Mathematical Association of America

MAA TEXTBOOKS

Combinatorics

A Guided Tour

David R. Mazur

Combinatorics

A Guided Tour

Library of Congress Catalog Card Number 2009937059

Electronic ISBN: 978-1-61444-607-1

Print ISBN: 978-0-88385-762-5

Printed in the United States of America

Current Printing (last digit):
10 9 8 7 6 5 4 3 2 1

Combinatorics

A Guided Tour

David R. Mazur
Western New England College

Published and distributed by
The Mathematical Association of America

MAA TEXTBOOKS

Calculus Deconstructed: A Second Course in First-Year Calculus, Zbigniew H. Nitecki
Combinatorics: A Guided Tour, David R. Mazur
Combinatorics: A Problem Oriented Approach, Daniel A. Marcus
Complex Numbers and Geometry, Liang-shin Hahn
A Course in Mathematical Modeling, Douglas Mooney and Randall Swift
Cryptological Mathematics, Robert Edward Lewand
Differential Geometry and its Applications, John Oprea
Elementary Cryptanalysis, Abraham Sinkov
Elementary Mathematical Models, Dan Kalman
Essentials of Mathematics, Margie Hale
Field Theory and its Classical Problems, Charles Hadlock
Fourier Series, Rajendra Bhatia
Game Theory and Strategy, Philip D. Straffin
Geometry Revisited, H. S. M. Coxeter and S. L. Greitzer
Graph Theory: A Problem Oriented Approach, Daniel Marcus
Knot Theory, Charles Livingston
Lie Groups: A Problem-Oriented Introduction via Matrix Groups, Harriet Pollatsek
Mathematical Connections: A Companion for Teachers and Others, Al Cuoco
Mathematical Interest Theory, Second Edition, Leslie Jane Federer Vaaler and James W. Daniel
Mathematical Modeling in the Environment, Charles Hadlock
Mathematics for Business Decisions Part 1: Probability and Simulation (electronic textbook), Richard B. Thompson and Christopher G. Lamoureux
Mathematics for Business Decisions Part 2: Calculus and Optimization (electronic textbook), Richard B. Thompson and Christopher G. Lamoureux
The Mathematics of Games and Gambling, Edward Packel
Math Through the Ages, William Berlinghoff and Fernando Gouvea
Noncommutative Rings, I. N. Herstein
Non-Euclidean Geometry, H. S. M. Coxeter
Number Theory Through Inquiry, David C. Marshall, Edward Odell, and Michael Starbird
A Primer of Real Functions, Ralph P. Boas
A Radical Approach to Real Analysis, 2nd edition, David M. Bressoud
Real Infinite Series, Daniel D. Bonar and Michael Khoury, Jr.
Topology Now!, Robert Messer and Philip Straffin
Understanding our Quantitative World, Janet Andersen and Todd Swanson

MAA Service Center
P.O. Box 91112
Washington, DC 20090-1112
1-800-331-1MAA FAX: 1-301-206-9789

Preface

This book provides a journey through introductory combinatorics that the reader can undertake during one semester, two quarters, or in a independent study or self-study setting. It is not intended to be encyclopedic. Rather, it surveys a good cross-section of combinatorics as it has developed within the last century with an eye towards its characteristic brand of thinking, its interconnections with other mathematical fields, and some of its applications.

Combinatorics can rightly be called the mathematics of counting. More specifically, it is the mathematics of the enumeration, existence, construction, and optimization questions concerning finite sets. Here are some brief illustrations.

- **Enumeration: How many?** How many different 9×9 Sudoku boards are there? This number has been computed exactly and it is astronomical—about 6.6 sextillion. Determining this number by simply listing every possible board is not a viable approach. Combinatorics involves mathematical techniques for determining the answer to a counting question without listing the objects being counted.
- **Existence: Is it possible?** Take any 25 people living on the earth. Among the members of this group will you always be able to find four people who all know each other or else five people who all don't know each other? Yes: this is guaranteed no matter what group of 25 you choose. Despite its innocent-sounding nature, this question wasn't answered until 1993 and required careful combinatorial analysis as well as thousands of hours of computer time.
- **Construction: Can it be built?** The Mariner 9 spacecraft orbited Mars in 1971-72 and sent back photographs that gave a complete picture of the planet's surface. Your CD player can play a disc flawlessly despite occasional scratches on the disc's surface. Both of these applications involve error-correcting codes that transmit information with 100% accuracy despite occasional errors in transmission. Construction methods for many error-correcting codes use combinatorics.
- **Optimization: What is the best way?** Your car's GPS navigation system quickly finds the fastest route from point A to point B. It essentially solves instances of a combinatorial optimization problem called the shortest path problem, which is but one of a broad class of network optimization problems that have widespread modern application.

In this book we consider enumeration, existence, and construction questions.

The examples above rightly suggest that combinatorics has many modern applications. Counting techniques are indispensable in applied probability when the sample space is finite and outcomes are equally likely. Combinatorial design theory grew out of a need

that statisticians had in constructing valid experimental designs. Computer science is replete with applications as combinatorial thinking informs the efficiency of algorithms and data structures as well as the correctness of recursive procedures. Linear programming and combinatorial optimization are fields born from the large-scale logistical planning problems of World War II and now include, among many others, applications to the design of transportation and telecommunications networks. Operations research, management science, and industrial engineering are other fields in which combinatorial analysis is used to solve important and practical problems.

Beyond specific examples and problems, though, the broader view is that combinatorial thinking is beneficial and applicable to many areas of mathematics, statistics, computer science, and engineering. Two of the largest professional societies in the fields of mathematics and computer science—the Mathematical Association of America (MAA) and the Association for Computing Machinery (ACM)—recommend that majors and minors in mathematics and computer science take courses involving a good amount of discrete mathematics and combinatorics.

As such, combinatorics is now properly intertwined with modern mathematics. In the recent past, combinatorics was viewed as a useful set of tools and, at best, a surrogate to other fields. Now that combinatorics has gelled into a more coherent whole, it is interesting to see how fields such as calculus, analysis, number theory, abstract and linear algebra, and differential equations can be used as tools to solve purely combinatorial problems. Some of those results are true mathematical highlights.

What's on the tour and what's not

As mentioned earlier, this book provides an introductory survey of enumeration, existence, and construction questions. The emphasis is on enumeration and the first five chapters provide the core material on counting techniques and number families. The remaining chapters take up graphs, combinatorial designs, error-correcting codes, and partially ordered sets.

In Chapter 1 we begin with the classification and analysis of basic counting questions. We also lay the groundwork for the rest of our journey by introducing five essential combinatorial principles: the product and sum principles, the bijection principle, the equivalence principle, and the pigeonhole principle. The latter is existential, not enumerative, in nature.

In Chapter 2 we undertake the study of distribution problems. Most counting questions are equivalent to questions of counting the ways to distribute "objects" to "recipients." Through these distribution problems we meet several major players: binomial coefficients, Stirling numbers, and integer partition numbers. We also introduce and emphasize combinatorial proofs as well as the technique of recursion: breaking up a large problem into smaller subproblems of the same type.

In Chapter 3 we introduce inclusion-exclusion, mathematical induction, generating functions, and recurrence relations. These are algebraic techniques in contrast to the combinatorial techniques of the previous chapters. The coverage of generating functions includes techniques for solving recurrence relations.

In Chapter 4 we use the techniques of the previous chapters to give a more in-depth study of the binomial and multinomial coefficients, Fibonacci numbers, Stirling numbers of the first and second kinds, and integer partition numbers. Among other lines of investigation, we derive generating functions for these families of numbers, count triangulations

of the regular n-gon, give combinatorial proofs of Fibonacci number identities using the idea of tiling, derive a beautiful formula for the Bell numbers, and explore formulas and an asymptotic estimate for the integer partition numbers.

