, n}$, is the convex hull of all the vectors $(\bar{t}_{H_1}(G), \ldots, \bar{t}_{H_k}(G))$ as $G$ ranges over all graphs with $n$ vertices.

Since the normalized graph count statistics put all these polytopes into the cube $[0, 1]^k$, it is natural to compare these polytopes. One result is:

Proposition 11.3.4. [ENT1] Proposition 2.7 Suppose that each graph in $\mathcal{H}$ has at most $n$ vertices, and let $n \leq n' \leq n''$. Then $P_{\mathcal{H}, n''} \subseteq P_{\mathcal{H}, n'}$.

Proof. Let $G$ be any graph, and let $U$ be a subset of the vertices of $G$ and denote by $G[U]$ the induced subgraph of $G$ on the vertex set $U$. A basic fact about the subgraph density is that it can be averaged over subsets, which gives the following formula

$$\bar{t}_H(G) = \frac{1}{\binom{|G|}{n'}} \sum_{U \subseteq V(G): |U| = n'} \bar{t}_H(G[U]).$$

Indeed, each subgraph isomorphic to $H$ contributes the same amount to each of the subgraph statistics $\bar{t}_H(G[U])$ for any $U$ that contains that subgraph. For any subgraph isomorphic to $H$, the number of $U$ that contain it is the same. This equation implies that the vector $(\bar{t}_{H_1}(G), \ldots, \bar{t}_{H_k}(G)) \in P_{\mathcal{H}, n''}$ is in the convex hull of the vectors $(\bar{t}_{H_1}(G[U]), \ldots, \bar{t}_{H_k}(G[U])) \in P_{\mathcal{H}, n'}$. □

Since the polytopes $P_{\mathcal{H}, n}$ form a decreasing sequences as $n \to \infty$, there is a well-defined limiting object $\bigcap_{n \geq n'} P_{\mathcal{H}, n}$ where $n$ is the number of vertices in
the largest subgraph of $\mathcal{H}$. A natural goal in this area is to try to understand the geometry of these polytopes or at least the limiting object. One useful fact is that all the polytopes contain certain semialgebraic sets formed by considering random graph models.

**Definition 11.3.5.** Let $\mathcal{H} = \{H_1, \ldots, H_k\}$ be a collection of graphs and suppose that graph $H_i$ has $e_i$ edges. The spine of the polytope of subgraph statistics consists of the set of points $\{(p^{e_1}, p^{e_2}, \ldots, p^{e_k}) : p \in [0, 1]\}$.

The spine is a coordinate project of the familiar moment curve from combinatorial geometry.

**Proposition 11.3.6.** Let $\mathcal{H} = \{H_1, \ldots, H_k\}$ be a collection of graphs and suppose that graph $H_i$ has $e_i$ edges, and let $n$ be the largest number of vertices in each of the $H_i$. The spine is contained in $P_{\mathcal{H}, n'}$ for all $n' \geq n$.

**Proof.** Consider an Erdős-Rényi random graph $G(n', p)$, with $n'$ vertices and probability $p$ of an edge occurring. The probability that a particular subgraph $H$ occurs as a subgraph on a specific set of $|H|$ vertices is $p^e$, where $e$ is the number of edges in $H$. Hence, the expected density of $E[\bar{t}_H(G)] = p^e$ as well. This implies that the point on the spine $(p^{e_1}, p^{e_2}, \ldots, p^{e_k})$, arising as the expected value of a probability distribution on random graphs, belongs to the polytope $P_{\mathcal{H}, n'}$. □

**Example 11.3.7.** Consider the graph statistics from Example 11.1.4, which consist of a $K_2$ and a $K_3$. The spine in this case consists of the points $\{(p, p^3) : p \in [0, 1]\}$. This is illustrated in Figure 11.3.1 which shows the spine contained in the polytope $P_{\{K_2, K_3\}, n}$.

It remains a difficult open problem to try to give a complete description of the polytopes $P_{\mathcal{H}, n}$, or the limiting objects and $n \to \infty$. Engström and Norén [EN11] has some further work on inner approximations to these polytopes as well as conjectures related to the limiting objects. The theory of flag algebras [Raz07] and the theory of graph limits [Lov12] are closely related and also shed light on these structures.

### 11.4. Exercises

**Exercise 11.1.** Prove that the conditions of Theorem 11.2.3 are necessary for a sequence to be a degree sequence of a graph.

**Exercise 11.2.** Determine the formula for the normalizing constant in the Rasch model, analogous to the formula in Proposition 11.2.2 for the beta model.
Exercise 11.3. Show that the degree 2 and 3 moves suffice to provide a Markov basis for the $p_1$-model with no reciprocation. (See [KTV99]. Fast mixing of the Markov chain is even known for various classes of degree sequences, see e.g. [EMTI16].)

Exercise 11.4. Construct the subgraph statistics polytope associated to the set of graphs $\{K_2, K_3, K_4 \setminus e\}$ on 7 vertices, and draw the associated spine.
Design of Experiments

Statistics is concerned with answering scientific questions using data. There might be many differing interacting covariates that can explain a response variable and one is interested in determining what these interactions might be. In a controlled experiment, the researcher tries to measure the magnitudes of different effects by setting up each of a number of possible configurations of the covariates to measure the effects of each of the random variables on the response variables. This “design of experiments” originated in agricultural and industrial experiments. The researchers were interested in knowing how various factors affected the yield of various crops. In these settings it can be prohibitively expensive to run experiments in all possible combinations of the covariates, so the researchers are interested in designing experiments that only involve testing a small subset of all possible combinations that still captures that main interaction effects of the random variables measured. The experimental design is thus a choice of the particular combinations to use to actually run the experiments on. Typically this subset is chosen with particular assumptions about what effects might matter, which effects are assumed to be zero or inconsequential, and the experimental design is chosen in such a way that all of the desired effects can be measured. Further combinatorial considerations might also be made, for instance, for every pair of covariates every combination of those pairs should be measured.

The study of experimental designs, and the combinatorial aspects which are part of combinatorial design theory, have a long tradition using tools from both algebra and combinatorics. Pistone, Riccomagno, and Wynn realized that methods from computational algebraic geometry could be used to study the design of experiments, which was the subject of the first book
that used the title “Algebraic Statistics” [PRW01]. We discuss some of these aspects here.

12.1. Designs

From a mathematical standpoint, a design $D$ is a set of points in a finite dimensional vector space. Computational methods from algebraic geometry and commutative algebra can be used to analyze properties of designs and decide which models can be estimated using a given design.

Let $\mathbb{K}$ be a field, and let $D \subseteq \mathbb{K}^m$ be a finite subset of a finite dimensional vector space over $\mathbb{K}$. Such a set is called a design.

Example 12.1.1. Let $D \subseteq \mathbb{K}$ be a finite set of numbers and let $D = D^m$. Designs of this type are often called full factorial designs. The most important special cases include $D = \{0, 1\}$, $D = \{-1, 0, 1\}$, or $D = \{0, 1, \ldots, p\}$.

Example 12.1.2. If $D$ is a full factorial design, a subset $D' \subseteq D$ is sometimes called a fractional factorial design. Sometimes this expression is used to denote subsets with specific properties, though there does not appear to be a standard definition in the literature on what properties a set $D'$ must satisfy to be a fractional factorial design.

For example, if $D = \{0, 1\}^m$, and $D' \subseteq D$ consists of all $(x_1, \ldots, x_m) \in D$ such that $\sum_{i=1}^m x_i \equiv 0 \mod 2$, this is called the standard $2^m - 1$ fractional factorial design.

A key tool in the algebraic approach to the design of experiments is the vanishing ideal $I(D) \subseteq \mathbb{K}[x]$ of the design $D$. Note that we use the indeterminates $x_1, \ldots, x_m$ in our polynomial ring when discussing the design of experiments (as opposed to working in the polynomial ring $\mathbb{R}[p]$ or $\mathbb{R}[\Sigma]$ as we have done in previous chapters). This is because for a design we are actually looking at the states of random variables we are considering (rather than coordinates on the probability simplex, or in the space of symmetric matrices, etc.). Also we need not require the $\mathbb{K} = \mathbb{R}$, and there are many situations where finite fields are relevant in the design of experiments.

A key property for vanishing ideals of finite sets is the following proposition regarding the quotient ring $\mathbb{K}[x]/I(D)$.

Proposition 12.1.3. Let $D \subseteq \mathbb{K}^m$ be a finite set. Then the quotient ring $\mathbb{K}[x]/I(D)$ is the vector space of all functions from $D$ to $\mathbb{K}$.

Proof. We have already seen that for any variety $V$, $\mathbb{K}[x]/I(V)$ consists of all polynomial functions from $V$ to $\mathbb{K}$. The claim in the special case of finite sets is that every function from $D$ to $\mathbb{K}$ can be represented as a polynomial function. To prove this, it suffices to show that for each $y \in D$, there is a
polynomial \( f \in \mathbb{K}[x] \) such that \( f(y) \neq 0 \), and \( f(z) = 0 \) for all \( z \in \mathcal{D} \setminus \{y\} \).

An example of such a polynomial is
\[
\prod_{i=1}^{m} \prod_{z \in \mathcal{D} : z \neq y_i} (x_i - z_i). \quad \square
\]

One basic goal in the design of experiments is to determine which polynomial regression models are estimable given a particular design. In this setting, we have a polynomial with generic coefficients:
\[
f = \sum_{a \in A} c_a x^a
\]
where the \( c_a \) are the coefficients and \( A \) is a specific set of exponent vectors characterizing the model. We are typically interested in modeling a response variable \( Y \) as the polynomial function \( f(X) \) of covariates \( X \) plus a noise term \( \epsilon \). The goal in such an analysis is to determine which terms in the regression are important (e.g. large values of \( c_a \)) and which terms can be ignored.

To say that a particular polynomial regression model is estimable given the design \( \mathcal{D} \), means that the coefficients of the polynomial \( c_a \) can be determined from data. This is equivalent to saying that the set of functions \( \{x^a : a \in A\} \) are linearly independent functions in \( \mathbb{K}[x]/I(\mathcal{D}) \). This is clearly the same concept as identifiability studied in detail in Chapter 16. However, for the polynomial regression models studied in this section, the methods are more straightforward.

In statistics, the estimability of the design is expressed in terms of the design matrix: \( X(A, \mathcal{D}) \) whose \((y,a)\) entry is the evaluation of \( x^a \) at \( y \).

**Definition 12.1.4.** The polynomial regression model with support \( A \) is estimable from the design \( \mathcal{D} \) if the matrix \( X(A, \mathcal{D}) \) has full column rank.

**Example 12.1.5.** Consider the design \( \mathcal{D} = \{(0,0), (2,0), (1,3), (4,5)\} \) and the set \( A \) consisting of exponent vectors \( A = \{(0,0), (1,0), (2,0), (0,1)\} \) corresponding to the monomials \( \{1, x_1, x_1^2, x_2\} \). The design matrix in this case is
\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
1 & 2 & 4 & 0 \\
1 & 1 & 1 & 3 \\
1 & 4 & 16 & 5
\end{pmatrix},
\]
which has rank 4. So the polynomial regression model
\[
f(x_1, x_2) = c_{00} + c_{10}x_1 + c_{20}x_1^2 + c_{01}x_2
\]
is estimable from the design \( \mathcal{D} \).
A basic problem in design of experiments is to determine which polynomial regressions models are estimable from a given design $D$. Usually arbitrary polynomials models are not of interest, but rather ones that satisfy certain properties that make them reasonable from a practical standpoint. A typical assumption is that the set of monomials that appears is hierarchical. This means that if a monomial $x^u$ appears in the expansion, then any monomial $x^v$ such that $x^v|x^u$ also appears in the expansion. In other words:

**Definition 12.1.6.** A set of monomials $M$ is hierarchical if and only if it is the set of standard monomials of some monomial ideal.

So the main problem in the algebraic theory of design of experiments is to determine which monomial ideals correspond to identifiable models with respect to a given design $D$. A large class is obtained by looking at initial ideals.

**Proposition 12.1.7.** Let $D \subseteq \mathbb{K}^m$ be a design, and $\prec$ a term order. Then the standard monomials of $\text{in}_\prec(I(D))$ are the support of an estimable model with respect to the design $D$.

**Proof.** By Proposition 10.3.4, the standard monomials of an initial ideal of $I(D)$ form a $\mathbb{K}$-vector space basis for $\mathbb{K}[x]/I(D)$, so in particular these standard monomials are linearly independent modulo $I(D)$. □

**Example 12.1.8.** Let $D = \{(0,0), (1,1), (-1,1), (1,-1), (-1,-1)\} \subseteq \mathbb{R}^2$. The vanishing ideal of the design is

$$I(D) = \langle x_1^2 - x_2^2, x_1^3 - x_1x_2^2 - x_2^3 - x_2 \rangle.$$

A reduced Gröbner basis of $I(D)$ with respect to lexicographic order with $x_1 \prec x_2$ is:

$$\{x_2^3 - x_1^2, x_1^2x_2 - x_2, x_1^3 - x_1\}$$

where the initial terms have been underlined. This means that the set of monomials

$$\{1, x_1, x_1^2, x_2, x_1x_2\}$$

provides the support for an estimable model with respect to the design $D$.

Computing Gröbner bases and analyzing initial ideals of the ideal of points $I(D)$ is a useful tool for finding identifiable polynomial regression models. Understanding which ideals can arise in this way is an interesting question. Recall that a condition is said to be generic if it holds off of a set of measure zero. In algebraic geometry a condition is generic if it holds on the complement of the union of countably many hypersurfaces (here we need to assume that our field is uncountable, to be certain that there are any points satisfying the condition). For example, we have the following proposition about generic designs.
Proposition 12.1.9. Let $\mathcal{D} \subseteq \mathbb{K}^m$ be a generic design where $\mathbb{K}$ is an uncountable field. Then every polynomial regression model with $\leq |\mathcal{D}|$ terms is estimable given $\mathcal{D}$.

Proof. Fix a number $d$ representing the size of the design. A set $\mathcal{D}$ of $d$ points in $\mathbb{K}^k$ can be thought of as the columns of an $m \times d$ matrix with entries in $\mathbb{K}$. We just need to show that there is a set of countably many hypersurfaces in $\mathbb{K}^{m \times d}$, such off of those hypersurfaces any polynomial regression will be identifiable. For each set of $d$ exponent vectors we get the design matrix $X(A, \mathcal{D})$, which we can consider as a matrix whose entries are monomials in the coordinates on the space $\mathbb{K}^{m \times d}$. The determinant of $X(A, \mathcal{D})$ is zero if and only the model is not estimable given the design. Note that the determinant of $X(A, \mathcal{D})$ is not identically zero because each monomial in the expansion has a unique occurrence. Thus, each set $A$ gives a condition on the set of points under consideration. There are countably many sets $A$ of exponent vectors with $|\mathcal{D}|$ elements. □

On the other hand, not every hierarchical set of monomials with $\mathcal{D}$ elements can arise as the set of standard monomials of an initial ideal of $I(\mathcal{D})$. In fact, for generic sets of points $\mathcal{D}$ there is a precise characterization of which initial ideals are possible.

Definition 12.1.10. A monomial ideal $M \subseteq \mathbb{K}[x]$ is called a corner cut ideal if there exists a vector $a \in \mathbb{R}^m_{>0}$ and $b > 0$ such that

$$M = \langle x^u : au > b \rangle.$$  

Theorem 12.1.11. Let $\mathbb{K}$ be an infinite field and $\mathcal{D} \subseteq \mathbb{K}^m$ a generic set of $d$ points. A monomial ideal $M \subseteq \mathbb{K}[x]$ is an initial ideal of $I(\mathcal{D})$ if and only if $M$ is a corner cut ideal with exactly $d$ standard monomials.

Of course, most designs that arise in practice have specific combinatorial structure, arising as fractions of a full factorial design. So they are rarely generic and will have initial ideals that are not corner cut ideals. Conversely, there will be corner cut ideals that are not estimable from the design. Furthermore, there can be more hierarchical polynomial regression models that are estimable that do not arise as an initial ideal.

Example 12.1.12. Consider the design from Example 12.1.8. The only estimable hierarchical polynomial models for this design have monomial support

$$\{1, x_1, x_2, x_1x_2\} \quad \text{and} \quad \{1, x_1, x_2, x_1^2, x_1x_2\}.$$  

Both of these sets are standard monomials of corner cut ideals. However, other corner cut ideals do not yield estimable models with respect to these
data points for example the set of monomials
\[ \{1, x_1, x_2, x_2^2, x_2^3\} \]
is the set of standard monomials of a corner cut ideal but is not estimable with respect to the design \( D \).

Every hierarchical set of monomials can be realized as the set of standard monomials of a design ideal \( I(D) \). This can be seen by employing a construction called the distraction.

**Definition 12.1.13.** Let \( M \) be a monomial ideal such that \( \mathbb{K}[x]/M \) is a finite dimensional \( \mathbb{K} \)-vector space. For each monomial \( x^a \) we associate the product of linear polynomials
\[ x^{(a)} := \prod_{i=1}^{m} x_i(x_i - 1) \cdots (x_i - a_i + 1) \]
The distraction of \( M \) is the ideal
\[ \text{Dist}(M) := \langle x^{(a)} : x^a \in M \rangle. \]

**Proposition 12.1.14.** For any monomial ideal \( M \in \mathbb{K}[x] \) such that \( \mathbb{K}[x]/M \) is a finite dimensional \( \mathbb{K} \)-vector space, \( V(\text{Dist}(M)) \) is equal to the set of exponent vectors of the standard monomials of \( M \). For any term order \( \preceq \), \( \text{in}_{\preceq}(\text{Dist}(M)) = M \).

**Proof.** Since \( \mathbb{K}[x]/M \) is a finite dimensional \( \mathbb{K} \)-vector space, for each \( i \), there is \( r_i \) such that \( x_i^{r_i} \in M \). The polynomial
\[ x_i^{(r_i)} = x_i(x_i - 1) \cdots (x_i - r_i + 1) \]
belongs to \( \text{Dist}(M) \), so \( V(\text{Dist}(M)) \) consists of only points with nonnegative integer coordinates. Let \( x^u \) be a standard monomial of \( M \) and let \( x^a \in M \). Then there in \( i \) such that \( u_i < a_i \). This implies that \( u \in V(\{x^{(a)}\}) \), and thus \( u \in V(\text{Dist}(M)) \). Conversely, \( a \notin V(\{x^{(a)}\}) \) so this implies that \( V(\text{Dist}(M)) \) is the set of exponent vectors of standard monomials of \( M \).

Now let \( \preceq \) be an arbitrary term order. Since each polynomial \( x^{(a)} \) is a product of linear terms, each of whose leading terms is \( x_i \), this forces \( \text{in}_{\preceq}(x^{(a)}) = x^a \). Hence \( M \subseteq \text{in}_{\preceq}(\text{Dist}(M)) \). However this initial ideal \( \text{in}_{\preceq}(\text{Dist}(M)) \) could not be bigger then \( M \), since otherwise \( \text{Dist}(M) \) would have fewer standard monomials that the number of points in \( V(\text{Dist}(M)) \).

**Example 12.1.15.** The set of monomials
\[ \{1, x_1, x_1^2, x_2, x_2^2\} \]
is not the set of standard monomials of a corner cut. Indeed, a set of standard monomials which is a corner cut ideal that does not include \( x_1x_2 \) either
12.2. Computations with the Ideal of Points

The monomial ideal with this set of standard monomials is $M = \langle x_1^3, x_1 x_2, x_2^2 \rangle$. The distraction is the ideal

$$\text{Dist}(M) = \langle x_1(x_1 - 1)(x_1 - 2), x_1 x_2, x_2(x_2 - 1)(x_2 - 2) \rangle$$

and the resulting design consists of the points

$$\{(0, 0), (0, 1), (0, 2), (1, 0), (2, 0)\}.$$

12.2. Computations with the Ideal of Points

A key role in the algebraic approach to the design of experiments is played by $I(D)$, the vanishing ideal of the finite set of points $D \subseteq \mathbb{K}^m$. To make this useful requires methods for developing quick computations with the ideal of points, in particular, computing generating sets, Gröbner bases, and interpolating polynomials. Besides design of experiments, these methods also have applications in other contexts, including to the analysis of discrete dynamical systems [DJLS07, LS04]. We describe methods for computing with the ideal of points in this section.

Let $D = \{y_1, \ldots, y_r\} \subseteq \mathbb{K}^m$ be a design. The simplest theoretical approach to computing the vanishing ideal $I(D)$ is to use the relations between unions of varieties and intersections of ideals to compute the vanishing ideal of $D$. Indeed, for the point $y_i = (y_{i1}, \ldots, y_{im}) \in D$, the vanishing ideal is

$$I(\{y_i\}) = \langle x_1 - y_{i1}, \ldots, x_m - y_{im} \rangle.$$

Hence, by Proposition 3.2.13 we have

$$I(D) = \bigcap_{i=1}^r \langle x_1 - y_{i1}, \ldots, x_m - y_{im} \rangle.$$

The intersection of two ideals can be computed via elimination using the following:

**Proposition 12.2.1.** Let $I, J \in \mathbb{K}[x_1, \ldots, x_m]$ and let $t$ be a new indeterminate. Then

$$I \cap J = (t \cdot I + (1 - t) \cdot J) \cap \mathbb{K}[x_1, \ldots, x_m].$$

This procedure for computing intersections of ideals is implemented in most computer algebra packages. In practice this is not the most efficient way to compute the vanishing ideal of a finite set of points. A more efficient algorithm is the Buchburger-Möller algorithm [MB82] which we describe here in broad strokes. We use $\text{Mono}(\mathbb{K}[x_1, \ldots, x_m])$ to denote the set of all monomials in $\mathbb{K}[x_1, \ldots, x_m]$.

**Algorithm 12.2.2.** Input: A set of points $D = \{y_1, \ldots, y_r\} \subseteq \mathbb{K}^m$ and a term order $\preceq$. 

12. Design of Experiments

Output: A reduced Gröbner basis \( G \) for \( I(\mathcal{D}) \) with respect to \( \preceq \), a set \( S \) of exponent vectors of standard monomials of \( \mathbb{K}[x_1, \ldots, x_m]/I(\mathcal{D}) \), and the initial ideal \( M = \text{in}_{\preceq}(I(\mathcal{D})) \).

Initialize: \( S = \emptyset \), \( G = \emptyset \), \( M = \langle 0 \rangle \)

While: \( \text{Mono}(\mathbb{K}[x_1, \ldots, x_m]) \setminus (S \cup M) \neq \emptyset \)

- Let \( x^a \) be the smallest monomial in \( \text{Mono}(\mathbb{K}[x_1, \ldots, x_m]) \setminus (S \cup M) \) with respect to \( \preceq \).
- If \( \text{rank}(X(S \cup \{a\}, \mathcal{D})) > \text{rank}(X(S, \mathcal{D})) \)
  - Then, \( S := S \cup \{a\} \)
  - Else, there is a unique polynomial \( g = x^a + \sum_{b \in S} c_b x^b \in I(\mathcal{D}) \).
    Set \( G = G \cup \{g\} \) and \( M := M + \langle x^a \rangle \)

Output: \( S \), \( G \), and \( M \).

The algorithm terminates in finitely many steps because one never needs to look at any monomial of degree larger than \( |\mathcal{D}| \). A more detailed description of the algorithm shows how to directly compute the polynomial \( x^a + \sum_{b \in S} c_b x^b \) while checking the rank condition \( \text{rank}(X(S \cup \{a\}, \mathcal{D})) > \text{rank}(X(S, \mathcal{D})) \) (and technically avoids any rank computations at all). See [MB82] for the details.

Once we have a method to compute the ideal of points, we can use our Gröbner basis for the ideal of points to answer various questions about the underlying designs. A first topic of consideration is the notion of aliasing of two polynomial regression models.

Definition 12.2.3. Given two finite sets of exponent vectors \( A, B \subseteq \mathbb{N}^m \) defining polynomial regression models, we say they are aliased with respect to the design \( \mathcal{D} \) if the two vector spaces of functions \( \{\sum_{a \in A} c_a x^a : c_a \in \mathbb{K}\} \) and \( \{\sum_{b \in B} c_b x^b : c_b \in \mathbb{K}\} \) are the same vector space in the quotient ring \( \mathbb{K}[x]/I(\mathcal{D}) \).

Among the simplest types of designs where it is easy to analyze aliasing are when the design has a group structure. For example, consider the full factorial design \( \{\pm 1\}^m \). This design is an abelian group under coordinate-wise multiplication. Any subgroup is obtained by adding binomial constraints of the form \( x^u - 1 = 0 \), which induces a subdesign \( \mathcal{D} \subseteq \{\pm 1\}^m \). Since all equations in the resulting defining ideal are binomial, this will force aliasing relations to show that certain monomials in a polynomial regression model over the design will be equal to each other as functions.

Example 12.2.4. Let \( \mathcal{D} \) be the subgroup design consisting of the following 8 points in \( \mathbb{R}^5 \):

\[(1, 1, 1, 1, 1), (1, 1, 1, -1, -1), (1, -1, -1, 1, -1), (1, -1, -1, -1, 1), \]
The vanishing ideal of the design is

\[ I(D) = \langle x_1^2 - 1, x_2^2 - 1, x_3^2 - 1, x_4^2 - 1, x_5^2 - 1, x_1x_2x_3 - 1, x_3x_4x_5 - 1 \rangle. \]

The Gröbner basis for \( I(D) \) with respect to the lexicographic term order where \( x_1 \succ x_2 \succ x_3 \succ x_4 \succ x_5 \) is

\[ G = \{ x_5^2 - 1, x_4^2 - 1, x_3 - x_4x_5, x_2^2 - 1, x_1 - x_2x_4x_5 \}. \]

From the Gröbner basis we already see some aliasing relations between monomial terms in polynomial regression with respect to \( D \), in particular, the function \( x_3 = x_4x_5 \) as functions on \( D \), and \( x_1 = x_2x_4x_5 \) as functions on \( D \). But, there are many other relations besides these. Two monomials \( x^a \) and \( x^b \) represent that same function on \( D \) if and only if \( x^a - x^b \) is the zero function on \( I(D) \), if and only if \( x^a - x^b \in I(D) \). This can be checked by determining if \( NF_G(x^a - x^b) = 0 \) or not.

More generally, aliasing not just between individual monomials but entire polynomial regression models can be detected by performing normal form calculations. To do this, one considers the two polynomial regression models \( \{ \sum_{a \in A} c_a x^a : c_a \in \mathbb{K} \} \) and \( \{ \sum_{b \in B} c_b x^b : c_b \in \mathbb{K} \} \), computes the normal form of each monomial appearing to get equivalent representations as the models span(\( NF_G(x^a) : a \in A \)) and span(\( NF_G(x^b) : b \in B \)) and checks whether or not these two vector spaces are equal.

### 12.3. The Gröbner Fan and Applications

As we have see in Section [12.1], variation of term order allows for the choice of different estimable models with respect to a given design. The results of all possible term orders are encoded in a polyhedral object called the Gröbner fan, who structure can be useful for choosing estimable models that satisfy certain features. We describe the Gröbner fan here and discuss some of its applications. More details on the Gröbner fan and the related state polytope can be found in [Stu95, Chapter 2].

A vector \( c \) defines a weight order \( \prec_c \) on the set of monomials in \( \mathbb{K}[x] \) by \( x^u \prec_c x^v \) if and only if \( c^T u < c^T v \). The weight of a monomial \( x^u \) with respect to \( c \) is \( c^T u \). Given a polynomial \( f \in \mathbb{K}[x] \), its initial form \( \text{in}_c(f) \) with respect to the weight order \( c \) is the sum of all terms of \( f \) that have the highest weight. Note that the weight order \( \prec_c \) might not be a term order because there can be monomials that have the same weight, and the monomial 1 might not be the smallest weight monomial with respect to the weight order. Given an ideal \( I \subseteq \mathbb{K}[x] \) we can also define the initial ideal

\[ \text{in}_c(I) = \langle \text{in}_c(f) : f \in I \rangle. \]
Not every term order can be realized by a weight order. For example, for the lexicographic term order, there is no weight vector \( c \in \mathbb{R}^m \) such that \( \text{in}_c(f) = \text{in}_{\text{lex}}(f) \) for all \( f \in \mathbb{K}[x] \). However, once we fix a particular ideal and focus on computing the initial ideal, it is always possible to find a weight vector that realizes a particular term order.

**Proposition 12.3.1.** Let \( I \subseteq \mathbb{K}[x] \) be an ideal and \( \prec \) be a term order on \( \mathbb{K}[x] \). Then there exists a weight vector \( c \in \mathbb{R}^m \) such that \( \text{in}_c(I) = \text{in}_\prec(I) \).

**Proof.** Let \( G = \{g_1, \ldots, g_k\} \) be a reduced Gröbner basis for \( I \) with respect to the term order \( \prec \). Each polynomial \( g_i \in G \) can be written as

\[
g_i = x^{u_i} + \sum_{j=1}^{l_i} c_{ij} x^{v_{ij}}
\]

where each of the monomials \( x^{u_i} \) is larger in the term order than any \( x^{v_{ij}} \) for \( j = 1, \ldots, l_i \). The set of all possible cost vectors that could produce the initial ideal \( \text{in}_\prec(I) \) is the open polyhedral cone

\[
\{ c \in \mathbb{R}^m : c^T u_i > c^T v_{i,j} \text{ for } i \in [k], j \in [l_i] \}.
\]

The proof of the proposition amounts to showing that this cone is nonempty. This can be shown via an application of the Farkas Lemma of convex geometry: if the system of inequalities were inconsistent, the ordering \( \prec \) would not be a term order.

**Example 12.3.2.** Consider the ideal \( I = \langle x_1^2 - x_2, x_2^2 - x_1 \rangle \). Then two polynomial generators are a Gröbner basis of \( I \) with respect to any graded term order (e.g. graded reverse lexicographic). The set of possible weight vectors that realize the same initial ideal is the cone

\[
\{(c_1, c_2) \in \mathbb{R}^2 : 2c_1 > c_2, 2c_2 > c_1 \}.
\]

We say that a weight vector \( c \in \mathbb{R}^m \) is in the Gröbner region of the ideal \( I \), if it is in the closure of the set of all cost vectors for which there exists a term order \( \prec \) on \( \mathbb{K}[x] \) such that \( \text{in}_c(I) = \text{in}_\prec(I) \). If \( c \in \mathbb{R}^m \) with all positive entries that are linearly independent over the rational numbers, then \( c \) defines a term order on \( \mathbb{K}[x] \) (regardless of the ideal). So this shows that the Gröbner region of an ideal contains the positive orthant.

The proof of Proposition 12.3.1 shows that the set of weight vectors that realize a specific monomial initial ideal of an ideal \( I \subseteq \mathbb{K}[x] \) is an open polyhedral cone. For any term order \( \prec \), let \( C(\prec) \) denote the closure of this cone, the Gröbner cone of the term order. Hence, the Gröbner region is a union of polyhedral cones. In fact we have:
Theorem 12.3.3. For any ideal \( I \subseteq \mathbb{K}[x] \) there are only finitely many distinct monomial initial ideals of \( I \). Hence the Gröbner region of \( I \) is the union of finitely many polyhedral cones.

Proof. The set of all monomial ideals in a polynomial ring is ordered by inclusion. Since the set of standard monomials of an initial ideal of an ideal are a basis for the quotient ring (Proposition 10.3.4), two different initial ideals of the same monomial ideal must be incomparable in the containment order. However, there are no infinite sets of monomial ideals that are incomparable \([\text{Mac01}]\). \(\square\)

The cones of the Gröbner region are arranged with respect to each other in a nice way.

Definition 12.3.4. Let \( \mathcal{C} \) be a set of polyhedra in \( \mathbb{R}^m \). This set is called a polyhedral cell complex if it satisfies the following conditions:

1. \( \emptyset \in \mathcal{C} \).
2. If \( F \in \mathcal{C} \) and \( F' \) is a face of \( F \) then \( F' \in \mathcal{C} \).
3. If \( F, F' \in \mathcal{C} \) then \( F \cap F' \) is a face of both \( F \) and \( F' \).

A polyhedral complex \( \mathcal{C} \) is called a fan if all the polyhedra in \( \mathcal{C} \) are cones with apex at the origin.

Proposition 12.3.5. Let \( C_1 \) and \( C_2 \) be two Gröbner cones of the ideal \( I \subseteq \mathbb{K}[x] \). Then \( C_1 \cap C_2 \) is a common face of both cones. In particular, the set of all the Gröbner cones and their faces forms a fan called the Gröbner fan of the ideal \( I \), denoted \( GF(I) \).

Proof. See \([\text{Stu95}]\) Chapter 2. \(\square\)

A fan is called complete if the union of all the cones in the fan is \( \mathbb{R}^m \). Note that the Gröbner fan need not be complete in general, but they are in special cases.

Proposition 12.3.6. Let \( I \subseteq \mathbb{K}[x] \) be a homogeneous ideal. Then the Gröbner fan of \( I \) is a complete fan.

Proof. Let \( I \) be homogeneous. Let \( c \in \mathbb{R}^m \), let \( \alpha \in \mathbb{R} \), and let \( 1 \in \mathbb{R}^m \) denote the vector of all ones. Then for any homogeneous polynomial \( f \in I \), \( \text{in}_c(f) = \text{in}_{c+\alpha}(f) \). By choosing \( \alpha \) very large, we see that for any weight vector \( c \), there is a vector of all positive entries that realizes the same initial ideal. Since vectors in the positive orthant are in the Gröbner region for any ideal, this implies that every vector is in the Gröbner region. \(\square\)
More generally, the Gröbner fan will be a complete fan if the ideal is homogeneous with respect to a nonstandard grading that gives every variable a positive weight. The simplest situation to think about the Gröbner fan of an ideal is in the case of principal ideals. This requires a few definitions.

**Definition 12.3.7.** Let \( f = \sum_{u \in \mathbb{N}^n} c_u x^u \in \mathbb{K}[x] \) be a polynomial. The *Newton polytope* of \( f \) is the convex hull of all exponent vectors of monomials appearing in \( f \); that is,

\[
\text{Newt}(f) = \text{conv}(u : c_u \neq 0).
\]

Let \( P \) be a polytope. To each face \( F \subseteq P \), let \( C(F) \) be the set of cost vectors such that \( F \) is the optimal set of points in \( P \):

\[
C(F) = \{ c \in \mathbb{R}^m : c^T x \geq c^T y \text{ for all } x \in F \text{ and } y \in P \}.
\]

The set \( C(F) \) is a polyhedral cone, since it can be defined by finitely many linear inequalities (e.g. by taking all the inequalities \( c^T x \geq c^T y \) where \( x \in \text{vert}(F) \) and \( y \in \text{vert}(P) \)).

**Proposition 12.3.8.** Let \( P \) be a polytope. The set of cones \( \mathcal{N}_P = \{ C(F) : F \text{ a face of } P \} \) is a complete fan called the normal fan of the polytope \( P \).

**Proof.** See [Zie95, Example 7.3]. \( \square \)

The normal fan of a polytope can be thought of as the parametric solution to all possible linear programs over that polytope. As the cost vector varies, the optimal solution moves from one vertex of \( P \) to another.

**Proposition 12.3.9.** Let \( f \in \mathbb{K}[x] \). Then \( \text{GF}(\langle f \rangle) \) consists of all cones in the normal fan of the Newton polytope of \( f \) that intersect the positive orthant. If \( f \) is homogeneous then

\[
\text{GF}(\langle f \rangle) = \mathcal{N}_{\text{Newt}(f)}.
\]

**Proof.** Every monomial initial ideal of \( \langle f \rangle \) arises from taking a vertex of the Newton polytope. The corresponding Gröbner cone associated to a given weight vector is the cone of the normal fan that realizes that vertex as the optimum. Vectors from the normal fan will actually yield term orders if and only if the corresponding normal cone intersects the positive orthant. \( \square \)

**Example 12.3.10.** Consider the polynomial \( f = 3 + 7x_1 + 2x_1x_2 - 4x_1^2x_2 + 6x_1x_2^2 + x_1^2x_2^2 \). The Newton polytope \( \text{Newt}(f) \) is a pentagon, and the normal fan \( \mathcal{N}_{\text{Newt}(f)} \) has five 2-dimensional cones. The Gröbner fan consists of the two of those cones that intersect the positive orthant.

**Example 12.3.11.** The following Macaulay2 code uses the package \texttt{gfan} [Jen] to compute the Gröbner fan and all monomial initial ideals of the ideal \( I = \langle x_1^2 - x_2^2, x_1^3 - x_1, x_2^3 - x_2 \rangle \) from Example 12.1.8.
loadPackage "gfanInterface"
R = QQ[x1,x2];
I = ideal(x1^2-x2^2, x1^3-x1, x2^3-x2);
gfan I
grobnerFan I

The first command `gfan I` computes all the distinct initial ideals of $I$ and also shows the corresponding reduced Gröbner bases. The second command `grobnerFan I` computes a representation of the Gröbner fan as the union of polyhedral cones. In this case, there are two distinct initial ideals:

$$\langle x_1^2, x_1x_2^2, x_2^3 \rangle \quad \text{and} \quad \langle x_3^3, x_1^2x_2, x_2^2 \rangle$$

corresponding to the two estimable sets of monomials seen in Example 12.1.12. The Gröbner fan consists of two cones:

$$\{(c_1, c_2) \in \mathbb{R}^2 : c_1 \geq c_2 \geq 0\} \quad \text{and} \quad \{(c_1, c_2) \in \mathbb{R}^2 : c_2 \geq c_1 \geq 0\}$$

The Gröbner region is the positive orthant.

We saw in Proposition 12.3.9 that the Gröbner fan of a principal ideal $\langle f \rangle$ can be realized as (part of) the normal fan of a polytope, namely, the Newton polytope of the $f$. One might wonder if the Gröbner fan always has such a nice polyhedral realization. A polytope $P$ such that $NF(P)$ is the Gröbner fan of an ideal $I$ is called a state polytope for $I$. Every homogeneous ideal has a state polytope [MR88] but they do not need to exist for nonhomogeneous ideals.

Since the positive orthant usually has the most interesting weight vectors for computing Gröbner bases, we could restrict to the intersection of the Gröbner fan with the positive orthant. For this restricted Gröbner fan, we could ask if there is a a state polyhedron whose normal fan is the resulting restricted Gröbner fan. Denote by $GF_+(I)$ the restricted Gröbner fan of $I$. State polyhedra for the restricted Gröbner fan need not exist in
12. Design of Experiments

Figure 12.3.2. The state polyhedron of the ideal of four generic points of Example 12.3.14 and the corresponding restricted Gröbner fan.

general [Jen07]. However, state polyhedra do always exist for the ideals $I(D)$ where $D$ is a finite set of any affine space (over any field), and there is a straightforward construction. This construction can be phrased in terms of estimable staircase models associated to the design $D$.

Definition 12.3.12. Let $D \subseteq \mathbb{K}^m$ be a design. An estimable polynomial regression model for $D$ is saturated if it has the same number of terms as $|D|$. Let $\text{Est}(D)$ denote the set of estimable saturated hierarchical polynomial regression models.

Theorem 12.3.13. [OS99, Thm 5.2] Let $D \subseteq \mathbb{K}^m$ be a finite set. To each $S \in \text{Est}(D)$ associate the vector $v_S = \sum_{s \in S} s$. Then the polyhedron

$$\text{conv}\{ -v_S : S \in \text{Est}(D) \} + \mathbb{R}_{\leq 0}^m,$$

is a state polyhedron for the restricted Gröbner fan of $I(D)$.

Example 12.3.14. Suppose that $D \subseteq \mathbb{R}^2$ is a generic design with four elements. There are five estimable saturated hierarchical designs, whose monomials are

$$\{1, x_1, x_1^2, x_1^3\}, \{1, x_1, x_1^2, x_2\}, \{1, x_1, x_2, x_1x_2\}, \{1, x_1, x_2, x_2^2\}, \{1, x_2, x_2^2, x_3\}.$$

Their corresponding vectors $v_S$ are

$$(6, 0), (3, 1), (2, 2), (1, 3), (0, 6)$$

respectively. The state polyhedron and restricted Gröbner fan are illustrated in Figure 12.3. Note that the point $(-2, -2)$ does not appear as a vertex of the state polyhedron, because the monomial ideal with standard monomial set $\{1, x_1, x_2, x_1x_2\}$ is not a corner cut ideal.

The state polyhedron/Gröbner fan of a design is a useful object associated to the design because it parametrizes all the estimable models for the given design which have an algebraic representation. One application of this machinery is to regression models of minimal aberration.
Definition 12.3.15. Consider a linear model consisting of exponent vector set $B \subseteq \mathbb{N}^m$ with $d$ elements. Let $w \in \mathbb{R}_{\geq 0}^m$ be a vector of nonnegative weights such that $\sum_{i=1}^m w_i = 1$. The weighted linear aberration of the model is

$$A(w, B) = \frac{1}{d} \sum_{b \in B} w^T b.$$ 

Theorem 12.3.16. Given a design $D \subset \mathbb{R}^m$ with $r$ points and a weight vector $w \in \mathbb{R}_{>0}^m$, there is at least one hierarchical staircase model $B$ that minimizes $A(w, B)$ which can be chosen to be an algebraic model. In particular, such a model can be obtained by computing a Gröbner basis with respect to the weight vector $w$, or, equivalently, maximizing the linear functional $w$ over the state polyhedron of $w$.

Proof. Minimizing $A(w, B)$ over all hierarchical models is equivalent to maximizing $-w^T v_B$ where $v_B$ are the vector associated to a monomial ideal defined in Theorem 12.3.13. By Theorem 12.3.13, this amounts to maximizing over the vertices of the state polyhedron of $I(D)$. Since an optimum can always be attained at a vertex, this means that a minimum aberration model can always be taken to correspond to one coming from the term order induced by $w$. □

Note that if we also want to find a design and a polynomial regression model that has as small an aberration as possible, among all designs with a fixed number of points $r$, this is also provided by a combination of Theorems 12.3.16 and 12.1.11. Indeed, on a fixed number of points $r$, the largest state polytope possible is obtained by taking a design $D$ whose initial ideals are precisely all the corner cut ideals with $r$ standard monomials. Hence, simply taking a generic design will achieve the desired optimality.

12.4. 2-level Designs and System Reliability

In this section we focus on certain two level designs, their connections to system reliability, and how tools from commutative algebra can be used to gain insight into them. Key tools are the study of squarefree monomial ideals and their Hilbert series.

Consider a system consisting of $m$ components, $[m]$, and suppose that for the system to function properly, certain subsets of the components must not fail simultaneously. We suppose that the set of failure modes is closed upwards, so if $S \subseteq [m]$ is a failure mode, and $S \subseteq T \subseteq [m]$ then $T$ is also a failure mode. Thus, the set $\Gamma$ of all subsets of $[m]$ whose failure does not cause the system to fail is a simplicial complex, as defined in Section 9.3.
Example 12.4.1. Consider the graph with 5 vertices and 7 edges as shown in Figure 12.4. The vertices $s$ and $t$ are the source and recipient of a transmission which will be sent over the network. The various edges in the network work or fail each with their own independent probability. This system will function (i.e. be able to successfully transmit a message from $s$ to $t$) if the set of failed edges do not disconnect $s$ and $t$. The set of failure modes which still allow the system to function will form a simplicial complex, since failure states that break the system will still break the system if further elements are added. The list of minimal failure states that break the system are minimal sets of edges that disconnect $s$ and $t$. These are

$$12, 67, 234, 457, 1357, 2356$$

By associating to each subset $S \subseteq [m]$ the 0/1 indicator vector $u_S \in \mathbb{R}^m$, the reliability system naturally corresponds to a design. As in previous sections we could associate the vanishing ideal $I(D)$ to the design. However, it because substantially more useful to associate an alternate ideal, the Stanley-Reisner ideal, to the resulting simplicial complex.

Definition 12.4.2. Let $\Gamma \subseteq 2^{[m]}$ be a simplicial complex on $m$ vertices. The Stanley-Reisner ideal associated to $\Gamma$ is the ideal

$$SR_{\Gamma} := \langle \prod_{i \in S} x_i : S \notin \Gamma \rangle.$$ 

That is, $SR_{\Gamma}$ is generated by monomials corresponding to the subsets of $[m]$ that are not faces of the complex $\Gamma$.

Note that we only need to consider the minimal nonfaces of $\Gamma$ when writing down the generating sets of $SR_{\Gamma}$. The Stanley-Reisner ideal is a squarefree monomial ideal, in particular, it is a radical ideal, and its variety $V(SR_{\Gamma})$ is a union of coordinate subspaces. It is easy to describe the primary decomposition of this ideal.
Proposition 12.4.3. Let $\Gamma$ be a simplicial complex on $m$ vertices. Then

$$SR_\Gamma = \bigcap_{S \in \text{facet}(\Gamma)} \langle x_i : i \notin S \rangle.$$ 

In other words, the variety $V(SR_\Gamma)$ consists of the union of those coordinate subspaces, one for each facet of $S$, and such that nonzero coordinates appear precisely at the coordinates corresponding to the elements of the facet.

Note that the semialgebraic set $V(SR_\Gamma) \cap \Delta_{m-1}$ gives a geometric realization of the simplicial complex $\Gamma$.

Example 12.4.4. Consider the network connectivity problem from Example 12.4.1 with associated simplicial complex of failure modes that allow the system to transmit messages $\Gamma$. The Stanley-Reisner ideal $SR_\Gamma$ is generated by all of the monomials corresponding to minimal system failures in Example 12.4.1 so

$$RS_\Gamma = \langle x_2x_5x_7, x_2x_3x_4, x_4x_5x_7, x_1x_3x_5x_7, x_2x_3x_5x_6 \rangle.$$ 

This Stanley-Reisner ideal has primary decomposition

$$RS_\Gamma = \langle x_2, x_7 \rangle \cap \langle x_1, x_3, x_7 \rangle \cap \langle x_1, x_4, x_6 \rangle \cap \langle x_2, x_5, x_6 \rangle \cap \langle x_1, x_3, x_5, x_6 \rangle \cap \langle x_2, x_3, x_4, x_6 \rangle \cap \langle x_1, x_4, x_5, x_7 \rangle.$$ 

Note that the variety of each of the minimal primes of $RS_\Gamma$ corresponds to a maximal set of edges that could fail but so that the network will continue to transmit messages. Conversely, the generators of the minimal primes correspond to minimal sets of edges which, when all function, will allow the network to transmit messages. In this particular problem, these are precisely the simple paths that connected $s$ with $t$.

A key problem in reliability theory is to determine what is the probability that the system actually functions. An idealized setting is to imagine that the components function or do not function independently of each other, and component $i$ has probability $p_i$ of functioning. The probability of the system functioning is then given by the following formula:

$$\sum_{S \subseteq \Gamma} \left( \prod_{i \in S} p_i \prod_{j \notin S} (1 - p_j) \right).$$ 

This formula is related to the Stanley-Reisner ideal through its Hilbert series.

Definition 12.4.5. Let $M \subseteq \mathbb{K}[x_1, \ldots, x_m]$ be a monomial ideal. The multigraded Hilbert series of the quotient ring $\mathbb{K}[x_1, \ldots, x_m]/M$ is the multivariable power series:

$$H(\mathbb{K}[x_1, \ldots, x_m]/M; x) = \sum_{x^a \notin M} x^a.$$
248  12. Design of Experiments

If the Hilbert series of $H(\mathbb{K}[x_1, \ldots, x_m]/M; x)$ is expressed as a rational function in the form

$$H(\mathbb{K}[x_1, \ldots, x_m]/M; x) = \frac{K(\mathbb{K}[x_1, \ldots, x_m]/M; x)}{(1-x_1) \cdots (1-x_m)}$$

then $K(\mathbb{K}[x_1, \ldots, x_m]/M; x)$ is the $K$-polynomial of $\mathbb{K}[x_1, \ldots, x_m]/M$.