In Chapter 5 we cover counting problems involving equivalence and symmetry considerations. The main results are the Cauchy-Frobenius-Burnside theorem and Pólya's enumeration theorem. Though Pólya's theorem arose from an application to the enumeration of chemical compounds, it has since proved to be a powerful and versatile tool in all sorts of other applications. We begin this chapter by introducing those aspects of group theory necessary to understand the theorems, and then give many illustrations of how to apply them.

In Chapter 6 we give a short survey of some combinatorial problems in graph theory. These include the enumeration of labeled trees and binary search trees, coloring and the chromatic polynomial, and introductory Ramsey theory. Though Ramsey theory can be introduced without the aid of graphs, the edge-coloring interpretation is convenient and concrete. The first section of this chapter covers basic graph theory concepts for the reader who is unfamiliar with graphs.

In Chapter 7 we cover two of the most compelling applications of combinatorics: combinatorial designs and error-correcting codes. As a bonus, the mathematical questions surrounding these applications are just as compelling if not more so. In the three sections on designs we cover existence and construction methods, symmetric designs, and triple systems. In the two sections on error-correcting codes, we construct the family of binary Hamming codes and derive their error-correcting properties, study the interplay between codes and designs, and discuss the truly astonishing results concerning the existence of perfect codes.

In Chapter 8 we conclude our journey by studying relations that are, in some sense, lurking behind much of combinatorics: partially ordered sets or "posets." We study some classical results (Sperner's theorem and Dilworth's theorem) and also the concept of poset dimension. In the final two sections we introduce the theory of Möbius inversion and do so with a two-fold purpose: to provide a unifying framework for several combinatorial ideas and to prepare the reader for further study.

There are several important topics not included on the tour. The coverage of graph theory in Chapter 6, though it contains an introductory section, is focused fairly narrowly on the topics mentioned earlier. A major branch of combinatorics, namely combinatorial optimization, is left out entirely. Also, the coverage of designs and codes is driven by the particular applications. As such, we do not cover projective planes, combinatorial geometries, or Latin squares.

Features of this book

Reading questions. What makes this book a guided tour are the approximately 350 Questions spread throughout the eight chapters. These allow the reader to be an active participant in the discussion and are meant to provide a more honest reflection of the process by which we all learn mathematics. Reading a math book without pencil and paper in hand is like staying in your hotel and viewing the interesting sites from your window. You'll get more out of the tour if you leave the hotel and go explore on foot.

Combinatorial proofs. To count the cows in a field you could either (1) count their heads, or (2) count their legs and divide by 4. In a combinatorial proof one asks a counting question and then answers it correctly using two different approaches. This little idea leads to some beautiful, memorable, and even fun (!) proofs. Wherever possible, we present combinatorial proofs because they promote understanding and build combinatorial thinking skills.

Classification of counting problems. The hard part about counting is determining the type of objects being counted. Instead of covering lists, lists without repetition (permutations), subsets (combinations), and multisets (combinations with repetition) in separate sections, in Section 1.1 we learn how to distinguish among these four types.

Conversational style, some big examples. I've tried to maintain a conversational and somewhat informal tone throughout the book. This occasionally means that brevity is sacrificed for the sake of clarity. Also, small and/or simple examples of difficult new concepts sometimes frustrate me. In certain situations I've included bigger examples when helpful. For two examples see Figure 3.1 on page 104 and Figure 7.2 on 279.

Links with continuous mathematics. At appropriate places in the text I've highlighted where calculus, differential equations, linear algebra, etc. are useful in combinatorics. These help dispel the notion that combinatorics is a "discrete-only" field.

Instructor flexibility. Completion of the reading questions prior to class frees the instructor from lecturing on basic material. Class time could then be used to clarify difficulties, lecture on advanced topics, have a problem session, or assign group work. This also allows class time for reviewing proof techniques, linear algebra, power series, or modular arithmetic, if necessary. See below for optional prerequisites.

Courses and ways to use this book

This book has two primary uses. The first is as a text for a combinatorics course at the sophomore/junior/senior level. A one semester or two-quarter course could cover most of the book. The other use is as a text for an independent study or reading course and it should work quite well "out of the box" for this purpose. The author has used various versions of the manuscript for both purposes. The book would also be appropriate for some introductory graduate courses in applied mathematics or operations research programs. In that case, the whole book could be covered in a semester and appropriate exercises could be chosen. In addition, the text would be appropriate for anyone curious about combinatorics and who wants to learn something about the field at a leisurely pace.

Core topics that every course would most likely include are

- Sections 1.1–1.5: basic counting and existence principles;
- Sections 2.1–2.4: distribution problems and combinatorial proofs;
- Sections 3.1, 3.3–3.5: inclusion-exclusion, generating functions, recurrence relations;
- Sections 5.1–5.4, 5.6: Pólya theory of counting; and
- Sections 7.1–7.5: combinatorial designs and error-correcting codes.

Additional material can be selected from

- Section 3.2: mathematical induction (if needed for review);
- Section 3.6: formulas for the solution of linear first- and second-order recurrence relations;
- Sections 4.1–4.4: further study of binomial and multinomial coefficients, Fibonacci numbers, Stirling numbers, and integer partition numbers;
- Section 5.5: a proof of Cauchy-Frobenius-Burnside theorem;
- Sections 6.1–6.4: graph theory topics; and
- Sections 8.1–8.6: partially ordered sets and Möbius inversion.

Prerequisites

The reader embarking on this tour should be familiar with single-variable calculus, sets and set notation, proof techniques, and basic modular arithmetic. In short, they should have had a year of calculus as well as a "transition" course. Usually this means sophomores or juniors and includes majors and minors in the mathematical sciences including statistics, most majors and minors in computer science, and some engineers.

We now discuss some optional prerequisites.

Optional: mathematical induction. Induction is covered in Section 3.2 although most most readers meeting the prerequisites will have seen induction already. This section could serve as a first-time introduction even though its primary purpose is to emphasize how induction is used in combinatorics.

Optional: linear algebra. Linear algebra is not a necessary prerequisite to most of the book but a basic understanding of linear systems, matrix algebra, and a couple of vector space concepts will greatly enhance some of the material. First and foremost is Chapter 7 on combinatorial designs and error-correcting codes which, in the author's opinion, represents some of the most interesting material in the book. Most readers meeting the prerequisites will have taken linear algebra or will take it concurrently. Linear algebra is also used briefly in Section 4.3 on Stirling numbers, in two sections of Chapter 6 but only for the adjacency matrix, and at the end of Chapter 8 on Möbius inversion.

Optional: graph theory. In Chapter 6 we investigate some enumeration and existence questions related to graphs. No prior knowledge of graph theory is assumed and Section 6.1 serves as a self-contained introduction to the ideas necessary for the rest of the chapter. This introductory material would be familiar to a student whose transition course included some graph theory, as many such courses do these days.

Optional: abstract algebra. Chapter 5, on Pólya's theory of counting, represents a pinnacle of enumeration. No previous experience with abstract algebra is assumed and we introduce only the group theory required to understand the results and to solve problems. A reader who has had a course in abstract algebra would naturally get more from this chapter but such experience is by no means necessary. Finite fields are briefly mentioned in Section 7.5.

Acknowledgments

Whatever you do, work at it with all your heart, as working for the Lord, not for men.
—Colossians 3:23

To God be the glory for this project! I had no idea about how much of an undertaking this task would be but He saw it through to completion. I'm grateful for His steadfast love and faithfulness as I look back on the eight-year journey of writing this book.

In graduate school I had two wonderful teachers of combinatorics in Ed Scheinerman and Alan Goldman. The inspiration for this book can be traced back to their influence and encouragement as I struggled with this fascinating subject.

I wrote a draft of the first two chapters during summer 2001 supported by a Western New England College Summer Research Grant. Many thanks go to Anne Poirot and Jerry Hirsch for their interest in this project, as well as to Dennis Luciano and Dick Pelosi for commenting on the grant proposal. My students Kara Acken, Nicholas Brundage, Holly Coleman, Jason Dean, Brendan Ketcham, and Paul Lewis suffered through the manuscript in fall 2001. Thanks to their feedback those chapters have been significantly overhauled. Thank you also to Jason Molitierno of Sacred Heart University who read that same manuscript and provided insightful comments and suggestions.

During fall 2005, I spent a sabbatical making significant changes and writing all but the final two chapters. During fall 2006, my students Mike Boisseau, Kaitlyn Crilley, Kevin Douthwright, Kevin Dwyer, Cori Eggert, C. J. Elsdon, Mark Fratini, Dan Jock, Lauren Klicka, Robert Maulucci, Sara Peck, Giselle Pile, B. J. Stratton, and James Tierney provided much helpful feedback. It was a joy to teach you all. Thanks also to Diane Sturtevant who caught several errors even after I thought the manuscript was finalized.

Zaven Karian, the editor of the MAA Textbooks series, was kind enough to encourage me to submit a second manuscript for consideration after review of my first draft. I'm extremely grateful for his patience as well as for the seven reviewers who provided helpful and detailed feedback on that first draft. Their comments have made an extremely significant impact on the book. Thanks also to Don Van Osdol for originally encouraging me to submit the book to the MAA, and to Elaine Pedreira and Bev Ruedi at MAA headquarters for guiding the book through the production process in such a quick and friendly manner.

My colleagues and friends in the Department of Mathematics provided tremendous encouragement and support over the years it took to complete this book. Enam Hoq gave me much encouragement and advice as he experienced my day-to-day frustrations as I made the final push. Dennis Luciano and Dick Pelosi spent time reviewing some of the chapters and offering invaluable feedback. Thanks also to Dennis and to Saeed Ghahramani, our Dean, for creating an enjoyable environment in which to work. Saeed also provided helpful suggestions on the book prospectus.

Finally, I owe a debt of tremendous gratitude to my wonderful wife Dani and my children Suzy, Gracie, and Davey. It was they who lovingly supported me and gave me the time to work on the book on weekends, evenings, and vacations. Now that it's done I'll miss Suzy asking me whether I'm "Möbius functioning," but I will look forward to more time with the people that I love the most.

Springfield, MA
August 2009

For Danielle

Before you go

The reading questions, from Question 1 on page 2 to Question 356 on page 363, are an integral part of this book. Have pencil and paper ready to answer each Question as you encounter it in the text. Some are straightforward, some ask for the solution to a problem that is similar to an example, and some ask for a natural generalization of a new idea. Others ask for an explanation, a recall of a concept from another course, or a justification of a step in a proof. Still others might ask for an entire proof, but only if the main idea is well-motivated.

Beginning with Section 1.5, most of the sections conclude with Travel Notes. These add color to the material of the section via interesting anecdotes, open problems, the current state-of-the-art, suggestions for further reading, and background information on the mathematicians responsible for the discoveries.

Also included at the end of the book are hints and answers to selected end-of-section Exercises. Consult them only if you get stuck. Answers are given to help you check your work, but keep two things in mind. One, combinatorial problems usually admit multiple solution approaches so answers that look different may in fact be the same. Two, an answer alone is usually not sufficient. The approach you took to analyze the problem is the real key.

I appreciate corrections, comments, and other feedback on the book. Please email them to `dmazur@wnec.edu`. You can visit the book's website by following the link from my homepage

`mars.wnec.edu/~dmazur`

for updates, errata, and other resources.

Enjoy your trip!

Contents

CHAPTER 1

Principles of Combinatorics

Our journey begins with counting because combinatorics, in part, is the mathematics of counting. What does it mean to count? It means to determine the exact number of objects specified by a "How many?" question. What makes counting questions so appealing is that they arise in all sorts of settings, answering them builds your problem solving skills, and the answers are often fascinating in their sheer size.

In this chapter we study the principles of counting that are foundational to combinatorics and that we will use in every other chapter. In the first two sections we practice classifying and solving basic counting questions. In the next two sections we study two principles (the bijection principle and the equivalence principle) that are useful for analyzing more difficult problems. In the last section, we introduce existence questions with the pigeonhole principle.

Counting vs. enumerating

We first make a note on the difference between counting and enumerating. One possible method of counting is to make a systematic and complete list of the objects being counted. This is called a ***complete enumeration*** or simply an ***enumeration***. For example, if we wanted to know how many integers between 1 and 100 (inclusive) are divisible by 5 or 6, we could list them all:

5 6 10 12 15 18 20 24 25 30 35
36 40 42 45 48 50 54 55 60 65 66
70 72 75 78 80 84 85 90 95 96 100.

There are 33.

Complete enumeration is a viable counting technique for small problems but not for large ones. If we want to count the number of 9×9 filled-in Sudoku boards[1] then we should not make a list because there are exactly

6,670,903,752,021,072,936,960

boards, about 6.6 sextillion. Even a computer that could generate 100 billion different Sudoku boards per second (exceedingly generous to the point of absurdity) would still take

[1] Visit `en.wikipedia.org/wiki/Sudoku` if you somehow missed the Sudoku craze.

over 20,000 years to list every single board. Also, if you were to print each board on a 3-inch square piece of paper, then it would require 15 trillion square miles of paper—enough to cover the planet Jupiter 625 times.

What we want is a formula that allows us to find the answer without making a complete list, and we will find many in this chapter and elsewhere. Yet, complete enumeration is important for at least two reasons. For one, a complete enumeration of a smaller but similar problem can give insight into how to solve the larger problem. We shall make good use of this in this chapter. For another, some large, difficult problems exist whose only known solution involves a complete enumeration (by computer) of some appropriately reduced subproblem.

1.1 Typical counting questions and the product principle

Our goal in the first two sections of this chapter is to identify some important types of counting questions and then to get a lot of practice in answering them. Here are four such questions.

Q1 How many eight-character passwords are possible if each character is either an uppercase letter A–Z, a lowercase letter a–z, or a digit 0–9?

Q2 Given nine players, in how many different ways can a manager write out a batting lineup?

Q3 You play a pick-six lottery by specifying six different numbers from 1-40. How many different lottery tickets are possible?

Q4 How many different orders for a dozen donuts are possible if a store offers 30 donut varieties?

The first step is to identify the key features of the objects being counted. Once accomplished, standard formulas provide the answer.

Question 1 *Take a guess at ordering the questions from smallest answer to largest answer.*

Throughout this book, we use $[n]$ to denote the set of the first n positive integers. For example, $[4] = \{1, 2, 3, 4\}$ and $[1] = \{1\}$. We use $\mathbb{Z}$ to denote the set of integers, $\mathbb{N}$ to denote the set of natural numbers (positive integers), $\mathbb{Q}$ to denote the set of rational numbers, and $\mathbb{R}$ to denote the set of real numbers.

Question Q1: Counting lists or words

Solving a similar but smaller version of a problem is an important problem-solving technique. Here is a smaller version of question Q1: How many three-character passwords are possible if each of the first two characters is either A, B, or g, and the last character is either 5 or 6?

Some of the passwords we wish to count look like `BA5` or `AA6` `gA6`. Let's think about choosing the characters one at a time and seeing how the number of choices for each influences the total number of passwords. The first character must be either `A`, `B`, or `g`, so any password begins in one of the three ways:

`A__` `B__` `g__`.

The next character must either be A, B, or g, so this increases the possibilities by a factor of 3:

```
AA_        BA_        gA_
AB_        BB_        gB_
Ag_        Bg_        gg_.
```

The last character must either be 5 or 6, so this in turn increases the possibilities by a factor of 2:

```
AA5 AA6    BA5 BA6    gA5 gA6
AB5 AB6    BB5 BB6    gB5 gB6
Ag5 Ag6    Bg5 Bg6    gg5 gg6.
```

From the complete enumeration above we see that there are 18 possible passwords. We could have obtained this answer by simply multiplying together the number of possibilities for each of the three characters: $3 \cdot 3 \cdot 2 = 18$.

Question 2 *How many four-character passwords are possible if each of the first three characters is either A, B, g, or x, and the last character is an even digit?*

There is a nice way to visualize the solution to the smaller Question Q1 using the tree diagram shown in Figure 1.1. If we write the password in the form $l_1 l_2 l_3$, then the branches to the right of each circle labeled l_1, l_2, or l_3 represent the choices for that character once the previous characters are specified.