We can also define the multigraded Hilbert series for any module, though we will not have formally introduced modules in the present text. For monomial ideals $M$, the multigraded Hilbert series is defined by

$$H(M; x) = \sum_{x^a \in M} x^a.$$ 

Hilbert series and reliability are connected via the following:

**Theorem 12.4.6.** The $K$-polynomial of the quotient ring $\mathbb{K}[x_1, \ldots, x_m]/RS_\Gamma$ is

$$(12.4.1) \quad K(\mathbb{K}[x_1, \ldots, x_m]/RS_\Gamma; x) = \sum_{S \in \Gamma} \left( \prod_{i \in S} x_i \prod_{j \notin S} (1-x_j) \right).$$

**Proof.** The Hilbert series of $\mathbb{K}[x_1, \ldots, x_m]/RS_\Gamma$ is the sum over all monomials that are not in $RS_\Gamma$. Each such monomial $x^a$ has a vector $a$ whose support $\text{supp}(a)$ is a face of $\Gamma$ (where $\text{supp}(a) = \{ i \in [m] : a_i \neq 0 \}$). Hence we can write

$$H(\mathbb{K}[x_1, \ldots, x_m]/RS_\Gamma; x) = \sum \{ x^a : a \in \mathbb{N}^m \text{ and } \text{supp}(a) \in \Gamma \}$$

$$= \sum_{S \in \Gamma} \sum \{ x^a : a \in \mathbb{N}^m \text{ and } \text{supp}(a) = S \}$$

$$= \sum_{S \in \Gamma} \prod_{i \in S} x_i \prod_{i \notin S} (1-x_i).$$

The $K$-polynomial is obtained by clearing the denominator. \( \square \)

**Corollary 12.4.7.** Let $\Gamma$ be a simplicial complex of functioning failure modes of a reliability system. Suppose that each component functions independently with probability $p_i$. Then the probability that the system functions is

$$K(\mathbb{K}[x_1, \ldots, x_m]/SR_\Gamma; p).$$

While Corollary 12.4.7 demonstrates the connection of the $K$-polynomial to the systems reliability problem, the formula of Equation design:eq:kpoly is typically an inefficient method for actually calculating the $K$-polynomial, since it involves determining and summing over every element of $\Gamma$. For applications to problems of system reliability, one needs a more compact format for the $K$-polynomial. A straightforward approach that can save
in the computation is to use the principle of inclusion and exclusion to compute the multigraded Hilbert series of the quotient \( \mathbb{K}[x_1, \ldots, x_m]/M \) for a monomial ideal \( M \). We illustrate in a small example first:

**Example 12.4.8.** Let \( M = \langle x_1^2 x_2, x_2^3 x_3^2 \rangle \). We want to enumerate the monomials not in \( M \). Clearly, this is the set of all monomials in \( \mathbb{K}[x_1, x_2, x_3] \) minus the monomials in \( M \), so that \( H(\mathbb{K}[x_1, x_2, x_3]/M; x) = H(\mathbb{K}[x_1, x_2, x_3]; x) - H(M; x) \). The Hilbert series of \( \mathbb{K}[x_1, x_2, x_3] \) is
\[
H(\mathbb{K}[x_1, x_2, x_3]; x) = \frac{1}{(1 - x_1)(1 - x_2)(1 - x_3)}.
\]
Similarly, if we have a principal monomial ideal \( \langle x^a \rangle \) then
\[
H(\langle x^a \rangle; x) = \frac{x^a}{(1 - x_1)(1 - x_2)(1 - x_3)}.
\]
Since our ideal is generated by two monomials, we can reduce to the principal case using the principle of inclusion and exclusion. Monomials in \( M \) are either divisible by \( x_1^2 x_2 \) or \( x_2^3 x_3^2 \) or both. If they are divisible by both, they are divisible by the least common multiple. Putting these all together yields the following as the Hilbert series of \( \mathbb{K}[x_1, x_2, x_3]/M \):
\[
H(\mathbb{K}[x_1, x_2, x_3]/M; x) = \frac{1 - x_1^2 x_2 - x_2^3 x_3^2 + x_1^2 x_2^3 x_3^2}{(1 - x_1)(1 - x_2)(1 - x_3)}.
\]

More generally, we have the following general form for the multigraded Hilbert series of a monomial ideal using the principle of inclusion and exclusion.

**Theorem 12.4.9.** Let \( M = \langle x_1^{a_1}, \ldots, x_1^{a_k} \rangle \). Then
\[
K(\mathbb{K}[x_1, \ldots, x_m]/M; x) = \sum_{S \subseteq [m]} (-1)^{|S|} \text{LCM}(\{x_1^{a_i} : i \in S\}).
\]

Theorem [12.4.9] can be useful for computing the \( K \) polynomial in small examples, however it is clearly exponential in the number of generators (of course, it might not be possible to avoid exponential complexity, however). For instance, in Example [12.4.4] the monomial ideal \( SR_1 \) has six generators so the inclusion exclusion formula will involve summing over 64 terms, whereas expanding this expression and cancelling out, and collecting like terms yields 27 terms in total in the \( K \)-polynomial.

Developing methods for computing the \( K \)-polynomials of monomial ideals is an active and complex area that we will not cover here. A key tool for computing the \( K \)-polynomial is the free resolution of the resulting quotient ring. This is an important topic in combinatorial commutative algebra [MS04]. Applications to reliability theory include in tree percolation [MSdCW16] and developing formulas for failure probabilities for communication problems on networks [Moh16].
12.5. Exercises

**Exercise 12.1.** Suppose that \( \mathcal{D} = D^m \subseteq \mathbb{K}^m \) is a full factorial design. Show that the only polynomial regression model that is estimable is the model with support set:

\[ \{ x^u : u_i < |D| \text{ for all } i \}. \]

**Exercise 12.2.** Prove Proposition 12.2.1. Design an algorithm that takes as input the generating sets of two ideals \( I \) and \( J \) and outputs a generating set for \( I \cap J \).

**Exercise 12.3.** Consider the design

\( \mathcal{D} = \{(0, 0, 0), (\pm 2, 0, 0), (0, \pm 2, 0), (0, 0, \pm 2), \\
(\pm 1, \pm 1, 0), (\pm 1, 0, \pm 1), (0, \pm 1, \pm 1)\} \subseteq \mathbb{R}^3 \)

consisting of 19 points in \( \mathbb{R}^3 \). Compute the vanishing ideal of the design, determine the number distinct initial ideals, and calculate the Gröbner fan.

**Exercise 12.4.** Let \( \mathcal{D} = D^m \subseteq \mathbb{K}^m \) be a full factorial design, \( \mathcal{D}' \subseteq \mathcal{D} \) a fraction, and \( \mathcal{D}'' = \mathcal{D} \setminus \mathcal{D}' \) be the complementary fraction. Let \( \prec \) be a term order. Explain how in \( \prec(I(\mathcal{D}')) \) and in \( \prec(I(\mathcal{D}'')) \) are related [MASdCW13].

**Exercise 12.5.** Consider the graph from Example 12.4.1 but now consider a system failure to be any failure of edges that makes it impossible to transmit messages between any pair of vertices. If each edge \( i \) has probability \( p_i \) of functioning, calculate the probability that the system does not fail.
Graphical Models

In this chapter we describe graphical models, an important family of statistical models that are used to build complicated interaction structures between many random variables by specifying local dependencies between pairs or small subsets of the random variables. This family of statistical models has been widely used in statistics [HEL12, Whi90], computer science [KF09], computational biology [SM14] and many other areas. A standard reference for a mathematical treatment of graphical models is [Lau96]. Graphical models will play an important role throughout the remainder of the book as they are an important example about which we can ask very general questions. They are also useful from a computational standpoint. Special cases of graphical models include the phylogenetic models from Chapter [15] and the hidden Markov models which are widely used in biological applications and discussed in Chapter [18].

13.1. Conditional Independence Description of Graphical Models

Let \( X = (X_v \mid v \in V) \) be a random vector and \( G = (V, E) \) a graph with vertex set \( V \) and some set of edges \( E \). In the graphical model associated to the graph \( G \) each edge \((u, v) \in E\) of the graph denotes some sort of dependence between the variables \( X_u \) and \( X_v \). The type of graph that is used (for example, undirected graph, directed graph, chain graph [AMP01, Drt09a], mixed graph [STD10], ancestral graph [RS02], etc.) will determine what is meant by “dependence” between the variables, and often this can be expressed as a parametrization of the model, which will be explained in more detail in Section [13.2]. Since the edges correspond to dependence between
the random variables, the non-edges will typically correspond to independence or conditional independence between collections of random variables. It is this description which we begin with in the present section. We focus in this chapter on the two simplest versions of graphical models, those whose underlying graph is an undirected graph, and those whose underlying graph is a directed acyclic graph.

Let $G = (V, E)$ be an undirected graph. Formally this means that $E$ is a set of ordered pairs $(u, v)$ with $u, v \in V$ and such that if $(u, v) \in E$ then so is $(v, u)$. The pairs $(u, v) \in E$ are called the edges of the graph and the set $V$ is the set of vertices of the graph. We will assume that the graph has no loops, that is, for no $v \in V$ is the pair $(v, v) \in E$.

Associated to the undirected graph are various Markov properties which are lists of conditional independence statements that must be satisfied by all random vectors $X$ consistent with the graph $G$. To describe these Markov properties, we need some terminology from graph theory. A path between vertices $u$ and $w$ in an undirected graph $G = (V, E)$ is a sequence of vertices $u = v_1, v_2, \ldots, v_k = w$ such that each $(v_{i-1}, v_i) \in E$. A pair of vertices $a, b \in V$ is separated by a set of vertices $C \subseteq V \setminus \{a, b\}$ if every path from $a$ to $b$ contains a vertex in $C$. If $A, B, C$ are disjoint subsets of $V$, we say that $C$ separates $A$ and $B$ if $a$ and $b$ are separated by $C$ for all $a \in A$ and $b \in B$. The set of neighbors of a vertex $v$ is the set $N(v) = \{u : (u, v) \in E\}$.

**Definition 13.1.1.** Let $G = (V, E)$ be an undirected graph.

(i) The pairwise Markov property associated to $G$ consists of all conditional independence statements $X_u \perp \perp X_v | X_{V \setminus \{u, v\}}$ where $(u, v)$ is not an edge of $G$.

(ii) The local Markov property associated to $G$ consists of all conditional independence statements $X_v \perp \perp X_{V \setminus (N(v) \cup \{v\})} | X_{N(v)}$ for all $v \in V$.

(iii) The global Markov property associated to $G$ consists of all conditional independence statements $X_A \perp \perp X_B | X_C$ for all disjoint sets $A, B, C$ such that $C$ separates $A$ and $B$ in $G$.

Let pairwise($G$), local($G$), and global($G$) denote the set of pairwise, local, and global Markov statements associated to the graph $G$.

Note that the Markov properties are arranged in order of increasing strength. If a distribution satisfies the global Markov property associated to the graph $G$, it necessarily satisfies the local Markov property on the graph $G$. And if a distribution satisfies the local Markov property on the graph $G$, it necessarily satisfies the pairwise Markov property. The reverse implication is not true in general.
Example 13.1.2. Let $G$ be the graph with vertex set $V = \{3\}$ and the single edge $2 \rightarrow 3$. The pairwise Markov property for this graph yields the two conditional independence statements $X_1 \perp \perp X_2 | X_3$ and $X_1 \perp \perp X_3 | X_2$. On the other hand, both the local and global Markov property for this graph consists of the single statement $X_1 \perp \perp (X_2, X_3)$. For discrete random variables, there are distributions that satisfy the pairwise statements and not the local statements, in particular, the distributions that fail to satisfy the intersection axiom (see Proposition 4.1.5 and Theorem 4.3.3).

Example 13.1.3. Consider the path of length five $P_5$ with vertex set $\{5\}$ and edges $\{12, 23, 34, 45\}$. In this example the pairwise, local, and global Markov properties associated to $P_5$ are all different. For example, the local Markov statement associated to the vertex 3, which is $X_3 \perp \perp (X_1, X_5) | (X_2, X_4)$ is not implied by the pairwise Markov statements. The global Markov statement $(X_1, X_2) \perp \perp (X_4, X_5) | X_3$ is not implied by the local Markov statements.

Characterizations of precisely which graphs satisfy the property that the pairwise Markov property equals the local Markov property, and the local Markov property equals the global Markov property can be found in [Lau96]. Remarkably, the failure of the intersection axiom is the only obstruction to the probabilistic equality of the three Markov properties.

Theorem 13.1.4. If the random vector $X$ has a joint distribution $P$ that satisfies the intersection axiom, then $P$ obeys the pairwise Markov property for the undirected graph $G$ if and only if it obeys the global Markov property for the graph $G$. In particular, if $P(x) > 0$ for all $x$ then the pairwise, local, and global Markov properties are all equivalent.

Proof. ($\Leftarrow$): If $u$ and $v$ are vertices in $G$ that are not adjacent, then $V \setminus \{u, v\}$ separates $\{u\}$ and $\{v\}$ in $G$. Hence the pairwise conditional independence statement $X_u \perp \perp X_v | X_{V \setminus \{u, v\}}$ appears among the global conditional independence statements.

($\Rightarrow$): Suppose that $C$ separates nonempty subsets $A$ and $B$. First of all, we can assume that $A \cup B \cup C = V$. If not, there are supersets $A'$ and $B'$ of $A$ and $B$, respectively, such that $A' \cup B' \cup C = V$ and $C$ separates $A'$ and $B'$. Then if we have proven that $X_{A'} \perp \perp X_{B'} | X_C$ is implied by the local Markov statements, this will also imply that $X_{A} \perp \perp X_{B} | X_{C}$ follows from the local Markov statements by applying the decomposition axiom (Proposition 4.1.4 (ii)).

So suppose that $A \cup B \cup C = V$. We will proceed by induction on $#(A \cup B)$. If $#(A \cup B) = 2$ then both $A$ and $B$ are singletons, $A = \{a\}$ and $B = \{b\}$, there is no edge between $a$ and $b$, and so $X_A \perp \perp X_B | X_C$ is a local Markov statement. So suppose $#(A \cup B) > 2$. Without loss of generality we may assume that $#B \geq 2$. Let $B_1 \cup B_2 = B$ be any bipartition of $B$ into
nonempty parts. Then \( C \cup B_1 \) separates \( A \) and \( B_1 \) and \( C \cup B_2 \) separates \( A \) and \( B_2 \). Also, \( \#(A \cup B_1) < \#(A \cup B) \) and \( \#(A \cup B_2) < \#(A \cup B) \) so we can apply the induction hypothesis to see that

\[
X_A \perp \perp (X_{B_2}, X_C) \quad \text{and} \quad X_A \perp \perp (X_{B_1}, X_C)
\]  

are implied by the local Markov statements for \( G \), plus the intersection axiom. But then application of the intersection axiom to the two statements in Equation 13.1.1 shows that \( X_A \perp \perp X_B | X_C \) is implied by the local Markov statements and the intersection axiom. \( \square \)

Note that for multivariate Gaussian random variables, the interpretation of the local Markov statement is especially simple. A conditional independence statement of the form \( X_u \perp \perp X_v | X_{V \setminus \{u,v\}} \) holds if and only if \( \det \Sigma_{V \setminus \{u,v\}, V \setminus \{u\}} = 0 \). By the cofactor expansion formula for the inverse matrix, this is equivalent to requiring that \( (\Sigma_{uv}^{-1} = 0 \). Hence:

**Proposition 13.1.5.** The set of covariance matrices of nonsingular multivariate Gaussian distribution compatible with the Markov properties for the graph \( G \) is precisely the set

\[
\mathcal{M}_G = \{ \Sigma \in PD_{[V]} : \Sigma_{uv}^{-1} = 0 \text{ if } u \neq v \text{ and } (u,v) \notin E \}.
\]

In particular, the Gaussian graphical model is an example of a Gaussian exponential family, where the subspace of concentration matrices that is used in the definition is a coordinate subspace.

The global Markov property for undirected graphs satisfies an important completeness property.

**Proposition 13.1.6.** Let \( G \) be an undirected graph and suppose that \( A, B, \) and \( C \) are disjoint subsets of \( V \) such that \( C \) does not separate \( A \) and \( B \) in \( G \). Then there is a probability distribution satisfying all the global Markov statements of \( G \) and not satisfying \( X_A \perp \perp X_B | X_C \).

**Proof.** We show this with the example of a multivariate normal random vector. Consider a path \( \pi \) of vertices from \( a \in A \) to \( b \in B \) that does not pass through any vertex in \( C \), and construct a concentration matrix \( \Sigma^{-1} = K \) which has ones along the diagonal, a small nonzero \( \epsilon \) in entries corresponding to each edge in the path \( \pi \), and zeroes elsewhere. The corresponding covariance matrix belongs to the Gaussian graphical model associated to \( G \) since \( K \) only has nonzero entries on the diagonal and in positions corresponding to edges of \( G \), and by the fact that pairwise property implies the global property for multivariate normal random vector (whose density is positive).
After reordering vertices, we can assume that the concentration matrix is a tridiagonal matrix of the following form

\[
K = \begin{pmatrix}
1 & \epsilon & \cdots & \\
\epsilon & 1 & \cdots & \\
\cdots & \cdots & \cdots & \epsilon \\
\cdots & \cdots & \cdots & 1 & \epsilon \\
& & & \cdots & 1
\end{pmatrix}
\]

\[
K^{-1} = I_{V \setminus \pi}
\]

so that \(\Sigma = K^{-1}\) is a block matrix, with nonzero off-diagonal entries only appearing precisely in positions indexed by two elements of \(\pi\). The conditional independence statement \(X_A \perp\!\!\!\perp X_B | X_C\) holds if and only if \(\Sigma_{A,B} - \Sigma_{A,C} \Sigma_{C,C}^{-1} \Sigma_{C,B} = 0\). However, \(\Sigma_{A,C}\) and \(\Sigma_{C,B}\) are both zero since \(C \cap \pi = \emptyset\). But \(\Sigma_{A,B} \neq 0\) since both \(a, b \in \pi\). So the conditional independence statement \(X_A \perp\!\!\!\perp X_B | X_C\) does not hold for this distribution.

A second family of graphical models in frequent use are graphical models associated to directed acyclic graphs. Let \(G = (V, E)\) be a directed graph. The directed graph \(G\) is acyclic if there does not exist a directed cycle of edges in \(G\). In this setting, the directions of the arrows are sometimes given causal interpretations (i.e. some events happen before and affect other events), though we will primarily focus on only the probabilistic interpretation of these models. See [Pea09] for further information on using directed acyclic graphs for causal inference.

In a directed graph \(G\) we have directed paths, which are sequences of vertices \(u_0, \ldots, u_k\) such that for each \(i\), \(u_i \to u_{i+1} \in E\). On the other hand, an undirected path is a sequence of vertices with \(u_0, \ldots, u_k\) such that for each \(i\) either \(u_i \to u_{i+1}\) is an edge or \(u_{i+1} \to u_i\) is an edge. In an undirected path, a collider is a vertex \(u_i\) such that \(u_{i-1} \to u_i\) and \(u_{i+1} \to u_i\) are both edges of \(G\).

Let \(v \in V\). The parents of \(v\), denoted \(\text{pa}(v)\) consists of all \(w \in V\) such that \(w \to v\) is an edge of \(G\). The descendants of \(v\), denoted \(\text{de}(v)\) consists of all \(w \in V\) such that there is a directed path from \(v\) to \(w\). The nondescendants of \(v\) are denoted \(\text{nd}(v) = V \setminus \{v\} \cup \text{de}(v)\). The ancestors of \(v\), denoted \(\text{an}(v)\) consists of all \(w \in V\) such that there is a directed path from \(w\) to \(v\).

**Definition 13.1.7.** Two nodes \(v\) and \(w\) in a directed acyclic graph \(G\) are \(d\)-connected given a set \(C \subseteq V \setminus \{v, w\}\) if there is an undirected path \(\pi\) from \(v\) to \(w\) such that

1. all colliders on \(\pi\) are in \(C \cup \text{an}(C)\) and
2. no non-collider on \(\pi\) is in \(C\).
If \( A, B, C \subseteq V \) are pairwise disjoint with \( A \) and \( B \) nonempty, then \( C \) d-separates \( A \) and \( B \) if no pair of nodes \( a \in A \) and \( b \in B \) are d-connected given \( C \).

The definition of d-separation can also be reformulated in terms of the usual separation criterion in an associated undirected graph, the moralization. For a directed acyclic graph \( G \), let the moralization \( G^m \) denote the undirected graph which has an undirected edge \((u, v)\) for each directed edge in \( u \to v \) in \( G \), plus we add the undirected edge \((u, v)\) if \( u \to w, \ v \to w \) are edges in \( G \). Thus the moralization “marries the parents” of each vertex. For a set of vertices \( S \subseteq V \), let \( G_S \) denote the induced subgraph on \( S \).

**Proposition 13.1.8.** Let \( G \) be a directed acyclic graph. Then \( C \) d-separates \( A \) and \( B \) in \( G \) if and only if \( C \) separates \( A \) and \( B \) in the moralization \((G_{\text{an}(A \cup B \cup C)})^m\).

**Proof.** See, for example, [Lau96, Prop. 3.25]. □

As for undirected graphs, we can define pairwise, local, and global Markov properties associated to any directed acyclic graph \( G \).

**Definition 13.1.9.** Let \( G = (V, E) \) be a directed acyclic graph.

(i) The **directed pairwise Markov property** associated to \( G \) consists of all conditional independence statements \( X_u \perp \!
\!\!\!\!
\perp X_v | X_{\text{nd}(u) \setminus \{v\}} \) where \((u, v)\) is not an edge of \( G \).

(ii) The **directed local Markov property** associated to \( G \) consists of all conditional independence statements \( X_v \perp \!
\!\!\!\!
\perp X_{\text{nd}(v) \setminus \text{pa}(v)} | X_{\text{pa}(v)} \) for all \( v \in V \).

(iii) The **global Markov property** associated to \( G \) consists of all conditional independence statements \( X_A \perp \!
\!\!\!\!
\perp X_B | X_C \) for all disjoint sets \( A, B, \) and \( C \) such that \( C \) d-separates \( A \) and \( B \) in \( G \).

Let \( \text{pairwise}(G) \), \( \text{local}(G) \), and \( \text{global}(G) \) denote the set of pairwise, local, and global Markov statements associated to the DAG \( G \).

![Figure 13.1.1. The DAG from Example 13.1.10](image)
Example 13.1.10. Consider the DAG with 6 vertices illustrated in Figure [13.1.1]. In this DAG, we can see that the conditional independence statement $X_1 \perp \perp X_2$ holds, since $\emptyset$ $d$-separates 1 and 2 in the graph. This is an example of a pairwise Markov statement. On the other hand, the conditional independence statement $(X_1, X_2) \perp \perp (X_5, X_6)|(X_3, X_4)$ holds in this graph, and is an example of a global Markov statement that is not a directed local Markov statement.

Although the list of conditional independence statements can be strictly larger as we go from pairwise to local to global Markov statements, the global and local Markov properties are, in fact, equivalent on the level of probability distributions.

**Theorem 13.1.11.** If the random vector $X$ has a joint distribution $P$ that obeys the directed local Markov property for the directed acyclic graph $G$ then $P$ obeys the directed global Markov property for the graph $G$.

Theorem [13.1.11] is intimately connected with the parametrizations of graphical models which we will explore in the next section, where we will also give its proof. The global Markov property is also complete with respect to a given directed acyclic graph $G$.

**Proposition 13.1.12.** Let $G$ be a directed acyclic graph and suppose that $A, B, C \subseteq V$ are disjoint subsets such that $C$ does not $d$-separate $A$ and $B$ in $G$. Then there is a probability distribution satisfying all the global Markov statements of $G$ and not satisfying $X_A \perp X_B|X_C$.

**Proof Sketch.** As in the proof of Proposition [13.1.6] this can be shown by constructing an explicit example of a distribution that satisfies the global Markov statements but not satisfying the statement $X_A \perp X_B|X_C$. By the moralization argument, this reduces to the case of undirected graphs, assuming that we have a reasonable method to parametrize distributions satisfying the directed global Markov property. This will be dealt with in the next section. □

For undirected graphical models, each graph gives a unique set of global Markov statements, and hence each graph yields a different family of probability distributions. The same is not true for directed graphical models, since different graphs can yield precisely the same conditional independence statements, because two different directed graphs can have the same moralization on all induced subgraphs.

**Example 13.1.13.** The graphs $G_1 = ([3], \{1 \rightarrow 2, 2 \rightarrow 3\})$ and $G_2 = ([3], \{3 \rightarrow 2, 2 \rightarrow 1\})$ both have the global Markov property consisting of the single independence statement $X_1 \perp X_3|X_2$. 

Two graphs are called Markov equivalent if they yield the same set of global Markov statements. Markov equivalence for directed acyclic graphs is completely characterized by the following result.

**Theorem 13.1.14.** Two directed acyclic graphs $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ are Markov equivalent if and only if the following two conditions are satisfied:

1. $G_1$ and $G_2$ have the same underlying undirected graph,
2. $G_1$ and $G_2$ have the same unshielded colliders, which are triples of vertices $u, v, w$ which induce a subgraph $u \rightarrow v \leftarrow w$.

A proof of this is found in [AMP97, Thm 2.1].

**Example 13.1.15.** Note that DAG models and undirected graphical models give fundamentally different families of probability distributions. For a given DAG, $G$ there is usually not an undirected graph $H$ whose (undirected) global Markov property is the same the (directed) global Markov property of $G$. For instances, there is no undirected graph on 3 vertices that has the same global Markov statements as the graph $G = ([3], \{1 \rightarrow 3, 2 \rightarrow 3\})$.

### 13.2. Parametrizations of Graphical Models

A useful counterpoint to the definition of graphical model via conditional independence statements from Section 13.1 is the parametric definition of graphical models which we describe here. In many applied contexts, the parametric description is the natural description for considering an underlying process that generates the data. As usual with algebraic statistical models, we have a balance between the model’s implicit description (via conditional independence constraints) and its parametric description. For both undirected and directed acyclic graphical models there are theorems which relate the description via conditional independence statements to parametric description of the model (the Hammersley-Clifford Theorem (Theorem 13.2.3) and the recursive factorization theorem (Theorem 13.2.10), respectively). We will see two important points emerge from the comparison of the parametric and implicit model descriptions: 1) for discrete undirected graphical models, there are distributions which satisfy all the global Markov statements but are not in the closure of the parametrization, 2) even when the parametric description of the model gives exactly the distributions that satisfy the global Markov statements of the graph, the prime ideal of all functions vanishing on the model might not equal the global conditional independence ideal of the graph.

First we consider parametrizations of graphical models for undirected graphs. Let $G$ be an undirected graph with vertex set $V$ and edge set $E$. A
clique $C \subseteq V$ in $G$ is a set of vertices such that $(i, j) \in E$ for all $i, j \in C$. The set of all maximal cliques in $G$ is denoted $\mathcal{C}(G)$. For each $C \in \mathcal{C}(G)$, we introduce a continuous potential function $\phi_C(x_C) \geq 0$ which is a function on $X_C$, the state space of the random vector $X_C$.

**Definition 13.2.1.** The *parametrized undirected graphical model* consists of all probability density functions on $X$ of the form

$$f(x) = \frac{1}{Z} \prod_{C \in \mathcal{C}(G)} \phi_C(x_C)$$  \hspace{1cm} (13.2.1)

for some potential functions $\phi_C(x_C)$, where

$$Z = \int_X \prod_{C \in \mathcal{C}(G)} \phi_C(x_C) d\mu(x)$$

is the normalizing constant (also called the partition function). The parameter space for this model consists of all tuples of potential functions such that the normalizing constant is finite and nonzero. A probability density is said to factorize according to the graph $G$ if it can be written in the product form (13.2.1) for some choice of potential functions.

**Example 13.2.2.** Let $G$ be the graph with vertex set $[5]$ and edge set $\{12, 13, 23, 25, 34, 45\}$, pictured in Figure 13.2.1. The set of maximal cliques of $G$ is $\{123, 25, 34, 45\}$. The parametric description from (13.2.1) asks for probability densities with the following factorization:

$$f(x_1, x_2, x_3, x_4, x_5) = \frac{1}{Z} \phi_{123}(x_1, x_2, x_3)\phi_{25}(x_2, x_5)\phi_{34}(x_3, x_4)\phi_{45}(x_4, x_5).$$

The Hammersley-Clifford theorem gives the important result that the parametric graphical model described in Definition 13.2.1 yields the same family of distributions as the pairwise Markov property when restricted to strictly positive distributions. The original proof of this theorem has an interesting story, see [Cli90].
**Theorem 13.2.3** (Hammersley-Clifford). A continuous positive probability density \( f \) on \( \mathcal{X} \) satisfies the pairwise Markov property on the graph \( G \) if and only if if factorizes according to \( G \).

**Proof.** \((\Leftarrow)\) Suppose that \( f \) factorizes according to \( G \) and that \( i \) and \( j \) are not connected by an edge in \( G \). Then no potential function in the factorization of \( f \) depends on both \( x_i \) and \( x_j \). Letting \( C = V \setminus \{i, j\} \), we can multiply potential functions together that depend on \( x_i \) as \( \psi_i(x_i, x_C) \) and those together that depend on \( x_j \) as \( \psi_i(x_i, x_C) \), and the remaining functions that depend on neither has \( \psi_C(x_C) \), to arrive at the factorization:

\[
f(x_i, x_j, X_C) = \frac{1}{Z} \psi_i(x_i, x_C) \psi_i(x_i, x_C) \psi_C(x_C).
\]

This function plainly satisfies the relation

\[
f(x_i, x_j, X_C) f(x_i', x_j', X_C) = f(x_i, x_j, X_C) f(x_i', x_j, X_C)
\]

for all \( x_i, x_i', x_j, x_j' \) by which we deduce that \( X_i \indep X_j | X_C \) holds. Hence, \( f \) satisfies the local Markov property.

\((\Rightarrow)\) Suppose that \( f \) satisfies the local Markov property on \( G \). Let \( y \in \mathcal{X} \) be any point. For any subset \( C \subseteq V \) define a potential function

\[
\phi_C(x_C) = \prod_{S \subseteq C} f(x_S, y_{V \setminus S})^{(-1)^{\#C - \#S}}.
\]

Note that by the principle of Möbius inversion,

\[
f(x) = \prod_{C \subseteq V} \phi_C(x_C).
\]

We claim that if \( C \) is not a clique of \( G \), then \( \phi_C \equiv 1 \), by which we deduce that

\[
f(x) = \prod_{C \subseteq C^*(G)} \phi_C(x_C).
\]

where \( C^*(G) \) is the set of all cliques in \( G \). This proves that \( f \) factorizes according to the model since we can merge the potential functions associated to nonmaximal cliques into those associated to one of the maximal cliques containing it.

To prove that claim, suppose that \( C \) is not a clique of \( G \). Then there is a pair \( i, j \subseteq C \) such that \( (i, j) \notin E \). Let \( D = V \setminus \{i, j\} \). We can write \( \phi_C(x_C) \) as

\[
\phi_C(x_C) = \prod_{S \subseteq C \cap D} \left( \frac{f(x_i, x_j, x_S, y_{D \setminus S}) f(y_i, y_j, x_S, y_{D \setminus S})}{f(x_i, y_j, x_S, y_{D \setminus S}) f(x_i, y_j, x_S, y_{D \setminus S})} \right)^{(-1)^{\#C - \#S}}.
\]

Since the conditional independence statement \( X_i \indep X_j | X_D \) holds, each of the terms inside the product is equal to one, hence the product equals one. \( \square \)
While the Hammersley-Clifford theorem only compares the local Markov statements to the parametrization, it also implies that any distribution in the image of the parametrization associated to the graph $G$ satisfies the global Markov statements.

**Corollary 13.2.4.** Let $P$ be a distribution that factors according to the graph $G$. Then $P$ satisfies the global Markov property on the graph $G$.

**Proof.** The Hammersley-Clifford theorem shows that if $P$ is positive, then $P$ satisfies the local Markov property. All positive $P$ satisfy the intersection axiom, and hence by Theorem 13.1.4, such positive $P$ must satisfy the global Markov property. However, the global Markov property is a closed condition, so all the distributions that factorize and have some zero probabilities, which must be limits of positive distributions that factorize, also satisfy the global Markov property. □

Focusing on discrete random variables $X_1, \ldots, X_m$, let $X_j$ have state space $[r_j]$. The joint state space of the random vector $X = (X_1, \ldots, X_m)$ is $\mathcal{R} = \prod_{j=1}^m [r_j]$. In the discrete case, the condition that the potential functions $\psi_C(x_C)$ are continuous on $\mathcal{R}_C$ is vacuous, and hence we are allowed any nonnegative function as a potential function. Using an index vector $i_C = (i_j)_{j \in C} \in \mathcal{R}_C$, to represent the states we can write the potential function $\psi_C(x_C)$ as $\theta_{i_C}^{(C)}$, so that the parametrized expression for the factorization in the Equation 13.2.1 becomes a monomial parametrization. Hence, the discrete undirected graphical model is a hierarchical model. For discrete graphical models and a graph (either directed, undirected, or otherwise) let $I_G$ denote the homogeneous vanishing ideal of the graphical model associated to $G$.

**Proposition 13.2.5.** The parametrized discrete undirected graphical model associated to $G$ consists of all probability distributions in $\Delta_{\mathcal{R}}$ given by the probability expression

$$p_{i_1i_2\cdots i_m} = \frac{1}{Z(\theta)} \prod_{C \in \mathcal{C}(G)} \theta_{i_C}^{(C)}$$

where $\theta = (\theta^{(C)})_{C \in \mathcal{C}(G)}$ is the vector of parameters. In particular, the positive part of the parametrized graphical model is the hierarchical log-linear model associated to the simplicial complex of cliques in the graph $G$.

Proposition 13.2.5 implies that the homogeneous vanishing ideal of a discrete undirected graphical model $I_G$ is a toric ideal.

**Example 13.2.6.** Consider the graph from Example 13.2.2, and let $r_j = 2$ for all $j$, so that all $X_i$ are binary random variables. The homogenized
version of the parametrization of the undirected graphical model has the form
\[ p_{i_1 i_2 i_3 i_4 i_5} = \theta^{(123)}_{i_1 i_2 i_3} \theta^{(25)}_{i_2 i_5} \theta^{(34)}_{i_3 i_4 i_5}. \]

The toric vanishing ideal of the graphical model can be computed using techniques described in Chapter [6]. In this case the vanishing ideal \( I_G \) is generated by homogeneous binomials of degrees 2 and 4. This can be computed directed in Macaulay 2, or using results from Section 9.3 on the toric ideal of hierarchical models for reducible complexes.

Turning now to Gaussian undirected graphical models, the structure is determined in a very simple way from the graph. The density of the multivariate normal distribution \( \mathcal{N}(\mu, \Sigma) \) can be written as
\[
f(x) = \frac{1}{Z} \prod_{i=1}^{m} \exp \left( -\frac{1}{2} (x_i - \mu_i)^2 k_{ii} \right) \prod_{1 \leq i < j \leq m} \exp \left( -(x_i - \mu_i)(x_j - \mu_j) k_{ij} \right)
\]
where \( K = (k_{ij}) = \Sigma^{-1} \) is the concentration matrix, and \( Z \) is the normalizing constant. In particular, we see that the density always factorizes into pairwise potential according to the graph \( G \) if and only if \( k_{ij} = 0 \) for all \( (i, j) \notin E \).

**Proposition 13.2.7.** The parametrized Gaussian undirected graphical model corresponds to the set of pairs \((\mu, \Sigma) \in \mathbb{R}^m \times PD_m \) with \((\Sigma^{-1})_{ij} = 0 \) for all \((i, j) \notin E \).

There are a number of approaches that can be used to compute the vanishing ideal of the Gaussian graphical model associated to \( G \). One strategy is to use the classical adjoint formula for the matrix inverse to get a parametrization for the ideal system. Alternately, we can perform an elimination on the system \( Id - \Sigma K = 0 \), where \( Id \) denotes an \( m \times m \) identity matrix. It is not clear which of these is best in general, but we illustrate the second method with an example. For a given graph \( G \), whether undirected or directed, we use \( J_G \) to denote the vanishing ideal of the associated Gaussian graphical model.

**Example 13.2.8.** Let \( G \) be the four cycle graph with edges set \( E = \{12, 23, 34, 14\} \). Since the Gaussian graphical model makes no restrictions on the mean vector of our Gaussian random variables, we can focus on the covariance matrix. We want to find the vanishing ideal of the set of covariance matrices \( \Sigma \) such that \((\Sigma^{-1})_{13} = (\Sigma^{-1})_{24} = 0 \). The following Singular code computes the vanishing ideal in this case.

```
ring R = 0, (s11,s12,s13,s14,s22,s23,s24,s33,s34,s44, k11,k12,k14,k22,k23,k33,k34,k44), dp;
matrix K[4][4] = k11,k12,0,k14,k12,k22,k23,0,
```
13.2. Parametrizations of Graphical Models

\[0,k23,k33,k34,k14,0,k34,k44;\]
matrix S[4][4] = s_{11},s_{12},s_{13},s_{14},s_{12},s_{22},s_{23},s_{24},
\quad s_{13},s_{23},s_{33},s_{34},s_{14},s_{24},s_{34},s_{44};
matrix eye[4][4] = 1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1;
ideal JG = K*S-eye;
LIB "elim.lib";
elim(I,11..18);

In this case, we see that the vanishing ideal of the parametrization is equal to the conditional independence ideal associated to the global Markov statements of this model. It is the ideal

\[J_G = J_{\text{global}(G)} = \langle |\Sigma_{124},234|, |\Sigma_{123},134| \rangle.\]

Now we consider the parametric description of graphical models for directed acyclic graphs. Let \(G = (V,E)\) be such a DAG. For each node \(j \in V\) we have a conditional distribution of variable \(X_j\) conditional on the parents of node \(j\) in the graph \(G\), \(f_j(x_j|x_{\text{pa}(j)})\) and consider probability densities of the form

\[(13.2.2) \quad f(x) = \prod_{j \in V} f_j(x_j|x_{\text{pa}(j)}).
\]

**Definition 13.2.9.** The *parametric directed graphical model* consists of all probability densities that factorize as the product of conditionals (13.2.2).

The recursive factorization structure that arises in graphical models associated to directed acyclic graphs can be quite useful for Bayesian data analysis. Indeed, some more ancestral vertices in the graph can represent prior distributions, which hierarchically determine the distributions of other variables given the values of those priors. For this reason, DAG models are often called Bayesian networks.

The situation in the directed case is much better than in the undirected case: factorizations are equivalent to satisfying the global Markov property.

**Theorem 13.2.10 (Recursive Factorization).** A probability density satisfies the recursive factorization property (13.2.2) if and only if it satisfies the local Markov property.

**Proof.** Since \(G\) is a directed acyclic graph, we can assume the vertex set is \(V = [m]\) and that after renaming vertices, we have that \(i \rightarrow j\) implies that \(i < j\). This is called a topological ordering of the vertices in the graphical models literature.

(\(\Rightarrow\)) We will show the stronger statement that a distribution that factorizes satisfies the global Markov property. Let \(A, B, C\) disjoint subsets of \(V\) such that \(C\) d-separates \(A\) and \(B\), and let \(f\) be a distribution with
factorization \(13.2.2\). We can assume that \(V = \text{an}(A \cup B \cup C)\), otherwise we marginalize over \(V \setminus \text{an}(A \cup B \cup C)\) which does not change the factorization structure. To say that \(C\) d-separates \(A\) and \(B\) we have that \(C\) separates \(A\) and \(B\) in the moral graph of \(G\). Moralization makes each set \(\{j\} \cup \text{pa}(j)\) a clique in the graph \(G^m\). Hence, the factorization \(13.2.2\) gives a parametrization by potential functions in the graph \(G^m\). Hence, by Corollary \(13.2.4\) the conditional independence statement \(X_A \perp \perp X_B | X_C\) is satisfied.

\((\Leftarrow)\) Any density \(f\) whatsoever can be factorized as

\[
f(x) = \prod_{j=1}^{m} f_j(x_j|x_{[j-1]}),
\]

where \(f_j(x_j|x_{[j-1]})\) is the conditional density of \(X_j\) given the variables \(X_1, \ldots, X_{j-1}\). Since the vertices of \(G\) are topologically ordered, we always have \(\text{pa}(j) \subseteq [j-1]\), and similarly, \([j-1] \subseteq \text{nd}(j)\). Let \(C = [j-1] \setminus \text{pa}(j) \subseteq \text{nd}(j) \setminus \text{pa}(j)\). Thus, we can split this representation as \(f_j(x_j|x_{\text{pa}(j)}, x_C)\). But by the local Markov property \(X_j \perp \perp X_{\text{nd}(j) \setminus \text{pa}(j)} | X_{\text{pa}(j)}\), and the decomposition axiom implies that \(X_j \perp \perp X_C | X_{\text{pa}(j)}\). Thus,

\[
f_j(x_j|x_{[j-1]}) = f_j(x_j|x_{\text{pa}(j)}, x_C) = f_j(x_j|x_{\text{pa}(j)}),
\]

so the density \(f\) factorizes according to \(G\).

Theorem \(13.2.10\) allows us to explicitly parametrize both discrete or Gaussian directed graphical models and use those parametrizations to compute the vanishing ideal of the model. As we have mentioned previously, knowing the vanishing ideal can be useful for other statistical applications (i.e. it can be easier to compute the ML-degree), and we can try to understand the discrepancy between the parametrized model and the implicit model.

The recursive factorization theorem also allows us to prove the that the local Markov property implies the global Markov property for DAGs.

**Proof of Theorem \(13.1.11\)** This is a consequence of the proof of Theorem \(13.2.10\) If \(f\) satisfies the local Markov property with respect to \(G\) then \(f\) has a factorization of the form

\[
f(x) = \prod_{j \in V} f_j(x_j|x_{\text{pa}(j)}).
\]

But if \(f\) has such a recursive factorization, then it automatically satisfies the global Markov property associated to the DAG \(G\).

In the discrete case, the parametric representation of the directed graphical model \(G\) takes the form
\( \phi : p_{i_1i_2\ldots i_m} = \prod_{j=1}^{m} \theta^{(j)}(i_j | i_{\text{pa}(j)}) \)

where the parameters \( \theta^{(j)}(i_j | i_{\text{pa}(j)}) \) represent the conditional probabilities. Although this looks like a monomial parametrization, and hence the model appears to be a log-linear model, the fact that these are conditional probabilities means that the parameters satisfy linear constraints:

\[
\sum_{k=1}^{r_j} \theta^{(j)}(k | i_{\text{pa}(j)}) = 1
\]

for all \( i_{\text{pa}(j)} \in R_{\text{pa}(j)} \).

**Example 13.2.11.** Let \( G \) be the graph with vertex set \( [3] \) and edges \( 1 \to 3 \) and \( 2 \to 3 \). The parametric description of this model will be:

\[
p_{i_1i_2i_3} = \theta^{(1)}(i_1) \theta^{(2)}(i_2) \theta^{(3)}(i_3 | i_1i_2).
\]

Letting \( r_1 = r_2 = r_3 = 2 \), we can compute the vanishing ideal of the model in Macaulay 2 using the following code:

```plaintext
S = QQ[t,a,b,c11,c12,c21,c22];
R = QQ[p111,p112,p121,p122,p211,p212,p221,p222];
f = map(S,R, { t*a*b*c11, t*a*b*(1-c11), t*a*(1-b)*c12,
               t*a*(1-b)*(1-c12), t*(1-a)*b*c21, t*(1-a)*b*(1-c21),
               t*(1-a)*(1-b)*c22, t*(1-a)*(1-b)*(1-c22)});
I = kernel f
```

Note that we use the following substitutions \( a = \theta^{(1)}(1) \) (so \( 1-a = \theta^{(1)}(2) \)), \( b = \theta^{(2)}(1) \), \( c_{i_1i_3} = \theta^{(3)}(1i_1i_2) \). The homogenization parameter \( t \) is introduced so that we eliminate the trivial equations \( p_{111} + \cdots + p_{222} - 1 \). The vanishing ideal in this case is equal to the conditional independence ideal of all global Markov statements of the graph.

We now turn attention to the case of Gaussian Bayesian networks. The recursive factorization of the joint density translates into a sequence of recursive regressions of random variables lower in the graph in terms of random variables further up the graph. Indeed, in the jointly normal case, the conditional density of \( X_j | X_{\text{pa}(j)} \) is also normal and is specified parametrically by a formula like

\[
(13.2.3) \quad X_j = \sum_{k \in \text{pa}(j)} \lambda_{kj} X_k + \epsilon_j,
\]

where \( \epsilon_j \sim N(\nu_j, \omega_j) \) is a univariate normal distribution, and \( \lambda_{jk} \) is a real parameter, sometimes called the regression normal coefficient.
Let \( \Lambda \) be the \( m \times m \) upper triangular matrix such that
\[
\Lambda_{kj} = \begin{cases} 
\lambda_{kj} & \text{if } k \to j \in E \\
0 & \text{otherwise}
\end{cases}
\]

We can write (13.2.3) in matrix format as
\[
X = \Lambda^T X + \epsilon
\]
where \( \epsilon = (\epsilon_1, \ldots, \epsilon_m) \) is the jointly normal random vector with mean \( \nu = (\nu_1, \ldots, \nu_m) \) and diagonal covariance matrix \( \Omega = \text{diag}(\omega_1, \ldots, \omega_m) \). Solving for \( X \) yields
\[
X = (\text{Id} - \Lambda)^{-T} \epsilon
\]
where \( \text{Id} \) is an \( m \times m \) identity matrix and \((\text{Id} - \Lambda)^{-T}\) denotes the transpose of the inverse of the matrix \( \text{Id} - \Lambda \). By Lemma 2.4.3, \( X \) is a multivariate normal with covariance matrix \( \Sigma = (\text{Id} - \Lambda)^{-T} \Omega (\text{Id} - \Lambda)^{-1} \).

**Proposition 13.2.12.** The parametrized Gaussian graphical model associated to the directed acyclic graph \( G \) consists of all pairs \((\mu, \Sigma) \in \mathbb{R}^m \times \text{PD}_m\) such that 
\[
\Sigma = (\text{Id} - \Lambda)^{-T} \Omega (\text{Id} - \Lambda)^{-1}
\]
for some \( \Omega \) diagonal with positive entries and upper triangular \( \Lambda \in \mathbb{R}^E \).

**Example 13.2.13.** Let \( G = ([4], \{1 \to 2, 1 \to 3, 2 \to 4, 3 \to 4\}) \). The matrices \( \Lambda \) and \((\text{Id} - \Lambda)^{-1}\) are
\[
\Lambda = \begin{pmatrix} 
0 & \lambda_{12} & \lambda_{13} & 0 \\
0 & 0 & 0 & \lambda_{24} \\
0 & 0 & 0 & \lambda_{34} \\
0 & 0 & 0 & 0
\end{pmatrix}
\]
\[
(\text{Id} - \Lambda)^{-1} = \begin{pmatrix} 
1 & \lambda_{12} & \lambda_{13} & \lambda_{12}\lambda_{24} + \lambda_{13}\lambda_{34} \\
0 & 1 & 0 & \lambda_{24} \\
0 & 0 & 1 & \lambda_{34} \\
0 & 0 & 0 & 1
\end{pmatrix}.
\]

From the formula \( \Sigma = (\text{Id} - \Lambda)^{-T} \Omega (\text{Id} - \Lambda)^{-1} \) we see for example that
\[
\sigma_{24} = \omega_1 \lambda_{12} \lambda_{13} \lambda_{34} + \omega_2 \lambda_{24}.
\]

We can compute the vanishing ideal of the parametrization in the ring \( \mathbb{R}[\Sigma] \) of polynomial functions of the covariance matrix. The ideal is
\[
J_G = \langle |\Sigma_{12,13}|, |\Sigma_{123,234}| \rangle,
\]
which equals the conditional independence ideal of the global Markov statements, \( J_{\text{global}(G)} \).

At the time of this writing there is no known general characterization of which graphs the vanishing ideal of the model equals the global Markov ideal for a Gaussian Bayesian network. It is known to hold for trees, and all graphs with \( \leq 4 \) vertices [Stu08]. Already on 5 vertices there are graphs for which the global Markov ideal does not equal the vanishing ideal of the model. Somewhat surprisingly, there are graphs where the vanishing ideal contains vanishing subdeterminants of \( \Sigma \) that do not belong to the global Markov ideal.
Example 13.2.14. Let $G = ([5], \{1 \to 4, 2 \to 4, 3 \to 4, 3 \to 5, 4 \to 5\})$, then the vanishing ideal $J_G$ contains the minor $|\Sigma_{12,45}|$ which is not contained in the global Markov ideal $J_{\text{global}}(G)$.

![Figure 13.2.2. The directed acyclic graph from Example 13.2.14](image)

The characterization of which subdeterminants of $\Sigma$ belong to the ideal $J_G$ is through a combinatorial conditional called t-separation.

Definition 13.2.15. Let $G = (V, D)$ be a directed acyclic graph. A trek between two vertices $a$ and $b$ is a pair $(P_a, P_b)$ of directed paths $P_a$ and $P_b$ that have the same starting vertex and such that $P_a$ ends at $a$ and $P_b$ ends at $b$.

Definition 13.2.16. Let $A, B, C_A$, and $C_B$ be four subsets of $V$, not necessarily disjoint. The pair of sets $(C_A, C_B)$ t-separates $A$ and $B$ if for all $a \in A$ and $b \in B$ and any trek $(P_a, P_b)$ from $a$ to $b$, either $P_a$ has a vertex in $C_A$, or $P_b$ has a vertex in $C_B$, or both.

Theorem 13.2.17. Let $G = (V, D)$ be a directed acyclic graph, and $A$ and $B$ two subsets of $V$ with $\#A = \#B = k$. Then the minors $|\Sigma_{A,B}| \in J_G$ the vanishing ideal of the Gaussian graphical model associated to $G$ if and only if there exist a pair of sets $(C_A, C_B)$ that t-separate $A$ and $B$ such that $\#C_A + \#C_B < k$.

Example 13.2.18. Considering the graph $G$ from Example 13.2.14, the pair of sets $(\emptyset, \{4\})$ t-separates $\{1, 2\}$ and $\{4, 5\}$. This is because any trek $(P_L, P_R)$ from $\{1, 2\}$ to $\{4, 5\}$ has $P_L = \emptyset$, and must contain 4 as a vertex in $P_R$. Thus, $|\Sigma_{12,45}|$ belongs to the vanishing ideal of the Gaussian graphical model $J_G$.

Although we have tended to build our conditional independence and graphical model examples from scratch in this book, there is a package in Macaulay 2 specifically for working with the ideals and parametrizations of graphical models and conditional independence ideals (see GPS13 for more details). For example, the following code verifies that the vanishing ideal of the graph in Example 13.2.14 does not equal the global Markov ideal.
loadPackage "GraphicalModels"
G = digraph{{1,{4}},{2,{4}},{3,{4,5}},{4,{5}}}
R = gaussianRing G
I = conditionalIndependenceIdeal(R,globalMarkov(G))
J = gaussianVanishingIdeal(R)
I == J

13.3. Failure of the Hammersley-Clifford Theorem

The comparison of the implicit description of a graphical model by conditional independence statements to the parametric description of the model by factorization is especially interesting in the case of undirected graphical model on discrete variables. Given our focus on discrete and gaussian graphical models, this is the only case where it can happen that not every distribution that satisfies the conditional independence constraints need factor according to the model. In this case, primary decomposition can be helpful to determine which extra probability distributions there are.

The main theorem in this area is the following:

Theorem 13.3.1 ([GMS06]). Let \( G \) be an undirected graph. Then the vanishing ideal of the discrete graphical model, \( I_G \), is equal to the ideal of global Markov statements, \( I_{\text{global}(G)} \), if and only if \( G \) is a chordal graph.

Recall that a graph is chordal if and only if there are no induced cycles of length \( \geq 4 \), or equivalently a graph is chordal if and only if its complex of cliques is a decomposable simplicial complex (Theorem 8.3.5). We provide a sketch of the proof, see [GMS06] for complete details.

**Proof Sketch.** If \( G \) is chordal, \( I_G \) is the toric ideal of a decomposable hierarchical model, hence has a Markov basis/ generating set consisting of quadratic binomials by Corollary 9.3.18. It can be shown that those quadrics can be chosen to come from conditional independence statements.

Conversely, if \( G \) is not chordal, then it has an induced subgraph that is a cycle of length \( \geq 4 \). The toric ideal \( I_H \) associated to an induced subgraph \( H \) naturally corresponds to a facial subset of the vector configuration associated to \( G \). Hence, the generators of \( I_H \) appear as generators of \( I_G \). But the toric ideal of a cycle contains generators of degree \( \geq 4 \), so it could not equal the conditional independence ideal, which is necessarily generated by quadrics.

Beyond chordal graphs, the set of distributions which satisfy the global Markov statements associated to the graph \( G \) will decompose into a number of irreducible components. Only in a small number of examples is the explicit
decomposition of the binomial ideal \( I_{\text{global}(G)} \) known. Here is one example explicitly computed in [KRS14].

**Theorem 13.3.2.** Let \( C_m \) be the \( m \)-cycle graph with edges \((i, i + 1)\) for \( i = 1, \ldots, m - 1 \) and edge \((1, m)\). Suppose that all random variables \( X_i \) are binary, i.e. \( d_i = 2 \) for all \( i \in [m] \). The global independence ideal \( I_{\text{global}(C_m)} \) is radical and has \( 1 + \binom{m}{3} \times 2^{m-3} \) minimal primes. The minimal primes of \( I_{\text{global}(C_m)} \) are of two forms:

- The toric vanishing ideal \( I_{C_m} \) of the graphical model.
- \( \binom{m}{3} \times 2^{m-3} \) monomial prime ideals, each of dimension 8.

To explicitly describe these minimal primes, we need some notation. If \( \vec{i} = (i_1, \ldots, i_m) \in [2]^m \) is an index string, the let \( \vec{i} \) denote the binary complements \( \vec{i} = (3 - i_1, \ldots, 3 - i_m) \). Now, let \( A|B|C \) be any cyclic partition of the numbers \([m]\), of the sets, \( A, B, C \) is an interval of integers, considered modulo \( m \). Let \((i_A, i_B, i_C)\) be any binary index string, with \( i_A \in R_A \), etc. Associate to this pair of information the monomial ideal

\[
P = \langle p_{j_A,j_B,j_C} | (j_A, j_B, j_C) \notin \{(i_A, i_B, i_C), (i_A, i_B, \overline{i_C}), \ldots, (\overline{i_A}, \overline{i_B}, \overline{i_C})\} \rangle.
\]

There are \( \binom{m}{3} \times 2^{m-3} \) such monomial ideals, and these are precisely the non-toric minimal prime ideals of the ideal \( I_{\text{global}(C_m)} \).

**Example 13.3.3** (4 cycle). Letting \( m = 4 \), the binomial ideal \( I_{\text{global}(C_4)} \) has nine minimal prime ideals. There is the toric vanishing ideal \( I_{C_4} \) and either other monomial ideals. Associated to the cyclic tripartition \( 1\{23\}4 \) we have two monomial ideals:

\[
\langle p_{1111}, p_{1112}, p_{1221}, p_{1222}, p_{2111}, p_{2112}, p_{2221}, p_{2222} \rangle
\]

\[
\langle p_{1112}, p_{1112}, p_{1221}, p_{1222}, p_{2111}, p_{2112}, p_{2221}, p_{2222} \rangle
\]

Note that in Theorem [13.3.2] the conditional independence ideal \( I_{\text{global}(G)} \) was a radical ideal. The global Markov ideal for the complete bipartite graph \( K_{2,m} \) with all binary random variables was also shown to be radical in [KRS14]. Global Markov ideals are not, however, radical in general: for the complete bipartite graph \( K_{3,3} \), \( I_{\text{global}(K_{3,3})} \) is not radical already for binary random variables [KRS14]. In general, it is an open problem to give a characterization of those graphs and dimension vectors \( d \) for which \( I_{\text{global}(G)} \) is a radical ideal. Here is a specific conjecture:

**Conjecture 13.3.4.** Let \( G \) be a graph with no \( K_4 \) minors, and suppose that all random variables are binary. Then \( I_{\text{global}(G)} \) is radical.

For each of the other combination of type of graph and discrete or Gaussian random variables, it is an open problem to determine for which family
of graphs $I_G = I_{\text{global}(G)}$ or $J_G = J_{\text{global}(G)}$. Further conjectures of characterizations for when the global Markov ideal are radical are also open at this point, and an interesting area for further study.

13.4. Examples of Graphical Models from Applications

Graphical models are widely used in the applied sciences. We will give some examples of particular situations where they are used. More examples will follow in subsequent chapters. One feature of the way they are used in applications is that various types of restrictions might be made on some of the parameters, for example, some parameter might be required to be equal to (functions of) other parameters in the model.

**Example 13.4.1 (Markov Chain).** Let $X_1, X_2, \ldots, X_m$ be a sequence of discrete random variables, each with state space $[r]$. Consider the directed path graph $P_m$, with edges $i \to i+1$ for $i \in [m-1]$. According to the recursive factorization theorem, the joint probability distribution for the Bayesian network associated to this DAG has the form:

$$P(X_1 = x_1, \ldots, X_m = x_m) = P_1(X_1 = x_1) \prod_{i=2}^m P_i(X_i = x_i | X_{i-1} = x_{i-1}).$$

Note that the conditional independence structure in this model will have the form $X_{i+1} \perp \perp X_{i-1} | X_i$ for $i = 2, \ldots, m-1$, so that the sequence of random variables forms a Markov chain, as discussed in Chapter 1.

If, in addition, we require that each of the conditional distributions $P_i$ are equal:

$$P_i(X_i = x | X_{i-1} = y) = P_2(X_2 = x | X_1 = y)$$

for all $i, x, y$, then we have a *homogeneous Markov chain*, which is the way that discrete Markov chains are often discussed, for example in [Nor98]. Letting $A = (a_{i_1i_2})_{i_1,i_2 \in [r]}$ denote the matrix representing the conditions distribution, that is $a_{i_1i_2} = P(X_{t+1} = i_2 | X_t = i_1)$, then $A$ is the transition matrix of the homogeneous Markov chain.

As we saw in Example 13.4.1, models that can be expressed by a sequence of simple Markov processes connecting random variables can usually be thought of as graphical models on a directed acyclic graph, with the underly DAG being a directed tree. Another important example is the hidden Markov model model.

**Example 13.4.2 (Hidden Markov Model).** Let $Y_1, \ldots, Y_m$ be a sequence of discrete random variables each with state space $[r]$, and $X_1, \ldots, X_m$ a sequence of discrete random variables, each with state space $[s]$. Consider the directed graph with edges $Y_i \to Y_{i+1}$ for $i \in [m-1]$ and $Y_i \to X_i$ for
This DAG is illustrated in Figure 13.4.1, a type of tree called a caterpillar.

The recursive factorization property for this graph yields the joint distribution

$$P(X_1 = x_1, \ldots, X_m = x_m, Y_1 = y_1, \ldots, Y_m = y_m) =$$

$$P_1(Y_1 = Y_1) \prod_{i=2}^{m} P_i(Y_i = y_i | Y_{i-1} = y_{i-1}) \prod_{i=1}^{m} Q_i(X_i = x_i | Y_i = y_i).$$

In this model, we typically require that each of the conditional distributions of $Y_i$ given $X_{i-1}$ are the same, and that each of the conditional distributions of $X_i$ given $Y_i$ are the same. Furthermore, we assume that the random variables $X_1, \ldots, X_m$ are all hidden random variables, that is, they are unobserved (we discuss this point in more detail in later chapters).

In applications, one should think of the hidden Markov model in the following way. The sequence of random variables $Y_1, \ldots, Y_m$ evolves according to a homogeneous Markov chain model. However, we are not able to observe $Y$, we only observe a corrupted or noisy version of it or some information $X$ computed from $Y$ in a possibly random way. Usually we want to recover $Y$ from $X$. The hidden Markov model is commonly used in computational biology where it is used to align DNA sequences and annotate DNA for genes (see e.g. [DEKM98]). We will discuss it in more detail in Chapter 18.

The Ising model is an important interpretation of undirected graphical models. Although we usually associate the Ising model with statistical physics, this model and variations on it are also used in spatial statistical and agriculture.

**Example 13.4.3** (Ising Model). Let $G = (V,E)$ be an undirected graph and let $X$ be a discrete random vector where all random variables are binary
with state space \{-1, 1\}. Introduce a probability distribution

\[
P(x_1, \ldots, x_n) = \frac{1}{Z} \exp \left( \sum_{(i,j) \in E} \alpha_{ij} x_i x_j + \sum_{i \in V} \beta_i x_i \right).
\]

The number $Z$ is the normalizing constant, in this context often called a partition function. Note that, as written, we have expressed this as an exponential family, and the resulting distribution gives a distribution in the hierarchical model associated whose underlying simplicial complex is the graph $G$. With appropriately chosen potential functions this can be realized by the graphical model associated to $G$. If the graph $G$ has no triangles, then the Ising model is equal to the positive part of the graphical model associated to $G$. The most commonly used graph for the Ising model is the grid graph.

In some applications, e.g. spatial statistics, we restrict to a submodel where all the $\alpha_{ij}$ parameters are equal and all the $\beta_i$ parameters are equal.

13.5. Exercises

Exercise 13.1. List all the pairwise, local, and global conditional independence statements associated to the $G$ with $V = \{1, 2, 3, 4, 5, 6\}$ and undirected edge set $E = \{12, 13, 15, 23, 26, 34, 46, 56\}$.

Exercise 13.2. Let $G$ be the undirected path graph on 5 vertices. Give an example of distribution $P$ that satisfies all the local Markov statements associated to $G$ but not all the global Markov statements associated to $G$.

Exercise 13.3. (1) Let $G$ be a decomposable graph. Show that there is a directed graph $H$ which realizes exactly the same global Markov statements as $G$.

(2) Conversely, if $G$ is an undirected four-cycle, show that there is no directed graph which yields exactly the same global Markov statements as $G$.

Exercise 13.4. Give a proof of Proposition [13.1.6] by giving an example of discrete random vector satisfying the local Markov statements of a graph but that does not satisfying the conditional independence statement $X_A \perp \perp X_B | X_C$ when $C$ does not separate $A$ and $B$.

Exercise 13.5. Prove Proposition [13.1.8]

Exercise 13.6. Give a direct proof of Corollary [13.2.4] analogous to the proof of the only if direction of the proof of the Hammersley-Clifford theorem.
Exercise 13.7. Among the undirected gaussian graphical models on 5 vertices, which one has the largest maximum likelihood degree?

Exercise 13.8. Complete one direction of the proof of Theorem 13.3.1 as follows: Let $G$ be an undirected graph, and $I_G$ the toric ideal vanishing on the parametrized graphical models. Show that the degree 2 part of the toric ideal is spanned by the quadratic binomials associated to the global Markov property associated to $G$.

Exercise 13.9. Show that the maximum likelihood degree of any Bayesian network is 1. In particular, explain how to determine rational formulas for the maximum likelihood estimates of parameters in graphical models with directed acyclic graphs.
A random variable in a model is hidden or latent if it is not measured. This chapter introduces the detailed study of hidden variable models, whose various aspects will occupy us for the remainder of the book. Hidden variables tend to make models more complicated to analyze and lead to interesting geometric challenges.

The presence of hidden random variables in a model might be for any number of reasons. Hidden variables might represent quantities that we would directly like to measure but cannot or for which it is too expensive to measure directly. For example, in a mixture model, observed variables might represent symptom status of a subject (which are measured) and the hidden mixture classes might correspond to whether or not a subject has a particular disease. The hidden variables might represent quantities that are theoretically hypothesized to exist but are not directly measurable (in particular, the observed variables might be proxies for the unmeasured hidden variables). For example, in a factor analysis model, the hidden factors typically represent unmeasurable quantities that are supposed to give a low-dimensional explanation for the correlation between a collection of observed random variables. Or, the hidden variables might simply be covariates that were not collected in a data analysis, for whatever reason, but that are still affecting the interactions between the observed random variables.

Hidden variables in a model mean that the probability densities on the observed random variables are obtained by computing marginals of the joint distribution of a fully observed model on both observed and hidden random variables. While the fully observed model might be a familiar statistical model with nice properties (e.g. exponential family, graphical model, etc.), the simple operation of computing marginals usually produces a model that
Hidden Variables

is significantly more complex than the fully observed model. For example, hidden variable models typically have singularities, have nontrivial algebraic boundaries inside the probability simplex or cone of positive definite matrices, can fail to be identifiable in non-obvious ways, and can have multiple local maxima in their likelihood functions. The richness of the expressive power of hidden variable models is balanced by the increased difficulty of using them in practical settings. We begin to address the study of such hidden variable models in this and subsequent chapters.

14.1. Mixture Models

Mixture models are among the simplest hidden variable statistical models to describe, though they already lead to a complex mathematical structure. Mixture models can be used in many different settings. We focus in this chapter on the setting of discrete random variables. Mixture models with discrete random variables are closely related to secant varieties in algebraic geometry. We already introduced mixture models in Example 3.2.10 in the case of binomial random variables, but here we study them in substantially more detail.

Consider an underlying statistical model $\mathcal{M} \subseteq \Delta_{r-1}$. Here we consider an $r$ element state space but in practice this might be naturally considered as a product space (if there are many random variables involved in the model). We let $X$ denote the random variable being modeled by $\mathcal{M}$. Let $H$ be a (hidden) random variable with state space $[k]$. In a mixture model, we suppose that for some $\pi = (\pi_1, \ldots, \pi_k) \in \Delta_{k-1}$, and $p^1, \ldots, p^k \in \mathcal{M}$ we have that $P(H = i) = \pi_i$ and $P(X = j | H = i) = p^j_i$, where $p^i = (p^i_1, \ldots, p^i_r)$. Then we have $P(X = j) = \sum_{i=1}^k \pi_i p^j_i$ so that the probability distribution vector of $X$ is the convex combination

$$\pi_1 p^1 + \cdots + \pi_k p^k$$

of the distributions $p^1, \ldots, p^k$.

Definition 14.1.1. The $k$-th mixture model of the model $\mathcal{M} \subseteq \Delta_{r-1}$ is the family of probability distributions

$$\text{Mixt}^k(\mathcal{M}) = \{ \pi_1 p^1 + \cdots + \pi_k p^k : \pi \in \Delta_{k-1}, p^1, \ldots, p^k \in \mathcal{M} \}.$$

The natural interpretation for this model is as follows: the population is divided into $k$ subpopulations. The $i$th subpopulation follows a distribution in the $p^i \in \mathcal{M}$. The weight $\pi_i$ is the relative proportion of the population of the total population that belongs to the $i$th subpopulation. Finally, it is assumed that we do not observe which subpopulation an individual belongs
to. Introducing a random variable $H$ with state space $[k]$, we have that $P(H = i) = \pi_i$ and the conditional distributions of $X$ given $H$ satisfy $P(X = j | H = i) = p^{ij}$. The distributions in the $k$th mixture model then consist of the resulting marginal distribution of the variable $X$ which is the convex combination of $k$ elements of $\mathcal{M}$.

A natural situation when a mixture model can be used is when $H$ represents the (binary) infection status of individuals with respect to a disease and the discrete states of $X$ records various symptoms (e.g. cough, fever, rash, etc.) that a patient might have.

**Example 14.1.2.** Let $\mathcal{M}_{X_1 \perp \perp X_2}$ be the independence model on two discrete random variables. The model consists of probability matrices $p \in \Delta_R$ that are rank one as matrices. The $k$-th mixture model $\text{Mixt}^k(\mathcal{M}_{X_1 \perp \perp X_2})$ consists of all convex combinations of $k$ elements of $\mathcal{M}_{X_1 \perp \perp X_2}$. Said another way, these are probability matrices that can be written as the sum of $k$ nonnegative matrices of rank 1.

Here is a “classic” example illustrating the mixture model of the independence model [MSvS03]. Let $X_1$ be a random variable describing how much a person watches soccer, and $X_2$ a random variable describing how much hair a person has. Suppose that $X_1$ has three states: Never, Sometimes, Frequently, and $X_2$ has 4 states: Bald, Short, Medium, and Long. Although soccer watching habits and hair length seem like they are unrelated, they are not independent from each other: people with short hair tend to watch soccer more frequently. However, it might be reasonable to assume that $X_1 \perp \perp X_2 | H$ where $H$ is a binary hidden variable, namely, the gender. Hence, if we only observe the joint distribution of $X_1$ and $X_2$, we would observe a distribution in $\text{Mixt}^2(\mathcal{M}_{X_1 \perp \perp X_2})$.

**Example 14.1.3.** Let $\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3}$ be the complete independence model of three discrete random variables. This complete independence model consists of probability tensors $p \in \Delta_R$ that are rank one tensors. Indeed, in the model of complete independence, we have

$$P(X_1 = i_1, X_2 = i_2, X_3 = i_3) = P(X_1 = i_1)P(X_2 = i_2)P(X_3 = i_3)$$

for all $i_1 \in [r_1], i_2 \in [r_2], i_3 \in [r_3]$. Replacing the marginal distributions of $X_1$, $X_2$, and $X_3$ with parameter vectors, we have

$$p_{i_1i_2i_3} = \alpha_{i_1}\beta_{i_2}\gamma_{i_3}$$

where $\alpha \in \Delta_{r_1-1}, \beta \in \Delta_{r_2-1}, \gamma \in \Delta_{r_3-1}$, which represents a nonnegative $r_1 \times r_2 \times r_3$ tensor of rank 1. The $k$-th mixture model $\text{Mixt}^k(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3})$ consists of convex combinations of $k$ of these probability distributions.
are $r_1 \times r_2 \times r_3$ probability tensors that have nonnegative rank $\leq k$. Parametrically we can represent this model as distributions of the form

$$p_{i_1i_2i_3} = \sum_{h=1}^{k} \pi_h \alpha_{hi_1} \beta_{hi_2} \gamma_{hi_3}.$$

It is also natural to consider more general mixture models, where we do not require that all the conditional distributions $p^i$ to belong to the same underlying statistical model.

**Definition 14.1.4.** Let $\mathcal{M}_1, \ldots, \mathcal{M}_k \subseteq \Delta_{r-1}$ be $k$ statistical models. The mixture model $\mathcal{M}_1 \ast \cdots \ast \mathcal{M}_k$ consists of all distributions

$$\mathcal{M}_1 \ast \cdots \ast \mathcal{M}_k = \left\{ \pi_1 p^1 + \cdots + \pi_k p^k : \pi \in \Delta_{k-1}, p^i \in \mathcal{M}_i, i = 1, \ldots, k \right\}.$$

Upon taking the Zariski closure, mixtures models in statistics correspond to join varieties and secant varieties in algebraic geometry.

**Definition 14.1.5.** Let $V_1, V_2, \ldots, V_k \subseteq \mathbb{K}^r$ be algebraic varieties. The join variety is the variety

$$V_1 \ast V_2 \ast \cdots \ast V_k = \overline{\left\{ \pi_1 p^1 + \cdots + \pi_k p^k : \sum_{i} \pi_i = 1 \text{ and } p^i \in V_i \text{ for all } i \right\}}$$

where the bar denotes the Zariski closure. The $k$-th secant variety of $V$ is the variety

$$\text{Sec}^k(V) = \overline{V \ast V \ast \cdots \ast V}.$$

It is easy to see that

$$\overline{\mathcal{M}_1 \ast \cdots \ast \mathcal{M}_k} = \overline{\mathcal{M}_1} \ast \cdots \ast \overline{\mathcal{M}_k}$$

simply taking Zariski closures before or after a polynomial map. Note, however, that the definition of the join variety explicitly includes a Zariski closure. This is because there can be points on the join variety that are the limits of points on secant planes but are not themselves on secant planes. For example, this is usually the case with points that lie on the tangent planes to a variety. Note that the secant variety $\text{Sec}^2(V)$ is often called the secant variety of the variety $V$.

**Example 14.1.6.** Consider the mixture model of the independence model of discrete random variables $X_1$ and $X_2$. As we discussed in Example 14.1.2, the mixture model $\text{Mixt}^k(\mathcal{M}_{X_1 \perp X_2})$ consists of all probability matrices that can be written as a sum of $k$ nonnegative matrices of rank 1. For a matrix $A \in \mathbb{R}_{\geq 0}^{r_1 \times r_2}$ the nonnegative rank of $A$, denoted $\text{rank}_+(A)$, is the small $k$
such that $A$ can be written as the sum of $k$ nonnegative matrices of rank 1. So

$$\text{Mixt}^k(\mathcal{M}_{X_1 \perp \perp X_2}) = \{ P \in \Delta_R : \text{rank}_+(P) \leq k \}.$$ 

On the other hand,

$$\text{Sec}^k(\mathcal{M}_{X_1 \perp \perp X_2}) \cap \Delta_R = \{ P \in \Delta_R : \text{rank}(P) \leq k \}.$$ 

In general $\text{rank}(A) \leq \text{rank}_+(A)$, and there are abundant examples of probability matrices where $\text{rank}(A) < \text{rank}_+(A)$. For example, for the probability distribution:

$$P = \frac{1}{8} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

it is easy to see that $\text{rank}(P) = 3$ but $\text{rank}_+(P) = 4$. In particular, while we always have for any model

$$\text{Mixt}^k(\mathcal{M}) \subseteq \left( \text{Sec}^k(\mathcal{M}) \cap \Delta_R \right)$$

these two sets need not be equal, in general. In particular, the probability distribution $P$ above shows that $\text{Mixt}^3(\mathcal{M}_{X_1 \perp \perp X_2}) \neq \text{Sec}^3(\mathcal{M}_{X_1 \perp \perp X_2}) \cap \Delta_R$

where $X_1$ and $X_2$ both have at least 4 states.

**Example 14.1.7.** Let $\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3}$ be the complete independence model for binary random variables $X_1, X_2, X_3$ and consider its mixture model $\text{Mixt}^2(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3}) \subseteq \Delta_7$. Note that the on the algebraic geometric side, the complete independence model corresponds to the Segre variety $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \subseteq \mathbb{P}^7$. The secant variety $\text{Sec}^2(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1)$ has dimension seven (this can be proven using Kruskal’s Theorem (Theorem 16.3.2)) and so fills all of $\mathbb{P}^7$. The mixture model, however, $\text{Mixt}^2(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3})$ is very far from filling all of $\Delta_7$. As shown in [ARSZ15], a probability distribution lies in $\text{Mixt}^2(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3})$ if and only if it is $\pi$-supermodular for some $\pi \in S_2 \times S_2 \times S_2$. As a semialgebraic set, the mixture model decomposes into 4 components, one of which is the set of distributions satisfying the following system of inequalites:

$$p_{111} p_{222} \geq p_{112} p_{221}, \quad p_{111} p_{222} \geq p_{121} p_{212}, \quad p_{111} p_{222} \geq p_{211} p_{122},$$

$$p_{112} p_{222} \geq p_{122} p_{212}, \quad p_{121} p_{222} \geq p_{122} p_{211}, \quad p_{211} p_{222} \geq p_{212} p_{221},$$

$$p_{111} p_{122} \geq p_{112} p_{121}, \quad p_{111} p_{122} \geq p_{121} p_{121}, \quad p_{111} p_{122} \geq p_{121} p_{121}. $$

The other 3-components are obtained from this one by applying the symmetries in $S_2 \times S_2 \times S_2$. Simulations suggest that only about 8% of the probability simplex $\Delta_7$ lies in $\text{Mixt}^2(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3})$. 


Even the mixture model Mixt^3(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3}) does not fill the probability simplex. As shown in [MM15], a distribution in Mixt^k(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp \cdots \perp X_m}) can have at most k strong maxima. A strong maxima is an index string (i_1, \ldots, i_m) \in [r_1] \times \cdots \times [r_m] such that
\[ p_{i_1 \cdots i_m} > \sum_{(j_1 \cdots j_m) : d_H((i_1 \cdots i_m), (j_1 \cdots j_m)) = 1} p_{j_1 \cdots j_m} \]
where \(d(i, j)\) denotes the Hamming distance between strings \(i\) and \(j\). On the other hand, the distribution, \(p_{111} = p_{122} = p_{212} = p_{221} = \frac{1}{4},\ p_{112} = p_{121} = p_{211} = p_{222} = 0\) and all distributions near to it, clearly have four strong maxima. It is not difficult to see that Mixt^4(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3}) = \Delta_7, however. As this example shows, there can be significant discrepancy between the mixture model and its Zariski closure.

A common feature of hidden variable models is that they have singularities. This makes traditional asymptotic results about statistical inference procedures based on hidden variable models more complicated. For example, the asymptotics of the likelihood ratio test statistic will depend on the structure of the tangent cone as singular points, as studied in Section 7.4. Singularities will also play an important role in the study of marginal likelihood integrals in Chapter 17. Here is the most basic result on singularities of secant varieties.

**Proposition 14.1.8.** Let \(V \subseteq \mathbb{P}^{r_1-1}\) and suppose that Sec^k(V) is not a linear space. Then Sec^{k-1}(V) is in the singular locus of Sec^k(V).

**Proof.** The singular locus of Sec^k(V) is determined by the drop in rank of the Jacobian evaluated at a point. However, if Sec^k(V) is not a linear space, the main result of [SS09] shows that the Jacobian matrix of the equations of Sec^k(V) evaluated at a point of Sec^{k-1}(V) is the zero matrix. Hence all such points are singular. □

**Example 14.1.9.** Consider the Segre variety \(V = \mathbb{P}^{r_1-1} \times \mathbb{P}^{r_2-1} \subseteq \mathbb{P}^{r_1 r_2-1}\), the projectivization of the set of rank one matrices. The secant variety Sec^k(V) is the projectivization of the set of matrices of rank \(\leq k\), and its vanishing ideal \(\mathcal{I}(\text{Sec}^k(V))\) is generated by the \(k+1\) minors of a generic \(r_1 \times r_2\) matrix, provided \(k < \min(r_1, r_2)\). The partial derivative of a generic \(k+1\) minor with respect to one of its variables is a generic \(k\)-minor. Hence we see that the Jacobian matrix of the ideal \(\mathcal{I}(\text{Sec}^k(V))\) vanishes at all points on Sec^{k-1}(V)). For statistical models, this example implies that the mixture model Mixt^k(\mathcal{M}_{X_1 \perp X_2}) is singular along the submodule Mixt^{k-1}(\mathcal{M}_{X_1 \perp X_2}), provided that \(k < \min(r_1, r_2)\).
14.2. Hidden Variable Graphical Models

One of the simplest ways to construct hidden variable statistical models is using a graphical model where some variables are not observed. Graphical models where all variables are observed are simple models in numerous respects: They are exponential families (in the undirected case), they have closed form expressions for their maximum likelihood estimates (in the directed acyclic case), they have distributions largely characterized by conditional independence constraints, and the underlying models are smooth. Graphical models with hidden variables tend to lack all of these nice features. As such, these models present new challenges for their mathematical study.

Example 14.2.1. As a simple example in the discrete case, consider the claw tree $G$ with four vertices and with edges $1 \rightarrow 2$, $1 \rightarrow 3$, $1 \rightarrow 4$, and let vertex 1 be the hidden variable, illustrated in Figure 14.2.1.

![Figure 14.2.1. A claw tree](image)

This graphical model is parametrized given by the recursive factorization theorem:

$$p_{i_2i_3i_4} = \phi(\pi, \alpha, \beta, \gamma) = \sum_{i_1=1}^{r_1} \pi_{i_1} \alpha_{i_1i_2} \beta_{i_1i_3} \gamma_{i_1i_4}.$$  

where

$$\pi_{i_1} = P(X_1 = i_1), \quad \alpha_{i_1i_2} = P(X_2 = i_2|X_1 = i_1),$$

$$\beta_{i_1i_3} = P(X_3 = i_3|X_1 = i_1), \text{ and } \gamma_{i_1i_4} = P(X_4 = i_4|X_1 = i_1).$$

This parametrization is the same as the one we saw for the mixture model $\text{Mixt}^{r_1}(\mathcal{M}_{X_2 \perp \perp X_3 \perp \perp X_4})$ in the previous section. Since the complete independence model $\mathcal{M}_{X_2 \perp \perp X_3 \perp \perp X_4}$ is just the graphical model associated to the graph with 3 vertices and no edges, the hidden variable graphical model associated to $G$ corresponds to a mixture model of a graphical model.

Note that the fully observed model, as a graphical model with a directed acyclic graph, has its probability distributions completely characterized by conditional independence constraints. The conditional independence constraints for the fully observed model are $X_2 \perp \perp (X_3, X_4)|X_1$, $X_3 \perp \perp (X_2, X_4)|X_1$, and so on.
and $X_4 \perp (X_2, X_3)|X_1$. Since there are no conditional independence statements in this list, or implied using the CI axioms, that do not involve variable $X_1$, we see that we cannot characterize the distributions of a hidden variable graphical model by CI constraints alone among the observed variables.

Graphical models with hidden variables where the underlying graph is a tree play an important role in phylogenetics. These models will be studied in detail in Chapter 15. The model associated to the claw tree is an important building block for the study.

Now we move to the study of hidden variable models under a multivariate normal distribution. Let $X \sim \mathcal{N}(\mu, \Sigma)$ be a normal random vector, and $A \subseteq [m]$. Recall from Theorem 2.4.2 that $X_A \sim \mathcal{N}(\mu_A, \Sigma_{A,A})$. This means that when we pass to the vanishing ideal of a hidden variable model we can compute it by computing an elimination ideal.

**Proposition 14.2.2.** Let $\mathcal{M} \subseteq \mathbb{R}^m \times \text{PD}_m$ be an algebraic exponential family with vanishing ideal $I = I(\mathcal{M}) \subseteq \mathbb{R}[\mu, \Sigma]$. Let $H \sqcup O = [m]$ be a partition of the index labeling into hidden variables $H$ and observed variables $O$. The hidden variable model consists of all marginal distributions on the variables $X_O$ for a distribution with parameters in $\mathcal{M}$. The vanishing ideal of the hidden variable model is the elimination ideal

$$I \cap \mathbb{R}[\mu_O, \Sigma_{O,O}].$$

**Example 14.2.3.** Consider the graphical model associated to the directed claw graph from Example 14.2.1 but now under a multivariate normal distribution. The vanishing ideal of the fully observed model is generated by the degree 2 determinantal constraints:

$$I(\mathcal{M}_G) = \langle \sigma_{11}\sigma_{23} - \sigma_{12}\sigma_{13}, \sigma_{11}\sigma_{24} - \sigma_{12}\sigma_{14}, \sigma_{13}\sigma_{24} - \sigma_{14}\sigma_{23},$$

$$\sigma_{11}\sigma_{34} - \sigma_{13}\sigma_{14}, \sigma_{12}\sigma_{34} - \sigma_{14}\sigma_{23} \rangle.$$

The hidden variable graphical model where $X_1$ is hidden is obtained by computing the elimination ideal

$$I(\mathcal{M}_G) \cap \mathbb{R}[\sigma_{22}, \sigma_{23}, \sigma_{24}, \sigma_{33}, \sigma_{34}, \sigma_{44}].$$

In this case we get the zero ideal. Note that the resulting model is the same as the 1-factor model $F_{3,1}$ which was studied in Example 6.5.4. In particular, the resulting hidden variable model, in spite of having no non-trivial constraints vanishing on it, is subject to complicated semialgebraic constraints.

Our usual intuition about hidden variable models is that they are much more difficult to describe than the analogous fully observed models, and that these difficulties should appear in all contexts (e.g. computing vanishing ideals, describing the semialgebraic structure, solving the likelihood
14.2. Hidden Variable Graphical Models

Surprisingly, for Gaussian graphical models, computing the vanishing ideal is just as hard for hidden variable models as for the fully observed models, at least in one important case.

Definition 14.2.4. Let $G = (V, D)$ be a directed acyclic graph, and let $H \uplus O = [m]$ be a partition of the index labeling into hidden variables $H$ and observed variables $O$. The hidden variables are said to be upstream of the observed variables if there is no edge $o \to h$, where $o \in O$ and $h \in H$.

Suppose that $H \uplus O$ is a partition of the variables in a DAG, where the hidden variables are upstream. We introduce the following two dimensional grading on $R[\Sigma]$, associated to this partition of the variables:

\[
\deg \sigma_{ij} = \left( \begin{array}{c} 1 \\
\#( \{i\} \cap O ) + \#( \{j\} \cap O ) \end{array} \right).
\]

Proposition 14.2.5. Let $G = (V, D)$ be a directed acyclic graph and let $H \uplus O = [m]$ be a partition of the index labeling into hidden variables $H$ and observed variables $O$, where the $H$ variables are upstream. Then the ideal $I_G \subseteq R[\Sigma]$ is homogeneous with respect to the upstream grading in Equation 14.2.1. In particular, any homogeneous generating set of $I_G$ in this grading contains as a subset a generating set of the vanishing ideal of the hidden variable model $I_G \cap R[\Sigma_{O,O}]$.

Proof. The fact that the ideal $I_G$ is homogeneous in this case is proven in [Sul08]. The second statement follows by noting that the subring $R[\Sigma_{O,O}]$ consists of all elements of $R[\Sigma_{O,O}]$ whose degree lies on the face of the grading semigroup generated by the ray $\left( \begin{array}{c} 1 \\ 2 \end{array} \right)$.

For instance, in the case of the factor analysis model from Example 14.2.3 all the generators of the ideal $I_G$ that are listed are homogeneous with respect to the upstream grading. Since none of these generating polynomials involve only the indices $\{2, 3, 4\}$, we can see that the vanishing ideal of the hidden variable model must be the zero ideal. We can also look at this the other way around.

Example 14.2.6. The factor analysis model $F_{m,s}$ is the hidden variable model associated to the graph $K_{s,m}$ the directed complete bipartite graph with vertex set $H$ and $O$ of sizes $s$ and $m$ respectively with every edge $h \to o$ for $h \in H$ and $o \in O$. It is well known that the vanishing ideal of the factor analysis model $F_{5,2}$ consists of a single polynomial of degree 5, the pentad (see e.g. [DSS07]), which is the polynomial

\[
f = \sigma_{12}\sigma_{13}\sigma_{24}\sigma_{35}\sigma_{45} - \sigma_{12}\sigma_{13}\sigma_{25}\sigma_{34}\sigma_{45} - \sigma_{12}\sigma_{14}\sigma_{23}\sigma_{35}\sigma_{45} + \sigma_{12}\sigma_{14}\sigma_{25}\sigma_{34}\sigma_{35} + \sigma_{12}\sigma_{15}\sigma_{23}\sigma_{34}\sigma_{45} - \sigma_{12}\sigma_{15}\sigma_{24}\sigma_{34}\sigma_{35} + \sigma_{13}\sigma_{14}\sigma_{23}\sigma_{25}\sigma_{45} - \sigma_{13}\sigma_{14}\sigma_{24}\sigma_{25}\sigma_{35} - \sigma_{13}\sigma_{15}\sigma_{23}\sigma_{24}\sigma_{45}
\]
\[ +\sigma_{13}\sigma_{15}\sigma_{24}\sigma_{25}\sigma_{34} - \sigma_{14}\sigma_{15}\sigma_{23}\sigma_{25}\sigma_{34} + \sigma_{14}\sigma_{15}\sigma_{23}\sigma_{24}\sigma_{35}. \]

Proposition \[14.2.5\] implies that any minimal generating set of the fully observed model associated to the graph \( K_{2,5} \) must contain a polynomial of degree 5.

Graphical models with hidden variables are most useful in practice if we know explicitly all the hidden structures that we want to model. For example, in the phylogenetics models studied in Chapter 15, the hidden variables correspond to ancestral species, which, even if we do not know exactly what these species are, we know they must exist by evolutionary theory. On the other hand, in some situations it is not clear what the hidden variables are, nor how many hidden variables should be included. In some instances with Gaussian graphical models, there are ways around this difficulty.

**Figure 14.2.2.** Graph for an instrumental variables model with a hidden variable

**Example 14.2.7.** Consider the graph on four nodes in Figure \[14.2.2\]. Here \( X_1, X_2, X_3 \) are the observed variables and \( H \) is a hidden variable. Such a model is often called an *instrumental variable model*. Here is the way that it is used. The goal of an investigator is to measure the direct effect of variable \( X_2 \) on \( X_3 \). However, there is an unobserved hidden variable \( H \) which affects both \( X_2 \) and \( X_3 \), confounding our attempts to understand the effect of \( X_2 \) on \( X_3 \). To defeat this confounding we measure a new variable \( X_1 \) which we know has a direct effect on \( X_2 \) but is otherwise independent of \( X_3 \). The variable \( X_1 \) is called the instrumental variable. (We will discuss issue of whether or not it is possible to recover the direct effect of \( X_2 \) on \( X_3 \) in such a model in Chapter 16 on identifiability.)

To make this example concrete, suppose that \( X_2 \) represents how much a mother smokes and \( X_3 \) represents the birth weight of that mother’s child. One wants to test the magnitude of the causal effect of smoking on the birth weight of the child. Preventing us from making this measurement directly is the variable \( H \). The instrumental variable \( X_1 \) would be some variable that direct affects how much a person smokes, but not the child development,
14.2. Hidden Variable Graphical Models

e.g. the size of taxes on cigarette purchases. A natural choice to imagine for
the hidden variable $H$ is some socio-economic indicator (e.g. how rich/poor
the mother is). However other variables might be proposed, for instance,
perhaps there is a genetic factor that makes women more likely to smoke
and their children to have a lower birth weight (R.A. Fisher famously hy-
pothesized there might be a genetic factor that makes both a person want to
smoke more and be more likely to have lung cancer \cite{Sto91}). There might
be many other variables that play a direct role on $X_2$ and $X_3$. Despite the
simple setting of this example, one might like to add any number of hidden
variables for each of these possible different effects (socio-economic, genetic,
etc.). Situations like this can present a problem for hidden variable modeling
in some situations.

To get around the problem of not knowing which hidden variables to
include in the model, in the case of gaussian graphical models there is a
certain work-around that is used. The resulting models are called linear
structural equation models. Let $G = (V, B, D)$ be a mixed graph with vertex
set $V$ and two types of edges: bidirected edges $i \leftrightarrow j \in B$ and directed edges
$i \rightarrow j \in D$. (Technically, the bidirected edges are really no different from
undirected edges, but the double arrowheads are useful for a number of a
reasons.) Let

$$PD(B) = \{ \Omega \in PD_m : \omega_{ij} = 0 \text{ if } i \neq j \text{ and } i \leftrightarrow j \notin B \}$$

be the set of positive definite matrices with zeroes in off-diagonal positions
corresponding to $ij$ pairs where $i \leftrightarrow j$ is not a bidirected edge. To each
directed edge $i \rightarrow j$ we have a real parameter $\lambda_{ij} \in \mathbb{R}$. Let

$$\mathbb{R}^D = \{ \Lambda \in \mathbb{R}^{m \times m} : \Lambda_{ij} = \lambda_{ij} \text{ if } i \rightarrow j \in D, \text{ and } \Lambda_{ij} = 0 \text{ otherwise} \}.$$  

Let $\epsilon \sim N(0, \Omega)$ where $\Omega \in PD(B)$. Define the random variables $X_j$ for
$k \in V$ by

$$X_j = \sum_{k \in \text{pa}(j)} \lambda_{kj} X_k + \epsilon_j.$$  

Note that this is the same linear relations we saw for directed Gaussian
graphical models (Equation 13.2.3) except that now we allow correlated
error terms. From this it is easy to see that:

**Proposition 14.2.8.** Let $G = (V, B, D)$ be a mixed graph. Let $\Omega \in PD(B)$,
and $\epsilon \sim N(0, \Omega)$ and $\Lambda \in \mathbb{R}^D$. Then the random vector $X$ is a multivariate
normal random variable with covariance matrix

$$\Sigma = (Id - \Lambda)^{-T} \Omega (Id - \Lambda)^{-1}.$$  

**Definition 14.2.9.** Let $G = (V, B)$ be a mixed graph. The linear struc-
tural equation model $M_G \subseteq PD_m$ consists of all covariance matrices

$$M_G = \{ (Id - \Lambda)^{-T} \Omega (Id - \Lambda)^{-1} : \Omega \in PD(B), \Lambda \in \mathbb{R}^D \}.$$
In the linear structural equation model, instead of having hidden variables we have bidirected edges that represent correlations between the error terms. This allows us to avoid specifically modeling what types of hidden variables might be causing interactions between the variables. The bidirected edges in these models allow us to explicitly relate error terms that we think should be correlated because of unknown confounding variables.

The connection between graphical models with hidden variables and the linear structural equation models is obtained by imagining the bidirected edge $i \leftrightarrow j$ as a subdivided pair of edges $i \leftarrow k \rightarrow j$.

**Definition 14.2.10.** Let $G = (V, B, D)$ be a mixed graph. Let $G^{\text{sub}}$ be the graph obtained from $G$ whose vertex set is $V \cup B$, and with edge set

$$D \cup \{b \rightarrow i : i \leftrightarrow j \in B\}.$$  

The resulting graph $G^{\text{sub}}$ is the bidirected subdivision of $G$.

For example, the graph in Figure 14.2.2 is the bidirected subdivision of the graph in Figure 14.2.3

**Proposition 14.2.11.** Let $G = (V, B, D)$ be a mixed graph with $m$ vertices and $G^{\text{sub}}$ the bidirected subdivision. Let $\mathcal{M}_G \subseteq PD_m$ be the linear structural equation model associated to $G$ and $\mathcal{M}'_{G^{\text{sub}}}$ the gaussian graphical model associated to the directed graph $G^{\text{sub}}$ where all variables $B$ are hidden variables. Then $\mathcal{M}'_{G^{\text{sub}}} \subseteq \mathcal{M}_G$.

One point of Proposition 14.2.11 is to apply it in reverse: take a model with hidden variables and replace the hidden variables and outgoing edges with bidirected edges instead, which should, in principle, be easier to work with. To prove Proposition 14.2.11 we will need to pay attention to a comparison between the parametrization of the model $\mathcal{M}_G$ and the model $\mathcal{M}'_{G^{\text{sub}}}$. The form of the parametrization of a linear structural equation model is described by the *trek rule*.

**Definition 14.2.12.** Let $G = (V, B, D)$ be a mixed graph. A *trek* from $i$ to $j$ in $G$ consists of either

1. a directed path $P_L$ ending in $i$, and a directed path $P_R$ ending in $j$ which have the same source, or
2. a directed path $P_L$ ending in $i$, and a directed path $P_R$ ending in $j$ such that the source of $P_L$ and $P_R$ are connected by a bidirected edge.

Let $\mathcal{T}(i, j)$ denote the set of treks in $G$ connecting $i$ and $j$.

To each trek $T = (P_L, P_R)$ we associated the trek monomial $m_T$ which is the product with multiplicities of all $\lambda_{st}$ over all edges appearing in $T$ times
where $s$ and $t$ are the sources of $P_L$ and $P_R$. Note that this generalizes the definition of trek that we saw in Definition 13.2.15 to include bidirected edges. The proof of Proposition 14.2.11 will be based on the fact that the bidirected edges in a trek act exactly like the corresponding pair of edges in a bidirected subdivision.

**Proposition 14.2.13** (Trek Rule). Let $G = (V, B, D)$ be a mixed graph. Let $\Omega \in PD(B)$, $\Lambda \in \mathbb{R}^D$, and $\Sigma = (I - \Lambda)^{-T} \Omega (I - \Lambda)^{-1}$. Then

$$\sigma_{ij} = \sum_{T \in T(i,j)} m_T.$$

**Proof.** Note that in the matrix

$$(Id - \Lambda)^{-1} = Id + \Lambda + \Lambda^2 + \cdots$$

The $(i,j)$ entries is the sum over all directed paths from $i$ to $j$ in the graph $G$ of a monomial which consists of the product of all edges appearing on that path. The transpose yields paths going in the reverse direction. Hence the proposition follows from multiplying the three matrices together. \(\blacksquare\)

**Example 14.2.14.** Consider the mixed graph in Figure 14.2.3. We have

$$\Omega = \begin{pmatrix} \omega_{11} & 0 & 0 \\ 0 & \omega_{22} & \omega_{23} \\ 0 & \omega_{23} & \omega_{33} \end{pmatrix}, \quad \Lambda = \begin{pmatrix} 0 & \lambda_{12} & 0 \\ 0 & 0 & \lambda_{23} \\ 0 & 0 & 0 \end{pmatrix}.$$

So in $\Sigma = (Id - \Lambda)^{-T} \Omega (Id - \Lambda)^{-1}$ we have

$$\sigma_{23} = \omega_{11} \lambda_{12}^2 \lambda_{23} + \omega_{22} \lambda_{23} + \omega_{23}$$

which is realized as the summer over the three distinct treks from 2 to 3 in the graph.

**Proof of Proposition 14.2.11.** We need to show how we can choose parameters for the graph $G$ to get any covariance matrix associated to the hidden variable model associated to the graph $G_{sub}$. Use the same $\lambda_{ij}$ parameters for each $i \rightarrow j$ edge in $D$. Let $\Omega'$ be the diagonal matrix of parameters associated to the bidirected subdivision $G_{sub}$. For each bidirected edge $b = i \leftrightarrow j$ let $\omega_{ij} = \omega_{ib}^b \lambda_{bi} \lambda_{bj}$. Set

$$\omega_{ii} = \omega_{ii}^j + \sum_{b=i \rightarrow j \in B} \omega_{ib}^b \lambda_{bi}^2.$$

Note that the resulting matrix $\Omega$ is a positive definite matrix in $PD(B)$ since it can be expressed as a sum of a set of PSD rank one matrices (one for each edge in $B$) plus a positive diagonal matrix. Furthermore, the trek rule implies that this choice of $\Omega$ gives the same matrix as from the hidden variable graphical model associated to the graph $G_{sub}$. \(\blacksquare\)
Example 14.2.15. For the instrumental variable model from Example 14.2.7, the associated graph with bidirected edges is illustrated in Figure 14.2.3. Note that now we do not need to make any particular assumptions about what might be the common cause for correlations between smoking and babies birth weight. These are all subsumed in the condition that there is nontrivial covariance between $\epsilon_2$ and $\epsilon_3$.