The same counting principle applies to the original question Q1, where we wish to count case-sensitive, eight-character passwords such as rQ8xt9Pb and V93Vvd99. Each of the eight characters may be specified in one of 62 ways (26 uppercase letters plus 26 lowercase letters plus 10 digits). Therefore, there are

$$62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 \cdot 62 = 62^8 = 218{,}340{,}105{,}584{,}896$$

possible passwords. A complete enumeration of the approximately 218 trillion passwords is certainly out of the question!

Question 3 *Which is larger, the number of four-character passwords where each character is a letter A–H, or the number of eight-character passwords where each character is a letter A–D?*

How to count lists or words

The passwords we just counted are examples of lists. A ***list*** is an ordered sequence of objects, and a ***k-list*** is a list of length k. In a list, the order in which the objects appear matters. Also, an object can appear more than once on the list unless forbidden by the constraints of the problem. Lists are also called ***words***.

For clarity, lists are sometimes written by enclosing the sequence in parentheses and separating the objects by commas. For example, (V, 9, 3, V, v, d, 9, 9) is an equivalent way to write the password V93Vvd99. An ordered pair like $(-2, 3)$ is a 2-list and an ordered triple like (x, y, z) is a 3-list.

Just as we use k-list as an abbreviation for a list of length k, we use ***n-set*** as an abbreviation for a set of size n. In Question Q1, each password is an 8-list where each list element belongs to the 62-set

$$\{\mathtt{A}, \mathtt{B}, \mathtt{C}, \ldots, \mathtt{Z}, \mathtt{a}, \mathtt{b}, \mathtt{c}, \ldots, \mathtt{z}, 0, 1, 2, \ldots, 9\}.$$

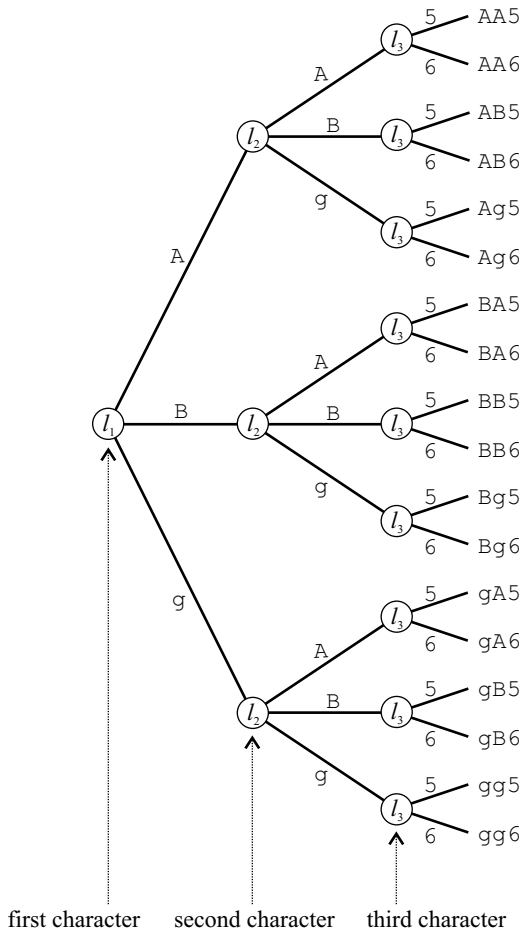


Figure 1.1. Tree diagram for counting three-character passwords $l_1 l_2 l_3$.

In this case we simply say that each password is "an 8-list taken from a 62-set."

Here is a summary of what we have learned about counting lists.

Counting lists:

- *Notation:* n^k equals the number of k-element lists taken from an n-element set.
- *Key features:* Order matters, repeated elements allowed.
- *Typical question:* How many ways are there to form a k-letter word where there are n choices for each letter?
- *Formula:*

$$n^k = \underbrace{n \cdot n \cdot \cdots \cdot n}_{k \text{ factors}}.$$

We included a "formula" for n^k because it is important to distinguish between *the objects that n^k counts* and *how to calculate n^k*. The distinction will become clear by the end of this section.

Question 4 *Create a counting question whose answer is* 3^m.

The product principle

The ***product principle*** is the general counting method that handles the counting questions we've answered so far. It is quite flexible and perhaps the most widely used basic rule in combinatorics.

The product principle: *In counting k-lists of the form $(l_1, l_2, \ldots, l_k)$, if*

- *there are c_1 ways to specify element l_1 of the list, and each such specification ultimately leads to a different k-list; and*
- *for every other list element l_i, there are c_i ways to specify that element no matter the specification of the previous elements $l_1, \ldots, l_{i-1}$, and that each such specification of l_i ultimately leads to a different k-list,*

then there are $c_1 c_2 \cdots c_k$ such lists.

In the context of a tree diagram like that of Figure 1.1, the product principle applies when the number of branches to the right of each circle labeled l_i is the same, for each fixed i.

Counting binary numbers

A ***binary number*** is a sequence of digits, each either 0 or 1. How many n-digit binary numbers are there?

An n-digit binary number is a number of the form $d_1 d_2 \cdots d_n$ where each d_i is 0 or 1. As such it is an n-list taken from a 2-set, namely $\{0, 1\}$, and so there are 2^n such numbers.

Question 5 *How many n-digit binary numbers do not start with 0?*

Counting all possible subsets

How many subsets of an n-set are there?

Besides answering a fundamental counting question, this example's significance lies in the way we use lists (in which order matters) to count sets (in which order *doesn't* matter). The idea is to encode each possible subset with an n-digit binary number that indicates whether each element of the n-set belongs to the subset.

For example, when $n = 3$ and our 3-set is [3], we associate each subset of [3] with a 3-digit binary number as follows:

$$\begin{aligned} \emptyset &\longrightarrow 000 & \{1,2\} &\longrightarrow 110 \\ \{1\} &\longrightarrow 100 & \{1,3\} &\longrightarrow 101 \\ \{2\} &\longrightarrow 010 & \{2,3\} &\longrightarrow 011 \\ \{3\} &\longrightarrow 001 & \{1,2,3\} &\longrightarrow 111. \end{aligned}$$

That is, each subset is associated with the 3-digit binary number $d_1 d_2 d_3$ that has $d_i = 1$ if i is in the subset and $d_i = 0$. This shows that there are as many subsets of [3] as there are 3-digit binary numbers, namely 2^3. In general, there are as many subsets of an n-set as there are n-digit binary numbers, so there are 2^n subsets of an n-set.

The set of all possible subsets of a set A is called the ***power set of*** A and we denote it with the special notation 2^A. The reason for the notation is to make the formula $\left|2^A\right| = 2^{|A|}$ memorable. For example, $\left|2^{[n]}\right| = 2^n$.

Question 6 *Let $X = [100]$ and let Y be the set of odd integers. Find $\left|2^{X \cap Y}\right|$.*

Question Q2: Counting lists without repetition

Now we move on to Question Q2: Given nine players, in how many different ways can a manager write out a batting lineup?

Let's answer the smaller, four-player version first. If the players are A, B, C, D, then a lineup corresponds to a 4-list in which each of these letters appears exactly once. The list can begin in four ways:

A___ B___ C___ D___.

The second player in the lineup can be anyone but the first player, so this increases the possibilities by a factor of 3:

AB__	BA__	CA__	DA__
AC__	BC__	CB__	DB__
AD__	BD__	CD__	DC__.

The third player can be anyone but the first two players, so this increases the possibilities by a factor of 2:

ABC_ ABD_	BAC_ BAD_	CAB_ CAD_	DAB_ DAC_
ACB_ ACD_	BCA_ BCD_	CBA_ CBD_	DBA_ DBC_
ADB_ ADC_	BDA_ BDC_	CDA_ CDB_	DCA_ DCB_.