While Proposition 14.2.11 shows that the models $M_G$ and $M_{G_{\text{sub}}}'$ are related by containment, they need not be equal for general graphs $G$. The argument in the proof of Proposition 14.2.11 implies that they have the same vanishing ideal, but the semialgebraic structure might be different. The paper [DY10] has a detailed analysis in the case of graphs with only bidirected edges. See also Exercise 14.5.

14.3. The EM Algorithm

Even if one begins with a statistical model with concave likelihood function, or with a model with closed form expressions for maximum likelihood estimates, in associated hidden variable models the likelihood function might have multiple local maxima and large maximum likelihood degree. This presents a challenge when we want to perform data analysis with hidden variable models because they can be challenging to work with, even if the corresponding fully observed model is well-behaved. When the underlying fully observed model is an exponential family, the EM algorithm [DLR77] is a general purpose algorithm that is guaranteed to improve the likelihood function at each step, though it might not converge to the global maximum of the likelihood function. The EM algorithm is a widely used algorithm for calculating maximum likelihood estimates that deserves further mathematical study.

The EM algorithm consists of two steps, the Expectation Step and the Maximization Step, which are iterated until some termination criterion is reached. In the Expectation Step we compute the expected values of the sufficient statistics in the fully observed model given the current parameter...
estimates. In the Maximization Step these estimated sufficient statistics are used to compute the maximum likelihood estimates in the fully observed model to get new estimates of the parameters. The fact that this procedure leads sequence of estimates with increasing likelihood function values appears in [DLR77], but we will give a simplified argument shortly in the case of discrete random variables.

Here is the structure of the algorithm with discrete random variables in a hidden variable model. Assume for simplicity that we work with only two random variables and observed random variable $X$ with state space $[r_1]$ and a hidden random variable $Y$ with state space $[r_2]$. Let $p_{ij} = P(X = i, Y = j)$ denote a coordinate of the joint distribution, and let $p_i = \sum_{j=1}^{r_2} p_{ij}$ a coordinate of the marginal distribution of $X$. Let $\mathcal{M} \subseteq \Delta_{r_1r_2-1}$ be a fully observed statistical model and $\mathcal{M}' \subseteq \Delta_{r_1-1}$ be the hidden variable model obtained by computing marginal distributions.

Let $p^{(t)} \in \mathcal{M} \subseteq \Delta_{r_1r_2-1}$ denote the $t$-th estimate for the maximum likelihood estimate of the fully observed model.

**Algorithm 14.3.1. (Discrete EM algorithm)**

**Input:** Data $u \in \mathbb{N}^{r_1}$, an initial estimate $p^{(0)} \in \mathcal{M}$.

**Output:** A distribution $p \in \mathcal{M}'$ (candidate for the MLE)

**While:** Some termination condition is not yet satisfied do

- **(E-Step)** Compute estimates for fully observed data

  $$v_{ij} = u_i \cdot \frac{p_{ij}^{(t)}}{p_i^{(t)}}$$

- **(M-Step)** Compute $p^{(t+1)}$ the maximum likelihood estimate in $\mathcal{M}$ given the “data” $v \in \mathbb{R}^{r_1 \times r_2}$.

**Return:** The marginal distribution of the final $p^{(t)}$.

We wish to show that the likelihood function of the hidden variable model does not decrease under application of a step of the EM-algorithm, and that a fixed point of the EM algorithm must be a critical point of the likelihood function. To do this let

$$\ell'(p) = \sum_{i=1}^{r_1} u_i \log p_i$$

be the log-likelihood function of the hidden variable model $\mathcal{M}'$, and let

$$\ell(p) = \sum_{i=1}^{r_1} \sum_{j=1}^{r_2} v_{ij} \log p_{ij}$$

be the log-likelihood of the fully observed model $\mathcal{M}$. 
Theorem 14.3.2. For each step of the EM algorithm $\ell'(p^{(t+1)}) \geq \ell'(p^{(t)})$.

Proof. Let $p = p^{(t)}$ and $q = p^{(t+1)}$. Consider the difference $\ell'(q) - \ell'(p)$ which we want to show is nonnegative. We compute:

$$\ell'(q) - \ell'(p) = \sum_{i=1}^{r_1} u_i \left( \log p_i - \log q_i \right)$$

$$= \sum_{i=1}^{r_1} u_i \left( \log \frac{q_i}{p_i} \right)$$

$$= \sum_{i=1}^{r_1} u_i \left( \log \frac{q_i}{p_i} + \sum_{j=1}^{r_2} v_{ij} \log \frac{q_{ij}}{p_{ij}} \right)$$

$$= \sum_{i=1}^{r_1} u_i \left( \log \frac{q_i}{p_i} \right) + \sum_{j=1}^{r_2} \sum_{i=1}^{r_1} v_{ij} \log \frac{q_{ij}}{p_{ij}}$$

Looking at this expression, we have that

$$\ell(q) - \ell(p) = \sum_{i=1}^{r_1} \sum_{j=1}^{r_2} v_{ij} \log \frac{q_{ij}}{p_{ij}}$$

and since $q$ was chosen to be the maximum likelihood estimate in the model $M$ with data vector $v$, this expression is nonnegative. We will show nonnegativity of the remaining expression. To this end, it suffices to show nonnegativity of

$$\log \frac{q_i}{p_i} - \sum_{j=1}^{r_2} \frac{v_{ij}}{u_i} \log \frac{q_{ij}}{p_{ij}}$$

for each $i$. Since $\sum_{j=1}^{r_2} v_{ij} = u_i$ we get that this expression equals

$$\sum_{j=1}^{r_2} \frac{v_{ij}}{u_i} \left( \log \frac{q_i}{p_i} - \log \frac{q_{ij}}{p_{ij}} \right) = \sum_{j=1}^{r_2} \frac{v_{ij}}{u_i} \left( \log \frac{q_i \cdot P_{ij}}{q_i P_{ij}} \right)$$

By the definition of $v_{ij}$ we have that $\frac{v_{ij}}{u_i} = \frac{p_{ij}}{p_i}$ to arrive at the expression

$$\sum_{j=1}^{r_2} \frac{p_{ij}}{p_i} \left( \log \frac{q_i}{p_i} \cdot \frac{p_{ij}}{q_{ij}} \right) = \sum_{j=1}^{r_2} \frac{p_{ij}}{p_i} \left( - \log \frac{q_i P_{ij}}{q_i P_{ij}} \right)$$

$$\geq \sum_{j=1}^{r_2} \frac{p_{ij}}{p_i} \left( 1 - \frac{P_i Q_{ij}}{q_i P_{ij}} \right)$$

$$= \sum_{j=1}^{r_2} \left( \frac{p_{ij}}{p_i} - \frac{q_{ij}}{q_i} \right)$$

$$= 0$$
where we used the inequality $-\log x \geq 1 - x$. This shows that the log-likelihood function can only increase with iteration of the EM algorithm. □

The behavior of the EM algorithm is not understood well, even in remarkably simple statistical models. It is known that if the model maximum likelihood estimate lies in the relative interior of the model $M$, then it is a fixed point of the EM algorithm. However, fixed points of the EM algorithm need not be critical points when those points lie on the boundary of the model, and the maximum likelihood estimate itself need not be a critical point of the likelihood function in the boundary case. Kubjas, Robeva, and Sturmfels \cite{KRS15} studied in detail the case of mixture of independence model \text{Mixt}$(\mathcal{M}_X \perp \perp Y)$, and also give a description of general issues that might arise with the EM algorithm. Even in this simple mixture model, the EM algorithm might have fixed points that are not critical points of the likelihood function. There might be an infinite number of fixed points of the EM algorithm. The two steps of the EM algorithm are quite simple for the model \text{Mixt}$(\mathcal{M}_X \perp \perp Y)$, so we write it out here explicitly to help focus ideas on this algorithm.

**Algorithm 14.3.3.** (EM algorithm for \text{Mixt}$(\mathcal{M}_X \perp \perp Y)$)

\begin{itemize}
  \item **Input:** Data $u \in \mathbb{N}^{r_1 \times r_2}$, an initial parameter estimates $\pi \in \Delta_{r-1}$, $A \in \mathbb{R}^{r \times r_1}$, $B \in \mathbb{R}^{r \times r_2}$
  \item **Output:** A distribution $p \in \text{Mixt}^r(\mathcal{M}_X \perp \perp Y)'$ (candidate for the MLE)
  \item **While:** Some termination condition is not yet satisfied do
    \begin{itemize}
      \item **(E-Step)** Compute estimates for fully observed data
        \[ v_{ijk} = u_{ij} \cdot \frac{\pi_k^{(t)} a_{ki}^{(t)} b_{kj}^{(t)}}{\sum_{k=1}^{r} \pi_k^{(t)} a_{ki}^{(t)} b_{kj}^{(t)}} \]
      \item **(M-Step)** $\pi_k^{(t+1)} = \frac{\sum_{i,j,k} v_{ijk} a_{ki}^{(t+1)}}{\sum_{i,j,k} v_{ijk} a_{ki}^{(t+1)}} = \frac{\sum_{j,k} v_{ijk} b_{kj}^{(t+1)}}{\sum_{i,k} v_{ijk}}$
    \end{itemize}
  \item **Return:** The final $\pi^{(t)}$, $A^{(t)}$, and $B^{(t)}$.
\end{itemize}

When working with models with continuous random variables, the thing to remember is that in the E-step we do not compute the expected values of the missing data but the expected values of the missing statistics of the data. For continuous random variables this can involve doing complicated integrals.

**Example 14.3.4** (Censored Gaussians). For $i = 1, 2, 3$, let $X_i \sim N(\mu_i, \sigma_i^2)$, and let $T \sim N(0, 1)$, and suppose that $X_1 \perp \perp X_2 \perp \perp X_3 \perp \perp T$. For $i = 1, 2, 3$, let
$Y_i \in \{0, 1\}$ be defined by

$$Y_i = \begin{cases} 
1 & \text{if } X_i < T \\
0 & \text{if } X_i > T 
\end{cases}$$

Suppose that we only observe the discrete random variable $Y \in \{0, 1\}^3$. If we want to compute maximum likelihood estimates of the parameters $\mu_i, \sigma_i^2$ we can use the EM algorithm. In this case the M-step is trivial (sample mean and variance of a distribution), but the E-step requires a nontrivial computation. In particular, we need to compute the expected sufficient statistics of the Gaussian model namely

$$E_{\mu, \sigma}[X_i | Y] \quad \text{and} \quad E_{\mu, \sigma}[X_i^2 | Y].$$

Let

$$f(x_i | \mu_i, \sigma_i) = \frac{1}{\sigma_i \sqrt{2\pi}} \exp \left( -\frac{1}{2\sigma_i^2} (x_i - \mu_i)^2 \right)$$

be the density function of the univariate Gaussian distribution. Computing $E_{\mu, \sigma}[X_i | Y]$ and $E_{\mu, \sigma}[X_i^2 | Y]$ amounts to computing the following integrals:

$$E_{\mu, \sigma}[X_i | Y] = \frac{1}{P(Y)} \iiint \limits_V x_i \prod \limits_{j=1}^3 f(x_j | \mu_j, \sigma_j) \times f(t | 0, 1) dx dt$$

$$E_{\mu, \sigma}[X_i^2 | Y] = \frac{1}{P(Y)} \iiint \limits_V x_i^2 \prod \limits_{j=1}^3 f(x_j | \mu_j, \sigma_j) \times f(t | 0, 1) dx dt$$

where

$$P(Y) = \iiint \limits_V \prod \limits_{j=1}^3 f(x_j | \mu_j, \sigma_j) \times f(t | 0, 1) dx dt$$

and $V$ is the region

$$V = \{(x_1, x_2, x_3, t) \in \mathbb{R}^4 : x_i < t \text{ if } Y_i = 1, \text{ and } x_i > t \text{ if } Y_i = 0\}.$$ 

A detailed analysis of generalizations of these models appears in [Boc15], including their application to the analysis of certain mutation data. That work uses Monte Carlo methods to approximate the integrals. The integrals that appear here are integrals of Gaussian density functions over polyhedral regions and can also be computed using the holonomic gradient method [Koy13, KT15].

14.4. Exercises

**Exercise 14.1.** Let $X_1, X_2, X_3$ be binary random variables. Prove that

$$\text{Mixt}^4(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3}) = \Delta_7.$$
Exercise 14.2. Show that $\text{Mixt}^2(\mathcal{M}_{X_1 \perp \perp X_2})$ is equal to the set of joint distributions $P \in \Delta_{r_1, r_2 - 1}$ for two discrete random variables such that $\text{rank } P \leq 2$.

Exercise 14.3. Consider the DAG $G$ on five vertices with edges $1 \to 2$, $1 \to 4$, $1 \to 5$, $2 \to 3$, $3 \to 4$, and $3 \to 5$. Let $X_1, \ldots, X_5$ be binary random variables. Compute the vanishing ideal of the hidden variable graphical model where $X_1$ is hidden. Is the corresponding variety the secant variety of the variety associated to some graphical model?

Exercise 14.4. Show that the factor analysis model $\mathcal{F}_{m,s}$ as introduced in Example 6.5.4 gives the same family of covariance matrices as the hidden variable gaussian graphical model associated to the complete directed bipartite graph $K_{s,m}$ as described in Example 14.2.6.

Exercise 14.5. Consider the complete bidirected graph on 3 vertices, $K_3$. The linear structural equation model for this graph consists of all positive definite matrices $\mathcal{M}_{K_3} = PD_3$. Compare this to the set of covariance matrices that arise when looking at the hidden variable model on the bidirected subdivision. In particular, give an example of a positive definite matrix that could not arise from the hidden variable model on the bidirected subdivision.

Exercise 14.6. Show that if $p$ is in the relative interior of $\mathcal{M}'$ and $\ell'(p^{(t)}) = \ell'(p^{(t+1)})$ then $p^{(t)}$ is a critical point of the likelihood function. This shows that the termination criterion in the EM algorithm can be taken to run the algorithm until $\ell'(p^{(t+1)}) - \ell'(p^{(t)}) < \epsilon$ for some predetermined tolerance $\epsilon$.

Exercise 14.7. Implement the EM-algorithm for the mixture model over two independent discrete random variables $\text{Mixt}^r(\mathcal{M}_{X \perp \perp Y})$ and run it from 1000 random starting points with $r = 3$ on the data set

$$u = \begin{pmatrix} 10 & 1 & 1 & 3 \\ 1 & 10 & 1 & 1 \\ 1 & 1 & 10 & 1 \\ 1 & 1 & 1 & 10 \end{pmatrix}.$$  

Report on your findings.
Chapter 15

Phylogenetic Models

Phylogenetics is the area of mathematical biology concerned with reconstructing the evolutionary history of collections of species. It has an old history, originating in the works of Linneaus on classification of species and Darwin in the development of the theory of evolution.

The phylogeny of a collection of species is typically represented by a rooted tree. The tips (leaves) of the tree correspond to extant species (i.e. those that are current alive), and internal nodes in the tree represent most recent common ancestors of the extant species which lie below them. The major goal of phylogenetics is to reconstruct this evolutionary tree from data about species at the leaves.

Before the advent of modern sequencing technology, the primary methods for reconstructing phylogenetic trees were to look for morphological similarities between species and group species together that had similar characteristics. This, of course, also goes back to the Linnaean classification system: all species with a backbone are assumed to have a common ancestor, bird species should be grouped based on how many toes they have, etc. Unfortunately, a focus only on morphological features might group together organisms that have developed similar characteristics through different pathways (convergent evolution) or put apart species that are very closely related evolutionarily simply because they have a single disparate adaptation. Furthermore, collections of characteristics of different species might not all compatibly arise from a single tree, so combinatorial optimization style methods have been developed to reconstruct trees from such character data. Systematic development of such methods eventually led to the maximum parsimony approach to reconstruct phylogeny, trying to find
the tree on which the fewest mutations are necessary to observe the species with the given characteristics.

Since the 1970’s sequencing technology has been developed that can take a gene and reconstruct the sequence of DNA bases that make up that gene. From similar information we can also construct a amino acid sequence for the corresponding protein that the gene codes for. Modern methods for reconstructing phylogenetic trees are based on comparing these sequences for genes that appear in all species under consideration, using a phylogenetic model to model how these sequences might have descended through mutations from a common ancestor, and applying statistical procedures to recover the tree that best fits the data.

Phylogenetics is a vast field, with a wealth of papers, results, and algorithms. The methods of phylogenetics are applied throughout the biological sciences. We could not hope to cover all this material in the present book but refer the interested reader to the standard texts [Fei03, SS03b, Ste16]. Our goal here is to cover the basics of phylogenetic models and how these models can be analyzed using methods from algebraic statistics. We will return to discuss phylogenetics from a more polyhedral and combinatorial perspective in Chapter 19.

The algebraic study of phylogenetic models was initiated by computational biologists [CF87, Lak87] under the name phylogenetic invariants. The determination of phylogenetic invariants for many of the most commonly used models is understood, but for more complex models, it remains open to determine them. We will discuss tools that make it easier to determine phylogenetic invariants in this chapter. In Chapter 16 we discuss applications of phylogenetic invariants to identifiability problems for phylogenetic models.

15.1. Trees and Splits

In this section we summarize some basic facts about trees that we will need throughout our discussion of phylogenetics. We typically treat the phylogenetic models on trees that we will study as directed graphical models with all arrows directed away from a given root vertex, but the unrooted perspective plays an important role because of identifiability issues.

A tree $T = (V, E)$ is an graph that is connected and does not have any cycles. These two conditional imply that the number of edges in a tree with $m$ vertices is $m - 1$. A leaf is a vertex of degree 1 in $T$. Because phylogenetics is usually concern with constructing trees based on data associated only with extant species, which are associated with leaves of the tree, it is useful to discuss combinatorial features of trees with only the leaves labeled.
15.1. Trees and Splits

Definition 15.1.1. Let $X$ be a set of labels and let $T = (V, E)$ be a tree. Let $\phi : X \to V$ be a map from the label set to the vertices of $T$.

- The pair $T = (T, \phi)$ is called an $X$-tree if each vertex of degree one and two in $T$ is in the image of $\phi$.
- The pair $T = (T, \phi)$ is called a phylogenetic $X$-tree if the image of $\phi$ is exactly the set of leaves of $T$ and $\phi$ is injective.
- A binary phylogenetic $X$-tree is a phylogenetic $X$-tree where each non-leaf vertex has degree 3.

We will usually just write that $T$ is a phylogenetic $X$-tree (or just phylogenetic tree if $X$ is clear) without referring to the map $\phi$. In a rooted tree we designate a prescribed vertex as the root, which is also required to have a special label $\rho$. In a binary rooted phylogenetic tree, the root vertex has degree 2 and all other non-leaf vertices have degree 3. Although our rooted trees could be considered as undirected trees, we will typically draw them as directed with all edges directed away from the root node. This will be useful when we consider phylogenetic models on these trees, as they are naturally related to DAG models from Chapter 13. An example of $[6]$-tree and a rooted binary phylogenetic $[6]$-tree appear in Figure 15.1.1.

In addition to the standard representation of a tree as a vertex set and list of edges, it can be useful to also encode the tree by a list of splits, which are bipartitions of the label set $X$ induced by edges.

Definition 15.1.2. A split $A|B$ of $X$ is a partition of $X$ into two disjoint nonempty sets. The split $A|B$ is valid for the $X$-tree $T$ is obtained from $T$ by removing some edge $e$ of $T$ and taking $A|B$ to the two sets of labels and the two connected components of $T \setminus e$. The set of all valid splits for the $X$-tree $T$ is $\Sigma(T)$.
Example 15.1.3. Let $X = [6]$ and consider the $X$-tree $T$ on the left in Figure 15.1.1. The associated set of valid splits $\Sigma(T)$ is

\[(15.1.1) \quad \Sigma(T) = \{1|23456, 14|2356, 26|1345, 3|12456, 5|12346\}.
\]

For the rooted binary phylogenetic $[6]$-tree on the right in Figure 15.1.1, the associated set of valid splits (including the root) are

\[
\Sigma(T) = \{i|\{1, 2, 3, 4, 5, 6, \rho\} \setminus \{i\}: i = 1, \ldots, 6\} \cup \{16|2345\rho, 23|1456\rho, 1236|45\rho, 12346|5\rho\}.
\]

Not every set of splits could come from an $X$-tree. For example, on four leaves, there is no tree that has both of the splits $12|34$ and $13|24$. This notion is encapsulated in the definition of compatible splits.

Definition 15.1.4. A pair of splits $A_1|B_1$ and $A_2|B_2$ is called compatible if at least one of the sets

\[(15.1.2) \quad A_1 \cap A_2, A_1 \cap B_2, B_1 \cap A_2, B_1 \cap B_2
\]

is empty. A set $\Sigma$ of splits is pairwise compatible if every pair of splits $A_1|B_1, A_2|B_2 \in \Sigma$ is compatible.

Proposition 15.1.5. If $T$ is an $X$-tree then $\Sigma(T)$ is a pairwise compatible set of splits.

Proof. The fact that removing an edge of $T$ disconnects it, guarantees that at least one pair of intersections in Equation (15.1.2) is empty. □

The Splits Equivalence Theorem says that the converse to Proposition 15.1.5 is also true:

Theorem 15.1.6 (Splits Equivalence Theorem). Let $\Sigma$ be a set of $X$-splits that is pairwise compatible. Then there exists a unique $X$-tree $T$ such that $\Sigma = \Sigma(T)$.

Proof Sketch. The idea of the proof is to “grow” the tree by adding one split at a time, using induction on the number of splits in a pairwise compatible set. Suppose that $T'$ is the unique tree we have constructed from a set of pairwise compatible splits, and we want to add one more split $A|B$. The pairwise compatibility of $A|B$ with the splits in $T'$ identifies a unique vertex in $T'$ that can be grown out to produce an edge in a tree $T$ that has all the given splits. This process is illustrated in Figure 15.1.2 with the set of splits in (15.1.1), adding the splits in order from left to right. □

The splits equivalence theorem allows us to uniquely associate a tree with its set of edges (the splits). This fact can be useful in terms of descriptions of phylogenetic models associated to the trees. For instance, it will
15.2. Types of Phylogenetic Models

We describe in this section the general setup of phylogenetic models broadly speaking. We will explain how these models are related to the latent variable DAG models of previous chapters. However, in most applications, the phylogenetic models are not equal to a graphical model, but is merely a subset of a graphical model, because of certain structures that are imposed on the conditional. We will illustrate what types of assumptions are made in these models, to illustrate the imposed structures. Subsequent sections will focus in on algebraic aspects of these models.

Phylogenetic models are used to describe the evolutionary history of sequence data over time. Let \( T \) be a rooted tree, which we assume is a directed graph with all edges pointing away from the root vertex. To each vertex \( i \) in the tree associate a sequence \( S_i \) on some alphabet. For simplicity the alphabet is assumed to be the set \([\kappa]\) for some integer \( \kappa \). For biological applications, the most important values of \( \kappa \) are \( \kappa = 4 \), where the alphabet consists of the four DNA bases \( \{A,C,G,T\} \) and then the sequence \( S_i \) is a fragment of DNA, usually corresponding to a gene, and the node corresponds to a species that has that gene. The value \( \kappa = 20 \), is also important, where the alphabet consists of the 20 amino acids, and so the sequences \( S_i \) is a protein sequence. Other important values include \( \kappa = 61 \), corresponding to the 61 codons (DNA triplets that code for amino acids, excluding three stop codons) and \( \kappa = 2 \), still corresponding to DNA sequences but where purines \( (A,G) \) and pyrimidines \( (C,T) \) are grouped together as one element.

The sequences \( S_i \) are assumed to be related to each other by common descent, i.e. they all code for a gene with the same underlying function in the species corresponding to each node. So the sequence corresponding to the root node is the most ancestral sequence, and all the other sequences in the tree have descended from it via various changes in the sequence. We
Phylogenetic Models typically do not have access to the sequence data of ancestral species (since those species are long extinct), and so that sequence data is treated as hidden variables.

In the most basic phylogenetic models that are used, the only changes that happen to the sequences are point mutations, that is a random points in time, a change to a single position in a sequence. This means that all the sequences have the same length. Furthermore, it is assumed that the point mutations happen independently at each position in the sequence. So our observed data under these assumptions looks something like this:

- **Human:** ACCGTGAACGTGAACGA
- **Chimp:** ACCTTGGAAGGTAAACGA
- **Gorilla:** ACCTGCAACGTAAACTA

These are the DNA sequences for sequences at the leaves of some tree explaining the evolutionary history of the genes these three genes. The goal of phylogenetics is to figure out which (rooted) tree produced this data. Each tree yields a different family of probability distributions, and we would like to find the tree that best explains the observed data.

The assumption of site independence means that each column of the alignment has the same underlying probability distribution. For example, the probability of observing the triple AAA is the same at any position in the alignment. Hence with these assumptions of only point mutations and site independence, to describe a phylogenetic model, we need to use the tree and model parameters to determine the probability of observing each column in the alignment. For example, with 3 observed sequences, and $\kappa = 4$, we need to write down formulas for each of the 64 probabilities $p_{AAA}, p_{AAC}, p_{AAG}, \ldots, p_{TTT}$.

For general $\kappa$ and number of taxa at the leaves, $m$, we need a probability distribution for each of the $\kappa^m$ different possible columns in the alignment.

Consider the hidden variable graphical model associated to the rooted phylogenetic tree $\mathcal{T}$. We have a random variable associated to each vertex that has $\kappa$ states and all random variables associated to internal vertices (that is, vertices that are not tips in the tree) are hidden random variables. According to our discussion above, this gives a phylogenetic model because it assigns probabilities to each of the $\kappa^m$ possible columns in the alignment of the $m$ sequences. The resulting phylogenetic model that arises is called the general Markov model. It has interesting connections to mathematics and has received wide study, though it is not commonly used in phylogenetics practice because its large number of parameters make it computationally unwieldy. We will study this model in detail in Section 15.4.
Example 15.2.1. Consider the 3-leaf tree in Figure 15.2.1. Here root is the node labeled $Y_1$. The variables $Y_1$ and $Y_2$ are hidden random variables, whereas the random variables associated to the leaf nodes $X_1, X_2, X_3$ are observed random variables. In the DAG model associated to this tree, the parameters are the marginal probability distribution of $Y_1$, and the conditional probability distributions of $Y_2$ given $Y_1$, $X_1$ given $Y_1$, $X_2$ given $Y_2$, and $X_3$ given $Y_3$. The probability of observing $X_1 = x_1, X_2 = x_2, X_3 = x_3$ at the leaves has the form

$$P(x_1, x_2, x_3) = \sum_{y_1 \in [\kappa]} \sum_{y_2 \in [\kappa]} P_{Y_1}(y_1) P_{Y_2|Y_1}(y_2|y_1) P_{X_1|Y_1}(x_1|y_1) P_{X_2|Y_2}(x_2|y_2) P_{X_3|Y_2}(x_3|y_2)$$

where we used shorthand like

$$P_{Y_2|Y_1}(y_2|y_1) = P(Y_2 = y_2|Y_1 = y_1).$$

The structure of these conditional distribution matrices associated to each edge in the tree are important for the analysis of the phylogenetic models. Point substitutions are happening instantaneously across the sequence and across the tree. The conditional distribution like $P(Y_2 = y_2|Y_1 = y_1)$ along a single edge summarizes (or integrates out) this continuous time process.

Since $T$ is a rooted tree and all edges are directed away from the root, each vertex in $T$ except the root has exactly one parent. This means that the conditional probability distributions that appear in the directed graphical model $P(X_i = x_i|X_{pa(i)} = x_{pa(i)})$ are matrices, and can be thought of as transition matrices of Markov chains. (This explains the name general Markov model, above). Most phylogenetic models that are used in practice are obtained as submodels of the general Markov model by placing restrictions on what types of transition matrices are used.

The starting point for discussing the general structure of the Markov models that are used in practice is to start with some basic theory of Markov chains. Let $Q \in \mathbb{R}^{\kappa \times \kappa}$ be a matrix such that $q_{ij} \geq 0$ for all $i \neq j$ and such
that for each $i$, $\sum_{j=1}^{\infty} q_{ij} = 0$. The resulting matrix describes a continuous time Markov chain. Roughly speaking the probability that our random variable jumps from state $i$ to state $j$ in infinitesimal time $dt$ is $q_{ij} dt$. The matrix $Q$ is called the *rate matrix* of the continuous time Markov chain.

To calculate the probability that after $t$ time units our random variable ends up in state $j$ given that it started at $t = 0$ in state $i$ we can solve a system of linear differential equations to get the conditional probability matrix $P(t) = \exp(Qt)$, where

$$\exp(Qt) = I + Qt + \frac{Q^2t^2}{2!} + \frac{Q^3t^3}{3!} + \cdots$$

denotes the matrix exponential. See a book on Markov chains for more details (e.g. [Nor98]).

The various phylogenetic models arise by requiring that all the transition matrices are of the form $\exp(Qt)$ for some rate matrix $Q$, and then further specifying what types of rate matrices are allowed. The time parameter is an important one from the biological standpoint because it tells how far back in time the most recent common ancestors occurred. Note that even if we allowed each edge $e$ of the tree to have a different, and completely arbitrary, rate matrix $Q_e$, the resulting model that arises is smaller than the general Markov model, since a conditional probability distribution of the form $\exp(Qt)$ has a restricted form.

**Example 15.2.2.** The transition matrix

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

could not arise as $P = \exp(Qt)$ for any rate matrix $Q$ or any time $t$. Indeed, from the identity

$$\det \exp(A) = \exp(\text{tr } A)$$

we see that if $\det \exp(Qt)$ is positive for any rate matrix $Q$ and any $t \in [0, \infty)$. On the other hand, $\det P = -1$, in the preceding example.

Phylogenetic models are usually specified by describing the structure of the rate matrix $Q$. Here are some common examples.

The simplest model for 2 state Markov chain is the Cavender-Farris-Neyman model (CFN) [Cav78, Far73, Ney71] which has rate matrices of the form:

$$Q^{CFN} = \begin{pmatrix} -\alpha & \alpha \\ \alpha & -\alpha \end{pmatrix}$$
for some positive parameter $\alpha$. This model is also called the binary symmetric model since the transition matrix
\[
P(t) = \exp(Q^{\text{CFN}}t) = \begin{pmatrix}
\frac{1+\exp(-2\alpha t)}{2} & \frac{1-\exp(-2\alpha t)}{2} \\
\frac{1-\exp(-2\alpha t)}{2} & \frac{1+\exp(-2\alpha t)}{2}
\end{pmatrix}
\]
is symmetric. The CFN model is the only significant model for $\kappa = 2$ besides the general Markov model.

From here on we focus on models for the mutation of DNA-bases. We order the rows and columns of the transition matrix $A, C, G, T$. The simplest model for DNA bases is the Jukes-Cantor model (JC69) [JC69].

\[
Q^{\text{JC}} = \begin{pmatrix}
-3\alpha & \alpha & \alpha & \alpha \\
\alpha & -3\alpha & \alpha & \alpha \\
\alpha & \alpha & -3\alpha & \alpha \\
\alpha & \alpha & \alpha & -3\alpha
\end{pmatrix}.
\]

Note that JC69 model, while widely used, is not considered biologically reasonable. This is because it gives equal probability to each of the mutations away from a given DNA base. This is considered unrealistic in practice because the mutations are more likely to occur within the purine group \{A, G\} and within the pyrimidine group \{C, T\}, than from purine to pyrimidine or vice versa. In phylogenetics a within group mutation is called a transition and mutation across groups is called a transversion. Kimura [Kim80] tried to correct this weakness of the Jukes-Cantor model by explicitly adding separate transversion rates. These are summarized in the Kimura 2-parameter and Kimura 3-parameter models:

\[
Q^{\text{K2P}} = \begin{pmatrix}
-\alpha - 2\beta & \beta & \alpha & \beta \\
\beta & -\alpha - 2\beta & \beta & \alpha \\
\alpha & \beta & -\alpha - 2\beta & \beta \\
\beta & \alpha & \beta & -\alpha - 2\beta
\end{pmatrix}
\]

\[
Q^{\text{K3P}} = \begin{pmatrix}
-\alpha - \beta - \gamma & \beta & \alpha & \gamma \\
\beta & -\alpha - \beta - \gamma & \alpha & \gamma \\
\alpha & \gamma & -\alpha - \beta - \gamma & \beta \\
\gamma & \alpha & \beta & -\alpha - \beta - \gamma
\end{pmatrix}.
\]

The CFN, JC69, K2P, and K3P models all have a beautiful mathematical structure which we will analyze in detail in Section 15.3.

A key feature of a Markov chain is its stationary distribution. Let $P$ be the transition matrix of a Markov chain. Form a graph $G(P)$ with vertex set $[\kappa]$, and with an edge $i \to j$ if $p_{ij} > 0$ (including loops $i \to i$ if $p_{ii} > 0$). The Markov chain is said to be irreducible if between any ordered pair of vertices $\langle i, j \rangle$ there is directed path from $i$ to $j$ in $G(P)$. The Markov chain is aperiodic the greatest common divisor of cycle lengths in the graph is 1.
Theorem 15.2.3 (Perron-Frobenius). Let $Q$ be a rate matrix such that $P(t) = \exp(Qt)$ describes an irreducible, aperiodic Markov chain. Then there is a unique probability distribution $\pi \in \Delta_{\kappa-1}$ such that $\pi Q = 0$, or equivalently $\pi \exp(Qt) = \pi$. This distribution is called the stationary distribution of the Markov chain.

For each of the CFN, JC69, K2P, and K3P models described above, the stationary distribution is the uniform distribution, that is $\pi = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ for the CFN model and $\pi = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ for the other models. For aperiodic irreducible Markov chains, the stationary distribution also has the property that if $\mu$ is any probability distribution on $[\kappa]$ then $\mu P^t$ converges to $\pi$ as $t \to \infty$. This is part of the reason $\pi$ is called the stationary distribution.

Considering the Markov chain associated to a rate matrix $Q$ arising from a phylogenetic model, if one believes that these models truly describe the long-term behavior of mutational processes in DNA sequences, one would expect to see a relatively uniform distribution of bases in DNA, with one fourth of bases being, e.g. A. However, this is generally not what is observed in practice as C’s and G’s are generally rarer than A’s and T’s. Various models have been constructed which attempt to allow for other stationary distributions to arise, besides the uniform distributions that are inherent in the CFN, JC69, K2P, and K3P models.

The Felsenstein model (F81) \cite{Felsenstein1981} and the Hasegawa, Kishino and Yano (HKY85) \cite{Hasegawa1985} model are two simple models that take into account these structures. Their rate matrices have the following forms where the $*$ in each row denotes the appropriate number so that the row sums are all zero:

$$Q_{F81} = \begin{pmatrix} * & \pi_C & \pi_G & \pi_T \\ \pi_A & * & \pi_G & \pi_T \\ \pi_A & \pi_C & * & \pi_T \\ \pi_A & \pi_C & \pi_G & * \end{pmatrix}, \quad Q_{HKY} = \begin{pmatrix} * & \pi_C & \alpha \pi_G & \pi_T \\ \pi_A & * & \pi_G & \alpha \pi_T \\ \alpha \pi_A & \pi_C & * & \pi_T \\ \pi_A & \alpha \pi_C & \pi_G & * \end{pmatrix}. $$

Note that the addition of the parameter $\alpha$ to the HKY model allows to increase the probability for transitions versus transversions (so $\alpha \geq 1$).

A further desirable property of the Markov chains that arise in phylogenetics is that they are often time reversible. Intuitively, this means that random point substitutions looking forward in time should look no different from random point substitutions looking backwards in time. This is a reasonable assumption on shorter time-scales for which we could discuss comparing two DNA sequences to say they evolved from a common source. Time reversibility amounts to the following condition on the rate matrix

$$\pi_i Q_{ij} = \pi_j Q_{ji}. $$
for all pairs $i, j$. All the models we have encountered so far, except the general Markov model, are time reversible. The most general time reversible model is called the general time reversible model (GTR). Its rate matrices have the following form:

$$Q^{GTR} = \begin{pmatrix}
* & \pi_{G\alpha} & \pi_{G\beta} & \pi_{T\gamma} \\
\pi_{A\alpha} & * & \pi_{T\epsilon} & \pi_{T\zeta} \\
\pi_{A\beta} & \pi_{C\delta} & * & \pi_{T\zeta} \\
\pi_{A\gamma} & \pi_{C\epsilon} & \pi_{G\zeta} & *
\end{pmatrix}$$

where the $*$ is in each row chosen so that the row sums are zero.

These Markov mutation models are just a fraction of the many varied models that might be used in practice. The most widely used models are the ones that are implemented in phylogenetic software, probably the most commonly used model is the GTR model.

Up to this point we have added conditions to our models based on increasing assumptions of biological realism. However, there are also mathematical considerations which can be made which might be useful from a theoretical standpoint, or lead us to rethink their usefulness as biological tools. We conclude this section by discussing one such practical mathematical consideration now.

It is often assumed that the rate matrix $Q$ is fixed throughout the entire evolutionary tree. This is mostly for practical reasons since this assumption greatly reduces the number of parameters in the model. It might be a reasonable assumption for very closely related species but is probably unreasonable across large evolutionary distances. So let us assume throughout the remainder of this section that we use different rate matrices along each edge of the tree.

Note that if we construct a phylogenetic tree that has a vertex of degree two we do not really get any information about this vertex as it is a hidden node in the tree. If $\exp(Q_1t_1)$ is the transition matrix associated with the first edge and $\exp(Q_2t_2)$ is the transition matrix associated to the second edge the new transition matrix we get by suppressing the vertex of degree two will be the matrix product $\exp(Q_1t_1)\exp(Q_2t_2)$. The mathematical property we would like this matrix to satisfy for a model to be reasonable is that this resulting matrix also has the form $\exp(Q_3(t_1 + t_2))$ for some $Q_3$ in our model class. It seems difficult to characterize which sets of rate matrices are closed in this way. One useful way to guarantee this of this property is handled by the theory of Lie Algebras.

**Definition 15.2.4.** A set $L \subseteq K^{\kappa \times \kappa}$ is a matrix Lie algebra if $L$ is a $K$-vector space and for all $A, B \in L$

$$[A, B] := AB - BA \in L.$$
We say a set of rate matrices $\mathcal{L}$ is a Lie Markov model if it is a Lie algebra.

The quantity $[A, B] = AB - BA$ is called the Lie bracket or commutator of the matrices $A$ and $B$.

**Theorem 15.2.5.** [SFSJ12a] Let $\mathcal{L} \subset \mathbb{R}^{\kappa \times \kappa}$ be a collection of rate matrices. If $\mathcal{L}$ is a Lie Markov model then for any $Q_1, Q_2 \in \mathcal{L}$ and $t_1, t_2$, there is a $Q_3 \in \mathcal{L}$ such that $\exp(Q_1 t_1) \exp(Q_2 t_2) = \exp(Q_3 (t_1 + t_2))$.

**Proof.** This follows directly from application of the Baker-Campbell-Hausdorff [Cam97] for the product of two matrix exponentials:

$$\exp(X) \exp(Y) = \exp \left( X + Y + \frac{1}{2} [X, Y] + \frac{1}{12} [X, [X, Y]] + \cdots \right). \quad \square$$

The group-based phylogenetic models (CFN, JC69, K2P, K3P) all have the property that the matrices in the models are simultaneously diagonalizable (this will be discussed in more detail in Section 15.3). This in particular, implies that any pair of rate matrices $Q_1, Q_2$ in one of these models commute with each other, and hence, the commutator $[Q_1, Q_2] = 0$. Thus, the group based models give abelian Lie algebras, and so are Lie Markov models. Since the general Markov model includes all rate matrices, the general Markov model is clearly closed under taking Lie brackets, so it is a Lie Markov model. The F81 model is also a Lie Markov model, though it is not abelian.

On the other hand, the HKY, and GTR models are not Lie Markov models, as can be verified by directly calculating the commutators between a pair of elements. If one works with models with heterogeneous rate matrices across the tree, this might present difficulties for using these models in practice [SFSJ+12b].

**15.3. Group-based Phylogenetic Models**

In this section, we study the group-based models, which are the CFN, JC, K2P, and K3P models (though in theory the idea of a group-based model holds much more generally). The rate matrices of these models (and hence the transition matrices) all have the remarkable property that they can be simultaneously diagonalized (without regard to what particular rate matrices is used on a particular edge in a tree). In the resulting new coordinate system, the models turn out to be toric varieties and it is considerably easier to describe their vanishing ideals.

To explain the construction of explicit generating sets of the vanishing ideals of group-based models we need some language from group theory. Let $G$ be a finite abelian group, which we write with an additive group operation.
15.3. Group-based Phylogenetic Models

In all the applications we consider either \( G = \mathbb{Z}_2 \) or \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \), though any finite abelian group would work for describing a group-based model. We replace the state space \( \kappa \) with the finite abelian group \( G \) (whose cardinality equals \( \kappa \)). Let \( M = \exp(Qt) \) be the transition matrix along an edge of the tree \( T \).

**Definition 15.3.1.** A phylogenetic model is called a *group-based model* if for all transition matrices \( M = \exp(Qt) \) that arise from the model, there exists a function \( f : G \to \mathbb{R} \) such that \( M(g, h) = f(g - h) \).

Here \( M(g, h) \) denotes the \((g, h)\) entry of \( M \), the probability of going to \( g \) given that we are in state \( h \) at the previous position. Explicit calculation of the matrix exponentials shows that all of the CFN, JC, K2P, K3P models are all group-based. For example, in the CFN model:

\[
Q = \begin{pmatrix}
-\alpha & \alpha \\
\alpha & -\alpha
\end{pmatrix}
\]

\[
\exp(Qt) = \begin{pmatrix}
\frac{1}{2}(1 + e^{-2\alpha t}) & \frac{1}{2}(1 - e^{-2\alpha t}) \\
\frac{1}{2}(1 - e^{-2\alpha t}) & \frac{1}{2}(1 + e^{-2\alpha t})
\end{pmatrix}.
\]

So the function \( f : \mathbb{Z}_2 \to \mathbb{R} \) has \( f(0) = \frac{1}{2}(1 + e^{-2\alpha t}) \) and \( f(1) = \frac{1}{2}(1 - e^{-2\alpha t}) \).

In the K3P model we have

\[
Q = \begin{pmatrix}
-\alpha - \beta - \gamma & \beta & \alpha & \gamma \\
\beta & -\alpha - \beta - \gamma & \gamma & \alpha \\
\alpha & \gamma & -\alpha - \beta - \gamma & \beta \\
\gamma & \alpha & \beta & -\alpha - \beta - \gamma
\end{pmatrix}
\]

and

\[
\exp(Qt) = \begin{pmatrix}
a & b & c & d \\
b & a & d & c \\
c & d & a & b \\
d & c & b & a
\end{pmatrix}
\]

where

\[
a = \frac{1}{4}(1 + e^{-2(\alpha+\beta)t} + e^{-2(\alpha+\gamma)t} + e^{-2(\beta+\gamma)t})
\]

\[
b = \frac{1}{4}(1 - e^{-2(\alpha+\beta)t} - e^{-2(\alpha+\gamma)t} + e^{-2(\beta+\gamma)t})
\]

\[
c = \frac{1}{4}(1 - e^{-2(\alpha+\beta)t} + e^{-2(\alpha+\gamma)t} - e^{-2(\beta+\gamma)t})
\]

\[
d = \frac{1}{4}(1 + e^{-2(\alpha+\beta)t} - e^{-2(\alpha+\gamma)t} - e^{-2(\beta+\gamma)t}).
\]

So if we make the identification of the nucleotides \( \{A, C, G, T\} \) with elements of the group \( \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\} \) then we see that the K3P model is a group based model, and the corresponding function \( f \) has \( f(0, 0) = a \), \( f(0, 1) = b \), \( f(1, 0) = c \), and \( f(1, 1) = d \). The JC and K2P models can be seen to be group-based models with respect to \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) as they arise as submodels of K3P.
The presence of expressions like $f(g - h)$ in the formulas for the conditional probabilities suggest that the joint distributions in these models are convolutions of a number of functions. This suggests that applying the discrete Fourier transform might simplify the representation of these models. We now explain the general setup of the discrete Fourier transform which we then use to analyze the group-based models.

**Definition 15.3.2.** A one dimensional character of a group $G$ is a group homomorphism $\chi : G \to \mathbb{C}^\ast$.

**Proposition 15.3.3.** The set of one dimensional characters of a group $G$ is a group under the coordinate-wise product: $(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g)$. It is called the dual group of $G$ and is denoted $\hat{G}$. If $G$ is a finite abelian group then $\hat{G} \cong G$.

**Proof.** The conditions to check that $\hat{G}$ is a group are straightforward. For example, since $\mathbb{C}^\ast$ is abelian, we have that

$$(\chi_1 \cdot \chi_2)(g_1g_2) = \chi_1(g_1g_2)\chi_2(g_1g_2) = \chi_1(g_1)\chi_1(g_2)\chi_2(g_1)\chi_2(g_2)$$

$$= \chi_1(g_1)\chi_2(g_1)\chi_1(g_2)\chi_2(g_2) = (\chi_1 \cdot \chi_2)(g_1)(\chi_1 \cdot \chi_2)(g_2)$$

which shows that $(\chi_1 \cdot \chi_2)$ is a group homomorphism, so the product operation in $\hat{G}$ is well-defined.

It is also straightforward to see that $\hat{G} \times \hat{H} \cong \hat{G} \times \hat{H}$. If $G$ is a cyclic group $\mathbb{Z}_n$, then each group homomorphism sends the generator of $\mathbb{Z}_n$ to a unique $n$th root of unity. The group of $n$-th roots of unity is isomorphic to $\mathbb{Z}_n$. □

**Example 15.3.4.** Consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. The four characters of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are the rows in the following character table:

<table>
<thead>
<tr>
<th></th>
<th>(0, 0)</th>
<th>(0, 1)</th>
<th>(1, 0)</th>
<th>(1, 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
</tr>
</tbody>
</table>

Note that there is no canonical isomorphism between the $G$ and $\hat{G}$ in this case, some choice must be made in establishing the isomorphism.

**Definition 15.3.5.** Let $G$ be a finite abelian group, and $f : G \to \mathbb{C}$ a function. The discrete Fourier transform of $f$ is the function $\hat{f} : \hat{G} \to \mathbb{C}$ defined by

$$\hat{f}(\chi) = \sum_{g \in G} f(g)\chi(g).$$
The discrete Fourier transform is a linear change of coordinates. If we
think about $f$ as a vector in $\mathbb{C}^G$ then $\hat{f}$ is a vector in $\mathbb{C}^{\hat{G}}$ and two vectors
are related by multiplication by the matrix $\chi$ whose rows are the characters
of the group $G$. This linear transformation can be easily inverted via the
inverse Fourier transform stated as the following theorem.

**Theorem 15.3.6.** Let $G$ be a finite abelian group and $f : G \to \mathbb{C}$ a function. Then
\[
 f(g) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \overline{\chi(g)}
\]
where the bar denotes complex conjugation.

**Proof.** The rows of the character table are (complex) orthogonal to each
other and each has norm $|G|$. \hfill $\square$

A key feature of the discrete Fourier transform is that, in spite of being
a matrix-vector multiplication which seems like it might require $O(|G|^2)$
operations to calculate, the group symmetries involved imply that it can
be calculated rapidly, in $O(|G| \log |G|)$ time, when $|G| = 2^k$. This
is the fast Fourier transform (though we will not need this here). A final
piece we will need is the convolution of two functions and its relation to the
discrete Fourier transform.

**Definition 15.3.7.** Let $f_1, f_2 : G \to \mathbb{C}$ be two functions on a finite abelian
group. Their *convolution* is the function
\[
 (f_1 * f_2)(g) = \sum_{h \in G} f_1(h) f_2(g - h).
\]

**Proposition 15.3.8.** Let $f_1, f_2 : G \to \mathbb{C}$ be two functions on a finite abelian
group. Then
\[
 (\hat{f_1} * \hat{f_2}) = \hat{f_1} \cdot \hat{f_2}.
\]
i.e. the Fourier transform of a convolution is the product of the Fourier
transforms.