The final player must be the (only) player not yet on the list, and in order to fit the pattern we will say that this increases the possibilities by a factor of 1:

ABCD ABDC	BACD BADC	CABD CADB	DABC DACB
ACBD ACDB	BCAD BCDA	CBAD CBDA	DBAC DBCA
ADBC ADCB	BDAC BDCA	CDAB CDBA	DCAB DCBA.

There are 24 possible batting lineups. The complete enumeration suggests that we can calculate this as $4 \cdot 3 \cdot 2 \cdot 1 = 24$. The product $4 \cdot 3 \cdot 2 \cdot 1$ is denoted by 4! and read "four factorial."

Question 7 *You have a pile of six different books. How many ways are there to arrange three of them on a shelf? The order in which the books appear from left to right matters.*

We can apply this same method to the original Question Q2. There are nine choices for the first player, then eight choices for the second player, then seven choices for the third player, and so on. In all, there are $9! = 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 362{,}880$ different lineups.

In general, $n!$ stands for the product of the integers between 1 and n, inclusive. We define 0! to be 1.

Counting passwords again

How many passwords in Question Q1 have no repeated characters?

This means that a password like Gh64Fh4Z is no longer allowed, but oqwei9VQ still is. There are still 62 choices for the first character, but then 61 choices for the second (anything but the first), 60 choices for the third (anything but the first two), and so on. In total there are

$$62 \cdot 61 \cdot 60 \cdot 59 \cdot 58 \cdot 57 \cdot 56 \cdot 55 = 136{,}325{,}893{,}334{,}400$$

passwords. The notation for the product on the left is $(62)_8$ and it means to take the first eight terms of 62! starting with 62. In this case we are counting 8-lists without repetition from a 62-set. Another way to write it is

$$(62)_8 = \frac{62!}{(62-8)!} = \frac{62!}{54!}.$$

In general, $(n)_k = n(n-1)\cdots(n-k+1)$ or equivalently $(n)_k = \frac{n!}{(n-k)!}$. Notice that $(n)_n = n!$.

Question 8 *A softball coach has 14 players available but can only bat 10 players in a lineup. How many lineups are possible?*

Counting team assignments

A gymnastics team has seven members. The coach must assign one member to compete in each of the four event finals (floor exercise, balance beam, vault, uneven parallel bars). How many different assignments are possible if members are allowed to compete in more than one event? How many if no member can compete in more than one event?

Label the team members A-G and keep track of an assignment with a 4-list like DCGC where the first element is the member that competes in the floor exercise (here, D), the second in the beam (C), the third in the vault (G), and the fourth in the uneven bars (also C). The answer to the first question is 7^4 since any such assignment is a 4-list taken from a 7-set. The answer to the second is $(7)_4$ since any such assignment is a 4-list without repetition taken from a 7-set. The exact values are

$$7^4 = 2401 \qquad \text{and} \qquad (7)_4 = 7 \cdot 6 \cdot 5 \cdot 4 = 840.$$

How to count lists without repetition

A list without repetition is sometimes called a ***permutation***. If such a list has length k then it is a ***k-permutation***. When we counted the passwords in question Q1 that have no repeated characters, we counted the 8-permutations taken from a 62-set. An n-permutation of an n-set is simply called a ***permutation of the set***. This is a "complete permutation" of the set, like the 4-player batting lineups were permutations of the set $\{\texttt{A}, \texttt{B}, \texttt{C}, \texttt{D}\}$. Here is a summary.

Counting lists without repetition:

- *Notation:* $(n)_k$ equals the number of k-element lists without repetition taken from an n-element set.
- *Key features:* Order matters, repeated elements not allowed.
- *Typical question:* How many ways are there to form a k-letter word where there are n choices for each letter and no letter appears more than once?
- *Formulas:*

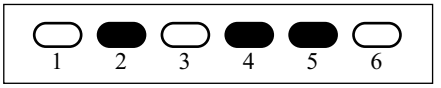
$$(n)_k = \frac{n!}{(n-k)!} \quad \text{or} \quad (n)_k = n(n-1)\cdots(n-k+1).$$

As a special case, $n!$ equals the number of n-element lists without repetition taken from an n-element set. That is, it equals the number of permutations of an n-set.

Question Q3: Counting subsets of a set

Now we answer Question Q3: You play a pick-six lottery by specifying six different numbers from 1-40. How many different lottery tickets are possible?

We first examine the case of a pick-three lottery involving the numbers 1-6. As a note of clarification, the order in which you list your numbers doesn't matter in this lottery. For example, to play the numbers 2-4-5 you fill in those ovals on your ticket:



Thus, a ticket is really just a size-3 subset of the set $\{1, 2, 3, 4, 5, 6\}$.

Here is a complete enumeration of all possible tickets. To ensure that we don't miss any, we take the systematic approach of first listing all the tickets that have 1 as the lowest number:

$$\{1,2,3\} \quad \{1,2,4\} \quad \{1,2,5\} \quad \{1,2,6\} \quad \{1,3,4\}$$
$$\{1,3,5\} \quad \{1,3,6\} \quad \{1,4,5\} \quad \{1,4,6\} \quad \{1,5,6\}.$$

Then list those that have 2 as the lowest number:

$$\{2,3,4\} \quad \{2,3,5\} \quad \{2,3,6\} \quad \{2,4,5\} \quad \{2,4,6\} \quad \{2,5,6\}.$$

Then list those that have 3 as the lowest number:

$$\{3,4,5\} \quad \{3,4,6\} \quad \{3,5,6\}.$$

Finally list those that have 4 as the lowest number: $\{4, 5, 6\}$. There are 20 tickets in all.

The notation $\binom{n}{k}$, read "n choose k," stands for the number of k-subsets of an n-set. The answer to the small lottery question above is $\binom{6}{3}$ and we calculated $\binom{6}{3} = 20$ by complete enumeration. The general formula is

$$\binom{n}{k} = \frac{(n)_k}{k!} \qquad \text{or} \qquad \binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Here is a brief justification. Let's count the k-permutations of an n-set. We know there are $(n)_k$ of them. An alternate way to count them involves first specifying which k elements of the n-set are in the permutation (there are $\binom{n}{k}$ ways to do this) and then lining those elements up in a particular order (there are $k!$ ways to do that). By the product principle, there are $\binom{n}{k} \cdot k!$ such permutations. Therefore $(n)_k = \binom{n}{k} \cdot k!$, or $\binom{n}{k} = \frac{(n)_k}{k!}$. See Section 1.4 for a somewhat different approach.

Now we can finish Question Q3. The answer is $\binom{40}{6}$ because any ticket corresponds to a size-6 subset of [40]. There are about 3.8 million tickets:

$$\binom{40}{6} = \frac{(40)_6}{6!} = \frac{40 \cdot 39 \cdot 38 \cdot 37 \cdot 36 \cdot 35}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 3{,}838{,}380.$$

Question 9 *You are dealt a five-card hand from a standard deck of 52 cards. How many different hands are there? (The order in which you receive the cards doesn't matter.)*

Counting binary numbers

How many n-digit binary numbers have exactly k 1s?

Here is a complete enumeration of the 5-digit binary numbers with exactly two 1s:

$$\begin{array}{lllll} 11000 & 10100 & 10010 & 10001 & 01100 \\ 01010 & 01001 & 00110 & 00101 & 00011. \end{array}$$

To specify such a number, we need only identify the locations of the two 1s because each remaining digit is then 0. Using a 2-set to keep track of the positions of the 1s gives the following correspondence:

$$\begin{array}{ll} 11000 \longrightarrow \{1,2\} & 01010 \longrightarrow \{2,4\} \\ 10100 \longrightarrow \{1,3\} & 01001 \longrightarrow \{2,5\} \\ 10010 \longrightarrow \{1,4\} & 00110 \longrightarrow \{3,4\} \\ 10001 \longrightarrow \{1,5\} & 00101 \longrightarrow \{3,5\} \\ 01100 \longrightarrow \{2,3\} & 00011 \longrightarrow \{4,5\}. \end{array}$$

Therefore there are as many 5-digit binary numbers with exactly two 1s as there are 2-subsets of a 5-set, so there are $\binom{5}{2} = 10$. In general, the number of n-digit binary numbers with exactly k 1s is $\binom{n}{k}$.

Question 10 *Explain why the number of 10-digit binary numbers with exactly three 1s equals the number of 10-digit binary numbers with exactly seven 1s.*

How to count subsets of a set

The numbers $\binom{n}{k}$ are called binomial coefficients and are so called because of the binomial theorem (see Theorem 2.2.2 on page 63). The term ***combination*** is sometimes used to indicate a subset or to indicate an unordered collection of distinct objects.

Counting subsets:

- *Notation:* $\binom{n}{k}$ equals the number of k-element subsets of an n-element set.
- *Key features:* Order doesn't matter, repeated elements not allowed.
- *Typical questions:* How many n-digit binary numbers have exactly k 1s? How many ways are there to form a k-person committee from a group of n people?
- *Formulas:*

$$\binom{n}{k} = \frac{(n)_k}{k!} \qquad \text{or} \qquad \binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Question 11 *How many ways are there to form a 20-person committee from a group of 435 people?*

Question Q4: Counting multisets

Now for Question Q4: How many different orders for a dozen donuts are possible if a store offers 30 donut varieties?

First we trim the problem to a smaller version involving an order of three from a store selling four varieties. In ordering donuts all that matters is how many donuts of each variety we want—the sequence in which we list them doesn't matter. We also assume that there

are no differences among donuts of a particular variety. Thus, we have a situation in which order doesn't matter (like a set and unlike a list) but repetition is allowed (like a list and unlike a set).

Let's say the store has Boston creme (B), chocolate (C), glazed (G), and maple (M) available. Here are all possible orders:

$$\begin{array}{lllll} \{B,B,B\} & \{B,C,C\} & \{B,C,M\} & \{C,C,M\} & \{G,G,G\} \\ \{B,B,C\} & \{B,G,G\} & \{B,G,M\} & \{C,G,G\} & \{G,G,M\} \\ \{B,B,G\} & \{B,M,M\} & \{C,C,C\} & \{C,M,M\} & \{G,M,M\} \\ \{B,B,M\} & \{B,C,G\} & \{C,C,G\} & \{C,G,M\} & \{M,M,M\}. \end{array}$$

These are known as ***multisets*** which are sets with repetition allowed. We use the same curly braces { } that indicate a set to indicate a multiset. The presence of a multiset should be clear from context.[2]

The notation $\left(\!\binom{n}{k}\!\right)$ stands for the number of k-multisets taken from an n-set. The latter phrase indicates that there are k elements in the multiset and each element belongs to a certain n-set. The answer to the small donut order question above is $\left(\!\binom{4}{3}\!\right)$ and we calculated $\left(\!\binom{4}{3}\!\right) = 20$ by complete enumeration. The general formula is

$$\left(\!\binom{n}{k}\!\right) = \binom{k+n-1}{k}.$$

We next explain the formula for the special case $n = 4$ and $k = 3$.

Examine the following correspondence between binary numbers and donut orders.

binary number	donut order	binary number	donut order
000111	$\{B,B,B\}$	100011	$\{C,C,C\}$
001011	$\{B,B,C\}$	100101	$\{C,C,G\}$
001101	$\{B,B,G\}$	100110	$\{C,C,M\}$
001110	$\{B,B,M\}$	101001	$\{C,G,G\}$
010011	$\{B,C,C\}$	101100	$\{C,M,M\}$
011001	$\{B,G,G\}$	101010	$\{C,G,M\}$
011100	$\{B,M,M\}$	110001	$\{G,G,G\}$
010101	$\{B,C,G\}$	110010	$\{G,G,M\}$
010110	$\{B,C,M\}$	110100	$\{G,M,M\}$
011010	$\{B,G,M\}$	111000	$\{M,M,M\}$

Notice that all of the 3-multisets taken from the 4-set $\{B,C,G,M\}$ are listed, as are all of the 6-digit binary numbers with exactly three 0s. In any such binary number, the number of 0s before the first 1 equals the number of B's in the order, the number of 0s between the first and second 1s equals the number of C's in the order, and so on. For example, 101100 has no 0s before the first 1 (no B's in the order), one 0 between the first and second 1 (one C), no 0s between the second and third 1 (no G's), and two 0s after the third 1 (two M's). Therefore, it corresponds to $\{C,M,M\}$.

Thus, each binary number has $k = 3$ zeros and $n-1 = 4-1$ ones. The 0s correspond to the donuts and the 1s correspond to "dividers" between donuts of different varieties.

[2] Some authors use different delimiters such as $\langle\ \rangle$ or [ ] to denote multisets.

(Notice that we use one fewer divider than the number of varieties available.) There are $\binom{k+n-1}{k} = \binom{3+4-1}{3}$ binary numbers having $k + n - 1 = 6$ digits and exactly $k = 3$ zeros, and hence that many donut orders. The same idea works in general to show that $\left(\!\binom{n}{k}\!\right) = \binom{k+n-1}{k}$.

Question 12 *Given the binary number* 10001101010011*, invent a multiset to which it would correspond under the type of correspondence just shown.*

The answer to Question Q4 is $\left(\!\binom{30}{12}\!\right)$ because any order corresponds to a size-12 multiset of [30]. There are about 7.9 billion orders since

$$\left(\!\binom{30}{12}\!\right) = \binom{12+30-1}{12} = \binom{41}{12} = 7{,}898{,}654{,}920.$$

Question 13 *Your friend sends you to the same store for a dozen donuts. He wants three Boston creme but the rest is up to you. How many different orders are there?*

Distributing candy

You have eight red lollipops to distribute among 12 children. In how many ways can you do this?

Make a record of how we distribute the candy using a multiset. For example, $\{2, 2, 5, 5, 5, 5, 10, 12\}$ means we give two lollipops to child 2, four to child 5, and one each to children 10 and 12. In that way any distribution is an 8-multiset taken from a 12-set. There are

$$\left(\!\binom{12}{8}\!\right) = \binom{8+12-1}{8} = \binom{19}{8} = 75{,}582$$

ways to distribute the lollipops.

How to count multisets

The notation $\left(\!\binom{n}{k}\!\right)$ is helpful because the double parentheses remind us that repetition is allowed.

Counting multisets:

- *Notation:* $\left(\!\binom{n}{k}\!\right)$ equals the number of k-element multisets taken from an n-element set.
- *Key features:* Order doesn't matter, repeated elements allowed.
- *Typical questions:* In how many ways can we place an order for k donuts if the store sells n varieties? In how many ways can we distribute k identical pieces of candy to n children?
- *Formula:*

$$\left(\!\binom{n}{k}\!\right) = \binom{k+n-1}{k}.$$

Putting it all together

Let's attack more counting questions using what we know so far. The crucial skill is to be able to determine whether we need to count lists, permutations, subsets, or multisets.

(a) Four candidates vie for the position of town selectman. If 1180 votes are cast, then how many different final vote totals could be reported on the news?

$\Longrightarrow$ Call the candidates A, B, C, and D. One way to record the final vote is with a multiset of size 1180 where each element is either A, B, C, or D. In fact, such a multiset corresponds exactly to the box containing the 1180 ballots cast where each ballot has an A, B, C, or D on it. Therefore the number of final vote totals equals the number of 1180-multisets taken from a 4-set, which is

$$\left(\!\!\binom{4}{1180}\!\!\right) = \binom{1180+4-1}{1180} = \binom{1183}{1180} = 275{,}233{,}231.$$

(b) In the era before cell phones, how many 10-digit U. S. phone numbers were there? Such a number is a 3-digit area code followed by a 3-digit exchange code followed by a 4-digit extension. Neither an area nor exchange code can begin with 0 or 1, but the middle digit of the area code must be either 0 or 1.