**Proof.** This follows by a directed calculation:
\[
 (\hat{f_1} * \hat{f_2})(\chi) = \sum_{g \in G} \sum_{h \in G} f_1(h) f_2(g - h) \chi(g)
 = \sum_{g' \in G} \sum_{h \in G} f_1(h) f_2(g') \chi(g' + h)
 = \sum_{g' \in G} \sum_{h \in G} f_1(h) f_2(g') \chi(g') \chi(h)
\]
\[ f_i(g - h) = M_i(g, h) \text{ which is guaranteed to exist since we are working with a group-based model.} \]

Now we compute the discrete Fourier transform over the group \( G^2 \).

\[ p(\chi_1, \chi_2) = \sum_{(g_1, g_2) \in G^2} \sum_{h \in G} \pi(h) f_1(g_1 - h) f_2(g_2 - h) \chi_1(g_1) \chi_2(g_2) \]

\[ = \sum_{g'_1 \in G} \sum_{g'_2 \in G} \sum_{h \in G} \pi(h) f_1(g'_1) f_2(g'_2) \chi_1(g'_1 + h) \chi_2(g'_2 + h) \]

\[ = \left( \sum_{g'_1 \in G} f_1(g'_1) \chi_1(g'_1) \right) \left( \sum_{g'_2 \in G} f_2(g'_2) \chi_2(g'_2) \right) \times \]

\[ \left( \sum_{h \in G} \pi(h) \chi_1(h) \chi_2(h) \right) \]

\[ = \hat{f}_1(\chi_1) \hat{f}_2(\chi_2) \hat{\pi}(\chi_1 \cdot \chi_2). \]

In particular, this shows that the probability of observing group elements \((g_1, g_2)\) can be interpreted as a convolution over the group \( G^2 \) and hence in the Fourier coordinate space (i.e. phase space) the transformed version factorizes as a product of transformed versions of the components. A special feature to notice is the appearance of the \( \chi_1 \cdot \chi_2 \) term.
Definition 15.3.10. Call a group-based model a **generic group-based model** if if the transition matrices that can arise consists of all transition matrices that satisfy $M(g, h) = f(g - h)$, and there is no restriction on the root distributions that can arise.

For example, the CFN model is the generic group-based model with respect to the group $\mathbb{Z}_2$ and the K3P model is the generic group-based model with respect to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. For a generic group-based model on a two leaf tree we can easily read off the representation of the model that is suggested in the Fourier coordinates.

Proposition 15.3.11. Consider the map $\phi_G : \mathbb{C}^G \times \mathbb{C}^G \times \mathbb{C}^G \to \mathbb{C}^G \times G$, such that
\[
(a_g)_{g \in G} \times (b_g)_{g \in G} \times (c_g)_{g \in G} \mapsto (a_{g_1} b_{g_2} c_{g_1 + g_2})_{g_1, g_2 \in G}.
\]
The Zariski closure of this map equals the Zariski closure of the cone over the image of the generic group-based model on a two-leaf tree. In particular, since $\phi_G$ is a monomial map whose image is the cone over the Zariski closure of the phylogenetic model is a toric variety.

Proof. From Example 15.3.9 we see that
\[
\hat{p}(\chi_1, \chi_2) = \hat{f}_1(\chi_1)\hat{f}_2(\chi_2)\hat{\pi}(\chi_1 \cdot \chi_2).
\]
Since we have assumed a generic group-based model, each of the functions $f_1$, $f_2$, and $\pi$ were arbitrary functions, subject to $\sum_{g \in G} f_i(g) = 1$, and $\sum_{g \in G} \pi(g) = 1$. Then the Fourier transforms are arbitrary functions subject to the constraints $\hat{f}_1(id) = 1$, $\hat{\pi}(id) = 1$, where $id$ denotes the identity element of $G$. Taking the cone and the Zariski closure yields the statement of the Proposition. □

In this proposition note that we have implicitly made the identification between $G$ and $\hat{G}$. Again, this is not canonically determined and some choice must be made.

Example 15.3.12. To illustrate the Proposition consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. We identify this group with the set of nucleotide bases (as in the K3P model) and declare that $A = (0, 0)$, $C = (0, 1)$, $G = (1, 0)$, and $T = (1, 1)$. The map $\phi_G$ in this example is
\[
(a_A, a_C, a_G, a_T, b_A, b_C, b_G, b_T, c_A, c_C, c_G, c_T) \mapsto \begin{pmatrix}
  a_A b_A c_A & a_A b_C c_C & a_A b_G c_G & a_A b_T c_T \\
  a_C b_A c_C & a_C b_C c_A & a_C b_G c_T & a_C b_T c_G \\
  a_G b_A c_G & a_G b_C c_T & a_G b_G c_A & a_G b_T c_G \\
  a_T b_A c_T & a_T b_C c_G & a_T b_G c_C & a_T b_T c_A
\end{pmatrix}.
\]
We can compute the vanishing ideal in the ring $\mathbb{C}[q_{AA}, \cdots q_{TT}]$, which is a toric ideal generated by 16 binomials of degree 3 and 18 binomials of degree 4. Here we are using $q_{g_1,g_2}$ to be the indeterminate corresponding to the Fourier transformed value $\hat{p}(g_1,g_2)$. These Fourier coordinates are the natural coordinate system after applying the Fourier transform. The following code in Macaulay2 can be used to compute those binomial generators:

```plaintext
S = QQ[aA,aC,aG,aT,bA,bC,bG,bT,cA,cC,cG,cT];
R = QQ[qAA,qAC,qAG,qAT,qCA,qCC,qCG,qCT,
    qGA,qGC,qGG,qGT,qTA,qTC,qTG,qTT];
f = map(S,R,{aA*bA*cA,aA*bC*cC,aA*bG*cG,aA*bT*cT,
    aC*bA*cC,aC*bC*cA,aC*bG*cT,aC*bT*cG,
    aG*bA*cG,aG*bC*cT,aG*bG*cA,aG*bT*cC,
    aT*bA*cT,aT*bC*cG,aT*bG*cC,aT*bT*cA});
I = kernel f
```

Among the generators of the vanishing ideal of this toric variety are the equation

$$q_{AA}q_{CG}q_{TC} - q_{TA}q_{CC}q_{AG}$$

in the Fourier coordinates. To express this equation in terms of the original probability coordinates we would need to apply the inverse Fourier transform, which expresses each of the $q_{g_1,g_2}$ as a linear combination of the probability coordinates. For example, if we make the identification that $A = (0,0), C = (0,1), G = (1,0), \text{ and } T = (1,1)$ in both $\mathbb{Z}_2 \times \mathbb{Z}_2$ and its dual group, then

$$q_{CG} = \sum_{(i,j),(k,l) \in \mathbb{Z}_2 \times \mathbb{Z}_2} (-1)^{i+k} p_{(i,j),(k,l)}$$

$$= p_{AA} + p_{AC} - p_{AT} - p_{CA} + p_{CG} + p_{CT}$$

$$+ p_{GA} + p_{GC} - p_{GT} - p_{TA} - p_{TC} + p_{TG} + p_{TT}.$$  

Here we are using the following forms of the characters of $\mathbb{Z}_2 \times \mathbb{Z}_2$: $\chi_A(i,j) = 1, \chi_C(i,j) = (-1)^j, \chi_G(i,j) = (-1)^i$, and $\chi_T(i,j) = (-1)^{i+j}$.

Now we state the general theorem about the Fourier transform of an arbitrary group-based model. To do this we need some further notation. Again, suppose that $T$ is a rooted tree with $m$ leaves. To each edge in the tree we have the transition matrix $M^e$, which satisfies $M^e(g,h) = f^e(g-h)$ for some particular function $f^e : G \to \mathbb{R}$. Also we have the root distribution $\pi$ which we write in function notation as $\pi : G \to \mathbb{R}$. Each edge $e$ in the graph has a head vertex and a tail vertex. Let $H(e)$ denote the head vertex and $T(e)$ denote the tail vertex. For each edge $e$, let $\lambda(e)$ be the set of leaves which lie below the edge $e$. Let $Int$ be the set of interior vertices of $T$. 

We can write the parametrization of the probability of observing group elements \( (g_1, g_2, \ldots, g_m) \) at the leaves of \( T \) as:

\[
p(g_1, \ldots, g_m) = \sum_{g \in G^{int}} \pi(g_r) \prod_{e \in T} M^e(g_{H(e)}, g_{T(e)})
\]

\[
= \sum_{g \in G^{int}} \pi(g_r) \prod_{e \in T} f^e(g_{H(e)} - g_{T(e)}).
\]

**Theorem 15.3.13.** Let \( p : G^m \rightarrow \mathbb{R} \) denote the probability distribution of a group-based model on an \( m \)-leaf tree. Then the Fourier transform of \( p \) satisfies:

\[
\hat{p}(\chi_1, \ldots, \chi_m) = \hat{\pi} \left( \prod_{i=1}^m \chi_i \right) \cdot \prod_{e \in T} \hat{f}^e \left( \prod_{i \in \lambda(e)} \chi_i \right).
\]

The use of the Fourier transform to simplify the parametrization of a group-based model was discovered independently by Hendy and Penny [HP96] and Evans and Speed [ES93]. Hendy and Penny refer to this technique as Hadamard conjugation (technically, a more involved application of the method is Hadamard conjugation) because the matrix that represents the Fourier transform for \( \mathbb{Z}_2^n \) is an example of a Hadamard matrix from combinatorial design theory.

**Proof of Theorem 15.3.13.** We directly apply the Fourier transform to equation \(15.3.1\).

\[
\hat{p}(\chi_1, \ldots, \chi_m) = \sum_{(g_1, \ldots, g_m) \in G^m} \sum_{g \in G^{int}} \pi(g_r) \prod_{e \in T} f^e(g_{H(e)} - g_{T(e)}) \prod_{i=1}^m \chi_i(g_i).
\]

As in Example 15.3.9 we change variables by introducing a new group element \( g_e \) associated to each edge in the tree

\[ g_e = g_{H(e)} - g_{T(e)}. \]

With this substitution, the group elements associated to the leaves are rewritten as \( g_i = g_r + \sum_{e \in P(i)} g_e \) where \( P(i) \) is the set of edges on the unique path from the root of \( T \) to leaf \( i \). In summary we can rewrite our expression for \( \hat{p} \) as

\[
\hat{p}(\chi_1, \ldots, \chi_m) = \sum_{g_r \in G} \sum_{g \in G^{E(T)}} \pi(g_r) \prod_{e \in T} f^e(g_e) \prod_{i=1}^m \chi_i(g_r + \sum_{e \in P(i)} g_e).
\]

Using the fact that \( \chi(g + h) = \chi(g)\chi(h) \) for any one-dimensional character, we can regroup this product with all terms that depend on \( g_e \) together to
produce:
\[\hat{p}(\chi_1, \ldots, \chi_m) = \left(\sum_{g_r \in G} \pi(g_r) \prod_{i=1}^{m} \chi_i(g_r)\right) \times \prod_{e \in E(T)} \left(\sum_{g_e \in G} f_e(g_e) \prod_{i \in \lambda(e)} \chi_i(g_e)\right)\]
\[= \hat{\pi} \left(\prod_{i=1}^{m} \chi_i\right) \cdot \prod_{e \in T} \hat{f}_e \left(\prod_{i \in \lambda(e)} \chi_i\right)\]
as claimed. 

Sturmfels and the author [SS05] realized that in certain circumstances (the Zariski closure of) a group-based model can be identified as a toric variety in the Fourier coordinates and so combinatorial techniques can be used to find the phylogenetic invariants in these models. The key observation is that the Equation 15.3.3 expresses the Fourier transform of the probability distribution as a product of Fourier transforms. If the functions \(f_e(g)\) depended in a complicated way on parameters, this might not be a monomial parametrization. However, if those transition functions were suitably generic, then each entry of the Fourier transform of the transition function can be treated as an independent “Fourier parameter”. This is the simplest case, the general group-based model.

**Corollary 15.3.14.** Let \(G\) be a finite abelian group and \(T\) a rooted tree with \(m\) leaves. In the Fourier coordinates, the Zariski closure of the general group-based model is equal to the Zariski closure of the image of the map \(\phi^{G, T}\)
\[\phi^{G, T}: \mathbb{C}^{\left|G\right| \times \left|E(T)\right| + 1} \to \mathbb{C}^{\left|G\right|^m}\]
\[\phi^{G, T}_{g_1, \ldots, g_m}((a_g^e)_{e \in E(T), g \in G}, (a_g^r)_{g \in G}) = a_g^r \sum_{i \in \left[m\right]} g_i \cdot \prod_{e \in E(T)} a_g^e \sum_{i \in \lambda(e)} g_i.\]

Here the \(a_g^r\) parameters play the role of the Fourier transform of the root distribution and the \(a_g^e\) play the role of the Fourier transform of the transition functions. Note that we have used the (nonunique) isomorphism \(G \cong \hat{G}\) to write our indices using the \(g \in G\) rather than with \(\chi \in \hat{G}\).

**Example 15.3.15.** Consider a generic group-based model for the three leaf tree illustrated in Figure 15.3.1. There are \(|G|\) parameters associated to each of the edges in the tree, and another \(|G|\) parameters associated to the root. The map \(\phi^{G, T}\) has coordinate functions
\[\phi^{G, T}_{g_1, g_2, g_3}(a) = a_{g_1}^r g_1 + a_{g_2}^e g_2 + a_{g_3}^1 g_3^1 a_{g_2}^2 a_{g_3}^3.\]
where the \( a_i \) indeterminates (for \( i = 1, 2, 3 \)) correspond to the edges incident to leaves, the \( a_r \) indeterminates correspond to the root, and the \( a_e \) indeterminates correspond to the single internal edge.

When a group-based model is not a general group-based model, some care is needed to see whether or not it is a toric variety, and, if so, how this affects the parametrization. First of all, we deal with the root distribution. Up to this point, in the group-based models we have treated the root distribution as a set of free parameters. This can be a reasonable assumption. However, often in phylogenetic models one takes the root distribution to be the (common) stationary distribution of all the transition matrices, should such a distribution exist. For all the group-based models it is not difficult to see that the uniform distribution is the common stationary distribution. Fixing this throughout our model, we can take the Fourier transform of this function.

**Proposition 15.3.16.** Let \( G \) be a finite abelian group and let \( f: G \to \mathbb{C} \) be the constant function \( f(g) = \frac{1}{|G|} \). Then \( \hat{f} \) is the function

\[
\hat{f}(\chi) = \begin{cases} 
1 & \text{if } \chi = id \in \hat{G} \\
0 & \text{otherwise.}
\end{cases}
\]

The consequence for group-based models is the following.

**Corollary 15.3.17.** Let \( G \) be a finite abelian group and \( T \) a rooted tree with \( m \) leaves. In the Fourier coordinates, the Zariski closure of the general group-based model with uniform root distribution is equal to the Zariski closure of the image of the map \( \phi^{G,T} \)

\[
\phi^{G,T}: \mathbb{C}^{|G|\times(|E(T)|)} \to \mathbb{C}^{|G|^m}
\]

\[
\phi^{G,T}((a^e_g)_{e \in E(T), g \in G}) = \left\{ \begin{array}{ll}
\prod_{e \in E(T)} a^e_{\sum_{i \in \lambda(e)} g_i} & \text{if } \sum_{i \in [m]} g_i = id \\
0 & \text{otherwise.}
\end{array} \right.
\]

From here we begin to focus on the other cases where \( f^e(g) \) is not allowed to be a generic function. The main cases of interest are the Jukes-Cantor
model and the Kimura 2-parameter model, but the questions make sense in more general mathematical setting.

For the Jukes-Cantor model we have
\[ f^e(A) = a, \quad f^e(C) = f^e(G) = f^e(T) = b \]
where \( a \) and \( b \) are specific functions of \( \alpha \) and \( t \). Indeed, for the rate matrix \( Q^{JC} \) we have
\[
\exp(Q^{JC} t) = \begin{pmatrix}
\frac{1+3e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} \\
\frac{1-e^{-4t\alpha}}{4} & \frac{1+3e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} \\
\frac{1-e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} & \frac{1+3e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} \\
\frac{1-e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} & \frac{1-e^{-4t\alpha}}{4} & \frac{1+3e^{-4t\alpha}}{4}
\end{pmatrix}.
\]
Computing the Fourier transform of \( f^e(g) \) produces the function
\[ \hat{f}^e(A) = a + 3b, \quad \hat{f}^e(C) = \hat{f}^e(G) = \hat{f}^e(T) = a - b. \]
As \( a + 3b \) and \( a - b \) are algebraically independent, we can treat these quantities as free parameters, so that the resulting model is still parametrized by a monomial map, akin to that in Corollary 15.3.17 but with the added feature that for each \( e \in E(T) \) \( a^e_C = a^e_G = a^e_T \). This has the consequence that there will exist pairs of tuples of group elements \((g_1, \ldots, g_m) \neq (h_1, \ldots, h_m)\) such that \( \hat{p}(g_1, \ldots, g_m) = \hat{p}(h_1, \ldots, h_m) \). The resulting linear polynomial constraints on the phylogenetic model are called linear invariants.

**Example 15.3.18.** Consider the tree from Figure 15.3.1 under the Jukes-Cantor model with the uniform root distribution. We use the indeterminates \( q_{AAA}, \ldots, q_{TTT} \) to denote coordinates on the image space. Then, for example
\[ q_{CGT} = a^1_C a^2_G a^3_T a^e_C = a^1_C a^2_C a^3_C a^e_C \]
and
\[ q_{GTC} = a^1_G a^2_T a^3_C a^e_G = a^1_C a^2_C a^3_C a^e_C \]
so \( q_{CGT} = q_{GTC} \) is a linear invariant for the Jukes-Cantor model on this three leaf tree.

A similar analysis can be run for the Kimura 2-parameter model to show that it is also a toric variety [SS05]. Analysis of the conditions on the functions \( f^e(g) \) that yield to toric varieties in the Fourier coordinates appears in [Mic11].

To conclude this section, we note one further point about the parametrizations in the case where \( G \) is a group with the property that every element is its own inverse (e.g. \( \mathbb{Z}_2 \) and \( \mathbb{Z}_2 \times \mathbb{Z}_2 \)). If \( G \) satisfies this property and we
are working with the model with uniform root distribution, we can pass to an unrooted tree and the parametrization can be written as:

$$
\phi^{G,T}_{g_1,\ldots,g_m}((a^A_B)_{A \in \Sigma(T), B \in G}) = \begin{cases} 
\prod_{A \in \Sigma(T), B \in G} a^A_B & \text{if } \sum_{i \in [m]} g_i = \text{id} \\
0 & \text{otherwise.}
\end{cases}
$$

The reason we can ignore the root in this case is because if $$\sum_{i \in [m]} g_i = \text{id}$$ then $$\sum_{a \in A} g_i = \sum_{i \in B} g_i$$ for groups with the property that every element is its own inverse. This can be a useful alternate representation of the parametrization which allows us to work with nonrooted trees.

15.4. The General Markov Model

As discussed previously, the general Markov model is the phylogenetic model that arises as the hidden variable graphical model on a rooted directed tree, where all vertices have random variables with the same number of states, $$\kappa$$, and all of the non-leaf vertices are hidden variables. While this model is not so widely used in phylogenetic practice, it does contain all the other models discussed in Section 15.2 as submodels and so statements that can be made about this model often carry over to the other models. Furthermore, the general Markov model has nice mathematical properties that make it worthwhile to study. We highlight some of the mathematical aspects here.

A first step in analyzing the general Markov model on a tree is that we can eliminate any vertex of degree two from our tree. Furthermore, we can relocate the root to any vertex in the tree that we wish, without changing the family of probability distributions that arises. Often, then, the combinatorics can be considered only in terms of the underlying unrooted tree alone.

**Proposition 15.4.1.** Let $$T_1$$ and $$T_2$$ be rooted trees with the same underlying undirected tree. Then under the general Markov model $$M_{GMM}^{T_1} = M_{GMM}^{T_2}$$.

**Proof.** To see why this is so, we just need to recall results about graphical models from Chapter 13. First to see that we can move the root to any vertex of the tree without changing the underlying distribution, we use Theorem 13.1.14 which characterizes the directed graphical models with all variables observed that yield the same family of probability distributions. Once we fix the underlying undirected graph to be a tree, choosing any node as the root, yields a new directed tree with the same unshielded colliders (namely, there are no unshielded colliders). Since they give the same probability distributions when all vertices are observed, they will give the same probability distributions after marginalizing the internal nodes. □

**Proposition 15.4.2.** Let $$T$$ and $$T'$$ be two rooted trees where $$T'$$ is obtained from $$T$$ by suppressing a vertex of degree 2. Then $$M_{GMM}^{T'} = M_{GMM}^{T}$$.
Proof. From Proposition 15.4.1, we can assume that the vertex of degree 2 is not the root. Let $v$ be this vertex. We consider what happens locally when we marginalize just the random variable $X_v$. Note that because the underlying graph is a tree, it will appear in the distribution a sequence of random variables $Y \rightarrow X_v \rightarrow Z$ and since the vertex has degree 2, these are the only edges incident to $X_v$. So, in the joint distribution for all the random variables in the tree will appear the product of conditional distribution $P(X_v = x|Y = y)P(Z = z|X_v = x)$. Since we consider the general Markov model, each of these conditional distributions is an arbitrary stochastic $\kappa \times \kappa$ matrix. Summing out over $x$, produces an arbitrary stochastic matrix which represents the conditional probability $P(Z = z|Y = y)$. Thus, marginalizing this one variable produces the same distribution family as the fully observed model on $T'$. This proves the proposition. \hfill \Box

Perhaps the best known results about the algebraic structure of the general Markov model concerns the case when $\kappa = 2$. The vanishing ideal is completely characterized in this case, combining results of Allman and Rhodes [AR08] and Raicu [Rai12]. To explain these results we introduce some results about flattenings of tensors.

Let $P \in \mathbb{C}^{r_1} \otimes \mathbb{C}^{r_2} \otimes \cdots \otimes \mathbb{C}^{r_m}$ be an $r_1 \times r_2 \times \cdots \times r_m$ tensor. Let $A|B$ be a split of $[m]$. We can naturally regroup the tensor product space as

$$
\left( \bigotimes_{a \in A} \mathbb{C}^{r_a} \right) \otimes \left( \bigotimes_{b \in B} \mathbb{C}^{r_b} \right)
$$

and consider $P$ inside of this space. This amounts to considering $P$ as a $\prod_{a \in A} r_a \times \prod_{b \in B} r_b$ matrix. The resulting matrix is called the flattening of $P$ and is denoted $\text{Flat}_{A|B}(P)$.

Example 15.4.3. Suppose that $\kappa = r_1 = r_2 = r_3 = r_4 = 2$, and let $A|B = \{1, 3\}|\{2, 4\}$. Then

$$
\text{Flat}_{13|24}(P) = 
\begin{pmatrix}
  p_{1111} & p_{1112} & p_{1211} & p_{1212} \\
  p_{1121} & p_{1122} & p_{1221} & p_{1222} \\
  p_{2111} & p_{2112} & p_{2211} & p_{2212} \\
  p_{2121} & p_{2122} & p_{2221} & p_{2222}
\end{pmatrix}.
$$

In Section 15.1, we introduced the set of splits $\Sigma(T)$ of a tree $T$. For the purposes of studying phylogenetic invariants of the general Markov model, it is also useful to extend this set slightly for nonbinary trees. Define $\Sigma'(T)$ to be the set of all splits of the leaf set of a tree that could be obtained by resolving vertices of degree $> 3$ into vertices of lower degree. For example, if $T$ is a star tree with one internal vertex and $m$ leaves, then $\Sigma'(T)$ will consist of all splits of $[m]$. 

Proposition 15.4.4. Let $T$ be a tree and let $\mathcal{M}_T$ be the phylogenetic model under the general Markov model with random variables of $\kappa$ states. Then for any $A|B \in \Sigma'(T)$, and any $P \in \mathcal{M}_T$

$$\text{rank Flat}_{A|B}(P) \leq \kappa.$$ 

Thus all $(\kappa+1) \times (\kappa+1)$ minors of $\text{Flat}_{A|B}(P)$ belong to the vanishing ideal of $\mathcal{M}_T$. Furthermore, if $A|B \notin \Sigma'(T)$ then for generic $P \in \mathcal{M}_T$

$$\text{rank Flat}_{A|B}(P) \geq \kappa^2.$$

Proof. Recall that we can subdivide an edge in the tree and make the new internal node of degree 2 the root vertex (directed all other edges away from this edge). Since the underlying graph of our model is a tree, the joint distribution of states at the leaves can be expressed as

$$(15.4.1) \quad P_{i_1...i_m} = \sum_{j=1}^{\kappa} \pi_j F(j, i_A) G(j, i_B)$$

where $F(j, i_A)$ is the function obtained by summing out over all the hidden variables between the root node and the set of leaves $A$, and $G(j, i_B)$ is the function obtained by summing out over all the hidden variables between the root node and the set of leaves $B$. Let $F$ denote the resulting $\kappa|A| \times \kappa$ matrix that is the flattening of this tensor and similarly let $G$ denote the resulting $\kappa \times \kappa|B|$ matrix. Then Equation 15.4.1 can be expressed in matrix form as:

$$\text{Flat}_{A|B}(P) = F \text{diag}(\pi) G,$$

which shows that $\text{rank Flat}_{A|B}(P) \leq \kappa$.

For the second part of the theorem, note that it suffices to find a single $P \in \mathcal{M}_T$ such that $\text{rank Flat}_{A|B}(P) > \kappa$. This is because the set of matrices with $\text{rank Flat}_{A|B}(P) \leq P$ is closed. So suppose that $A|B \notin \Sigma'(T)$. This means that there exists another split $C|D \in \Sigma(T)$ such that $A|B$ and $C|D$ are incompatible. Note that since $C|D \in \Sigma(T)$ that split actually corresponds to an edge in $T$ (whereas splits in $\Sigma'(T)$ need not correspond to edges in $T$. We construct the distribution $P$ as follows. Set all parameters on all edges besides the one corresponding to the edge $C|D$ to the identity matrix. Set the transition matrix corresponding to the edge $C|D$ to be a generic matrix $\alpha \in \Delta_{\kappa^2-1}$. The resulting joint distribution $P$ has the following form:

$$P(i) = \begin{cases} 
\alpha_{jk} & \text{if } i_c = j \text{ and } i_d = k \text{ for all } c \in C, d \in D \\
0 & \text{otherwise}
\end{cases}$$

Since $A|B$ and $C|D$ are not compatible this means that none of $A \cap C$, $A \cap D$, $B \cap C$, nor $B \cap D$ are empty. Now form the submatrix of $M$ of $\text{Flat}_{A|B}(P)$ whose row indices consists of all tuples $i_A$ such that $i_{A \cap C}$ and $i_{A \cap D}$ are constant, and whose column indices consist of all tuples $i_B$ such
that $i_{B\cap C}$ and $i_{B\cap D}$ are constant. The matrix $M$ will be a $\kappa^2 \times \kappa^2$ matrix which has one nonzero entry in each row and column. Such a matrix has rank $\kappa^2$, which implies that $\text{Flat}_{A|B}(P) \geq \kappa^2$. □

A strengthening of the second part of Proposition 15.4.4 due to Eriksson [Eri05] shows how the rank of $\text{Flat}_{A|B}(P)$ could be even larger if the split $A|B$ violates many splits in $\mathcal{T}$.

**Theorem 15.4.5.** [AR08, Rai12] Consider the general Markov model on a tree $\mathcal{T}$ and suppose that $\kappa = 2$. Then the homogeneous vanishing ideal of $\mathcal{M}_{\mathcal{T}}$ is generated by all the $3 \times 3$ minors of all flattenings $\text{Flat}_{A|B}(P)$ for $A|B \in \Sigma'(\mathcal{T})$:

$$I^h(\mathcal{M}_{\mathcal{T}}) = \sum_{A|B \in \Sigma'(\mathcal{T})} \langle 3 \times 3 \text{ minors of } \text{Flat}_{A|B}(P) \rangle \subseteq \mathbb{R}[P].$$

**Example 15.4.6.** Consider the unrooted tree with 5 leaves in Figure 15.4.1

This tree has two nontrivial splits 14|235 and 25|134. The homogeneous vanishing ideal $I^h(\mathcal{M}_{\mathcal{T}}) \subseteq \mathbb{R}[p_{i_1i_2i_3i_4i_5} : i_1, i_2, i_3, i_4, i_5 \in \{0, 1\}]$ is generated by the $3 \times 3$ minors of the following matrices:

$$\text{Flat}_{14|235}(P) = \begin{pmatrix} p_{00000} & p_{00001} & p_{00100} & p_{00101} & p_{01000} & p_{01001} & p_{01100} & p_{01101} \\ p_{00001} & p_{00011} & p_{01100} & p_{01101} & p_{01000} & p_{01001} & p_{01100} & p_{01101} \\ p_{10000} & p_{10001} & p_{10100} & p_{10101} & p_{10010} & p_{10011} & p_{11000} & p_{11001} \\ p_{10001} & p_{10011} & p_{10100} & p_{10101} & p_{10110} & p_{10111} & p_{11010} & p_{11011} \\ p_{10100} & p_{10101} & p_{11000} & p_{11001} & p_{11010} & p_{11011} & p_{11100} & p_{11101} \\ p_{10101} & p_{10111} & p_{11010} & p_{11011} & p_{11100} & p_{11101} & p_{11110} & p_{11111} \end{pmatrix}$$

$$\text{Flat}_{25|134}(P) = \begin{pmatrix} p_{00000} & p_{00001} & p_{00100} & p_{00101} & p_{01000} & p_{01001} & p_{01100} & p_{01101} \\ p_{00001} & p_{00011} & p_{01100} & p_{01101} & p_{01000} & p_{01001} & p_{01100} & p_{01101} \\ p_{01000} & p_{01001} & p_{01100} & p_{01101} & p_{10000} & p_{10001} & p_{10010} & p_{10011} \\ p_{01001} & p_{01011} & p_{01110} & p_{01111} & p_{10001} & p_{10011} & p_{10100} & p_{10101} \\ p_{01100} & p_{01101} & p_{01110} & p_{01111} & p_{10100} & p_{10101} & p_{10110} & p_{10111} \\ p_{01101} & p_{01111} & p_{10100} & p_{10101} & p_{10110} & p_{10111} & p_{11100} & p_{11101} \end{pmatrix}. $$

Allman and Rhodes [AR08] proved Theorem 15.4.5 in the case of binary trees and Raicu [Rai12] proved the theorem in the case of star trees.
The Allman-Rhodes-Draisma-Kuttler theorem, to be explained in the next section, shows that it suffices to prove the theorem in the case of star trees to get the result for general (nonbinary) trees.

It remains an open problem to describe the vanishing ideal of the general Markov model for larger $\kappa$. For the three leaf star tree and $\kappa = 4$, a specific set of polynomials of degree 5, 6, and 9 are conjectured to generate the vanishing ideal. While some progress has been made using numerical techniques to prove that these equations described the variety set-theoretically \cite{BO11, FG12} or even ideal theoretically \cite{DH16} it remains an open problem to give a symbolic or theoretical proof of this fact.

Besides the vanishing ideal of the general Markov model, a lot is also known about the semialgebraic structure of these models. For example, the paper \cite{ART14} gives a semialgebraic description of the general Markov model for all $\kappa$ (assuming the vanishing ideal is known) for the set of all distributions that can arise assuming that the root distribution does not have any zeroes in it and all transition matrices are non-singular matrices. Both of these assumptions are completely reasonable from a biological standpoint.

The paper \cite{ZS12} gave a complete semialgebraic description of the general Markov model in the case that $\kappa = 2$. While the techniques of that paper do not seem to extend to handle larger values of $\kappa$, the methods introduced there extend to other models on binary random variables and are worthwhile to study for these reasons. In some sense, the idea is similar to what has been done for group-based models above, namely make a coordinate change that simplifies the parametrization. In the case of the general Markov model, the coordinate change is a nonlinear change of coordinates that changes to cumulant coordinates (or what Zwiernik and Smith call tree cumulants). Here we focus on ordinary cumulants and their algebraic geometric interpretation (as studied in \cite{SZ13}).

For binary random variables (with state space $\{0, 1\}^m$) we encode the distribution by its probability generating function

$$P(x_1, \ldots, x_m) = \sum_{I \subseteq [m]} p_I \prod_{i \in I} x_i.$$ 

Here $p_I$ denotes the probability that $X_i = 1$ for $i \in I$ and $X_i = 0$ for $i \notin I$. The moment generating function of this distribution is

$$M(x_1, \ldots, x_m) = P(1 + x_1, \ldots, 1 + x_m) = \sum_{I \subseteq [m]} \mu_I \prod_{i \in I} x_i.$$ 

The logarithm of the moment generating function gives the cumulants:

$$K(x_1, \ldots, x_m) = \sum_{I \subseteq [m]} k_I \prod_{i \in I} x_i = \log M(x_1, \ldots, x_m).$$
This power series expansion is understood to be modulo the ideal \( \langle x_1^2, \ldots, x_m^2 \rangle \) so that we only keep the squarefree terms. The coefficients \( k_I \) for \( I \subseteq [m] \) are called the cumulants of the binary random vector \( X \).

It is known how to write an explicit formula for the cumulants in terms of the moments:

\[
k_I = \sum_{\pi \in \Pi(I)} (-1)^{|\pi| - 1}(|\pi| - 1)! \prod_{B \in \pi} \mu_B
\]

where \( \Pi(I) \) denotes the lattice of set partitions of the set \( I \), \( |\pi| \) denotes the number of blocks of the partition \( I \), and \( B \in \pi \) denotes the blocks of \( \pi \). For example

\[
k_i = \mu_i, \quad k_{ij} = \mu_{ij} - \mu_i \mu_j, \quad k_{ijk} = \mu_{ijk} - \mu_i \mu_{jk} - \mu_j \mu_{ik} - \mu_k \mu_{ij} + 2 \mu_i \mu_j \mu_k.
\]

We use the cumulant transformation to analyze the three leaf claw tree under the general Markov model with \( \kappa = 2 \). This is, of course, the same model as the \( \text{Mixt}^2(\mathcal{M}_{X_1 \perp X_2 \perp X_3}) \). Since the passage from the probability generating function to the moment generating function is linear, we can compute this first for the model \( \mathcal{M}_{X_1 \perp X_2 \perp X_3} \) and then pass to the mixture model. However, it is easy to see directly that the moment generating function for the complete independence model is

\[
(1 + \mu_1 x_1)(1 + \mu_2 x_2)(1 + \mu_3 x_3).
\]

Passing to the secant variety, we have the moment generating function of \( \text{Mixt}^2(\mathcal{M}_{X_1 \perp X_2 \perp X_3}) \) as

\[
1 + (\pi_0 \mu_{01} + \pi_1 \mu_{11})x_1 + (\pi_0 \mu_{02} + \pi_1 \mu_{12})x_2 + (\pi_0 \mu_{03} + \pi_1 \mu_{13})x_3
\]

\[
+ (\pi_0 \mu_{01} \mu_{02} + \pi_1 \mu_{11} \mu_{12})x_1 x_2 + (\pi_0 \mu_{01} \mu_{03} + \pi_1 \mu_{11} \mu_{13})x_1 x_3
\]

\[
+ (\pi_0 \mu_{02} \mu_{03} + \pi_1 \mu_{12} \mu_{13})x_2 x_3 + (\pi_0 \mu_{01} \mu_{02} \mu_{03} + \pi_1 \mu_{11} \mu_{12} \mu_{13})x_1 x_2 x_3.
\]

Then we pass to the cumulants. We have

\[
k_i = \mu_i = (\pi_0 \mu_{0i} + \pi_1 \mu_{1i})
\]

\[
k_{ij} = \mu_{ij} - \mu_i \mu_j = \pi_0 \pi_1 (\mu_{0i} - \mu_{1i})(\mu_{0j} - \mu_{1j})
\]

\[
k_{123} = -\pi_0 \pi_1 (\pi_0 - \pi_1)(\mu_{01} - \mu_{11})(\mu_{02} - \mu_{12})(\mu_{03} - \mu_{13}).
\]

From this we see that

\[
k_{123}^2 + 4k_{12}k_{13}k_{23} = \pi_0^2 \pi_1^2 (\mu_{01} - \mu_{11})^2(\mu_{02} - \mu_{12})^2(\mu_{03} - \mu_{13})^2
\]

and in particular is nonnegative.

**Proposition 15.4.7.** Let \( p \) be a distribution coming from the three leaf trivalent tree under the general Markov model with \( \kappa = 2 \). Then the cumulants satisfy the inequality:

\[
k_{123}^2 + 4k_{12}k_{13}k_{23} \geq 0.
\]
This inequality together with other obvious inequalities on the model turn out to characterize the distributions that can arise for a three leaf tree under the general Markov model. Similar arguments extend to arbitrary trees where it can be shown that a suitable analogue of the cumulants factorizes into a product. Hence, in cumulant coordinates these models are also toric varieties. This is explored in detail in [ZS12].

15.5. The Allman-Rhodes-Draisma-Kuttler Theorem

The most general tool for constructing generators of the vanishing ideals of phylogenetic models is a theorem of Allman and Rhodes [AR08] and Draisma and Kuttler [DK09] which allows one to reduce the determination of the ideal generators to the case of star trees. This result holds quite generally in the algebraic setting, for models that are called equivariant phylogenetic models. These models include the group-based models, the general Markov model, and the strand symmetric model. The full version of the result was proven by Draisma and Kuttler [DK09] based on significant partial results that appeared in earlier papers for group-based models [SS05], the general Markov model [AR08] and the strand symmetric model [CS05]. In particular, the main setup and many of the main ideas already appeared in [AR08] and for this reason we also credit Allman and Rhodes with this theorem. We outline this main result and the idea of the proof in this section.

Theorem 15.5.1. Let $\mathcal{T}$ be a tree and $\mathcal{M}_\mathcal{T}$ the model of a equivariant phylogenetic model on $\mathcal{T}$. Then the homogeneous vanishing ideal of $\mathcal{M}_\mathcal{T}$ is a sum

$$I(\mathcal{M}_\mathcal{T}) = \sum_{e \in E(\mathcal{T})} I_e + \sum_{v \in \text{Int}(\mathcal{T})} I_v$$

where $I_e$ and $I_v$ are certain ideals associated to flattenings along edges and vertices of $\mathcal{T}$ respectively.

In the case of the general Markov model, the $I_e$ ideals are generated by the $(\kappa + 1) \times (\kappa + 1)$ minors of the flattening matrix $\text{Flat}_{AB}(P)$ associated to the edge $e$. In the case of binary trees, the ideals $I_e$ correspond to flattening to 3-way tensors associated to the three-way partition from a vertex $v$ and the requirement that that 3-way tensor have rank $\leq \kappa$. For the other equivariant models, similar types of statements hold though we refer the reader to the references above for the precise details.

The main tool to prove Theorem 15.5.1 is a gluing lemma, which we describe in some detail for the case of the general Markov model. Let $\mathcal{M}_\mathcal{T}$ be a phylogenetic model and let $V_\mathcal{T}$ be the corresponding projective variety (obtained by looking at the cone over $\mathcal{M}_\mathcal{T}$). We assume that $\mathcal{T}$ has $m$
leaves. This variety sits naturally inside of the projective space over the
tensor produce space $P(C^\kappa \otimes \cdots \otimes C^\kappa)$. The product of general linear groups $Gl^n_\kappa$ naturally acts on the vector space $C^\kappa \otimes \cdots \otimes C^\kappa$ with each copy of $Gl_\kappa$ acting on one coordinate. Explicitly on tensors of rank one:

$$(M_1, \ldots, M_m) \cdot a_1 \otimes \cdots \otimes a_m = M_1a_1 \otimes \cdots \otimes M_ma_m.$$  

Proposition 15.5.2. The variety $V_T \subseteq P(C^\kappa \otimes \cdots \otimes C^\kappa)$ is fixed under the action of $Gl^n_\kappa$.

Proof. On the level of the tree distribution, multiplying by the matrix $M_i$ at the $i$th leaf is equivalent to adding a new edge $i \to i'$ with $i$ now being a hidden variable and $i'$ the new leaf, and $M_i$ the matrix on this edge. Since we can contract vertices of degree two without changing the model (Proposition 15.4.2), this gives us the same family of probability distributions, and hence the same variety $V_T$. □

Now let $T_1$ and $T_2$ be two trees, and let $T_1 \ast T_2$ denote the new tree obtained by gluing these two trees together at a leaf vertex in both trees. A specific vertex must be chosen on each true to do this, but we leave the notation ambiguous. This is illustrated in Figure 15.5.1. Suppose that $T_i$ has $m_i$ leaves for $i = 1, 2$. As in the proof of Proposition 15.4.4, we note that any distribution on the tree $T_1 \ast T_2$ could be realized by taking a distribution $P_1$ for the tree $T_1$, and $P_2$ for the tree $T_2$, flattening the first distribution down to a $\kappa^{m_1-1} \times \kappa$ matrix, flattening the second distribution down to a $\kappa^{m_2-1}$ matrix, and forming the matrix product $P_1P_2$. The resulting $\kappa^{m_1-1} \times \kappa^{m_2-1}$ matrix is an element of $V_{T_1 \ast T_2}$. Clearly that matrix has rank $\leq \kappa$ by Proposition 15.4.4 which tells us some equations in the vanishing ideal $I(V_{T_1 \ast T_2})$. Lemma 15.5.4 shows that all generators for $I(V_{T_1 \ast T_2})$ can be recovered from these minors plus equations that come from $I(V_{T_1})$ and $I(V_{T_2})$. We state this result in some generality.

Definition 15.5.3. Let $V \subseteq P(C^r_1 \otimes C^s)$ and $W \subseteq P(C^r_2 \otimes C^s)$ be projective varieties. The matrix product variety is the variety of $V$ and $W$ is

$$V \ast W = \{v \cdot w : v \in V, w \in W\}$$
where $v \cdot w$ denotes the product of the $r_1 \times \kappa$ matrix, $v$, and $\kappa \times r_2$ matrix, $w$.

**Lemma 15.5.4.** Let $V \subseteq \mathbb{P}(\mathbb{C}^{r_1} \otimes \mathbb{C}^\kappa)$ and $W \subseteq \mathbb{P}(\mathbb{C}^\kappa \otimes \mathbb{C}^{r_2})$ be projective varieties. Suppose that both $V$ and $W$ are invariant under the action of $\text{Gl}_\kappa$ (acting as right matrix multiplication of $V$ and left matrix multiplication on $W$). Then

$$\mathcal{I}(V \star W) = ((\kappa + 1) \times (\kappa + 1) \text{ minors of } P) + \text{Lift}(\mathcal{I}(V)) + \text{Lift}(\mathcal{I}(W)).$$

The lifting operation $\text{Lift}(\mathcal{I}(V))$ is defined as follows. Introduce a matrix of indeterminates $Z$ of size $r_2 \times \kappa$. The resulting matrix $PZ$ has size $r_1 \times \kappa$. Take any generator $f \in \mathcal{I}(V)$ and form the polynomial $f(PZ)$ and extract all coefficients of all monomials in $Z$ appearing in that polynomial. The resulting set of polynomials that arises is $\text{Lift}(\mathcal{I}(V))$ as we range over all generators for $\mathcal{I}(V)$. An analogous construction defines the elements of $\text{Lift}(\mathcal{I}(W))$. Note that the proof of Lemma 15.5.4 depends on some basic constructions of classical invariant theory (see [DK02]).

**Proof of Lemma 15.5.4.** We clearly have the containment $\subseteq$, so we must show the reverse containment. Let $f \in \mathcal{I}(V \star W)$. Since $((\kappa + 1) \times (\kappa + 1) \text{ minors of } P) \subseteq \mathcal{I}(V \star W)$, we can work modulo this ideal. This has the effect of plugging in $P = YZ$ in the polynomial $f$ where $Y$ is a $r_1 \times \kappa$ matrix of indeterminates and $Z$ is a $\kappa \times r_2$ matrix of indeterminates. The resulting polynomial $f(YZ)$ satisfies

$$f(YZ) \in \mathcal{I}(V) + \mathcal{I}(W) \subseteq \mathbb{C}[Y, Z]$$

by construction. We can explicitly write

$$f(YZ) = h_1(Y, Z) + h_2(Y, Z)$$

where $h_1 \in \mathcal{I}(V)$ and $h_2 \in \mathcal{I}(W)$.

Now both the varieties $V$ and $W$ are invariant under the action of $\text{Gl}_\kappa$ on the left and right, respectively. We let $\text{Gl}_\kappa$ act on $V \times W$ by acting by multiplication by $g$ on $V$ and by $g^{-1}$ on $W$, with the corresponding action on the polynomial ring $\mathbb{C}[Y, Z]$. The First Fundamental Theorem of Classical Invariant Theory says that when $\text{Gl}_\kappa$ acts this way on the polynomial ring $\mathbb{C}[Y, Z]$, the invariant ring is generated by the entries of $YZ$.

Apply the Reynolds operator $\rho$ with respect to the action of $\text{Gl}_\kappa$ to the polynomial $f(YZ)$. This produces

$$\rho(f)(YZ) = \rho(h_1)(Y, Z) + \rho(h_2)(Y, Z)$$

$$f(YZ) = \tilde{h}_1(YZ) + \tilde{h}_2(YZ).$$

The Reynolds operator produces $\tilde{h}_1(YZ)$ $\tilde{h}_2(YZ)$ which necessarily belong to the invariant ring $\mathbb{C}[YZ]$. Clearly, $f(YZ)$ is already in the invariant ring.
with respect to the action of $Gl_\kappa$ so it remains unchanged. The polynomials $h_1(YZ)$ and $h_2(YZ)$ are now in the invariant ring, so this means we can lift these polynomials to polynomials $h'_1(P)$ which is in the ideal generated by Lift($I(V)$) and $h'_2(P)$ which is in the ideal generated by Lift($I(W)$). But then $f - h'_1 - h'_2$ is a polynomial which evaluates to zero when we plug in $P = YZ$. This implies that $f - h'_1 - h'_2$ is in the ideal generated by the $(\kappa + 1) \times (\kappa + 1)$ minors of $P$, which completes the proof. □

To apply Lemma 15.5.4 to deduce Theorem 15.5.1 one successively breaks the trees into smaller and smaller pieces, gluing together a large tree out of a collection of star trees. One only needs to verify that the lift operation turns determinants into determinants, and preserves the structure of the ideal associated to internal vertices of the trees. See [DK09] for details.

15.6. Exercises

Exercise 15.1. Check that the stationary distributions of the CFN, JC69, K2P, and K3P models are uniform, and that the stationary distributions of the F81 and HKY models are $(\pi_A, \pi_C, \pi_G, \pi_T)$.

Exercise 15.2. Show that the F81 model is a Lie Markov model, but that the HKY model is not a Lie Markov model.

Exercise 15.3. Prove the analogue of Proposition 15.4.1 for group-based models.

Exercise 15.4. Compute phylogenetic invariants for the CFN model with uniform root distribution on a five leaf binary tree in both Fourier coordinates and probability coordinates.

Exercise 15.5. Consider the Jukes-Cantor model on an $m$-leaf binary tree $T$ with uniform root distribution. Show that the number of linearly independent linear invariants for this model is $4^m - F_{2m}$ where $F_k$ denotes the $k$th Fibonacci number $F_0 = 1, F_1 = 1, F_{k+1} = F_k + F_{k-1}$. That is, the number of distinct nonzero monomials that arise in the parametrization is $F_{2m}$.

Exercise 15.6. Let $G$ be an undirected graph, $H \sqcup O$ a partition of the vertices into hidden and observed variables, and $A|B$ a split of the observed variables. Let $P \in \mathcal{M}_G$ be a distribution from the graphical model on the observed variables. What can be said about the rank of $\text{Flat}_{A|B}(P)$ in terms of the combinatorial structure of the graph and the positioning of the vertices of $A$ and $B$?

Exercise 15.7. Generalize Proposition 15.4.4 to mixture models $\text{Mixt}^k(\mathcal{M}_T)$ over the general Markov model.
Exercise 15.8. Consider the general Markov model with $\kappa = 2$ on an $m$ leaf star tree. How does the parametrization of this model look like in the cumulant coordinates? What sort of equalities and inequalities arise for this model?
Identifiability

A model is identifiable if all of the model parameters can be recovered from the underlying observables of the model. Recall that a statistical model is a map \( p : \Theta \rightarrow P, \theta \mapsto p_\theta \). This statistical model is identifiable if \( \theta \) can be recovered from \( p_\theta \); that is, the mapping is one-to-one. Identifiability is an important property for a statistical model to have if the model parameters have special meaning for the data analysis. For example, in phylogenetic models the underlying rate matrices of the model tell how quickly or slowly evolution happened along a particular edge of the tree and the goal of a phylogenetic analysis is to recover those mutation rates/branch lengths. If a model is not identifiable, and we care about recovering information about the specific values of the parameters from data, there is no point in doing data analysis with such a model. Identifiability problems are often most difficult, and of most practical interest, in cases where there are hidden variables in the models.