$\Longrightarrow$ In a phone number, order matters and repetition of digits is allowed. Write a phone number as a 10-list $a_1a_2a_3e_1e_2e_3d_1d_2d_3d_4$. There are eight choices for a_1 (any digit 2 through 9), two choices for a_2 (0 or 1), 10 for a_3, 8 for e_1, and 10 for each of the six remaining digits. There are

$$8 \cdot 2 \cdot 10 \cdot 8 \cdot 10^6 = 1{,}280{,}000{,}000 = 1.28 \text{ billion}$$

phone numbers.

Question 14 *Springfield, MA is in the 413 area code. How many different exchanges, at minimum, will ensure that each of the approximately 160,000 citizens of Springfield can have their own phone number?*

(c) Let k and n be integers satisfying $1 \leqslant k \leqslant n$. How many subsets of $[n]$ contain k as their largest element?

$\Longrightarrow$ First look at a special case like $n = 6$ and $k = 4$. Here are the subsets of $[6]$ containing 4 as their largest element:

$$\begin{array}{cccc} \{4\} & \{1,4\} & \{2,4\} & \{3,4\} \\ \{1,2,4\} & \{1,3,4\} & \{2,3,4\} & \{1,2,3,4\} \end{array}$$

Ignoring element 4, which must be present in each subset, we see that we have simply listed all of the subsets of $[3]$, of which there are $2^3 = 8$. The answer to the original question is 2^{k-1}, because any subset of $[n]$ containing k as its largest element consists of k together with any one subset of $[k-1]$.

(d) A lock has the numbers 0-29 arranged in a circle around its dial. A combination for the lock consists of four numbers, but no two numbers that are adjacent or equal on the dial can be consecutive in the combination (0 and 29 are adjacent). How many combinations are there?

$\Longrightarrow$ Write the combination as a 4-list (d_1, d_2, d_3, d_4). There are 30 choices for d_1. For each such choice there are 27 choices for d_2 because it cannot equal d_1 or the two numbers adjacent to it. Similarly there are 27 choices for each of d_3 and d_4. There are $30 \cdot 27^3 = 590{,}490$ combinations.

(e) Fifty runners compete in a road race but the newspaper only publishes the names of the first, second, and third place finishers. How many different lists could the newspaper publish?

$\Longrightarrow$ If the runners are numbered 1-50, then a 3-list like $(34, 37, 2)$ indicates that runner 34 finishes first, 37 finishes second, and 2 finishes third. The order in which they finish matters, and repetition is not allowed since no runner can finish, say, both second and third. Thus we count the 3-lists without repetition taken from a 50-set. There are $(50)_3 = 50 \cdot 49 \cdot 48 = 117{,}600$ different lists.

Question 15 *If instead the paper publishes the order in which all 50 runners finish, how many are possible?*

(f) How many seven-letter palindromes using the letters A-Z are there? A palindrome reads the same forwards and backwards, like GHHTHHG or RACECAR.

$\Longrightarrow$ A seven-letter palindrome is completely determined by its first four letters. There are 26 choices for each of the first four letters, so there are $26^4 = 456{,}976$ palindromes.

Question 16 *Answer the same question but for eight-letter palindromes. Then, generalize to n-letter palindromes.*

Notation versus numbers

Understanding what n^k, $(n)_k$, $\binom{n}{k}$, and $\left(\!\binom{n}{k}\!\right)$ count is more important than knowing how to compute them. For example, writing 62^8 in addition to the final answer of 218,340,105,584,896 reveals what type of basic objects were counted—8-lists taken from a 62-set. Thus 62^8 gives important insight into the solution method. Likewise, writing $\binom{40}{6}$ in addition to 3,838,380 reveals that the problem amounted to counting the 6-subsets of a 40-set. We follow this practice throughout the book.

Summary

In this section we introduced four canonical counting problems. Each involves the arrangement of k objects where each object is chosen from a particular set of size n. Order may or may not matter in the arrangement of the objects, and repetition of objects may or may not be allowed in the arrangement. Using the notation introduced in this section, here are the answers to each of the four problems.

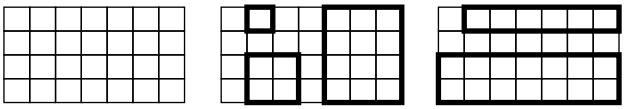
	order matters	**order doesn't matter**
repetition allowed	n^k	$\left(\!\binom{n}{k}\!\right)$
repetition not allowed	$(n)_k$	$\binom{n}{k}$

The key to analyzing basic counting problems is to understand which of the four cases can be applied. It is perfectly acceptable, and even preferable, to leave the answer to a counting question in terms of the notation shown in the table.

Exercises

1. How many different tickets are possible in each of the following lotteries? And which lottery offers the best chance of winning?
   (a) You pick six numbers from 1-16, a number can be picked more than once, and order doesn't matter.
   (b) You pick five different numbers from 1-25 and order doesn't matter.
   (c) You pick four different numbers from 1-18 and the order in which you specify them matters.
2. You flip a coin 20 times and record the ordered sequence of heads and tails.
   (a) How many sequences are there in which you get heads on (at least) flip #1, #4, #7, and #13?
   (b) How many sequences have the same number of heads and tails?
3. Count the n-digit numbers of the following types.
   (a) ***ternary***: each digit is 0, 1, or 2
   (b) ***octal***: each digit is 0, 1, 2, 3, 4, 5, 6, or 7
   (c) ***hexadecimal***: each digit is 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, or F
4. (see previous exercise) How many 10-digit hexadecimal numbers begin and end with F? How many 8-digit octal numbers begin and end with an even digit?
5. How many ways are there to pick a collection of 15 coins from bags of pennies, nickels, dimes, and quarters? (Assume coins of the same denomination are indistinguishable.)
6. In the pick-6 lottery involving the numbers 1-40, you win the Match-4 prize if exactly four of your six numbers appear on the winning ticket. In a given lottery drawing, how many different tickets would win the Match-4 prize?
7. How many 4-character passwords are possible if each character is taken from an n-set? What is the smallest n that guarantees at least one billion different passwords? Answer the same two questions but for 8-character passwords.
8. Consider the phone number 289-3447. How many alphabetic phone numbers can be made from this number using the letters on the phone buttons? For example, BUY-EGGS is one possibility and ATX-DIGR is another. Answer the same question if you're allowed the option of leaving numbers unchanged, like C8Y-F4IP.
9. How many subsets of [20] ...
   (a) have smallest element 4 and largest element 15?
   (b) contain no even numbers?
   (c) have size 10 and don't contain any number larger than 17?

10. A Maryland automobile license plate consists of three letters followed by three numbers. How many are possible? Decorum dictates that some three-letter combinations be outlawed. For each three-letter combination outlawed, how many possible license plates does this remove from circulation?
11. You throw five identical six-sided dice and write down the values showing, in nondecreasing order from left to right. For example, 22245 means you rolled three 2s, one 4, and one 5. How many outcomes are possible? How many in which all the values are different?
12. How many different regions are in a Venn diagram involving n pairwise intersecting sets?
13. How many 6-permutations of [15] have their digits listed in increasing order?
14. How many arithmetic problems of the following form are possible? You must use each of the digits 1 through 9, they must appear in numerical order from left to right, and you can use any combination of the $+$ and $\times$ symbols you like, as long as the resulting expression makes mathematical sense. For example, $1234 + 5 \times 6 \times 78 + 9$ and $123456 + 789$ and 123456789 are three possibilities, but $1 \times \times 234567 + 89$ is not.
15. How many ways are there to distribute 16 identical pieces of candy to five children such that every child receives at least one piece? Generalize to k identical pieces of candy and n children.
16. How many permutations of [9] have no adjacent odd digits? For example, a permutation like 385164927 is not allowed because 5 and 1 are adjacent.
17. Find the number of 3-lists of the form (x_1, x_2, x_3), where each x_i is a nonnegative integer and $x_1 + x_2 + x_3 = 10$.
18. A professor gives an exam on which she asks her students to answer any five of the eight questions. In how many ways could the students select the questions?
19. A 4×7 checkerboard is shown below at the left. How many different rectangles are hiding in it? Five examples of rectangles you need to count are shown in the two boards on the right.



20. (from *Measure Theory* by Paul R. Halmos, Springer-Verlag, 1950) Let S be a set. Suppose that s is an element of S, T is a subset of S, and $\mathcal{F}$ is a set of subsets of S. How many statements of the form $X\ R\ Y$ are possible, where X and Y are each taken from $\{S, s, T, \mathcal{F}\}$ and R is taken from $\{\in, \subseteq\}$? Classify each statement as always true, possibly true, or always false.

1.2 Counting, overcounting, and the sum principle

In this section we continue our study of basic counting problems by discussing several examples. We first shed light on two common misapplications of the product principle. We then identify two important techniques for fixing these problems and examine more examples.

More with the product principle

Ternary numbers

A ***ternary number*** is a sequence of digits, each either 0, 1, or 2. How many 8-digit ternary numbers have exactly three 1s?

Examples of 8-digit ternary numbers are 11102000 and 02212101 and 00011100. Think of building such a number in two stages: (1) specify the location of the three 1s, then (2) specify the remaining digits. There are $\binom{8}{3}$ ways to specify the location of the 1s. The remaining five digits are each 0 or 2, so there are 2^5 ways to specify them. We may apply the product principle and the answer is $\binom{8}{3} \cdot 2^5 = 1792$.

Question 17 *How many n-digit ternary numbers have exactly k 1s?*

Exam questions

A multiple choice exam has 20 questions with four possible answers for each question. How many different exam papers would earn a grade of 70%?

We can keep track of a student's answers using a 20-list taken from $\{a, b, c, d\}$ where the latter set represents the possible answers to each question. A grade of 70% means exactly 14 of 20 questions correct. There are $\binom{20}{14}$ different ways to specify those 14 questions. Then, each of the remaining six questions must be answered incorrectly. Since there are three wrong answers for each question, there are 3^6 ways to answer the remaining six incorrectly. By the product principle there are $\binom{20}{14} \cdot 3^6 = 28{,}256{,}040$ ways to earn 70% on the exam.

Question 18 *Divide the number of ways to earn 70% by the total number of ways to complete the exam. What is the likelihood that you'd earn 70% just by guessing?*

Palindromes

Of the integers from 1 to 999999, how many are palindromes?

A palindrome reads the same forwards and backwards so each of 4 and 555 and 9889 is a palindrome that we need to count. This means that a palindrome is completely determined by its first half. For example, there are $9 \cdot 10^2$ five-digit palindromes because the first digit can be any digit 1-9, the second any digit 0-9, and the third any digit 0-9. Once those are chosen the fourth and fifth digits are automatically determined.

Among the integers from 1 to 999999 are one-digit numbers up to six-digit numbers. The number of palindromes depends on the number of digits:

k	1	2	3	4	5	6
# palindromes with k digits	9	9	$9 \cdot 10$	$9 \cdot 10$	$9 \cdot 10^2$	$9 \cdot 10^2$

To count all the palindromes asked for, we add these answers to obtain

$$9 + 9 + (9 \cdot 10) + (9 \cdot 10) + (9 \cdot 10^2) + (9 \cdot 10^2) = 1998.$$

The sum principle

In answering the last question, we divided the palindromes into cases by number of digits, counted each case, and then added the answers to get the final total. The breaking-into-cases idea is indispensable in combinatorics and is called the sum principle.

The sum principle: *Suppose the objects in a counting question can be divided into k disjoint and exhaustive cases. If there are n_j objects in the j-th case, for $j = 1, 2, \ldots, k$, then there are $n_1 + n_2 + \cdots + n_k$ objects in total.*

The word "disjoint" means that there is no overlap among the cases, and the word "exhaustive" means that every object falls into some case. Together, they mean that every object falls into one and only one case.

Exam questions again

A multiple choice exam has 20 questions with four possible answers for each question. How many different exam papers would earn a grade of at least 70%?

Again we use a 20-list taken from $\{a, b, c, d\}$ to keep track of each exam. A grade of at least 70% means getting between 14 and 20 questions correct, inclusive. We split the exams into cases according to the number of questions correct and then use the sum principle. Earlier we found there are $\binom{20}{14} \cdot 3^6$ exams that earn exactly 70%. The other cases are similar and the answer is

$$\binom{20}{14}3^6 + \binom{20}{15}3^5 + \binom{20}{16}3^4 + \cdots + \binom{20}{19}3^1 + \binom{20}{20}3^0$$

which can also be written $\displaystyle\sum_{k=14}^{20} \binom{20}{k} 3^{20-k}$. This equals 32,448,508.

Question 19 *How many exam papers earn a grade of at least 90%?*

Overcounting and other perils

There are two key phrases in the statement of the product principle. For convenience we repeat it below with the key phrases in boldface.

The product principle: *In counting k-lists of the form $(l_1, l_2, \ldots, l_k)$, if*

- *there are c_1 ways to specify element l_1 of the list, and* ***each such specification ultimately leads to a different k-list****; and*
- *for every other list element l_i, there are c_i ways to specify that element* ***no matter the specification of the previous elements*** *$l_1, \ldots, l_{i-1}$, and that* ***each such specification of l_i ultimately leads to a different k-list****,*

then there are $c_1 c_2 \cdots c_k$ such lists.

We next illustrate how failure to heed these phrases can lead to incorrect counting.

A misapplication of the product principle

In blackjack, you are dealt a two-card hand. The first is placed face down and the second face up. How many hands are there in which the face-down card is an ace and the face-up card is a heart?

Represent a two-card hand as a 2-list (D, U) where D is the face-down card and U is the face-up card. There are four ways to specify D since there are four aces in the deck. Then there are 13 ways to specify U since there are 13 hearts in the deck. By the product principle there are $4 \cdot 13 = 52$ hands.

This is an incorrect application of the product principle because the number of ways to specify U depends on the way D was specified. The problem is the ace of hearts.

Card chosen for D	Number of choices for U
A♠	13
A♣	13
A♡	12
A◇	13

In other words the product principle doesn't apply because there are not 13 ways to specify D for every possible choice of U.

The fix

Since the ace of hearts is the problem, let's treat that case separately. If D is not the ace of hearts, there are three ways to specify it. For each such way there are 13 ways to specify U for a total of $3 \cdot 13 = 39$ two-card hands. If D is the ace of hearts, there are 12 ways to specify U for a total of 12 two-card hands. By the sum principle there are $3 \cdot 13 + 12 = 51$ hands.

Another way to fix it is simply to observe that the original, incorrect answer of $4 \cdot 13$ is too large, but only by one because it includes the hand (A♡, A♡). So there are $4 \cdot 13 - 1 = 51$ hands.

Question 20 *How many hands are there in which the face-down card is an ace and the face-up card is not a heart?*

Another misapplication of the product principle

How many 4-lists taken from [9] have at least one pair of adjacent elements equal?

For example, the 4-lists 1114 and 1229 and 5555 qualify, but 9898 does not. Let's specify such a list in three steps:

- Step 1: Specify the location of the adjacent equal elements.
- Step 2: Specify the value of those elements.
- Step 3: Specify the two remaining elements.

There are three ways to specify the location of the adjacent equal elements—the first two, middle two, or last two. Once accomplished, there are nine ways to specify their value. Then each of the remaining two elements can be any number 1-9, so there are 9^2 ways to specify them. By the product principle there are $3 \cdot 9 \cdot 9^2 = 2187$ numbers. Right?

Wrong! We misapplied the product principle and this led to an overcount. The problem occurred at the first step: each specification of the location of the adjacent equal digits does *not* lead to a different 4-digit number in the end. Here is why.

Among the 4-lists being counted by Steps 1-3 are those of the form $44cd$ which result from choosing the first two positions in Step 1 and value 4 in Step 2. Now when we complete the list in Step 3, we end up with the $9^2 = 81$ lists

$$4411, 4412, 4413, 4414, 4415, \ldots, 4497, 4498, 4499. \tag{1.1}$$

Also among the 4-lists begin counted by Steps 1-3 are those of the form $a44d$