Since the mappings that arise for many of these statistical models can be seen as polynomial mappings, identifiability of a statistical model often is equivalent to the injectivity of a polynomial or rational map. Hence, techniques from computational algebra and algebraic geometry can be used to decide the identifiability of these models. Another common features is that models might have both continuous and discrete parameters. For example, in a phylogenetic model, the continuous parameters are the mutation rates/branch lengths, and the discrete parameter is the underlying tree. Identifiability of parameters of both of these types can be addressed using algebraic tools.

Identifiability analysis has been one of the successful areas where tools from algebra have been applied to the study of statistical models. In this
chapter we give an overview of these methods, as well as a number of applications highlighting the methods’ applicability. We also discuss identifiability of dynamical systems models (i.e. ordinary differential equations) where similar algebraic techniques are also useful.

16.1. Tools for Testing Identifiability

A statistical model is identifiable if the parameters of the model can be recovered from the probability distributions. There are many variations on this definition and sometimes these distinctions are not so clear in research articles from different sources and in different research areas. We highlight these distinctions here. We also describe some of the basic computational algebra approaches that can be used to test identifiability.

In this chapter we assume throughout that we are working with an algebraic exponential family (see Section 6.5). So the map \( \phi : \Theta \to N \) maps the parameter space \( \Theta \) into (a possibly transformed version of) the natural parameter space \( N \) of an exponential family. We assume that \( \phi \) is a rational map, defined everywhere on \( \Theta \), and that \( \Theta \subseteq \mathbb{R}^d \) is a semialgebraic set of dimension \( d \). The model \( M \) is the image of \( \phi \).

**Definition 16.1.1.** Let \( \phi : \Theta \to N \) be as above, with model \( M = \text{im} \phi \). The parameter vector \( \theta \) is:

- **globally identifiable** if \( \phi \) is a one-to-one map on \( \Theta \);
- **generically identifiable** if \( \phi^{-1}(\phi(\theta)) = \{\theta\} \) for almost all \( \theta \in \Theta \);
- **rationally identifiable** if there is a dense open subset of \( U \subseteq \Theta \) and a rational function \( \psi : N \to \Theta \) such that \( \psi \circ \phi(\theta) = \theta \) on \( U \);
- **locally identifiable** if \( |\phi^{-1}(\phi(\theta))| < \infty \) for almost all \( \theta \in \Theta \);
- **non-identifiable** if \( |\phi^{-1}(\phi(\theta))| > 1 \) for some \( \theta \in \Theta \); and
- **generically non-identifiable** if \( |\phi^{-1}(\phi(\theta))| = \infty \) for almost all \( \theta \in \Theta \).

Note that some of these definitions also have varying names in the literature. Generic identifiability is also called *almost everywhere identifiability*. Local identifiability is sometimes called finite identifiability or algebraic identifiability. Note that the name local identifiability arises from the following alternate interpretation: if a model is locally identifiable then around a generic point \( \theta \) of parameter space, there exists an open neighborhood \( U_\theta \) such that \( \phi : U_\theta \to M \) is identifiable.

**Example 16.1.2.** Consider the independence model \( M_{X_1 \perp \perp X_2} \). This model is defined parametrically via the map

\[
\phi : \Delta_{r_1-1} \times \Delta_{r_2-1} \to \Delta_{r_1 r_2-1}, \quad (\alpha, \beta) \mapsto \alpha \beta^T.
\]
The independence model is globally identifiable because it is possible to recover \( \alpha \) and \( \beta \) from the probability distribution \( p = \alpha \beta^T \). Indeed
\[
\alpha_i = \sum_j p_{ij} \quad \text{and} \quad \beta_j = \sum_i p_{ij}
\]
for \( p \in \mathcal{M}_{X_1 \perp \perp X_2} \).

Also these formulas to recover the parameters are rational functions so the parameters are rationally identifiability as well.

**Example 16.1.3.** Consider the mixture model \( \text{Mixt}^k(\mathcal{M}_{X_1 \perp \perp X_2}) \). The number of parameters of this model is
\[
k(r_1 + r_2 - 2) + k - 1 = k(r_1 + r_2 - 1) - 1.
\]
This count arises by picking \( k \) points on the model \( \mathcal{M}_{X_1 \perp \perp X_2} \) which has dimension \( r_1 + r_2 - 2 \), and then a distribution \( \pi \in \Delta_{k-1} \) for the mixing weights.

On the other hand, the model \( \text{Mixt}^k(\mathcal{M}_{X_1 \perp \perp X_2}) \) is contained inside the set of probability distributions that are rank \( \leq k \) matrices. The dimension of this set can be calculated as
\[
k(r_1 + r_2 - k) - 1.
\]
Since the number of parameters of the model is less than the dimension of the model (when \( k > 1 \)) we see that this model is generically non-identifiable.

**Example 16.1.4.** Consider the 1-factor model \( F_{m,1} \) introduced in Example 6.5.4. This consists of all covariance matrices that are diagonal plus a rank one matrix:
\[
F_{m,1} = \{ \Omega + \lambda \lambda^T \in PD_m : \Omega > 0 \text{ is diagonal, and } \lambda \in \mathbb{R}^m \}.
\]
Here \( \Omega > 0 \) means \( \Omega \) is positive definite, i.e. it has all positive entries along the diagonal. Our parametrization map is \( \phi : \mathbb{R}^m_{>0} \times \mathbb{R}^m \to PD_m \) with
\[
\phi_{ij}(\omega, \lambda) = \begin{cases} 
\lambda_i \lambda_j & \text{if } i \neq j \\
\omega_i + \lambda_i^2 & \text{if } i = j.
\end{cases}
\]
Clearly \( \phi \) is not a one-to-one map since \( \phi(\omega, \lambda) = \phi(\omega, -\lambda) \) but perhaps this is the only thing that can go wrong.

Let \( \Sigma \in F_{m,1} \). Suppose that \( i \neq j \neq k \) and \( \sigma_{jk} \neq 0 \) then
\[
\frac{\sigma_{ij}\sigma_{ik}}{\sigma_{jk}} = \frac{\lambda_i \lambda_j \lambda_i \lambda_k}{\lambda_j \lambda_k} = \lambda_i^2
\]
giving two choices for \( \lambda_i \). If this value is not zero, once we make a choice of \( \pm \lambda_i \) the entry \( \sigma_{ij} = \lambda_i \lambda_j \) can be used to solve for \( \lambda_j \). Further more, we can solve for \( \omega_i \) via
\[
\omega_i = \sigma_{ii} - \frac{\sigma_{ij}\sigma_{ik}}{\sigma_{jk}}.
\]
This implies that the map $\phi$ parametrizing the 1-factor model is generically 2-to-1.

Note however, that model parameters are non-identifiable in this case, even if we restrict to require $\lambda \geq 0$ (in which case the map becomes generically 1-to-1). This is because there are some parameter choices $\theta$ where the preimage jumps in dimension, i.e. if $\lambda = 0$, then $\phi(\omega, 0)$ is a diagonal matrix. But there are many choices of $\lambda$ and changes to $\omega$ that could yield the same diagonal covariance matrix. For example, if we take $\lambda' = (\lambda_1, 0, 0, \ldots, 0)$, and set $\omega' = (\omega_1 - \lambda_2^2, \omega_2, \ldots, \omega_m)$ then $\phi(\omega, 0) = \phi(\omega', \lambda')$. This gives an (at least) one dimensional set that has the same image as the pair $(\omega, 0)$.

Often we might have a model that is (generically) non-identifiable but we might be interested in whether some individual parameters of the model are identifiable. For example, in the 1-factor model from Example 16.1.4 the $\omega_i$ parameters are generically identifiable while the $\lambda_i$ parameters are locally identifiable. We formalize this in a definition.

**Definition 16.1.5.** Let $\phi : \Theta \to N$ be as above, with model $M = \text{im}\phi$. Let $s : \theta \to \mathbb{R}$ be another function, called a *parameter*. We say the parameter $s$ is

- **identifiable** from $\phi$ if for all $\theta, \theta'$ such that $\phi(\theta) = \phi(\theta')$, $s(\theta) = s(\theta')$;
- **generically identifiable** from $\phi$ if there is a dense open subset $U \subseteq \theta$ such that $s$ is identifiable from $\phi$ on $U$;
- **rationally identifiable** from $\phi$ if there is a rational function $\psi : N \to \mathbb{R}$ such that $\psi \circ \phi(\theta) = s(\theta)$ almost everywhere;
- **locally identifiable** from $\phi$ if for almost all $\theta \in \Theta$ the set $\{s(\theta') : \phi(\theta) = \phi(\theta')\}$ is finite;
- **non-identifiable** from $\phi$ if there exists a $\theta, \theta' \in \Theta$ such that $\phi(\theta) = \phi(\theta')$ but $s(\theta) \neq s(\theta')$; and
- **generically non-identifiable** from $\phi$ if for almost all $\theta \in \Theta$, $|\{s(\theta') : \phi(\theta) = \phi(\theta')\}| = \infty$.

**Example 16.1.6.** Consider the instrumental variables model from Example 14.2.15 on the graph with a bidirected edge. The parametrization for this model has the form:

$$
\begin{pmatrix}
\sigma_{11} & \sigma_{12} & \sigma_{13} \\
\sigma_{12} & \sigma_{22} & \sigma_{23} \\
\sigma_{13} & \sigma_{23} & \sigma_{33}
\end{pmatrix}
= \begin{pmatrix}
1 & 0 & 0 \\
\lambda_{12} & 1 & 0 \\
\lambda_{12}\lambda_{23} & \lambda_{23} & 1
\end{pmatrix}
\begin{pmatrix}
\omega_{11} & 0 & 0 \\
0 & \omega_{22} & \omega_{23} \\
0 & \omega_{23} & \omega_{33}
\end{pmatrix}
\begin{pmatrix}
1 & \lambda_{12} & \lambda_{12}\lambda_{23} \\
0 & 1 & \lambda_{23} \\
0 & 0 & 1
\end{pmatrix}
$$
\[
\begin{pmatrix}
\omega_{11} & \omega_{11}\lambda_{12} & \omega_{11}\lambda_{12}\lambda_{23} \\
\omega_{22} + \omega_{11}\lambda_{12}^2 & \omega_{22}\lambda_{23} + \omega_{11}\lambda_{12}^2\lambda_{23} + \omega_{23} & \omega_{33} + \omega_{22}\lambda_{23}^2 + \omega_{23}\lambda_{23} + \omega_{11}\lambda_{12}\lambda_{23} \\
\end{pmatrix}.
\]

Note that we only display the upper entries to save space, since \(\Sigma\) is symmetric this is no loss of information. Recall that in the main use of this model, the desire is to uncover the effect of variable \(X_2\) on variable \(X_3\), that is, recover the parameter \(\lambda_{23}\). It is easy to see that

\[
\lambda_{23} = \frac{\sigma_{13}}{\sigma_{12}} = \frac{\omega_{11}\lambda_{12}\lambda_{23}}{\omega_{11}\lambda_{12}}
\]

in which case we see that \(\lambda_{23}\) is generically identifiable (since \(\sigma_{12}\) could be zero, this formula is not defined everywhere). On the other hand \(\lambda_{12}\) is globally identifiable by the formula \(\lambda_{12} = \frac{\sigma_{12}}{\sigma_{11}}\) which is defined everywhere since \(\sigma_{11} > 0\). Note that in the case that \(\lambda_{23}\) is not identified, namely when \(\lambda_{12} = 0\), the model fails to work in the desired manner for this model. Namely, the instrumental variable \(X_1\) is supposed to be chosen in a manner so that it does directly affect \(X_2\) (i.e. \(\lambda_{12} \neq 0\)).

There are a number of methods for directly checking identifiability of a statistical model, or for checking identifiability of individual parameters. Perhaps the simplest first approach is to check the dimension of the image of \(\phi\). If \(\dim \operatorname{im} \phi = \dim \Theta\) then, since the map \(\phi\) is a rational map, the number of preimages of a generic point has a fixed finite value (over the complex numbers). Checking the dimension is easy to do by calculating the rank of the Jacobian of \(\phi\).

**Proposition 16.1.7.** Let \(\Theta \subseteq \mathbb{R}^d\) with \(\dim \Theta = d\) and suppose that \(\phi\) is a rational map. Then \(\dim \operatorname{im} \phi\) is equal to the rank of the Jacobian matrix evaluated at a generic point:

\[
J(\phi) = \begin{pmatrix}
\frac{\partial \phi_1}{\partial \theta_1} & \cdots & \frac{\partial \phi_1}{\partial \theta_d} \\
\vdots & \ddots & \vdots \\
\frac{\partial \phi_m}{\partial \theta_1} & \cdots & \frac{\partial \phi_m}{\partial \theta_d}
\end{pmatrix}.
\]

In particular, the parameter vector \(\theta\) is locally identifiable if \(\text{rank}(J(\phi)) = d\) and the parameter vector is generically non-identifiable if \(\text{rank}(J(\phi)) < d\).

Proposition 16.1.7 can only tell us about local identifiability or generic non-identifiability. In practice, we would like to prove results about global identifiability or generic identifiability, as these are the most desirable identifiability properties for a model to possess. Algebraic geometry can be used to test for these conditions. A prototypical result of this type is Proposition 16.1.8. For a given map \(\phi\) and parameter \(s\), let \(\tilde{\phi}\) be the augmented map \(\phi : \Theta \to \mathbb{R}^{m+1}, \theta \mapsto (s(\theta), \phi(\theta))\). We denote the coordinates on \(\mathbb{R}^{m+1}\) by \(q, p_1, \ldots, p_m\).
Proposition 16.1.8. Suppose that $g(q,p) \in \mathcal{I}(\hat{\phi}(\Theta)) \subseteq \mathbb{R}[q,p]$ is a polynomial such that $q$ appears in this polynomial, $g(q,p) = \sum_{i=0}^{d} g_i(p)q^i$ and $g_d(p)$ does not belong to $\mathcal{I}(\phi(\Theta))$.

1. If $g$ is linear in $q$, $g = g_1(p)q - g_0(p)$ then $s$ is generically identifiable by the rational formula $s = \frac{g_0(p)}{g_1(p)}$. If, in addition, $g_1(p) \neq 0$ for $p \in \phi(\Theta)$ then $s$ is globally identifiable.

2. If $g$ has higher degree $d$ in $q$, then $s$ may or may not be generically identifiable. Generically, there are at most $d$ possible choices for the parameter $s(\theta)$ given $\phi(\theta)$.

3. If no such polynomial $g$ exists then the parameter $s$ is not generically identifiable.

Proof. If $g(q,p) \in \mathcal{I}(\hat{\phi}(\Theta))$ then $g(q,p)$ evaluates to zero for every choice of $\theta \in \Theta$. If there is a linear polynomial in $\mathcal{I}(\hat{\phi}(\Theta))$, this means that $g_1(\phi(\theta))s(\theta) - g_0(\phi(\theta)) = 0$. Since $g_1 \notin \mathcal{I}(\phi(\Theta))$, we can solve for $s(\theta)$ as indicated.

If $g(q,p)$ has degree $d$ in $q$, we can solve an equation of degree $d$ to find $s(\theta)$. This may mean the parameter is locally identifiable, but it might also mean the parameter is globally identifiable. For instance, if $g(q,p) = q^d - g(p)$ and we know that $s(\theta)$ must be a positive real, then the existence of this polynomial would imply global identifiability.

Finally, if there is no such polynomial then generically there is no constraint on $s(\theta)$ given $\phi(\theta)$ so the parameter is not generically identifiable. □

Note that Gröbner basis computations can be used to verify the existence or nonexistence of polynomials in $\mathcal{I}(\hat{\phi}(\Theta))$ of the indicated type.

Proposition 16.1.9. Let $\mathcal{G}$ be a reduced Gröbner basis for $\mathcal{I}(\hat{\phi}(\Theta)) \subseteq \mathbb{R}[q,p]$ with respect to an elimination ordering such that $q > p_i$ for all $i$. Then a polynomial of lowest nonzero degree in $q$ of the form of Proposition 16.1.8 appears in $\mathcal{G}$. If no such polynomials exist, then $\mathcal{G}$ does not contain any polynomials involving the indeterminate $q$.

Proof. Let $g(q,p) \in \mathcal{I}(\hat{\phi}(\Theta))$ be a polynomial of lowest nonzero degree $d$ in $q$ of the form of Proposition 16.1.8. However, suppose there is no polynomial of that degree in $q$ in the reduced Gröbner basis $\mathcal{G}$. Since $g_d(p) \notin \mathcal{I}(\phi(\Theta))$, we can reduce $g(q,p)$ with respect to $\mathcal{G} \cap \mathbb{R}[p]$ (which by the elimination property is a Gröbner basis for $\mathcal{I}(\phi(\Theta))$). The resulting polynomial $\tilde{g}(q,p)$ will have the property that its leading term is not divisible by the leading term of any of polynomial in $\mathcal{G} \cap \mathbb{R}[p]$. But then the leading term of $\tilde{g}(q,p)$ is divisible by $q^d$ by the elimination property. Since $\mathcal{G}$ is a Gröbner basis, this leading term is divisible by some leading term of a polynomial in $\mathcal{G}$.
The term that divides this must be a polynomial of the form of Proposition 16.1.8 and must have degree in \( q \) less than or equal to \( d \). Since \( d \) is the smallest possible degree for such a polynomial, we see that \( \mathcal{G} \) must contain a polynomial of the desired type. □

Similar reasoning can give qualitative information about the number of possible preimages over the complex numbers when we analyze the entire map at once.

**Proposition 16.1.10.** Consider a polynomial map \( \phi : \mathbb{C}^d \rightarrow \mathbb{C}^r \). Let \( I = \langle p_1 - \phi_1(\theta), \ldots, p_r - \phi_r(\theta) \rangle \) be the vanishing ideal of the graph of \( \phi \). Let \( \mathcal{G} \) be a Gröbner basis for \( I \) with respect to an elimination ordering such that \( \theta_i > p_j \) for all \( i \) and \( j \). Let \( M \subseteq \mathbb{C}[\theta] \) be the monomial ideal generated by all monomials \( \theta^u \) such that \( u \neq 0 \) and \( p^v\theta^u \) is the leading term of some polynomial in \( \mathcal{G} \). Then the number of complex preimages of a generic point in \( \phi(\Theta) \) equals the number of standard monomials of \( M \).

**Proof.** Let \( J \) be the elimination ideal \( I \cap \mathbb{C}[p] \), which is the vanishing ideal of the image of \( \phi \). Let \( K = K(\mathbb{C}[p]/I) \) be the fraction field of the coordinate ring of the image of \( \phi \). If we consider the ideal

\[
\tilde{I} = \langle p_1 - \phi_1(\theta), \ldots, p_r - \phi_r(\theta) \rangle \subseteq K[\theta]
\]

then the number of standard monomials of \( \tilde{I} \) with respect to any term order on the \( \theta \) indeterminates equals the generic number of preimages for a point \( p \) in the model.

The point of the proposition is that this initial ideal can be calculated by computing a Gröbner basis in the ring \( \mathbb{C}[p,\theta] \) rather than in the ring \( K[\theta] \). Indeed, any polynomial \( f \in \mathcal{G} \subseteq \mathbb{C}[p,\theta] \) is also yields a polynomial in \( \tilde{f} \in K[\theta] \). Since we have chosen an elimination term order on \( \mathbb{C}[p,\theta] \), the leading term of the highest coefficient appearing in \( f \) is not in the elimination ideal \( J \). This means that leading monomial \( p^v\theta^u \) of \( f \) yields the leading monomial \( \theta^u \) of \( \tilde{I} \). Conversely if \( \tilde{f} \) is a nonzero polynomial of \( \tilde{I} \) with leading monomial \( \theta^u \), then by clearing denominators we get a nonzero polynomial of \( I \) with leading monomial \( p^v\theta^u \) for some \( v \). This shows that the monomial ideal \( M \) is the leading term ideal of \( \tilde{I} \). □

**Example 16.1.11.** Consider the 1-factor model with \( m = 3 \). The following Macaulay 2 code computes the initial ideal with respect to the indicated lexicographic term order:

```plaintext
S = QQ[w1,w2,w3,l1,l2,l3,s11,s12,s13,s22,s23,s33, MonomialOrder => Lex];
I = ideal(s11 - w1 - l1^2, s12 - l1*l2, s13 - l1*l3, s22 - w2 - l2^2, s23 - l2*l3, s33 - w3 - l3^2)
leadTerm I
```
and the resulting initial ideal is
\[ \langle \lambda_3^2 \sigma_{12}, \lambda_2 \sigma_{13}, \lambda_2 \lambda_3, \lambda_1 \sigma_{23}, \lambda_1 \lambda_3, \lambda_1 \lambda_2, \omega_1, \omega_2, \omega_3 \rangle \]
and the monomial ideal \( M \) is
\[ \langle \lambda_3^2, \lambda_2, \lambda_1, \omega_1, \omega_2, \omega_3 \rangle \]
from which we deduce that a generic point in the image has 2 complex preimages.

Beyond identifiability of numerical parameters of models, as we have seen up to this point, it is also of interest in applications to decide the identifiability of the certain discrete parameters of models. What we mean by this is that, for example, we would like to know for two different phylogenetic trees \( T_1 \) and \( T_2 \) cannot produce the same probability distributions if \( T_1 \neq T_2 \). So global identifiability of tree parameters would mean that \( M_{T_1} \cap M_{T_2} = \emptyset \). Generic identifiability of tree parameters means that
\[ \dim(M_{T_1} \cap M_{T_2}) < \min(\dim M_{T_1}, \dim M_{T_2}) . \]

For graphical models we might desire that two different graphs \( G_1 \) and \( G_2 \) should yield different models, i.e. \( M_{G_1} \neq M_{G_2} \). This is often called model distinguishability. Both the problem of discrete parameter identifiability and model distinguishability can be addressed by using algebraic geometry techniques. A prototypical algebraic tool for this problem is the following:

**Proposition 16.1.12.** Let \( M_1 \) and \( M_2 \) be two algebraic exponential families which sit inside the same natural parameter space of an exponential family. If there exists a polynomial \( f \in I(M_1) \) such that \( f \notin I(M_2) \) then \( M_1 \neq M_2 \). If \( M_1 \) and \( M_2 \) are both irreducible (e.g. they are parametrized models) and there exists polynomials \( f_1 \) and \( f_2 \) such that
\[ f_1 \in I(M_1) \setminus I(M_2) \quad \text{and} \quad f_2 \in I(M_2) \setminus I(M_1) \]
then \( \dim(M_1 \cap M_2) < \min(\dim M_1, \dim M_2) \).

**Proof.** Since \( M_1 \) and \( M_2 \) are both irreducible, the ideals \( I(M_1) \) and \( I(M_2) \) are prime ideals. Then if \( \langle f_1 \rangle + I(M_2) \) yields a variety strictly contained in \( V(I(M_2)) \), in particular, it must have smaller dimension than \( M_2 \). Since
\[ M_1 \cap M_2 \subseteq V(\langle f_1 \rangle + I(M_2)) \]
this shows that \( \dim(M_1 \cap M_2) < \dim M_2 \). A similar argument shows the necessary inequality for \( M_1 \) to complete the proof. \( \square \)

Proposition [16.1.12] is a standard tool in proving identifiability results of discrete parameters, for instance, in proofs of identifiability of tree parameters in phylogenetic models and mixture models [APRS11, AR06, LS15, RS12]. It also arises in the well-known result in the theory of graphical
models on when two directed acyclic graphs give the same graphical model (Theorem 13.1.14). Here is a simple example of how this method might be applied in phylogenetics.

**Theorem 16.1.13.** The unrooted tree parameter in the phylogenetic model under the general Markov model for binary trees is generically identifiable.

**Proof.** It suffices to show that for any pair of unrooted binary trees $T_1$ and $T_2$ on the same number of leaves, there exists a polynomials $f_1$ and $f_2$ such that

$$f_1 \in \mathcal{I}(\mathcal{M}_{T_1}) \setminus \mathcal{I}(\mathcal{M}_{T_2}) \quad \text{and} \quad f_2 \in \mathcal{I}(\mathcal{M}_{T_2}) \setminus \mathcal{I}(\mathcal{M}_{T_1}).$$

Since $T_1$ and $T_2$ are binary trees, there exists splits $A_1 \mid B_1$ and $A_2 \mid B_2$ such that $A_1 \mid B_1 \in \Sigma(T_1) \setminus \Sigma(T_2)$ and $A_2 \mid B_2 \in \Sigma(T_2) \setminus \Sigma(T_1)$. Then Proposition 15.4.4 implies that we can choose $f_i$ among the $(\kappa + 1) \times (\kappa + 1)$ minors of $\text{Flat}_{A_i \mid B_i}(P)$. □

### 16.2. Linear Structural Equation Models

Among the most well-studied identifiability problems in statistics is the identifiability of parameters in linear structural equation models. This problem originates in the work of Sewell Wright [Wri34] where SEMs were first introduced, and has been much studied in the econometrics literature [Fis66]. Still, a complete classification of when linear SEMs models are generically identifiable, or necessary and sufficient conditions for when individual parameters are identifiable, remain illusive. In this section we highlight some of the main results in this area.

Let $G = (V, B, D)$ be a mixed graph with $m = |V|$ vertices. Recall that the linear structural equation model associated to the mixed graph $G$ consists of all positive definite matrices of the form

$$\Sigma = (I - \Lambda)^{-T} \Omega(I - \Lambda)^{-1}$$

where $\Omega \in PD(B)$ and $\Lambda \in \mathbb{R}^D$ (see Section 14.2). Identifiability analysis of the linear structural equation model concerns whether or not the map $\phi_G : PD(B) \times \mathbb{R}^D \to PD_m$ is one-to-one, under the various settings of Definition 16.1.1. One case where this is completely understood is the case of global identifiability which we explain now.

**Theorem 16.2.1.** [DFS11] Let $G = (V, B, D)$ be a mixed graph. The parameters of the linear structural equation model associated to $G$ are globally identifiable if and only if

1. The graph $G$ has no directed cycle and
(2) There is no mixed subgraph \( H = (V', B', D') \) such that the subgraph of \( H \) on the bidirected edges is connected and the subgraph of \( H \) on the directed edges forms a converging arborescence.

A **converging arborescence** is a directed graph whose underlying undirected graph is a tree and has a unique sink vertex. Examples of globally identifiable and globally non-identifiable models are given in Figure [16.2.1](#).

![Figure 16.2.1](#). The graph on the left yields a globally identifiable linear structural equation model while the graph on the right does not.

We do not give a complete proof of Theorem [16.2.1](#) here, but just show that condition one is necessary. Note that since we are concerned with global identifiability we always have the following useful proposition.

**Proposition 16.2.2.** Let \( G \) be a mixed graph and \( H \) a subgraph. If the linear structural equation model associated to \( G \) is globally identifiable, so is the linear structural equation model associated to \( H \).

**Proof.** Passing to a subgraph amounts to setting all parameters corresponding to deleted edges equal to zero. Since global identifiability means identifiability holds for all parameter choices, it must hold when we set some parameters to zero.

Hence to show that the two conditions of Theorem [16.2.1](#) are necessary, it suffices to show that directed cycles are not globally identifiable, and graphs that fail to satisfy the second condition are not globally identifiable.

**Proposition 16.2.3.** Suppose that \( G = (V, D) \) is a directed cycle of length \( \geq 3 \). Then the map \( \phi_G : \mathbb{R}^D \rightarrow PD_m \) is generically 2-to-1.

**Proof.** Without loss of generality, we can take \( G \) to be the directed cycle with edges \( 1 \rightarrow 2, 2 \rightarrow 3, \ldots m \rightarrow 1 \). Note that the determinant of \((I - \Lambda)\) in this case is \(1 + (-1)^{m-1} \prod_{i=1}^{m} \lambda_{i,i+1}\). We assume that this quantity is not equal to zero, and that all \(\lambda_{i,i+1} \neq 0\). Since we are considering generic behavior, we will use the useful trick that we can parametrize the concentration matrix, rather than the covariance matrix. This has the parametrization:

\[
K = (I - \Lambda)^T \Delta (I - \Lambda)
\]
where $\Delta = \Omega^{-1}$ is the diagonal matrix with diagonal entries $\delta_{ii} = \omega_{ii}^{-1}$. Expanding this parametrization explicitly gives

$$K = \begin{pmatrix}
\delta_{11} + \delta_{22}^2 \lambda_{12} & -\delta_{22} \lambda_{12} & 0 & \cdots \\
-\delta_{22} \lambda_{12} & \delta_{22} + \delta_{33}^2 \lambda_{23} & -\delta_{33} \lambda_{23} & \cdots \\
0 & -\delta_{33} \lambda_{23} & \delta_{33} + \delta_{44} \lambda_{34} & \cdots \\
\vdots & \vdots & \vdots & \ddots
\end{pmatrix}.$$ 

This tridiagonal matrix has

$$K_{ii} = \delta_{ii} + \delta_{i+1,i+1} \lambda_{i,i+1}^2, \quad K_{i,i+1} = -\delta_{i+1,i+1} \lambda_{i,i+1}.$$ 

We can solve for $\lambda_{i,i+1}$ in terms of $K_{i,i+1}$ and $\delta_{i+1,i+1}$, which produces the equation system

$$K_{ii} = \delta_{ii} + \frac{K_{i,i+1}^2}{\delta_{i+1,i+1}}.$$ 

Linearly eliminating $\delta_{ii}$ and plugging into the next equation for this system eventually produces a quadratic equation in $\delta_{mm}$. Since we know that one of the roots for this equation is real the other root must be as well. This produces all real roots for all the coefficients with two preimages over the reals, generically. We must show that the second pair $(\Delta', \Lambda')$ also corresponds to model parameters, i.e. $\Delta'$ is positive definite. To see this note that the second matrix $\Lambda'$ will also yield $(I - \Lambda')$ invertible generically. Since $K$ is positive definite, this means that $(I - \Lambda')^{-T} K (I - \Lambda')^{-1} = \Delta'$ is also positive definite. \[\square\]

To show that the second condition of Theorem 16.2.1 is necessary, requires a different argument. For graphs that have such a bad substructure it can be the case that the map $\phi_G$ is generically injective, so that the model is generically identifiable. So we need to find specific parameter values $\Omega, \Lambda$ such that $\phi_G(\Omega, \Lambda)$ has multiple preimages. In fact, it always happens in these cases that there are fibers that are not zero dimensional. See [DFS11] for the details.

The simplest example of the bad substructure in the second condition of Theorem 16.2.1 is a pair of vertices $i, j$ such that we have both edges $i \to j$ and $i \leftrightarrow j$. By passing to the subgraph with only those two edges, we see that this model could not be globally identifiable. Remarkably, if we just rule out this one subgraph and assume we have no directed cycles, we have generic identifiability of the associated linear SEM. Graphs with no pair of vertices with both $i \to j \in D$ and $i \leftrightarrow j \in B$ are called simple graphs or bow-free graphs.

**Theorem 16.2.4.** [BP02] Let $G = (V, B, D)$ be a simple directed acyclic mixed graph. Then $\phi_G$ is generically injective.
Proof. We assume that the ordering of vertices matches the acyclic structure of the graph (so, \( i \rightarrow j \in D \) implies that \( i < j \)). We proceed by induction on the number of vertices. The upper triangular nature of the matrix \((I - \Lambda)^{-1}\) implies that the submatrix \(\Sigma_{[m-1],[m-1]}\) has the following factorization:

\[
\Sigma_{[m-1],[m-1]} = (I - \Lambda_{[m-1],[m-1]})^{-T} \Omega_{[m-1],[m-1]} (I - \Lambda_{[m-1],[m-1]})^{-1}
\]

By induction on the number of vertices, we can assume that all parameters associated to the model on vertices in \([m-1]\) are identifiable.

So consider the vertices \(N(m)\) which are the neighbors of \(m\) (either a directed or undirected edge from \(i \in N(m)\) to \(m\)). Every trek from a vertex in \(N(m)\) to \(m\) has a single edge involving one of the yet underdetermined parameters which connects to vertex \(m\). Let \(P\) be the length \(|N(m)|\) vector consisting of all parameters corresponding to either the directed or bidirected edges connecting any \(i \in N(m)\) to \(m\). Since the graph is simple we can write a square system

\[
\Sigma_{N(m),m} = A(\Omega_{[m-1],[m-1]}, \Lambda_{[m-1],[m-1]}) P
\]

where \(A(\Omega_{[m-1],[m-1]}, \Lambda_{[m-1],[m-1]})\) is a square matrix whose entries are polynomial functions of the parameters whose values we know by induction. If we can show that \(A(\Omega_{[m-1],[m-1]}, \Lambda_{[m-1],[m-1]})\) is generically invertible, we will identify all parameters corresponding to edges pointing to \(m\). However, if we choose \(\Omega_{[m-1],[m-1]} = I\) and \(\Lambda_{[m-1],[m-1]} = 0\), \(A(\Omega_{[m-1],[m-1]}, \Lambda_{[m-1],[m-1]})\) will be the identity matrix, which is clearly invertible. Requiring a matrix to be invertible is an open condition, so \(A(\Omega_{[m-1],[m-1]}, \Lambda_{[m-1],[m-1]})\) will be invertible for generic choices of the parameters.

Finally, the entry \(\omega_{m,m}\) is identifiable as it appears in only the entry

\[
\sigma_{m,m} = \omega_{m,m} + f(\Omega, \Lambda)
\]

where \(f\) is a polynomial only in identifiable entries. \(\square\)

On the other hand, the basic instrumental variables model is generically identifiable (Example [16.1.6]), though the graph is not simple. It remains a major open problem in the study of identifiability to find a complete characterization of those mixed graphs for which the parametrization \(\phi_G\) is generically injective. Most partial results of this type attempt to follow the strategy of the proof of Theorem [16.2.4] by recursively solving for parameters in the model by writing linear equation systems whose coefficients involve either parameters that have already been solved for or entries of the matrix \(\Sigma\). One strong theorem of this type is the half-trek criterion [FDD12]. The paper also contains a similar necessary condition involving half-treks that a graph must satisfy to be identifiable. Further recent results extend the half-trek criterion by considering certain graph decompositions of the mixed
16.2. Linear Structural Equation Models

Figure 16.2.2. A graph whose linear SEM is proven identifiable by the half trek criterion.

graph $G$ [DW16]. See [CTP14] for related work. To state the results on the half-trek criterion requires a number of definitions.

**Definition 16.2.5.** Let $G = (V, B, D)$ be a mixed graph. Let $\text{sib}(v) = \{i \in V : i \leftrightarrow v \in V\}$ be the siblings of node $v \in V$. A *half trek* is a trek with left side of cardinality one. Let $\text{htr}(v)$ be the subset of $V \setminus (\{v\} \cup \text{sib}(v))$ of vertices reachable from $v$ via a half-trek.

**Definition 16.2.6.** A set of nodes $Y \subset V$ satisfies the half-trek criterion with respect to node $v \in V$ if

1. $|Y| = |\text{pa}(v)|$,
2. $Y \cap (\{v\} \cup \text{sib}(v)) = \emptyset$, and
3. there is a system of half-treks with no sided intersection from $Y$ to $\text{pa}(v)$.

Note that if $\text{pa}(v) = \emptyset$ then $Y = \emptyset$ will satisfy the half-trek criterion with respect to $v$.

**Theorem 16.2.7.** [FDD12] Let $(Y_v : v \in V)$ be a family of subsets of the vertex set $V$ of the mixed graph $G$. If, for each node $v$, the set $Y_v$ satisfies the half-trek criterion with respect to $v$, and there is a total ordering $\prec$ of the vertex set $V$ such that $w \prec v$ whenever $w \in Y_v \cap \text{htr}(v)$, then $\phi_G$ is generically injective and has a rational inverse.

We do not attempt to prove Theorem [16.2.7] here but illustrate it with an example taken from [FDD12].

**Example 16.2.8.** Consider the graph in Figure 16.2.2. This graph is identifiable via the half trek criterion. Take

$$Y_1 = \emptyset, \quad Y_2 = \{5\}, \quad Y_3 = \{2\}, \quad Y_4 = \{2\}, \quad Y_5 = \{3\}.$$  

Each $Y_v$ satisfies the half-trek criterion with respect to $v$. For example for $v = 3$, $2 \rightarrow 3$ is a half-trek from a nonsibling to 3. Taking the total order on the vertices to be the standard order $1 < 2 < 3 < 4 < 5$ we see that the conditions on the sets $\text{htr}(v)$ are also satisfied. For example, for $v = 3$, $\text{htr}(3) = \{4, 5\}$ so $Y_3 \cap \text{htr}(3) = \emptyset$. 
16.3. Tensor Methods

For hidden variable statistical models with discrete random variables, a powerful tool for proving identifiability results comes from methods related to the tensor rank of three-way tensors. The main theorem in this area is Kruskal’s theorem [Kru76, Kru77]. The methods for extending the technique to complicated hidden variable models appears in [AMR09]. In this section, we will explore the applications of Kruskal’s theorem to proving identifiability for hidden variable graphical models and mixture models.

The starting point for Kruskal’s theorem is the comparison of two mixture models, the mixture model \( \text{Mixt}^k(\mathcal{M}_{X_1 \perp \perp X_2}) \) and \( \text{Mixt}^k(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3}) \). As we saw in Example 16.1.3, the first model is always generically nonidentifiable for any \( k > 1 \). Perhaps the first natural response is that the model \( \text{Mixt}^k(\mathcal{M}_{X_1 \perp \perp X_2 \perp \perp X_3}) \) should be generically nonidentifiable as well since it contains the first model after marginalizing. However this intuition turns out to be wrong, and this three-factor mixture turns out to be generically identifiable if \( k \) satisfies a simple bound in terms of the number of states of \( X_1, X_2, X_3 \). Kruskal’s theorem can be stated purely in statistical language but it can also be useful to state it in the language of tensors.

Let \( a_1, \ldots, a_k, b_1, \ldots, b_k, c_1, \ldots, c_k \in \mathbb{K}^{r_1}, \ldots, \mathbb{K}^{r_3} \). Arrange these vectors into matrices \( A \in \mathbb{K}^{r_1 \times k}, B \in \mathbb{K}^{r_2 \times k}, \) and \( C \in \mathbb{K}^{r_3 \times k} \) whose columns are \( a_1, \ldots, a_k, b_1, \ldots, b_k, c_1, \ldots, c_k \), respectively. The \((i,j)\) entry of \( A \) is \( a_{ij} \) the \( i \)th entry of \( a_j \), and similarly for \( B \) and \( C \).

**Definition 16.3.1.** Let \( A \in \mathbb{K}^{r \times k} \) be a matrix. The *Kruskal rank* of \( A \), denoted \( \text{rank}_K(A) \) is the largest number \( l \) such that any \( l \) columns of \( A \) are linearly independent.

We can form the tensor

\[
M = \sum_{j=1}^{k} a_j \otimes b_j \otimes c_j \in \mathbb{K}^{r_1} \otimes \mathbb{K}^{r_2} \otimes \mathbb{K}^{r_3}.
\]

The tensor product space \( \mathbb{K}^{r_1} \otimes \mathbb{K}^{r_2} \otimes \mathbb{K}^{r_3} \) is the vector space of \( r_1 \times r_2 \times r_3 \) arrays with entries in \( \mathbb{K} \). Each tensor \( a_j \otimes b_j \otimes c_j \) is called a rank one tensor. A tensor \( M \in \mathbb{K}^{r_1} \otimes \mathbb{K}^{r_2} \otimes \mathbb{K}^{r_3} \) has rank \( k \) if it can be written as in Equation 16.3.1 for some \( a_1, \ldots, a_k, b_1, \ldots, b_k, c_1, \ldots, c_k \in \mathbb{K}^{r_1}, \ldots, \mathbb{K}^{r_3} \), and cannot be written as a sum of fewer rank one tensors. Kruskal’s theorem concerns the uniqueness of the decomposition of a tensor into rank one tensors.

**Theorem 16.3.2 (Kruskal).** Let \( M \in \mathbb{K}^{r_1} \otimes \mathbb{K}^{r_2} \otimes \mathbb{K}^{r_3} \) be a tensor and

\[
M = \sum_{j=1}^{k} a_j \otimes b_j \otimes c_j \in \mathbb{K}^{r_1} \otimes \mathbb{K}^{r_2} \otimes \mathbb{K}^{r_3}.
\]
16.3. Tensor Methods

\[ M = \sum_{j=1}^{k} a'_j \otimes b'_j \otimes c'_j \in \mathbb{K}^{r_1} \otimes \mathbb{K}^{r_2} \otimes \mathbb{K}^{r_3} \]

be two decompositions of \( M \) into rank one tensors. Let \( A, B, C \) be the matrices whose columns are \( a_1, \ldots, a_k, b_1, \ldots, b_k, \) and \( c_1, \ldots, c_k, \) respectively, and similarly for \( A', B', \) and \( C' \). If

\[ \text{rank}_K(A) + \text{rank}_K(B) + \text{rank}_K(C) \geq 2k + 2 \]

then there exists a permutation \( \sigma \in S_k, \) and nonzero \( \lambda_1, \ldots, \lambda_k, \gamma_1, \ldots, \gamma_k \in \mathbb{K} \) such that

\[ a_{\sigma(j)} = \lambda_j a'_j, \quad b_{\sigma(j)} = \gamma_j b'_j, \quad \text{and} \quad c_{\sigma(j)} = \lambda_j^{-1} \gamma_j^{-1} c'_j \quad \text{for all} \quad j \in [k]. \]

A useful compact notation for expressing Equation 16.3.1 is the triple product notation. We write \( M = [A, B, C] \) to denote the rank one decomposition from (16.3.1). Theorem 16.3.2 can also be rephrased as saying that if \( \text{rank}_K(A) + \text{rank}_K(B) + \text{rank}_K(C) \geq 2k + 2 \) and \( [A, B, C] = [A', B', C'] \) there is a permutation matrix \( P \) and invertible diagonal matrices \( D_1, D_2, D_3 \) with \( D_1 D_2 D_3 = I \) such that

\[ D_1 PA = A', \quad D_2 PB = B', \quad \text{and} \quad D_3 PC = C'. \]

So Kruskal’s theorem guarantees that a given decomposition of tensors is as unique as possible provided that the Kruskal ranks of the given tensors are large enough, relative to the number of factors. This theorem was originally proven in [Kru76, Kru77] and simplified versions of the proof can be found in [Lan12, RS12]. In this section, we explore applications of Kruskal’s theorem to the identifiability of hidden variable discrete models. A first application concerns the mixture model \( \text{Mixt}^k(M_{X_1 \perp \perp X_2 \perp \perp X_3}). \)

**Corollary 16.3.3.** Consider the mixture model \( \text{Mixt}^k(M_{X_1 \perp \perp X_2 \perp \perp X_3}) \) where \( X_i \) has \( r_i \) states, for \( i = 1, 2, 3. \) This model is generically identifiable up to relabeling of the states of the hidden variable if

\[ \min(r_1, k) + \min(r_2, k) + \min(r_3, k) \geq 2k + 2. \]

Note the phrase “up to relabeling of the states of the hidden variable” which appears in Corollary 16.3.3. This is a common feature in the identifiability of hidden variable models. Another interpretation of this result is that the model is algebraically identifiable and each point in the model has \( k! \) preimages.

**Proof of Corollary 16.3.3** Recall that \( \text{Mixt}^k(M_{X_1 \perp \perp X_2 \perp \perp X_3}) \) can be parametrized as the set of all probability distributions in \( p \in \Delta_{r_1r_2r_3-1} \) with

\[ p_{i_1i_2i_3} = \sum_{j=1}^{k} \pi_j \alpha_{i_1j} \beta_{i_2j} \gamma_{i_3j} \]
for some $\pi \in \Delta_{k-1}$ and $\alpha$, $\beta$, and $\gamma$ representing conditional distributions of $X_1 | Y$, $X_2 | Y$ and $X_3 | Y$, respectively. In comparison to the parametrization of rank $k$ tensors, we have extra restrictions on the matrices $\alpha, \beta, \gamma$ (their columns sums are all equal to one) and we have the appearance of the extra $\pi$. Let $\Pi$ denote the diagonal matrix diag$(\pi_1, \ldots, \pi_k)$. Let $A = \alpha \Pi, B = \beta, C = \gamma$. The triple product $[A, B, C]$ gives the indicated probability distribution in the mixture model. For generic choices of the conditional distributions and the root distributions we have

$$\text{rank}_K(A) + \text{rank}_K(B) + \text{rank}_K(C) = \min(r_1, k) + \min(r_2, k) + \min(r_3, k)$$

so we are in the position to apply Kruskal’s theorem. Suppose that

$$[A', B', C'] = [A, B, C].$$

By Kruskal’s theorem, it must be the case that there is a permutation matrix $P$ and invertible diagonal matrix $D_1, D_2, D_3$ with $D_1D_2D_3 = I$ such that

$$D_1PA = A', \quad D_2PB = B', \quad \text{and} \quad D_3PC = C'.$$

However, if we take $B'$ and $C'$ to give conditional probability distributions, this forces $D_2 = I$ and $D_3 = I$, which in turn forces $D_1 = I$. So the matrices $A, B, C,$ and $A', B', C'$ only differ by simultaneous permutations of the columns. So up to this permutation, we can assume that $A = A'$, $B = B'$, and $C = C'$. We means we recover $\beta$ and $\gamma$ up to permutation of states of the hidden variable. Lastly $\pi$ and $\alpha$ can be recovered from $A$ since $\pi$ is the vector of columns sums of $A$, and then $\alpha = A\Pi^{-1}$. \hfill \Box

There are direct generalizations of Kruskal rank to higher order tensors. They prove essential uniqueness of the rank one decomposition of tensors provided that the Kruskal ranks of certain matrices satisfy a linear condition in terms of the rank of the tensor. However, part of the power of Kruskal’s theorem for 3-way tensors is that it can be used to prove identifiability to much higher number of states of hidden variables if we are willing to drop the explicit check on identifiability that comes with calculating the Kruskal rank. For example:

**Corollary 16.3.4.** Let $X_1, \ldots, X_m$ be discrete random variables where $X_i$ has $r_i$ states. Let $\mathcal{M}_{X_1 \perp \cdots \perp X_m}$ denote the complete independence model. Let $A|B|C$ be a tripartition of $[m]$ with no empty parts. Then the mixture model $\text{Mixt}^k(\mathcal{M}_{X_1 \perp \cdots \perp X_m})$ is generically identifiable up to label swapping if

$$\min(\prod_{a \in A} r_a, k) + \min(\prod_{b \in B} r_b, k) + \min(\prod_{c \in C} r_c, k) \geq 2k + 2.$$
16.3. Tensor Methods

Proof. We would like to reduce to Corollary [16.3.3]. To do this we “clump” the random variables into three blocks to produce three super random variables $Y_A$ with $\prod_{a \in A} r_a$ states, $Y_B$ with $\prod_{b \in B} r_b$ states, and $Y_C$ with $\prod_{c \in C} r_c$ states. Here we are flattening our $m$-way array into a 3-way array (akin to the flattening to matrices we saw in Chapter 15).

Clearly the Corollary is true for these three random variables and the resulting mixture model $\text{Mixt}^k(M_{Y_A} \perp \perp Y_B \perp \perp Y_C)$. However, the resulting conditional distributions that are produced in this clumping procedure are not generic distributions, they themselves consist of rank 1 tensors. For example, the resulting conditional distribution of $Y_A|H = h$ is an $\prod_{a \in A} r_a$ rank 1 tensor. This means that we cannot apply Corollary [16.3.3] unless we can prove that generic parameters in the model $\text{Mixt}^k(M_{X_1} \perp \perp \ldots \perp X_m)$ map to the identifiable locus in $\text{Mixt}^k(M_{Y_A} \perp \perp Y_B \perp \perp Y_C)$. At this point, however, we can appeal to the proof of Corollary [16.3.3]. The resulting matrices whose columns are the conditional distributions obtained by the flattening will generically have full rank (hence, Kruskal rank will be $\min(\prod_{a \in A} r_a, k)$ for the first matrix, etc.). This follows because there are no linear relationships that hold on the set of rank 1 tensors, so we can always choose a generic set that are linearly independent. Then the proof of Corollary [16.3.3] implies we can recover all parameters in the model, up to renaming the hidden variables.

This type of technique has been used to prove identifiability of a number of different models. See [AMR09] for numerous examples and [RS12] for an application to identifiability of phylogenetic mixture models. We close with another example from [ARSV15] illustrating how the method can be used in graphical models with a more complex graphical structure.

Example 16.3.5. Consider the discrete directed graphical model in Figure [16.3.1] where all random variables are binary and variable $Y$ is assumed to be a hidden variable. We will show that this model is identifiable up to label swapping the two states of the hidden variable $Y$. The parametrization for

Figure 16.3.1. A graph for a hidden variable model that is identifiable up to label swapping.
this model takes the following form:

\[ p_{i_1i_2i_3i_4} = \sum_{j=1}^{2} \pi_j a_{i_1|j} b_{i_2|j} c_{i_3|j} d_{i_4|j} \]

where \( P(Y = j) = \pi_j \), \( P(X_1 = i_1|Y = j) = a_{i_1|j} \), etc., are the conditional distributions that go into the parametrization of the graphical model.

Fixing a value of \( X_1 = i_1 \) and regrouping terms yields the expression:

\[ p_{i_1i_2i_3i_4} = \sum_{j=1}^{2} (\pi_j a_{i_1|j}) b_{i_2|j} c_{i_3|j} d_{i_4|j} \]

For each fixed value of \( i_1 \), the resulting \( 2 \times 2 \times 2 \) array that is being parameterized in this way is a rank \( \leq 2 \) tensor. Each of the matrices

\[ B^{i_1} = \begin{pmatrix} b_{1|1i_1} & b_{1|2i_1} \\ b_{2|1i_1} & b_{2|2i_1} \end{pmatrix} \quad C^{i_1} = \begin{pmatrix} c_{1|1i_1} & c_{1|2i_1} \\ c_{2|1i_1} & c_{2|2i_1} \end{pmatrix} \quad D = \begin{pmatrix} d_{1|1} & c_{1|2} \\ d_{2|1} & c_{2|2} \end{pmatrix} \]

generically has full rank, and hence has Kruskal rank 2. From the argument in the proof of Corollary 16.3.3, we can recover all of the entries in these matrices (up to label swapping) plus the quantities

\[ \pi_1 a_{1|1}, \quad \pi_2 a_{1|2}, \quad \pi_1 a_{2|1}, \quad \pi_2 a_{2|2}. \]

Since \( \pi_1 a_{1|1} + \pi_1 a_{2|1} = \pi_1 \) and \( \pi_2 a_{1|2} + \pi_2 a_{2|2} = \pi_2 \) this allows us to recover all entries in the probability distributions that parametrize this model.

Corollaries to Kruskal’s theorem can also be restated directly in the language of algebraic geometry.

**Corollary 16.3.6.** Suppose that \( \min(r_1,k) + \min(r_2,k) + \min(r_3,k) \geq 2k+2 \). Then a generic point on the secant variety \( \text{Sec}^k(\text{Seg}(\mathbb{P}^{r_1-1} \times \mathbb{P}^{r_2-1} \times \mathbb{P}^{r_3-1})) \) lies on a unique secant \( \mathbb{P}^{k-1} \) to \( \text{Seg}(\mathbb{P}^{r_1-1} \times \mathbb{P}^{r_2-1} \times \mathbb{P}^{r_3-1}) \).

While Corollary 16.3.6 gives a cleaner looking statement, the full version of Theorem 16.3.2 is significantly more powerful because it gives an explicitly checkable condition (the Kruskal rank) to test whether a given decomposition is unique. This is the tool that often allows the method to be applied to more complex statistical models. In fact, tools from algebraic geometry provide stronger statements than Corollary 16.3.6.

**Theorem 16.3.7.** [CO12] Let \( r_1 \geq r_2 \geq r_3 \). A generic point on the secant variety \( \text{Sec}^k(\text{Seg}(\mathbb{P}^{r_1-1} \times \mathbb{P}^{r_2-1} \times \mathbb{P}^{r_3-1})) \) lies on a unique secant \( \mathbb{P}^{k-1} \) to \( \text{Seg}(\mathbb{P}^{r_1-1} \times \mathbb{P}^{r_2-1} \times \mathbb{P}^{r_3-1}) \) provided that \( (r_2+1)(r_3+1)/16 \geq k \).
Note that Kruskal’s theorem gives a linear bound on the tensor rank that guarantees the uniqueness of tensor decomposition while Theorem 16.3.7 gives a quadratic bound on uniqueness of decomposition where $r_1, r_2, r_3$ have the same order of magnitude. However, Theorem 16.3.7 lacks any explicit condition that guarantees that a specific tensor lies in the identifiable locus, so at present it does not seem possible to apply this result to complex identifiability problems in algebraic statistics. It remains an interesting open problem in the theory of tensor rank to give any explicit checkable condition that will verify a tensor has a specific rank when that rank is large relative to the tensor dimensions.

16.4. State Space Models

Models based on differential equations are widely used throughout applied mathematics and nearly every field of science. For example, the governing equations for physical laws are usually systems of partial differential equations, and the time evolution of a biological system is usually represented by systems of ordinary differential equations. These systems often depend on unknown parameters that cannot be directly measured, and a large part of applied mathematics concerns developing methods for recovering these parameters from the observed data. The corresponding research areas and the mathematical techniques that are used are variously known as the theory of inverse problems, parameter estimation, or uncertainty quantification. A fundamental property that needs to be satisfied for a model to be useful is that the data observations need to be rich enough that it is actually possible to estimate the parameters from the data that is given. That is, the model parameters need to be identifiable given the observation. While the study of differential equation systems is far removed from the bulk of the statistical problems studied in this book, the techniques for testing identifiability for such systems often relies on the same algebraic geometric ideas that we have seen in previous sections of this chapter. For this reason, we include the material here. Our focus in this section is state space models, a special class of dynamical system, that come from systems of ordinary differential equations.

Consider the state space model

\begin{equation}
\dot{x}(t) = f(t, x(t), u(t), \theta), \quad y(t) = g(x(t), \theta).
\end{equation}

In this equation system, \( t \in \mathbb{R} \) denotes time, \( x(t) \in \mathbb{R}^n \) are the state variables, \( u(t) \in \mathbb{R}^n \) are the control variables or system inputs, \( y(t) \in \mathbb{R}^m \) are the output variables or observations, and \( \theta \in \mathbb{R}^d \) is the vector of model parameters. The goal of identifiability analysis for differential equations to determine when the model parameters \( \theta \) can be recovered from the trajectory of the input and output variables.
In the identifiability analysis of state space models, one often makes the distinction between *structural identifiability* and *practical identifiability*. Structural identifiability is a theoretical property of the model itself and concerns whether the model parameters can be determined knowing the trajectory of the input \( u(t) \) and the output \( y(t) \) exactly. Practical identifiability is a data specific property and concerns whether or not, in a model that is structurally identifiable, it is possible to estimate the model parameters with high certainty given a particular data set. Our focus here is on structural identifiability, the situation where algebraic techniques are most useful.

We address structural identifiability problems for state space models using the differential algebra approach [BSAD07, LG94]. In this setting, we assume that the functions \( f \) and \( g \) in the definition of the dynamical system (16.4.1) are polynomial or rational functions. Under certain conditions there will exist a polynomial function \( F \) such that \( y, u \) and their derivatives satisfy:

\[
F(y, \dot{y}, \ddot{y}, \ldots, u, \dot{u}, \ddot{u}, \ldots, \theta) = 0.
\]

This differential equation systems just in the inputs and outputs is called the *input/output equation*. A basic result in differential algebra says that with a general choice of the input function \( u(t) \) the coefficients of the differential monomials in the input/output equation can be determined from the trajectory of \( u(t) \) and the output trajectory \( y(t) \). These coefficients are themselves rational functions of the parameters \( \theta \). Global identifiability for dynamical systems models reduces to the question of whether or not the coefficient mapping \( c : \mathbb{R}^d \to \mathbb{R}^k, \theta \to c(\theta) \) is a one-to-one function.

**Example 16.4.1.** Consider the compartment model represented by the following system of linear ODEs:

\[
\begin{align*}
\dot{x}_1 &= -a_{21} x_1 + a_{12} x_2 + u_1 \\
\dot{x}_2 &= a_{21} x_1 + (-a_{12} - a_{02}) x_2 
\end{align*}
\]

with 1-dimensional output variable \( y(t) = V x_1(t) \). The state variable \( x(t) = (x_1(t), x_2(t))^T \in \mathbb{R}^2 \) represents the concentrations of some quantity in two compartments. Here parameters \( a_{21} \) and \( a_{12} \) represent the flow of material from compartment 1 to 2 and 2 to 1 respectively, \( a_{02} \) represents the rate of flow out of the system through compartment 2, and \( V \) is a parameter that shows that we only observe \( x_1 \) up to an unknown scale. The input \( u(t) = (u_1(t), 0) \) is only added to compartment 1.

A natural setting where this simple model might be applied is as follows: Suppose we administer a drug to a person, and we want to know how much drug might be present in the body over time. Let \( x_1 \) represent the concentration of a drug in the blood and \( x_2 \) represents concentration of the same
drug in the liver. The drug leaves the system through decomposition in the liver, and otherwise does not leave the system. The drug enters the system through the blood (e.g. by injection) represented by $u_1$ and its concentration can be measured through measurements from the blood $y$ which only give the concentration to an unknown constant.

To find the input/output equation in this case is simple linear algebra. We solve for $x_2$ in the first equation and plug in to the second, and then substitute $x_1 = y/V$. This yields the input output equation:

$$
\ddot{y} + (a_{21} + a_{12} + a_{02}) \dot{y} + a_{21}a_{02}y = V \dot{u}_1 + V(a_{12} + a_{02})u_1.
$$

With generic input function $u(t)$ and initial conditions, this differential equation can be recovered from the input and output trajectories. Identifiability reduces to the question of whether the coefficient map

$$c : \mathbb{R}^4 \to \mathbb{R}^5, \quad (a_{21}, a_{12}, a_{02}, V) \mapsto (1, a_{21} + a_{12} + a_{02}, a_{21}a_{02}, V(a_{12} + a_{02}))$$

is one-to-one. In this particular example, it is not difficult to see that the map is rationally identifiable. Indeed, in terms of the coefficients $(1, c_1, c_2, c_3, c_4)$, we have that

$$V = c_3, \quad a_{21} = c_1 - \frac{c_4}{c_3}, \quad a_{02} = \frac{c_2c_3}{c_1c_3 - c_4}, \quad a_{12} = \frac{c_4}{c_3} - \frac{c_2c_3}{c_1c_3 - c_4}.$$

In fact, the model is globally identifiable when we restrict to the biologically relevant parameter space where all parameters are $> 0$.

Note that when we recover the input/output equation from data, we only know this equation up to scaling. To eliminate this ambiguity, we usually prefer to make a representation for the input/output equation that has one coefficient set to 1 by dividing through by one of the coefficient functions if necessary. Alternately, instead of viewing the coefficient map $c : \mathbb{R}^d \to \mathbb{R}^k$ we can view this as a map to projective space $c : \mathbb{R}^d \to \mathbb{P}^{k-1}$.

Compared with the statistical models whose identifiability we studied in previous sections, dynamical systems models have a two layer source of complexity in the study of their identifiability. First we must determine the input/output equation of the model, then we must analyze the injectivity of the coefficient map. The first problem is handled using techniques from differential algebra: the input/output equation can be computed using triangular set methods or differential Gröbner bases. These computations can be extremely intensive and it can be difficult to determine the input/output equations except in relatively small models. It seems an interesting theoretical problem to determine classes of models where it is possible to explicitly calculate the input/output equation of the system. Having such classes would facilitate the analysis of the identifiability of such models and could possibly make it easier to estimate the parameters.
One general family of models where the input/output equations are easy to write down explicitly is the family of linear compartment models, generalizing Example 16.4.1. Let \( G \) be a directed graph with vertex set \( V \) and set of directed edges \( E \). Each vertex \( i \in V \) corresponds to a compartment in the model and an edge \( j \to i \) represents a direct flow of material from compartment \( j \) to \( i \). Let \( \text{In}, \text{Out}, \text{Leak} \subseteq V \) be three sets of compartments corresponding to the compartments with input, with output, and with a leak, respectively. Note that the sets \( \text{In}, \text{Out}, \text{Leak} \) do not need to be disjoint. To each edge \( j \to i \) we associate an independent parameter \( a_{ij} \), the rate of flow from compartment \( j \) to compartment \( i \). To each leak node \( i \in \text{Leak} \) we associate an independent parameter \( a_{0i} \), the rate of flow from compartment \( i \) out of the system.

We associate a matrix \( A(G) \) to the graph and the set \( \text{Leak} \) as follows:

\[
A(G)_{ij} = \begin{cases} 
-a_{0i} - \sum_{k:i \to k \in E} a_{ki} & \text{if } i = j \text{ and } i \in \text{Leak} \\
-\sum_{k:i \to k \in E} a_{ki} & \text{if } i = j \text{ and } i \notin \text{Leak} \\
a_{ij} & \text{if } j \to i \in E \\
0 & \text{otherwise.}
\end{cases}
\]

We construct a system of linear ODEs with inputs and outputs associated to the quadruple \((G, \text{In}, \text{Out}, \text{Leak})\) as follows:

\[
\dot{x}(t) = A(G)(t) + u(t) \quad y_i(t) = x_i(t) \text{ for } i \in \text{Out}
\]

where \( u_i(t) \equiv 0 \) for \( i \notin \text{In} \). The functions \( x_i(t) \) are the state variables, the functions \( y_i(t) \) are the output variables, and the nonzero functions \( u_i(t) \) are the inputs. The resulting model is called a linear compartment model.

The following conventions are often used for presenting diagrams of linear compartment models: numbered vertices represent compartments, outgoing edges from compartments represent leaks, an edge with a circle coming out of a compartment represent an output measurement, and an arrowhead pointing into a compartment represents an input.

Figure 16.4.1. A basic linear compartment model.
Example 16.4.2. Consider the graph representing a linear compartment model from Figure [16.4.1]. The resulting ODE system takes the form:

\[
\begin{pmatrix}
\dot{x}_1 \\
\dot{x}_2 \\
\dot{x}_3
\end{pmatrix} = 
\begin{pmatrix}
-a_{01} - a_{21} & a_{12} & a_{13} \\
-a_{21} & -a_{02} - a_{12} - a_{32} & 0 \\
0 & a_{32} & -a_{13}
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3
\end{pmatrix}
+ 
\begin{pmatrix}
u_1 \\
u_2 \\
0
\end{pmatrix},
\]

y_1 = x_1.

Proposition 16.4.3. Consider the linear compartment model defined by the quadruple \((G, \text{In}, \text{Out}, \text{Leak})\). Let \(\partial\) denote the differential operator \(d/dt\) and let \((\partial I - A(G))^{ji}\) denote the matrix obtained by deleting the \(j\)th row and \(i\)th column of \(\partial I - A(G)\). Then the input/output equations of this model have the form

\[
\frac{\det(\partial I - A(G))}{g_i} y_i = \sum_{j \in \text{In}} (-1)^{i+j} \frac{\det(\partial I - A(G))^{ji}}{g_i} u_j,
\]

where \(g_i\) is the greatest common divisor of \(\det(\partial I - A(G))\) and the set of polynomials \(\det(\partial I - A(G))^{ji}\) such that \(j \in \text{In}\) for a given \(i \in \text{Out}\).

Proof. We perform formal linear algebra manipulations of the system (16.4.3). This differential equation system can be rewritten in the form:

\((\partial I - A(G))x = u\).

Using Cramer’s rule, for \(i \in \text{Out}\) we can “solve” for \(x_i = y_i\) by the formal expression

\[y_i = \frac{\det(B_i)}{\det(\partial I - A(G))},\]

where \(B_i\) is the matrix obtained from \(A(G)\) by replacing the \(i\)th column by \(u\). Clearing denominators and using the Laplace expansion down the \(i\)th column of \(B_i\) yields the formula

\[\det(\partial I - A(G))y_i = \sum_{j \in \text{In}} (-1)^{i+j} \frac{\det(\partial I - A(G))^{ji}}{g_i} u_j.\]

However, this expression need not be minimal. This is the reason for the division by the common factor \(g_i\) in the proposition.

With various reasonable assumptions on the structure of the model, it is often possible to show that for generic parameter choices the greatest common divisor polynomials that appears in Proposition 16.4.3 is one. Recall that a graph is strongly connected if for any pair of vertices \(i, j \in V\) there is a directed path from \(i\) to \(j\).

Proposition 16.4.4. Let \(G\) be a strongly connected graph. If \(\text{Leak} \neq \emptyset\) then the polynomial \(\det(\partial I - A(G))\) is irreducible as a polynomial in \(K(a)[\partial]\).

See [MSE15 Theorem 2.6] for a proof.
Example 16.4.5. Continuing Example 16.4.2 we see that the graph $G$ is strongly connected, so the input/output equation for this system is

$$y^{(3)} + (a_{01} + a_{21} + a_{12} + a_{13} + a_{02} + a_{32})y^{(2)} + (a_{01}a_{12} + a_{01}a_{13} + a_{21}a_{13} + a_{12}a_{13} + a_{01}a_{02} + a_{21}a_{02} + a_{13}a_{02} + a_{01}a_{32} + a_{21}a_{32} + a_{13}a_{32})y^{(1)} =$$

$$a_{12}u^{(1)} + (a_{12} + a_{13} + a_{02} + a_{32})u_1 + (a_{12}a_{13} + a_{13}a_{02} + a_{13}a_{32})u_1$$

One difference between the identifiability analysis of state space models compared to the statistical models studied in the majority of this chapter is that state space models are often not generically identifiable. In spite of the nonidentifiability, the models are still used and analysis is needed to determine which functions of the parameters can be identified from the given input/output data, and how the model might be reparametrized or nondimensionalized so that meaningful inferences can be made.

Example 16.4.6. Consider a modification of the two compartment model from Example 16.4.1 where now there are leaks from both compartments one and two:

$$\begin{align*}
\dot{x}_1 &= -(a_{21} - a_{01})x_1 + a_{12}x_2 + u_1 \\
\dot{x}_2 &= a_{21}x_1 + (-a_{12} - a_{02})x_2
\end{align*}$$

with 1-dimensional output variable $y(t) = Vx_1(t)$. The resulting input-output equation is:

$$\dot{y} + (a_{21} + a_{12} + a_{02} + a_{01})\dot{y} + (a_{01}a_{12} + a_{01}a_{02} + a_{21}a_{02})y = V\dot{u}_1 + V(a_{12} + a_{02})u_1.$$ 

We see that the model has five parameters but there are only 4 nonmonic coefficients in the input/output equation. Hence the model is unidentifiable. However, it is not difficult to see that following quantities are identifiable from the input/output equation:

$$V, \quad a_{12} + a_{02}, \quad a_{21} + a_{01}, \quad a_{12}a_{21}.$$ 

In general, the problem of finding a set of identifiable functions could be phrased in algebraic language as follows.

Problem 16.4.7. Let $c : \mathbb{R}^d \to \mathbb{R}^n$ be a rational map.

- (Rational identifiable functions) Find a “nice” transcendence basis of the field extension $\mathbb{R}(c_1, \ldots, c_m)/\mathbb{R}$.
- (Algebraic identifiable functions) Find a “nice” transcendence basis of the field extension $\mathbb{R}(c_1, \ldots, c_m)/\mathbb{R}$.
The word “nice” is used and appears in quotations because this meaning might depend on the context and does not seem to have a natural mathematical formulation. Nice might mean: sparse, low degree, with each element involving a small number of variables, or each element having a simple interpretation in terms of the underlying application. One strategy to attempt to find identifiable functions in the case when a model is non-identifiable is to use eliminations based on the following result:

**Proposition 16.4.8.** Let \( c : \mathbb{R}^d \to \mathbb{R}^m \) be a polynomial map and the \( I_c \) be the ideal
\[
I_c = \langle c_1(t) - c_1(\theta), \ldots, c_m(t) - c_m(\theta) \rangle \subseteq \mathbb{R}(\theta)[t].
\]
Let \( f \in \mathbb{R}[t] \). Then \( f \) is rationally identifiable if and only if \( f(t) - f(\theta) \in I_c \).

**Proof.** First we consider the variety \( V(I_c) \subseteq \mathbb{R}(\theta)^d \). The interpretation is that for a generic parameter choice \( \theta \), we look at the variety of preimages \( c^{-1}(c(\theta)) \). To say that \( f(t) - f(\theta) \in \sqrt{I_c} \) means that \( f(t) - f(\theta) \) vanishes on the variety \( V(I_c) \) by the Nullstellensatz. In turn, this means that every \( t \in V(I_c) \) has \( f(t) = f(\theta) \), which, since we work of an algebraically closed field implies that \( f(t) \) is rationally identifiable. Finally, Bertini’s theorem implies that generic fibers of a rational map are smooth and reduced, which implies that \( I_c \) is radical, i.e. \( \sqrt{I_c} = I_c \).

Proposition 16.4.8 is used as a heuristic to find identifiable functions that depend on a small number of variables as described in [MED09]. The user inputs the ideal \( I_c \), computes Gröbner bases with respect to random lexicographic orders, and inspects the elements at the end of the Gröbner basis (which only depend on a small number of indeterminates with lowest weight in the lexicographic ordering) for polynomials of the form \( f(t) - f(\theta) \).

16.5. Exercises

**Exercise 16.1.** Prove that the dimension of \( \text{Mixt}^k(M_{X_1 \perp X_2}) \) is \( k(r_1 + r_2 - k) - 1 \) when \( k \leq r_1, r_2 \).

**Exercise 16.2.** Explain how to modify Proposition [16.1.7] to check local identifiability or generic non-identifiability of individual parameters \( s(\theta) \).

**Exercise 16.3.** Consider the linear structural equation model on four random variables whose graph is indicated in Figure [16.5.1]. Which parameters of this model are globally identifiable, locally identifiable, algebraically identifiable, etc.?

**Exercise 16.4.** Complete Example [16.2.8] by showing that all the conditions of Theorem [16.2.7] are satisfied.
Exercise 16.5. Use Theorem 16.2.7 to give a direct proof of Theorem 16.2.4.

Exercise 16.6. Prove that every mixed graph $G$ is the subgraph of some graph $H$ whose linear structural equation model is generically identifiable. (Hint: For each node in $G$ add an instrumental variable that points to it.)

Exercise 16.7. Consider the graph shown in Figure 16.5.2. Suppose that all random variables are binary and that $Y$ is a hidden variable. Show that this model is identifiable up to label swapping on the hidden node $Y$.

Exercise 16.8. Consider the following SIR model for the transmission of infectious diseases. Here $S(t)$ is the number of susceptible individuals, $I(t)$ is the number of infected individuals, $R(t)$ is the number of recovered individuals, and $\beta$ and $\gamma$ are unknown parameters that represent the infection rate and the recovery rate, respectively:

\[
\begin{align*}
\frac{dS}{dt} &= -\beta IS \\
\frac{dI}{dt} &= \beta IS - \gamma I \\
\frac{dR}{dt} &= \gamma I
\end{align*}
\]

(1) Find the nonlinear second order differential equation in $I$ for the dynamics of $I$. (That is, perform differential elimination on this system to find a differential equation in terms of only $I$).
(2) Are the parameters $\beta$ and $\gamma$ generically identifiable from the observation of the trajectory of $I$ alone?

**Exercise 16.9.** Verify that the linear two compartment model of Example 16.4.1 is identifiable when all parameters are real and positive.

**Exercise 16.10.** Explain how the input-output equation of Proposition 16.4.3 should be modified when each output measurement is of the form $y_i(t) = V_i x_i(t)$ where $V_i$ is an unknown parameter.

**Exercise 16.11.** Decide whether or not the model from Example 16.4.2 is identifiable.

**Exercise 16.12.** Consider the linear compartment model whose graph is a chain $1 \rightarrow 2 \rightarrow \cdots \rightarrow n$, with input in compartment 1, output in compartment $n$ and a leak in compartment $n$. Is the model identifiable? What happens if there are more leak compartments besides just compartment $n$?

**Exercise 16.13.** Explain how to modify Proposition 16.4.8 to search for rational functions that are generically rationally identifiable.
Model Selection and Bayesian Integrals

To this point, we have primarily concerned ourselves with statistical tests that were hypothesis tests. These models either reject a hypothesis (usually a model) or conclude that the test was inconclusive. Model selection concerns the situation where there is a collection of models that are under consideration and we would like to choose the best model for the data. A typical situation is that the models themselves are nested, one inside the other $\mathcal{M}_1 \subseteq \mathcal{M}_2$. So, for instance, the likelihood score of $\mathcal{M}_2$ will necessarily be larger than that of $\mathcal{M}_1$, so the likelihood score alone could not be used to decide between the two models. The development of a practical model selection criterion must include some penalty for the fact that the larger model has more parameters/ higher dimensions, and so it is easier for that model to fit better.

Two well-known model selection criteria are the Akaike Information Criterion (AIC) and the Bayesian Information Criterion (BIC). The BIC can be shown to be consistent in a suitable sense provided that the underlying statistical models are smooth. Algebraic geometry enters the picture since many statistical models are not smooth. The singularities of the model can negatively affect the performance of the standard information criteria. To deal with this problem, corrections to the information criteria are needed that take into account the model singularities. This idea was developed in the work of Watanabe, summarized in the book [Wat08]. A primary technique for dealing with the singularities involves computing a resolution of singularities to compute the real log-canonical threshold of the singularity. We illustrate these ideas in this chapter.
17. Model Selection and Bayesian Integrals

17.1. Information Criteria for Regular Models

Fix a statistical model \( \mathcal{P}_\Theta = \{ P_\theta : \theta \in \Theta \} \) with parameter space \( \Theta \in \mathbb{R}^k \). Let

\[
X^{(1)}, \ldots, X^{(n)} \sim P_{\theta_0}
\]

be i.i.d. samples drawn from an unknown true distribution \( P_{\theta_0} \) where \( \theta_0 \in \Theta \). A submodel \( \mathcal{P}_{\Theta_0} \subseteq \mathcal{P}_\Theta \) given by \( \Theta_0 \subseteq \Theta \) is a true model if \( \theta_0 \in \Theta_0 \).

In this chapter, we consider the model selection problem, which attempts to use the information from the sample \( X^{(1)}, \ldots, X^{(n)} \) to find the "simplest" true model from a family of competing models associated with the sets \( \Theta_1, \ldots, \Theta_M \subseteq \Theta \).

We will assume that \( \mathcal{P}_\Theta \) is an algebraic exponential family, and that \( \Theta_1, \ldots, \Theta_M \) are semialgebraic sets of \( \Theta \), so that the \( \mathcal{P}_{\Theta_i} \) are also algebraic exponential families. Also, we suppose that to each distribution \( P_\theta \) is a density function \( p_\theta(x) \). Let

\[
\ell_n(\theta \mid X^{(1)}, \ldots, X^{(n)}) = \sum_{i=1}^{n} \log p_\theta(X^{(i)})
\]

be the log-likelihood function. Note that we include a specific dependence on \( n \) here because we will be interested in what happens as \( n \) tends to infinity.

The typical approach to deciding which of the models \( \mathcal{P}_{\Theta_1}, \ldots, \mathcal{P}_{\Theta_M} \) is a true model is to determine which of the models maximize the log-likelihood function. Letting

\[
\hat{\ell}_n(i) = \sup_{\theta \in \Theta_i} \ell_n(\theta \mid X^{(1)}, \ldots, X^{(n)})
\]

denote the maximum value of the likelihood function, the naive approach to model selection would select the model such that \( \hat{\ell}_n(i) \) is largest. Such a method is not satisfactory in practice because it will tend to pick models that are more complex (e.g., high dimensions) over models that are simple (e.g., low dimensional). Indeed, if \( \Theta_i \subseteq \Theta_j \) then a model selection procedure based solely on the likelihood score would always select the model \( \mathcal{P}_{\Theta_i} \) over \( \mathcal{P}_{\Theta_j} \). To correct for this problem, we modify the likelihood function score value by introducing penalties for the model complexity.

Definition 17.1.1. The information criterion associated to a family of penalty functions \( \pi_n : [M] \to \mathbb{R} \) assigns the score

\[
\tau_n(i) = \hat{\ell}_n(i) - \pi_n(i)
\]

to the \( i \)-th model, for \( i = 1, \ldots, M \).

A number of general purpose information criteria have been proposed in the literature.
Definition 17.1.2. The Akaike information criterion (AIC) \cite{Aka74} uses the penalty function \( \pi_n(i) = \dim(\Theta_i) \). The Bayesian information criterion \cite{Sch98} (sometimes called the Schwarz information criterion) has penalty function \( \pi_n(i) = \frac{1}{2} \dim(\Theta_i) \log(n) \).

The score-based approach to model selection now selects a model for which \( \tau_n(i) \) is maximized. Consistency results for model selection procedures can be formulated for very general classes of models in this context.

Theorem 17.1.3 (Consistency of Model Selection Procedures). Consider a regular exponential family \( \{P_\theta : \theta \in \Theta\} \). Let \( \Theta_1, \Theta_2 \subseteq \Theta \) be arbitrary sets. Denote the standard topological closure of \( \Theta_1 \) by \( \overline{\Theta}_1 \).

1. Suppose that \( \theta_0 \in \Theta_2 \setminus \overline{\Theta}_1 \). If the penalty functions are chosen such that the sequence \( |\pi_n(2) - \pi_n(1)|/n \) converges to zero as \( n \to \infty \), the
   \[ P_{\theta_0}(\tau_n(1) < \tau_n(2)) \to 1, \quad \text{as} \quad n \to \infty. \]

2. Suppose that \( \theta_0 \in \Theta_1 \cap \Theta_2 \). If the sequence of differences \( \pi_n(1) - \pi_n(2) \) diverges to infinity as \( n \to \infty \) then
   \[ P_{\theta_0}(\tau_n(1) < \tau_n(2)) \to 1, \quad \text{as} \quad n \to \infty. \]

Theorem 17.1.3 appears in \cite{Hau88}. Roughly speaking, it says that for reasonable conditions on the penalty functions \( \pi_n \), the model selection criterion will tend to pick the true model as the sample size \( n \) tends to infinity. Note that the AIC satisfies the first part of the theorem and not the second, whereas the BIC satisfies both of these conditions. The takeaway message comparing these two information criteria in the context of the consistency theorem is that the BIC will tend to pick the smaller dimensional model, provided that there is enough data.

Theorem 17.1.3 can be used as the starting point to construct new consistent model selection criteria. However, it is worth understanding how model selection criteria can be derived based on other principles. We will explain in the remainder of this section how the BIC can be derived from considering various Bayesian integrals. These derivations are based on smoothness assumptions concerning the underlying models. The derivations also suggest how to correct information criteria when the underlying model is not smooth, which will occupy the remainder of the chapter.

17.2. Resolution of Singularities and the Log Canonical Threshold

17.3. Information Criteria for Singular Models

17.4. Exercises
Chapter 18

MAP Estimation

In this chapter we consider the Bayesian procedure of maximum a posteriori estimation (MAP estimation) of hidden states in a hidden variable model given fixed values of the observed states and either fixed values or distribution on the model parameters. The estimation of hidden states given observed states and fixed parameter values is a linear optimization problem over potentially exponentially many possibilities for the hidden states. In graphical models based on trees or graphs with low complexity, it is possible to compute the MAP estimate rapidly using message passing algorithms. The most famous algorithm of this type is the Viterbi algorithm, which is specifically developed for Hidden Markov Models [Vit67]. More general message passing algorithms include the belief propagation algorithm [Pea82] and the generalized distributive law [AM00]. Computations for these message passing algorithms can be expressed in the context of tropical arithmetic, which we will introduce in Section 18.2. This connection appears to originate in the work of Pachter and Sturmfels [PS04].

To perform true MAP estimation requires a prior distribution over the parameters and calculating the posterior probabilities of each of the possible for hidden state vectors to get a distribution over hidden state vectors. These probability are typically approximated using Monte Carlo algorithms. As we shall see, normal fans of polytopes can be an important tool in analyzing the sensitivity of the basic MAP estimate to changes in the underlying parameters. This variation on the problem is usually called parametric inference [FBSS02]. The approaches for computing the appropriate normal fan for the parametric inference problem can also be approached using a recursive iterative procedure akin to the Viterbi algorithm, but in an algebra who elements are the polytopes themselves (or, their normal fans). We
illustrate these ideas in the present chapter focusing on the special case of
the hidden Markov model.

18.1. Hidden Markov Models

The hidden Markov model is a special case of a graphical model with hidden
variables, where the graph is a specific tree structure. The underlying tree
is sometimes called the *caterpillar tree*.

Let $Y_1, \ldots, Y_n$ be discrete random variables, all with the same state space $[r]$, and let $X_1, \ldots, X_n$ be discrete random variables all with the same state space $[s]$. We assume that the sequence $Y_1, \ldots, Y_n$ form a homogeneous Markov chain with transition matrix

$$A = (a_{i_1i_2})_{i_1, i_2 \in [r]} \in \mathbb{R}^{r \times r},$$

i.e.

$$P(Y_k = i_2 | Y_{k-1} = i_1) = a_{i_1i_2}.$$ 

To start the Markov chain we also need a root distribution $\pi \in \Delta_r$,
where

$$P(Y_1 = i) = \pi_i.$$ 

There is also an *emission matrix* $B = (b_{i_kj_k})_{i_k \in [r], j_k \in [s]} \in \mathbb{R}^{r \times s}$ which gives the probability of observing $X_k$ given the values of $Y_k$, i.e.

$$P(X_k = j_k | Y_k = i_k) = b_{i_kj_k}.$$ 

In addition to the Markov chain assumption, the hidden Markov model makes the further assumption of conditional independence:

$$X_k \independent (Y_1, \ldots, Y_{k-1}, X_1, \ldots, X_{k-1}) | Y_k$$

for $k = 2, \ldots, n$. With these assumptions on the random variables, the joint distribution of $Y = i = (i_1, \ldots, i_n)$ and $X = j = (j_1, \ldots, j_n)$ is given by the following formula

$$(18.1.1) \quad p_{i,j} = \pi_{i_1} \prod_{k=2}^{n} a_{i_{k-1}i_k} \prod_{k=1}^{n} b_{i_kj_k}. $$
In the Hidden Markov model, the variables $Y_1, \ldots, Y_n$ are hidden variables, so only the variables $X_1, \ldots, X_n$ are observed. Hence, the probability distribution that would actually be observed is given by the formula

\[(18.1.2) \quad p_j = \sum_{i \in [r]} p_{i,j} = \sum_{i \in [r]} \pi_i \prod_{k=2}^{n} a_{i_{k-1}i_k} \prod_{k=1}^{n} b_{i_kj_k}.\]

So in the hidden Markov model we assume that there is a homogeneous Markov chain $Y = (Y_1, \ldots, Y_n)$ that we do not get to observe. Instead we only observe $X = (X_1, \ldots, X_n)$ which could be considered a noisy version of $Y$, or rather, some type of probabilistic shadow of $Y$.

**Example 18.1.1 (Occasionally Dishonest Casino).** We illustrate the idea of the Hidden Markov model with a simple running example that we learned in \[DEKM98\]. Consider a casino that uses fair dice and loaded dice in some of their rolls. The fair die has a probability distribution $\left(\frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}\right)$ of getting $1,2,\ldots,6$, respectively whereas the loaded die has probability distribution $\left(\frac{1}{20}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}, \frac{1}{20}, \frac{3}{4}\right)$. If the die currently being used is a fair die, there is a .1 chance that the casino secretly swaps out the fair die with a loaded die. The the die currently being used is the loaded die there is a .05 chance that the casino secretly swaps out the loaded die for the fair die. Further suppose that the probability that the process starts with a fair die is .8.

After $n$ rolls we have two sequences $X \in [6]^n$ consisting of the sequence of die rolls, and the $Y \in [2]^n$ consisting of whether the die used was fair or loaded. As a visitor to the casino, we only observe $X$ and not $Y$. Note that this setup gives us a hidden Markov model with the following parameters:

\[\pi = (.8, .2), \quad A = \begin{pmatrix} .9 & .1 \\ .05 & .95 \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} & \frac{1}{6} \\ \frac{1}{20} & \frac{1}{20} & \frac{1}{20} & \frac{1}{20} & \frac{1}{20} & \frac{3}{4} \end{pmatrix}\]

From a practical standpoint, one might be interested in estimating whether or not the casino was likely to have used the loaded die, given an observation $X$ of rolls. We will explain how to do this use the Viterbi algorithm, later.

Hidden Markov models are used in a wide range of contexts. Perhaps their most well-known uses are in text and speech recognition and more broadly in signal processing. In these applications, the hidden states might correspond to letters and phonemes, respectively. The observed states are noisy versions of these things (and typically in this context they would be modeled by continuous random variables). The underlying Markov chain would be a first order Markov chain that approximates the probability that one letter (or phoneme) follows another in the language being modeled. The HMM is used to try to infer what the writer or speaker wrote or said based on the noisy sequence of signals received. A number of texts are
devoted to applications and practical aspects of using Hidden Markov models [EAM95, ZM09]. HMMs in the discrete setting laid out in this chapter also play an important role in bioinformatics. They are used to annotate DNA sequences to determine which parts code for proteins. More complex version (e.g. the pair hidden Markov model) can be used to give a probabilistic approach to sequence alignment. See [DEKM98] for more details about these biological applications.

A number of computational issues arise when trying to use the HMM on real data. The most basic question is the computation of the probability \( p_j \) itself. In the HMM, it is typically assumed that \( n \) is large, so applying the formula (18.1.2) directly would involve calculating a sum over \( r^n \) terms, which is exponential in \( n \). The standard approach to simplify the computational complexity is to apply the distributive law to reduce the number of terms at each step, while adding temporary storage of size \( r \). In symbols, we can represent this situation like this:

\[
p_j = \sum_{i_1 \in [r]} \pi_{i_1} b_{i_1 j_1} \left( \sum_{i_2 \in [r]} a_{i_1 i_2} b_{i_2 j_2} \left( \sum_{i_3 \in [r]} a_{i_2 i_3} b_{i_3 j_3} \left( \cdots \right) \right) \right).
\]

Starting at the inside and working out, we see that at each step we are essentially performing a matrix-vector multiplication of an \( r \times r \) matrix with a vector of length \( r \). These matrix-vector multiplications need to be formed \( n \) times. This leads to an algorithm that has a running time that is \( O(r^2 n) \). Since \( r \) is usually not too big, and fixed, but \( n \) could grow large, this is a desirable form for the computational complexity.

**Algorithm 18.1.2 (Calculation of marginal probability in HMM).**
*Input:* \( A \in \mathbb{R}^{r \times r}, B \in \mathbb{R}^{r \times s}, \pi \in \Delta_r, j \in [s]^n \)
*Output:* \( p_j \)

- **Initialize:** \( c = (c_1, \ldots, c_r) \) with \( c_\alpha = 1 \) for \( \alpha \in [r] \).
- **For** \( k = n, \ldots, 2 \) **do**
  - **Update** \( c_\alpha = \sum_{\beta=1}^r a_{\alpha \beta} b_{\beta j_2} c_\beta \).
- **Output:** \( p_j = \sum_{\beta=1}^r \pi_\beta b_{\beta j_1} c_\beta \).

Since at each step of the algorithm we perform \( 2r^2 \) multiplications and \( r(r-1) \) additions, this results in an \( O(r^2 n) \) algorithm, considerably faster than the naive \( O(n^2) \) algorithm. If \( r \) is very large, it can be necessary to consider the special structure built into \( A \) and \( B \), and tools like the fast Fourier transform to try to speed up this computation further.

A similar type of computation can be performed to calculate certain conditional probability of the hidden states given the parameter values and
the values of the observed variables, i.e.
\[ P(Y_k = i_k | X = j, \pi, A, B). \]

The EM-algorithm is typically used to compute estimates of the model parameters \( \pi, A, B \), given many observations of sequences \( X \).

18.2. The Viterbi Algorithm and Tropical Arithmetic

The Viterbi algorithm is a procedure for the HMM that, for given fixed values of the parameters \( \pi, A, B \), and a particular observation \( j \), finds the maximum a posteriori estimate of the hidden sequence \( i \). That is, we are interested in computing the hidden sequence \( i \in [r]^n \) that maximizes the probability \( p_{i,j} \), i.e. solving the following problem

\[
(18.2.1) \quad \arg \max_{i \in [r]^n} p_{i,j}.
\]

The calculation of the most likely value of the hidden states involves potentially evaluating \( p_{i,j} \) for all the exponentially many different strings \( i \in [r]^n \). The Viterbi algorithm is a procedure that implements the computation that finds the maximizing \( i \) with only \( O(r^2 n) \) arithmetic operations. A mathematically appealing way to explain how to run the Viterbi algorithm involves computations in the tropical semiring.

**Definition 18.2.1.** The tropical semiring consists of the extended real numbers \( \mathbb{R} \cup \{ -\infty \} \) together with the operations of tropical addition \( x \oplus y = \max(x,y) \) and tropical multiplication \( x \otimes y = x + y \).

The triple \( (\mathbb{R} \cup \{ -\infty \}, \oplus, \otimes) \) satisfies all the properties of a semiring, in particular the associative laws for both tropical addition and multiplication, and the distributive law of tropical multiplication over tropical addition. The “semi” part of the semiring is for the fact that elements do not have tropical additive inverses in the tropical semiring. (However, there are multiplicative inverses for all but the additively neutral element, so \( (\mathbb{R} \cup \{ -\infty \}, \oplus, \otimes) \) is in fact, a semifield.)

We now explain how computations in the tropical semiring are useful for rapidly computing the optimal value \( \max_{i \in [r]^n} p_{i,j} \), which in turn leads to the Viterbi algorithm. The first observation is that

\[
\arg \max_{i \in [r]^n} \log p_{i,j}
\]

is a linear optimization problem. Indeed, substituting in the expression for \( p_{i,j} \), we have

\[
\max_{i \in [r]^n} p_{i,j} = \max_{i \in [r]^n} \prod_{k=2}^{n} a_{i_{k-1}i_k} \prod_{k=1}^{n} b_{i_kj_k}.
\]
Let $\tilde{a}_{ij} = \log a_{ij}$, $\tilde{b}_{ij} = \log b_{ij}$ and $\tilde{\pi}_i = \log \pi_i$. Taking logarithms on both sides yields

$$\max_{i \in [r]^n} \log p_{i,j} = \max_{i \in [r]^n} \tilde{\pi}_i + \tilde{b}_{i_1,j_1} + \sum_{k=2}^n \left( \tilde{a}_{i_{k-1},i_k} + \tilde{b}_{i_k,j_k} \right).$$

Now we convert this to an expression in terms of the tropical arithmetic operations:

$$\bigoplus_{i_1 \in [r]} \cdots \bigoplus_{i_n \in [r]} \tilde{\pi}_{i_1, \ldots, i_n} \otimes \tilde{b}_{i_1,j_1} \otimes \bigotimes_{k=2}^n \left( \tilde{a}_{i_{k-1},i_k} + \tilde{b}_{i_k,j_k} \right).$$

Note that this is the same form as the formula for computing $p_j$ with $a_{ij}, b_{ij}, \pi_i$ replaced by $\tilde{a}_{ij}, \tilde{b}_{ij}, \tilde{\pi}_i$ and with the operations of $+$ and $\times$ replaced by $\oplus$ and $\otimes$ respectively. Since both $(\mathbb{R}, +, \times)$ and $(\mathbb{R} \cup \{-\infty\}, \oplus, \otimes)$ are semifields, we can apply the exact same form of the distributive law to simplify the calculation of $\max_{i \in [r]^n} \log p_{i,j}$. Indeed, the expression simplifies to

$$\bigoplus_{i_1 \in [r]} \tilde{\pi}_{i_1, \ldots, i_n} \otimes \tilde{b}_{i_1,j_1} \otimes \left( \bigoplus_{i_2 \in [r]} \tilde{a}_{i_2,i_2} \otimes \tilde{b}_{i_2,j_2} \otimes \left( \bigoplus_{i_3 \in [r]} \tilde{a}_{i_3,i_3} \otimes \tilde{b}_{i_3,j_3} \otimes \left( \cdots \right) \right) \right).$$

This formula/rearrangement of the calculation yields an $O(r^2n)$ algorithm to compute the maximum. Of course, what is desired in practice is not only the maximum value but the string $i$ that achieves the maximum. It is easy to modify the spirit of the formula to achieve this. Namely, one stores an $r \times n$ matrix of pointers which point from one entry to the next optimum value in the computation.

**Algorithm 18.2.2 (Viterbi Algorithm).**

**Input:** $A \in \mathbb{R}^{r \times r}, B \in \mathbb{R}^{r \times s}, \pi \in \Delta_r, j \in [s]^n$

**Output:** $i \in [r]^n$ such that $p_{ij}$ is maximized, and $\log p_{ij}$.

- **Initialize:** $c = (c_1, \ldots, c_r)$ with $c_\alpha = 0$ for $\alpha \in [r]$, $\tilde{a}_{ij} = \log a_{ij}, \tilde{b}_{ij} = \log b_{ij}, \tilde{\pi}_i = \log \pi_i$
- **For** $k = n, \ldots, 2$ do
  - $d_{ak} = \arg \max_{\beta \in [r]} (\tilde{a}_{\alpha \beta} \otimes \tilde{b}_{\beta j_k} \otimes c_\beta)$ for $\alpha \in [r]$.
  - Update $c_\alpha = \bigoplus_{\beta \in [r]} (\tilde{a}_{\alpha \beta} \otimes \tilde{b}_{\beta j_k} \otimes c_\beta)$ for $\alpha \in [r]$.
- **Compute** $d_1 = \arg \max_{\beta \in [r]} (\tilde{\pi}_\beta \otimes \tilde{b}_{\beta j_1} \otimes c_\beta)$
- **Define the sequence** $i$ by $i_1 = d_1$ and $i_k = d_{i_{k-1},k}$ for $k = 2, \ldots, n$.
- **$\log p_{ij} = \bigoplus_{\beta \in [r]} (\tilde{\pi}_\beta \otimes \tilde{b}_{\beta j_1} \otimes c_\beta)$**

Illustrate with example and explain how to do the pointers better.
18.3. MAP Estimation, Parametric Inference, and Normal Fans

The maximum a posteriori estimate for a model is the parameter value of the model that maximizes the posterior distribution. That is, given a model $P_\Theta = \{p_\theta(x) : \theta \in \Theta\}$ with density functions $p_\theta$, a prior distribution $\pi(\theta)$ on $\Theta$ and data $x$, the MAP estimate of the parameters is

$$\arg \max_{\theta \in \Theta} \frac{p_\theta(x)\pi(\theta)}{\int_{\Theta} p_\theta(x)\pi(\theta)d\mu(\theta)}.$$ 

In some sense, the MAP estimate is analogous to the MLE in frequentist statistics, because it is a mode of a function that comes out of the model and data. Note that the denominator, $\int_{\Theta} p_\theta(x)\pi(\theta)d\mu(\theta)$, is the marginal likelihood integral which played a prominent role in Chapter 17. While this expression is difficult to compute, it does not depend on $\theta$ and hence it is not actually necessary to calculate it to perform the optimization. Computing the MAP estimate is one part of Bayesian analysis. While other Bayesian methods consider properties of the entire posterior distribution, it can be useful to have a single or low dimensional summary of this complicated distribution. One such summary is the posterior mode, i.e. the MAP estimate of the parameters.

In latent variable models like the HMM, it is often the case that one considers both the continuous parameters (the root distribution $\pi$, the transition matrix $A$, and the emission matrix $B$) and the hidden random variables themselves as model parameters. This perspective is frequently taken in a machine learning context. In the simplest setting, one assume that the prior distribution has all mass on one particular choice of parameter values. This is the setting we explored in the previous section. So the calculation of the MAP estimate is concerned with determining the single choice of hidden states the maximizes the joint probability of the observed and hidden states. This setting assumes an absolute certainty about the values of the model parameters, an assumptions that is frequently made, but lacks justification in many setting. This naturally leads to the question: how does the MAP estimate vary as those fixed model parameters vary? This study of the sensitivity of the inference of the MAP estimate to the parameter choices is called parametric inference. For this specialized version of the MAP estimation problem to the more general MAP estimation problem, it becomes useful to understand the polyhedral geometry inherent in measuring how the variation of a cost vector in linear optimization affects the result of the optimization. From an algebraic perspective, we need to compute the normal fan of the Newton polytope of the associated polynomial $p_j = f(\pi, A, B)$. The definitions of Newton polytope and normal fan appear in Section 12.3.
We will illustrate these ideas in the case of the HMM, though the ideas also apply more widely. Perhaps the most well-known context where this approach is applied is in sequence alignment [FBSS02, GBN94, Vin09].

Now we explain how polyhedral geometry comes into play. To each pair \( i \in [r]^m \) and \( j \in [s]^n \), we have the monomial

\[
p_{i,j} = \pi_{i_1} b_{i_1 j_1} a_{i_1 i_2} \cdots a_{i_{n-1} i_n} b_{i_n j_n}
\]

Let \( \theta = (\pi, A, B) \) be the vector of model parameters. We can write

\[
p_{i,j} = \theta^{u_{i,j}}
\]

for some integer vector \( u_{i,j} \). For fixed values of \( \theta \) we want to compute

\[
\arg \max_{i \in [r]^n} \theta^{u_{i,j}} = \arg \max_{i \in [r]^n} (\log \theta)^T \cdot u_{i,j}
\]

Let \( c = \log \theta \), where the logarithm is applied coordinate-wise. Assuming that we can recover \( i \) from \( u_{i,j} \), we can express the problem instead as solving the optimization problem

\[
\max_{i \in [r]^n} c^T u_{ij}.
\]

Since \( c \) is a linear functional, we could instead solve the optimization problem

\[
\max_{u \in Q_j} c^T u \quad \text{where} \quad Q_j = \text{conv}(u_{i,j} : i \in [r]^m).
\]

The polytope \( Q_j \) reveals information about the solution to the MAP estimation problem. Indeed, if we want to know which parameter values \( \theta \) yield a given \( i \) as the optimum, this is obtained by determining the cone of all \( c \) that satisfy that

\[
\max_{u \in Q_j} c^T u = c^T u_{ij}
\]

and intersecting that cone with the set of vectors of the form \( \log \theta \). Without the log-theta constraint, the set of all such \( c \) is the normal cone to \( Q_j \) at the point \( u_{ij} \). So the complete solution to the parametric optimization problem for all choices of optimum vector is the normal fan of the polytope \( Q_j \). This is summarized in the following proposition.

**Proposition 18.3.1.**

The normal fan of the Newton polytope is also useful in the more general Bayesian setting of MAP estimation. Here we would like to know the distribution over possible hidden sequences \( i \) given a distribution on the parameters and the observed sequence \( j \). The only sequences with non-zero probability will be the ones corresponding to vertices of the polytope \( Q_j \). The posterior probability of such a sequence is obtained by integrating out the prior distribution on parameters over the normal cone at the corresponding vertex of \( Q_j \). While these integrals can be rarely calculated in closed form, the geometry of the solution can help to calculate the posterior probabilities.
18.4. Polytope Algebra

The polytopes $Q_j = \text{Newt}(p_j(A,B,\pi)$ reveal information about how the MAP estimate varies as the underlying parameters vary. A priori, it seems hopeless to actually compute these polytopes, as they are the convex hulls of the $r^n$ points $u_{i,j}$, clearly exponential in the length $n$. We will see in this section, however, that they only have polynomially many vertices as a function of $n$, and there are a number of clever algorithms for computing all the vertices without running through all the points $u_{i,j}$.

It is not difficult to see directly that there are at most a polynomial number of vertices of $Q_j$, as a function of $n$. Indeed, there are a total of $r + r^2 + rs$ parameters in the $\pi, A, B$, so each $u_{i,j}$ is a vector of length $r + r^2 + rs$. The sum of the coordinates of each $u_{i,j}$ is $2n$, since this is the number of terms in the monomial representing $p_{i,j}$. A basic fact from elementary combinatorics is that the total number of distinct nonnegative integer vectors $u \in \mathbb{N}^k$ such that $\sum_{i=1}^k u_i = m$ is \binom{m+k-1}{k-1}. When $k$ is fixed, this is a polynomial of degree $k-1$ as a function of $m$. Hence, when computing the convex hull to get $Q_j$, there are at most \binom{2n+r+r^2+rs-1}{r+r^2+rs-1}$ distinct points, which gives a naive bound on the number of vertices of $Q_j$. As a function of $n$, this is a polynomial of degree $r + r^2 + rs - 1$.

In fact, it is possible to derive a lower order polynomial bound on the number of vertices of $Q_j$ than this, using a classic result of Andrews that bounds the number of vertices of a lattice polytope in terms of its volume.

**Theorem 18.4.1.** [And63] For every fixed integer $d$ such that the number of vertices of any convex lattice polytope $Q$ in $\mathbb{R}^d$ is bounded above by $C_d \text{vol}(P)^{(d-1)/(d+1)}$.

Note that the polytope $Q_j$ is not $r + r^2 + rs$ dimensional, and in fact, there will be linear relations that hold between entries in the $u_{i,j}$ vectors. In fact, it is not hard to see that this polytope will generally be $(r-1)(s+1)+r^2$ dimensional for general $j$ and large enough $n$. We can project all the $u_{i,j}$’s onto a subset of the coordinates so that it will then be a full dimensional polytope in a suitable $\mathbb{R}^{(r-1)(s+1)+r^2}$ and will still be a lattice polytope. Since all coordinates of the projects of $u_{i,j}$ will be of size $\leq n$, we see that the $\text{vol}(Q_j) \leq n^{(r-1)(s+1)+r^2}$ combining this with Andrew’s theorem, we get the following bound:

**Corollary 18.4.2.** Let $D = (r-1)(s+1) + r^2$. The polytope $Q_j$ has at most $C_D n^{D(D-1)/(D+1)}$ vertices.

These types of bounds can be extended more generally to similar MAP estimation problems for directed graphical models with a fixed number of parameters. Results of this kind are developed in [EW07, Jos05]. Of
course, we are not only interested in knowing bounds on the number of vertices, but we would like to have algorithms for actually computing the vertices.

18.5. Exercises

Exercise 18.1. Explain how to construct a variation on Algorithm 18.1.2 to compute the conditional probabilities $P(Y_k = i_k | X = j, \pi, A, B)$. 

Finite Metric Spaces

This chapter concerns metric spaces consisting of finitely many points. Such metric spaces are occur in various contexts in algebraic statistics. Particularly, finite metric spaces arise when looking at phylogenetic trees. Finite metric spaces are also connected to some problems that arise with Gaussian graphical models, and have some relationships to hierarchical models. A key role in this side of the theory is played by the cut polytope. We elucidate these connections in this chapter.

19.1. Metric Spaces and The Cut Polytope

In this section, we explore key facts about finite metric spaces and particularly results about embedding metrics within other metric spaces with specific properties. Here we are summarizing some of the key results that appear in the book of Deza and Laurent [DL97].

Definition 19.1.1. Let $\mathcal{X}$ be a finite set. A dissimilarity map on $\mathcal{X}$ is a function $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ such that $d(x, y) = d(y, x)$ for all $x, y \in \mathcal{X}$ and $d(x, x) = 0$ for all $x \in \mathcal{X}$.

Note that we are explicitly allowing negative numbers as possible dissimilarities between elements of $\mathcal{X}$.

Definition 19.1.2. Let $\mathcal{X}$ be a finite set. A dissimilarity map on $\mathcal{X}$ is a semimetric if it satisfies the triangle inequality

$$d(x, y) \leq d(x, z) + d(y, z)$$

for all $x, y, z \in \mathcal{X}$. We denote the pair together as a metric space by $(\mathcal{X}, d)$. 
In the triangle inequality we allow that \( y = z \), in which case we deduce that \( d(x, y) \geq 0 \) for all \( x, y \in \mathcal{X} \) for any metric. If \( d(x, y) > 0 \) for all \( x \neq y \in \mathcal{X} \) then \( d \) is called a metric.

**Definition 19.1.3.** Let \((\mathcal{X}, d)\) and \((\mathcal{Y}, d')\) be metric spaces. We say that \((\mathcal{X}, d)\) embeds isometrically in \((\mathcal{Y}, d')\) if there is a map \( \phi : \mathcal{X} \to \mathcal{Y} \) such that \( d'(\phi(x), \phi(y)) = d(x, y) \) for all \( x, y \in \mathcal{X} \).

The notion of being able to embedded \((\mathcal{X}, d)\) isometrically from one space into another is most interesting in the case where \( \mathcal{Y} \) is an infinite space and \( d' \) is some standard metric, for instance an \( L^p \) metric space, where \( \mathcal{Y} = \mathbb{R}^k \) and

\[
d'(x, y) = d_p(x, y) := \left( \sum_{i=1}^{k} |x_i - y_i|^p \right)^{1/p}.
\]

**Definition 19.1.4.** Let \((\mathcal{X}, d)\) be a finite metric space. We say that \((\mathcal{X}, d)\) is \( L^p \) embeddable if there exists an \( k \) such that \((\mathcal{X}, d)\) is isometrically embeddable in \((\mathbb{R}^k, d_p)\).

Let \( \mathcal{X} \) be a finite set with \( m \) elements. The set of all semimetrics on \( \mathcal{X} \) is a polyhedral cone in \( \mathbb{R}^{m(m-1)/2} \) defined by the \( 3 \binom{m}{3} \) triangle inequalities together with the \( \binom{m}{2} \) nonnegativity inequalities. It is denoted \( \text{Met}_m \). The set of \( L^1 \) embeddable semimetrics forms a polyhedral subcone of the metric called the cut cone, which we describe now.

**Definition 19.1.5.** Let \( \mathcal{X} \) be a finite set with \( m \) elements and let \( A | B \) be a split of \( \mathcal{X} \). The cut semimetric of \( A | B \) is the semimetric \( \delta_{A|B} \) with

\[
\delta_{A|B}(x, y) = \begin{cases} 
1 & \text{if } \#(\{x, y\} \cap A) = 0 \\
0 & \text{otherwise}.
\end{cases}
\]

The cone generated by all \( 2^{m-1} \) cut semimetrics is the cut cone, denoted \( \text{Cut}_m \). The polytope obtained by taking the convex hull of all cut semimetrics is the cut polytope, denoted \( \text{Cut}_m^\square \).

Note that in the cut polytope we are allowing the split \( \emptyset | \mathcal{X} \) which gives the boring cut semimetric \( \delta_{\emptyset|\mathcal{X}} = 0 \). This is necessary for reasons of symmetry.

**Example 19.1.6.** Let \( m = 4 \). Then the cut polytope \( \text{Cut}_4^\square \) is the polytope whose vertices are the eight cut semimetrics which are the columns of the
19.1. Metric Spaces and The Cut Polytope

following matrix

\[
\begin{pmatrix}
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\]

The cut cone characterizes $L^1$ embeddability.

**Proposition 19.1.7.** A finite metric space $([m],d)$ is $L^1$ embeddable if and only if $d \in \text{Cut}_m$.

**Proof.** First suppose that $d \in \text{Cut}_m$. This means

\[d = \sum_{j=1}^{k} \lambda_{A_j|B_j} \delta_{A_j|B_j}\]

for some $k$ and some positive constants $\lambda_{A_j|B_j}$. Let $u_1, \ldots, u_m \in \mathbb{R}^k$ in the vectors such that

\[(u_i)_j = \begin{cases} \\
\frac{\lambda_{A_j|B_j}}{2} & \text{if } i \in A_j \\
-\frac{\lambda_{A_j|B_j}}{2} & \text{if } i \in B_j \\
\end{cases}\]

Then $d_1(u_i, u_{i'}) = \sum_{j=1}^{k} |(u_i)_j - (u_{i'})_j| = d(i, i')$ since $|(u_i)_j - (u_{i'})_j| = \lambda_{A_j|B_j}$ if $\#(\{i, i'\} \cap A_j) = 1$ and $|(u_i)_j - (u_{i'})_j| = 0$ otherwise.

Conversely, suppose that there exist $k$ and $u_1, \ldots, u_m \in \mathbb{R}^k$ such that $d(i, i') = d_1(u_i, u_{i'})$. We must show that $d$ is in the cut cone $\text{Cut}_m$. Being $L^1$-embeddable is additive on dimensions of the embedding, i.e. if $u_1, \ldots, u_m \in \mathbb{R}^k$ gives a realization of a metric $d$, and $u'_1, \ldots, u'_m \in \mathbb{R}^{k'}$ gives a realization of a metric $d'$ then $(u_1, u'_1), \ldots, (u_m, u'_m)$, gives a realization of the metric $d + d'$ as an $L^1$ embedding. Hence, we may suppose that $k = 1$. Furthermore, suppose that $u_1 \leq u_2 \leq \cdots \leq u_m$. Then it is straightforward to check that

\[d = \sum_{j=1}^{k-1} (u_{j+1} - u_j) \delta_{[j][m]\setminus[j]} \quad \square \]

Although the cut cone and cut polytope have a simple description in terms of listing their extreme rays, any general description of their facet defining inequalities remains unknown. Part V of [DL97] contains descriptions of many types of facets of these polytopes, but the decision problem of determining whether or not a given dissimilarity map $d$ belongs to the cut cone is known to be NP-complete.

The cut cone and the cut polytope are connected to probability theory via their relation to joint probabilities and the correlation polytope. We
explain this material next by first relating the results to measure spaces. For two sets $A, B$ let $A \triangle B$ denote the symmetric difference.

**Proposition 19.1.8.** A dissimilarity map $d : [m] \times [m] \to \mathbb{R}$ is in the cut cone $\text{Cut}_m$ (respectively, cut polytope $\text{Cut}^\square_m$) if and only if there is a measure space (respectively, probability space) $(\Omega, \mathcal{A}, \mu)$ and subsets $S_1, \ldots, S_m \in \mathcal{A}$ such that $d(i, j) = \mu(S_i \triangle S_j)$.

**Proof.** First suppose that $d \in \text{Cut}_m$, so that

$$d = \sum_{j=1}^{k} \lambda_{A_j|B_j} \delta_{A_j|B_j}$$

with $\lambda_{A_j|B_j} \geq 0$. We will construct a measure space with the desired properties. Let $\Omega$ be $2^{[m]}$, the power set of $[m]$, and let $\mathcal{A}$ consist of all subsets of $2^{[m]}$. For a set $S \subseteq \mathcal{A}$ define

$$\mu(S) = \sum_{A_i \in S} \lambda_{A_i|B_i}$$

(Here we will treat two splits $A|B$ and $B|A$ as different from each other, although they produce the same cut semimetrics $\delta_{A|B}$.) Let $S_i = \{S \in \Omega : i \in S\}$. Then

$$\mu(S_i \triangle S_j) = \mu(\{A \in \Omega : \#(A \cap \{i, j\}) = 1\}) = \sum_{A \in \Omega : \#(A \cap \{i, j\}) = 1} \lambda_{A|B} = d(i, j).$$

Furthermore, if $d \in \text{Cut}^\square_m$ then $\sum \lambda_{A|B} = 1$ which implies that $\mu(\Omega) = 1$, i.e. $(\Omega, \mathcal{A}, \mu)$ is a probability space.

Similar reasoning can be used to invert this construction, i.e. given a measure space and subsets $S_1, \ldots, S_m$, one can show that $d(i, j) = \mu(S_i \triangle S_j)$ yields an element of the cut cone. \qed

An analogous result concerns elements of the semigroup generated by the cut semimetrics.

**Proposition 19.1.9.** A dissimilarity $d : [m] \times [m] \to \mathbb{R}$ has the form $d = \sum_{j=1}^{k} \lambda_{A_j|B_j} \delta_{A_j|B_j}$ where $\lambda_{A_j|B_j}$ are nonnegative integers for $j = 1, \ldots, k$ if and only if there are finite sets $S_1, \ldots, S_m$ such that $d(i, j) = \#(S_i \triangle S_j)$.

Proposition 19.1.8 suggests that the cut cone, or a cone over the cut polytope, should be related to the cone of sufficient statistics of a discrete exponential family, since, for many natural occurring models, those cones have the interpretation as cones that record moments of some particular functions of the random variables. This is made precise by the correlation cone, correlation polytope, and a mapping between this object and corresponding cut objects.
**Definition 19.1.10.** Let \( \mathcal{X} \) be a finite set with \( m \) elements. For each \( S \subseteq \mathcal{X} \) let \( \pi_S \) be the *correlation vector* in \( \mathbb{R}^{(m+1)^2} \) whose coordinates are indexed by pairs \( i, j \in \mathcal{X} \) of not necessarily distinct elements with
\[
\pi_S(i, j) = \begin{cases} 
1 & \text{if } \{i, j\} \subseteq S \\
0 & \text{otherwise}.
\end{cases}
\]
The *correlation cone* \( \text{Corr}_m \) is the polyhedral cone generated by all \( 2^m \) correlation vectors \( \pi_S \). The correlation polytope \( \text{Corr}^\square_m \) is the convex hull of the \( 2^m \) correlation vectors.

**Example 19.1.11.** Let \( m = 3 \). Then the correlation polytope is the polytope whose vertices are the columns of the following matrix:
\[
\begin{pmatrix}
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 
\end{pmatrix}.
\]

The correlation mapping turns the cut cone into the correlation cone, and the cut polytope into the correlation polytope. To describe this we need to denote the coordinates on the ambient spaces for these objects in the appropriate way. The natural coordinates on space of dissimilarity maps is the set of \( d(i, j) \) where \( i, j \) is an unordered pair of distinct elements of \([m]\). The natural coordinates on the space of correlations are denoted \( p_{ij} \) where \( i, j \) is an unordered pair of not necessarily distinct elements of \([m]\).

**Definition 19.1.12.** Consider the mapping from \( d(i, j) \) to \( p_{ij} \) coordinates defined by the rule:
\[
\begin{align*}
p_{ii} &= d(i, m + 1) & \text{if } 1 \leq i \leq m \\
p_{ij} &= \frac{1}{2}(d(i, m + 1) + d(j, m + 1) - d(i, j)) & \text{if } 1 \leq i < j \leq m.
\end{align*}
\]
This map is called the *covariance mapping* and denoted \( \xi \).

Note that the corresponding inverse mapping satisfies
\[
\begin{align*}
d(i, m + 1) &= p_{ii} & \text{if } 1 \leq i \leq m \\
d(i, j) &= p_{ii} + p_{jj} - 2p_{ij} & \text{if } 1 \leq i < j \leq m.
\end{align*}
\]

**Proposition 19.1.13.** The correlation mapping sends the cut cone to the correlation cone and the cut polytope to the correlation polytope. That is
\[
\xi(\text{Cut}_{m+1}) = \text{Corr}_m \quad \text{and} \quad \xi(\text{Cut}^\square_{m+1}) = \text{Corr}^\square_m.
\]

**Proof.** Write a split of \([m+1]\] in a unique way \( A|B \) so that \( m+1 \in B \). It is straightforward to check that \( \xi(\delta_{A|B}) = \pi_A \).
\[\Box\]
The curious reader might try to verify this on Examples 19.1.6 and 19.1.11. Note that the operation from the correlation mapping allows us to easily transfer results about the polyhedral description from the cut side to the correlation side, and vice versa.

Applying the correlation mapping to Proposition 19.1.8, one can deduce the following Proposition, which explains the name correlation cone and correlation polytope.

**Proposition 19.1.14.** A correlation vector \( p \) belongs to the correlation cone (respectively correlation polytope) if and only if there exists events \( S_1, \ldots, S_m \) be events in a measure space \( (\Omega, \mathcal{A}, \mu) \) (respectively, probability space) such that \( p_{ij} = \mu(S_i \cap S_j) \).

If \( X_1, \ldots, X_m \) are indicator random variables of the events \( S_1, \ldots, S_m \) respectively then clearly

\[
p_{ij} = \mu(S_i \cap S_j) = E[X_i X_j].
\]

This means that the cone over the correlation polytope (by lifting each correlation vector \( \pi_S \) to the vector \((1, \pi_S)\)) is precisely the moment polytopes that are the cone of sufficient statistics of a discrete exponential family associated to the the complete graph \( K_m \), that were studied in Section 8.2. In that section, these moment polytopes were discussed for arbitrary graphs \( G \) on \( m \) vertices, and it makes sense to extend both the cut and correlation side to this more generalized setting.

**Definition 19.1.15.** Let \( G = ([m], E) \) be a graph with vertex set \([m]\). The cut cone associated to the graph \( G \), denoted \( \text{Cut}(G) \) is the cone spanned by the projection of the \( 2^m-1 \) cut semimetrics onto the coordinates indexed by edges \( E \). The cut polytope \( \text{Cut}^\square(G) \) is the convex hull of these projected cut semimetrics.

**Example 19.1.16.** Let \( m = 5 \) and consider the graph \( G = C_5 \), the 5-cycle with edges \( E = \{12, 23, 34, 45, 15\} \). Then the cut polytope \( \text{Cut}^\square(C_5) \) is the convex hull of the columns of the following matrix.

\[
\begin{pmatrix}
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\end{pmatrix}
\]

The cut cone and polytope for general graphs have been studied by many authors, and many results are known about their geometry. For instance, the switching operation can be used to take a complete set of facet defining inequalities for the cut cone and transform them to a complete set of facet
defining inequalities for the cut polytope. Lists of facet-defining inequalities for the cut cone \( \text{Cut}(K_m) = \text{Cut}_m \) are known up to \( m = 8 \) (at least at the time of the writing of [DL97]), and given the difficulty of solving related optimization problems over these polytopes, it seems unlikely that a complete description is possible for all \( m \).

Certain combinatorial structures in the graphs force related facet defining inequalities. The simplest are the cycle inequalities.

**Proposition 19.1.17.** Let \( C \subseteq G \) be an induced cycle in the graph \( G \) consisting of edges \( \{i_1i_2, i_2i_3, \ldots, i_ti_1\} \). Then for each \( j \) the inequality

\[
d(i_j, i_{j+1}) \leq \sum_{k \neq j} d(i_k, i_{k+1})
\]

is a facet defining inequality of the cut cone \( \text{Cut}(G) \). (Where \( i_{t+1} := i_1 \).)

Note that when the cycle has length 3, the facet defining inequalities from Proposition 19.1.17 are just the usual triangle inequalities. The cone cut out by the cycle inequalities for the graph \( G \) plus nonnegativity constraints \( d(i, j) \geq 0 \) is called the metric cone associated to the graph \( G \), denoted \( \text{Met}(G) \). Clearly \( \text{Cut}(G) \subseteq \text{Met}(G) \) for all graphs \( G \).

**Theorem 19.1.18.** [Sey81] The cut cone and metric cone of a graph \( G \) coincide if and only if the graph \( G \) is free of \( K_5 \) minors.

Similarly, one can define the correlation cone and polytope for an arbitrary graph, and more generally for simplicial complexes.

**Definition 19.1.19.** Let \( \Gamma \) be a simplicial complex on \( [m] \). For each \( S \subseteq [m] \) define the correlation vector \( \pi_S \) to be the vector in \( \mathbb{R}^\Gamma \) such that

\[
\pi_S(T) = \begin{cases} 
1 & \text{if } T \subseteq S \\
0 & \text{otherwise}
\end{cases}
\]

The correlation cone of \( \Gamma \) is the cone generated by the \( 2^m \) correlation vectors and is denoted \( \text{Corr}(\Gamma) \).

Note that this definition of correlation cone differs from our previous definition because we are including the face \( \emptyset \), which has the effect of lifting the correlation polytope up to one higher dimension and taking the cone over it. The correlation polytope of \( \Gamma \) arises in the study of hierarchical models.

**Proposition 19.1.20.** The correlation polytope \( \text{Corr}(\Gamma) \) is isomorphic to the cone of sufficient statistics of the hierarchical model associated to \( \Gamma \) with all random variables having two states \( \text{cone}(A_{\Gamma,2}) \).
In the case of graphs, we can still apply the correlation mapping to map between the correlation polytope and the cut polytope (and back). We need to modify the graphs in the appropriate way. If $G$ is a graph on $[m]$, let $\hat{G}$ denote the graph obtained from $G$ by adding the new vertex $m + 1$ and all edges $(i, m + 1)$ for $i \in [m]$. This graph is called the suspension of $G$.

**Proposition 19.1.21.** Let $G$ be a graph on $[m]$. Then the correlation mapping sends the cut polytope $\text{Cut}^{\Box}(\hat{G})$ to the correlation polytope $\text{Corr}^{\Box}(G)$.

This means that the myriad results for the cut cone and cut polytope can be employed to deduce results on the facet structure of the cone of sufficient statistics of hierarchical models.

### 19.2. Tree Metrics

A metric is called a **tree metric** if it can be realized by pairwise distances between leaves on a tree with edge lengths. These tree metrics play an important role in phylogenetics.

A key result about tree metrics is the four point condition of Buneman [Bun74], which shows that tree metrics can be detected in polynomial time. Furthermore, one only need to check locally that a metric is a tree metric.

**Theorem 19.2.1** (Four point condition). A metric $d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_{\geq 0}$ is a tree metric if and only if for all $x, y, z, w \in \mathcal{X}$

$$d(x, y) + d(z, w) \leq \max(d(x, z) + d(y, w), d(x, w) + d(y, z)).$$

We allow repetitions among $x, y, z, w$, which insures that $d$ satisfies non-negativity and the triangle inequalities. An equivalent description of the four point condition is that among the three quantities

(19.2.1) \[d(x, y) + d(z, w), \quad d(x, z) + d(y, w), \quad d(x, w) + d(y, z)\]

the maximum value is achieved by two of them.

**Proof.** It is easy to see that a tree metric satisfies the four point condition. This follows by looking just at four leaf trees as illustrated by Figure **Insert figure**.

To see that a metric that satisfies the four point condition comes from a tree, we proceed by induction on $\#\mathcal{X}$. If $\#\mathcal{X} = 3$ any metric is a tree metric, for example set

$$\lambda_{1/23} = \frac{d(1, 2) + d(1, 3) - d(2, 3)}{2} \quad \lambda_{2/13} = \frac{d(1, 2) + d(2, 3) - d(1, 3)}{2}$$

and

$$\lambda_{3/12} = \frac{d(1, 3) + d(2, 3) - d(1, 2)}{2}$$
in which case
\[ d = \lambda_1|23|23 + \lambda_2|13|23 + \lambda_3|12|23. \]
So assume that \( \#\mathcal{X} > 3 \). Let \( x, y, z \in \mathcal{X} \) such that
\[ d(x, y) + d(x, z) - d(y, z) \]
is maximized. Note that for any \( w \in \mathcal{X} \) this forces the pair of inequalities
\[
\begin{align*}
  d(w, x) + d(y, z) &\leq d(w, y) + d(x, z) \\
  d(w, x) + d(y, x) &\leq d(w, z) + d(x, y)
\end{align*}
\]
so by the four point condition, we have
\[
\begin{align*}
  d(w, x) + d(y, z) &\leq \max(d(w, y) + d(x, z), d(w, z) + d(x, y))
\end{align*}
\]
so that \( d(w, y) + d(x, z) = d(w, z) + d(x, y) \). This holds for any \( w \in \mathcal{X} \).
Combining two such equations with \( w \) and \( w' \) yields
\[
(19.2.2) \quad d(w, y) + d(w' z) = d(w, z) + d(w', y) \geq d(w, w') + d(y, z).
\]
Define a new element \( t \) and set
\[
\begin{align*}
  d(t, y) &= \frac{d(x, y) + d(y, z) - d(x, z)}{2} \\
  d(t, z) &= \frac{d(x, y) + d(y, z) - d(x, z)}{2}, \text{ and} \\
  d(t, u) &= d(u, y) - d(t, y) \text{ for all } u \in \mathcal{X} \setminus \{y, z\}.
\end{align*}
\]
We claim that the set \( \mathcal{X} \cup \{t\} \setminus \{y, z\} \) satisfies the four point condition with
the dissimilarity map \( d \). This is clear for any \( a, b, c, u \in \mathcal{X} \setminus \{y, z\} \), we must
handle the case where one of these is \( t \). For example:
\[
\begin{align*}
  d(a, b) + d(c, t) &= d(a, b) + d(c, y) - d(t, y) \\
  &\leq \max(d(a, y) + d(c, b), d(a, c) + d(b, y)) - d(t, y) \\
  &= \max(d(a, y) + d(c, b) - d(t, y), d(a, c) + d(b, y) - d(t, y)) \\
  &= \max(d(a, t) + d(c, b), d(a, c) + d(b, t)).
\end{align*}
\]
From this we also deduce nonnegativity and that the extended \( d \) forms a metric. By induction we have a tree representation for \( d \) on \( \mathcal{X} \cup \{t\} \setminus \{y, z\} \), and using the definitions of \( d(t, y) \) and \( d(t, z) \) we get a tree representation of \( d \) on \( \mathcal{X} \).

A key part of the proof of Theorem 19.2.1 is the identification of the pair \( \{y, z\} \) which form a cherry in the resulting tree representation. Many algorithms for reconstructing phylogenetic trees from distance data work by trying to identify cherries and proceeding inductively. We will discuss this in more detail in the next section.
A key feature of tree metric spaces is that the underlying tree representation of a tree metric is uniquely determined by the metric. This can be useful in identifiability proofs for phylogenetic models \cite{?}.

**Theorem 19.2.2.** Let \(d\) be a tree metric. Then there is a unique set of compatible splits \(\{A_1|B_1, \ldots, A_k|B_k\}\) and positive constants \(\lambda_{A_1|B_1}, \ldots, \lambda_{A_k|B_k}\) such that 
\[
d = \sum_{i=1}^{k} \lambda_{A_i|B_i} \delta_{A_i|B_i}.
\]

**Proof.** \(\square\)

In addition to tree metrics, it is also natural to consider ultrametrics or equidistant tree metrics. These are natural to consider in biological situations where there is a molecular clock assumption in the mutations.

**Definition 19.2.3.** A dissimilarity map \(d : \mathcal{X} \times \mathcal{X} \to \mathbb{R}\) is called an ultrametric if for all \(x, y, z \in \mathcal{X}\)
\[
d(x, y) \leq \max(d(x, z), d(y, z)).
\]

Note that an ultrametric is automatically a metric. Ultrametrics have representation on rooted trees that are equidistant, in the sense that the distance from any leaf in the tree to the root node is always the same.

**Need to explain this in a bit more detail.**

Tree metrics can be described as a union of polyhedral cones as well. We use the hierarchy structure for rooted trees. Let \(\mathcal{A}\) be the hierarchy of sets that is equivalent to a rooted tree. To each \(A \in \mathcal{A}\) introduce a semimetric \(\delta_A\) with
\[
\delta_A(i, j) = \begin{cases} 
0 & \text{if } i, j \in A \\
1 & \text{otherwise}.
\end{cases}
\]

**Proposition 19.2.4.** The set of ultrametrics compatible with a given rooted tree structure \(T\) represented by the hierarchy \(\mathcal{A}\) is the set of ultrametrics of the form
\[
\sum_{A \in \mathcal{A}} \lambda_A \delta_A
\]
such that \(\lambda_A \geq 0\).

**Remark 19.2.5.** Tree metrics are closely related to objects in tropical geometry. Though this does not play a major role here, we mention these connections to conclude our discussion.

The set of all tree metrics has the structure of a tropical variety, namely it is the tropical Grassmannian of tropical lines [SS04]. Indeed, the four point condition when written in the form of Equation 19.2.2, amounts to saying that the tropical polynomial
\[
d_{ij} \odot d_{kl} \oplus d_{ik} \odot d_{jl} \oplus d_{il} \odot d_{jk} = 0
\]
is the tropicalization of the $4 \times 4$ Pfaffian equation, and where $"= 0"$ is interpreted tropically to mean that the maximum is attained twice. Note however, that the tropical Grassmannian contains dissimilarity maps that are not tree metrics because it technically would allow negative entries.

Similarly, the set of ultrametrics also has the structure of a tropical variety. It is the tropicalization of the linear space associated to the $K_n$ matroid [AK06]. Even the property of a dissimilarity map being a metric has a tropical interpretation. Letting $D$ denote the matrix representation of the dissimilarity map, it will be a metric precisely when

$$-D \preceq (-D) \odot (-D)$$

where the $\odot$ in this formula denotes the tropical matrix multiplication.

### 19.3. Finding an Optimal Tree Metric

The main problem in phylogenetics is to reconstruct the evolutionary history of a collection of taxa from data on these taxa. In Chapter 15 we discussed phylogenetic models, their algebraic structure, and their use in reconstructing these evolutionary histories. The input for these procedures is typically a collection of aligned DNA sequences, and statistical procedures are used to infer the underlying model parameters and reconstruct the tree. An alternate approach is to summarize the alignment information by a dissimilarity map between the taxa and then use a method to try to construct a nearby tree metric. We describe such methods in this section.

Let $T_X$ denote the set of all tree metrics on the leaf label set $X$ and $U_X$ the set of ultrametrics on the leaf label set $X$. Note that if $\#X = m$, then $U_X \subset T_X \subset \mathbb{R}^{m(m-1)/2}$. Given a dissimilarity map $d \in \mathbb{R}^{m(m-1)/2}$ finding an optimal tree metric amounts to solving an optimization problem of the form

$$\min \|d - \hat{d}\|_p \quad \text{subject to } \hat{d} \in T_X.$$

Here $\|\cdot\|_p$ denotes a $p$-metric on $\mathbb{R}^{m(m-1)/2}$, $1 \leq p \leq \infty$. One could also look at the analogous problem over the set $U_X$ of ultrametrics. In fact, all these optimization problems are known to be NP-hard with the lone exception of $p = \infty$ over the set of ultrametrics []. There is an algorithm based for finding an $L^\infty$ optimal ultrametric given a dissimilarity map, based on finding the subdominant ultrametric and shifting it [?]. However, there is almost never a unique closest ultrametric in the $L^\infty$ norm and there are full dimensional regions of the metric cone where multiple different tree topologies are possible for points that are closest in the $L^\infty$ norm [BL16].

Perhaps the most appealing optimization from the statistical standpoint is to optimize with respect to the standard Euclidean norm (i.e. least-squares phylogeny, $p = 2$). This is also known to be NP-hard but there are greedy
version of the procedure that are consistent and fast. We describe two such procedures here, the unweighted pair group method with arithmetic mean (UPGMA) \([SM58]\) and neighbor-joining \([SN87]\). Both methods are agglomerative, in the sense that they use a criterion to decide which leaves in the tree form a cherry, then they join those two leaves together and continue the procedure.

UPGMA is a greedy algorithm that attempts to solve the NP-hard optimization problem of constructing the least-squares phylogeny among equidistant trees. UPGMA has a weighting scheme that remembers the sizes of groups of taxa that have been joined together. It can be seen as acting step-by-step to construct the rooted tree in the language of chains in the partition lattice.

**Algorithm 19.3.1** (UPGMA Algorithm).

- **Input:** A dissimilarity map \(d \in \mathbb{R}^{m(m-1)/2}\) on \(X\).
- **Output:** A maximal chain \(C = \pi_m < \pi_{m-1} < \cdots < \pi_1\) in the partition lattice \(\Pi_m\) and an equidistant tree metric \(\hat{d}\).
- **Initialize:** Set \(\pi_m = 1|2|\cdots|m\) and \(d^m = d\).
- **For** \(i = m-1, \ldots, 1\) do
  - From partition \(\pi_{i+1} = \pi_{i+1}^1 \cdots \pi_{i+1}^i\) and dissimilarity map \(d^{i+1} \in \mathbb{R}^{(i+1)i/2}\) choose \(j, k \in [i+1]\) such that \(d^{i+1}(\pi_{i+1}^j|\pi_{i+1}^k)\) is minimized.
  - Set \(\pi_i\) to be the partition obtained from \(\pi_{i+1}\) by merging \(\pi_{i+1}^j\) and \(\pi_{i+1}^k\) and leaving all other parts the same. So \(\pi_i^j = \pi_{i+1}^j \cup \pi_{i+1}^k\).
  - Create new dissimilarity \(d^i \in \mathbb{R}^{(i-1)/2}\) by defining \(d^i(\tau, \tau') = d^{i+1}(\tau, \tau')\) if \(\tau, \tau'\) are both parts of \(\pi_{i+1}\) and

\[
(19.3.1)\quad d^i(\tau, \pi_i^j) = \frac{|\pi_i^j|}{|\pi_i^1|} d^{i+1}(\tau, \pi_{i+1}^j) + \frac{|\pi_i^k|}{|\pi_i^1|} d^{i+1}(\tau, \pi_{i+1}^k),
\]

- For each \(x \in \pi_{i+1}^j\) and \(y \in \pi_{i+1}^k\) set \(\hat{d}(x, y) = d^{i+1}(\pi_{i+1}^j, \pi_{i+1}^k)\).
- **Return** the chain \(C = \pi_n < \cdots < \pi_1\) and the equidistant metric \(\hat{d}\).

Note that Equation 19.3.1 is giving an efficient recursive procedure to calculate the dissimilarity

\[
d^i(\tau, \tau') = \frac{1}{|\tau||\tau'|} \sum_{x \in \tau, y \in \tau'} d(x, y).
\]

The UPGMA algorithm is clearly a consistent algorithm. If we input a dissimilarity map \(d\) that is actually an ultrametric, the algorithm will return the same ultrametric. This is because the minimum value that occurs at
each step must be a cherry, and the averages that occur are always amongst values that are all the same. So one step of UPGMA takes an ultrametric and produces a new ultrametric on a smaller number of taxa.

The reader might be wondering why we say that UPGMA is a greedy procedure for solving the least-squares phylogeny problem. It is certainly greedy, always merging together pairs of leaves that are closest together, but what does this have to do with $L^2$ optimization. This is contained in the following proposition.

**Proposition 19.3.2.** [FHKT08] Let $d \in \mathbb{R}^{m(m-1)/2}$ be a dissimilarity map on $\mathcal{X}$ and let $C = \pi_m < \ldots < \pi_1$ and $\hat{d}$ be the chain and ultrametric returned by the UPGMA algorithm. Then $\hat{d}$ is a linear projection of $d$ onto one of the cones of $\mathcal{U}_\mathcal{X}$.

**Proof.** Let $C = \pi_m < \ldots < \pi_1$ be a chain of the $\Pi_m$ and let $L_C$ be the corresponding linear space. This space is obtained by setting $d(x,y) = d(x',y')$ for all tuples $x, x' \in \tau, y, y' \in \tau'$ where $\tau$ and $\tau'$ are a pair of parts of partition that get merged going from $\pi_{i+1}$ to $\pi_i$ for some $i$. In other words, this linear space is a direct product of linear spaces of the form

$$\{(t,t,\ldots,t) : t \in \mathbb{R}\} \subseteq \mathbb{R}^k$$

for some $k$. The projection onto a direct product is the product of the projections so we just need to understand what the projection of a point $(y_1,\ldots,y_k)$ onto such a linear space is. A straightforward calculation shows that this projection is obtained by the point $(\bar{y},\ldots,\bar{y})$ where $\bar{y} = \frac{1}{k}\sum_{i=1}^{k} y_i$. This shows that UPGA is a linear projection onto the linear space spanning by one of the cones that make up the space of ultrametric trees. However, by the UPGMA procedure that always the smallest element of the current dissimilarity map is chosen, this forces that the inequalities that define the cone will also be satisfied, and hence UPGMA will map into a cone. □

Although UPGMA does give a projection onto one of the cones of $\mathcal{U}_\mathcal{X}$, a property that the actual least squares phylogeny will satisfy, the result of UPGMA need not be the actual least squares phylogeny. This is because the greediness of the algorithm might project onto the wrong cone in $\mathcal{U}_\mathcal{X}$. This is illustrated in the following example.

**Example 19.3.3.**

Studies of the polyhedral geometry of the UPGMA algorithm and comparisons with the least-squares phylogeny were carried out in [DS13, DS14, FHKT08].
Neighbor-joining is a similar agglomerative method for constructing a tree from distance data, though it constructs an unrooted tree metric, instead of a rooted tree metric. It also is given by an agglomerative/recursive procedure, but uses the same formulas at each step, rather than relying on the structure of the partition of leaves that has been formed by previous agglomerations, as in the UPGMA algorithm. Associated to the given dissimilarity map we compute the matrix $Q$ defined by

$$Q(x, y) = (m - 2)d(x, y) - \sum_{k=1}^{m} d(x, k) - \sum_{k=1}^{m} d(y, k).$$

Then we pick the pair $x, y$ such that $Q(x, y)$ is minimized. These will form a cherry in the resulting tree. A new node $z$ is created and estimates of the distance from $z$ to $x, y$, and the other nodes $w \in \mathcal{X}$ are computed via the following formulas:

$$d(x, z) = \frac{1}{2}d(x, y) + \frac{1}{2(m - 2)}\left(\sum_{k=1}^{m} d(x, k) - \sum_{k=1}^{m} d(y, k)\right),$$

$$d(y, z) = d(x, y) - d(x, z), \text{ and } d(w, z) = \frac{1}{2}(d(x, z) + d(y, z) - d(x, y)).$$

**Proposition 19.3.4.** UPGMA and Neighbor-Joining are consistent. That is, given an ultrametric or a tree metric as input, respectively, the algorithm will return the same tree ultrametric or tree metric back.

**Proof.** In both cases it suffices to prove that at one step of the algorithm the selection criterion chooses a cherry in the tree. This is sufficient because the resulting reduction to smaller number of leaves gives a reduction to a smaller leaf tree if it is applied to a cherry. In the case of UPGMA, it is clear that the algorithm always picks a cherry when applied to an ultrametric since in an ultrametric, a cherry is always the closest pair together.

It remains to show consistency in the case of Neighbor-Joining. To do this, we must analyze the $Q$-matrix in some detail. First of all, note that subtracting the expressions

Details, need to find proof of this.  

Methods based $L^p$ optimization are not the only approaches to constructing phylogenetic trees from distance data, and there are a number of other methods that are proposed and used in practice. One other optimization criterion is the balanced minimal evolution criterion for constructing a tree.
To conclude this chapter, we discuss the ways that the toric varieties associated to the polytopes from finite metric spaces arise in various interesting contexts. In particular, for each graph $G$ the cut polytope $\text{Cut}(G)$ defines a toric variety. Lifting each cut semimetric $\delta_{A|B}$ into $\mathbb{R}^{|E|+1}$ by adding a single new coordinate and setting that equal to 1. These toric varieties and their corresponding ideals were introduced in \cite{SS08}. We study the toric ideals in the ring $C[q_{A|B}]$ where $A|B$ ranges over all $2^{m-1}$ splits and we denote the corresponding toric ideal via $I_G$.

**Example 19.4.1.** Let $G = C_4$ be the four-cycle graph. The toric ideal is

$$I_{C_4} \subseteq C[q_{\emptyset|1234}, q_{1|234}, q_{2|134}, q_{12|34}, q_{3|24}, q_{124}, q_{13}],$$

is the toric ideal associated to the following matrix:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}.$$ 

The toric ideal in this case is

$$I_{C_4} = \langle q_{\emptyset|1234}, q_{1|234}, q_{2|134}, q_{12|34}, q_{3|24}, q_{124}, q_{13}, q_{1234} \rangle.$$

The best general result on the generators of these cut ideals is due to Engström \cite{Eng11}.

**Theorem 19.4.2.** The cut ideal $I_G$ is generated by polynomials of degree $\leq 2$ if and only if $G$ is free of $K_4$ minors.

An outstanding open problem from \cite{SS08} is whether or not similar excluded minor conditions suffice to characterize when the generating degree of $I_G$ is bounded by any number. In particular, it was conjectured that $I_G$ is generated by polynomials of degree $\leq 4$ if and only if $G$ is free of $K_5$ minors.

Proposition \ref{prop:binary_hierarchical_models} allows us to realize an equivalence between the toric ideal $I_G$ and the toric ideals of the binary hierarchical models where the underlying simplicial complex $\Gamma = G$. This allows a straightforward importation of results about these cut ideals for hierarchical models.

A surprising further connection to other book topics comes from the connection to the toric ideals that arise in the study of group based phylogenetic models that were studied in Section \ref{sec:group_based_models} and some generalizations of those models. This relation was originally discovered in \cite{SS08}. 

**Proposition 19.1.21** allows us to realize an equivalence between the toric ideal $I_G$ and the toric ideals of the binary hierarchical models where the underlying simplicial complex $\Gamma = G$. This allows a straightforward importation of results about these cut ideals for hierarchical models.

**Theorem 19.4.2.** The cut ideal $I_G$ is generated by polynomials of degree $\leq 2$ if and only if $G$ is free of $K_4$ minors.
Definition 19.4.3. A cyclic split is a split $A|B$ where either $A$ or $B$ is of the form \{i, i+1, \ldots, j-1, j\} for some $i$ and $j$. A cyclic split system is a set of cyclic splits on the same ground set $[m]$.

The splits equivalence theorem (Theorem 15.1.6) says that each tree $T$ is equivalent to its set of displayed splits $\Sigma(T)$. Every isomorphism class of tree can be realized with a set of cyclic splits, after possibly relabeling the leaves. For instance, this can be obtained by drawing the tree in the plane with leaves all on a circle, and then cyclically labeling the leaves $1, 2, \ldots, m$ as the circle is traversed once. Hence, each phylogenetic tree corresponds to a cyclic split system. We will show that certain generalizations of the phylogenetic group based models associated to cyclic split systems are in fact isomorphic to the cut toric ideal $I_G$.

Let $\Sigma$ be a cyclic split system on $[m]$. We associate the matrix whose rows are indexed by the elements of $\Sigma$, and will columns are indexed by subsets of $[m]$ that have an even number of elements. To each such subset $S \subseteq [m]$ we associated the vector $\gamma_S$ where

$$\gamma_S(A|B) = \begin{cases} 1 & \text{if } |A \cap S| \text{ is odd} \\ 0 & \text{otherwise} \end{cases}.$$ 

The associated toric ideal is obtained from this set of vectors by adding a row of all ones to the matrix (as we did to associate the toric ideal to a cut polytope). Note that if the cyclic split system $\Sigma$ comes from a tree, then this toric ideal will be the same as the one introduced in Section 15.3 associated to the group $\mathbb{Z}_2$. This is true because firstly, subsets of $[m]$ with an even number of elements are in natural bijection with the subgroup of $\mathbb{Z}_2^m$ of elements $(g_1, \ldots, g_m)$ such that $g_1 + \cdots + g_m = 0$. And secondly, the sum of group elements associated to one side of an edge will contribute a trivial parameter precisely when the some on one side of a split if nonzero in the group, i.e. when $|S \cap A|$ is odd.

To an edge in the graph $G$ $i, j + 1$ we associate the split $A_{ij}|B_{ij}$ with $A = \{i, i+1, \ldots, j-1, j\}$ where we consider indices cyclically modulo $m$. This is clearly a bijection between unordered pairs in $[m]$ and cyclic splits. To an arbitrary split $A|B$ we associate an even subset $S(A|B)$ by the rule that $k \in S$ if and only if $|\{k, k+1\} \cap A| = 1$. It is easy to see this is a bijection between splits of $[m]$ and even subsets of $[m]$. Lastly, it is not difficult to see that

$$\delta_{A|B}(i, j + 1) = \gamma_{S(A|B)}(A_{ij}|B_{ij}).$$

To a graph $G$ let $\Sigma(G)$ denote the resulting set of cyclic splits that are induced by the map $i, j + 1 \rightarrow A_{ij}|B_{ij}$. Then we have the following proposition.
Proposition 19.4.4. Let $G$ be a graph with vertex set $[m]$. The cut ideal $I_G^\square$ of the graph $G$ is equivalent to the toric ideal associated to the set of vectors $\gamma_S$ associated to the set of cyclic splits $\Sigma(G)$.

In the special case where the graph $G$ is a triangulation of the $n$ cycle graph, then the corresponding set of cyclic splits is $\Sigma(G)$ is the set of cyclic splits of the dual tree. This is illustrated in the following example.

Example 19.4.5. Let $G$ be the graph with vertex set $[m]$ and edges $E = \{12, 23, 34, 45, 56, 16, 13, 35, 15\}$. The transformation from Proposition 19.4.4 gives the list of splits

$$\Sigma(G) = \{1|23456, 2|13456, 3|12456, 4|12356, 5|12346, 6|12345, 12|3456, 34|1256, 56|1234\}$$

which is the set of splits of a snowflake tree.

![Figure 19.4.1. A triangulation of a hexagon and the corresponding phylogenetic tree on six leaves from Example 19.4.5](image)

19.5. Exercises

Exercise 19.1. Prove Proposition 19.1.9

Exercise 19.2. Prove Proposition 19.1.20

Exercise 19.3. Compute generators for the toric ideal $I_K^\square$. 
Bibliography


[Bos47] R. C. Bose, Mathematical theory of the symmetrical factorial design, Sankhyå 8 (1947), 107–166. MR 0026781 (10,201g)


Bibliography


Bibliography


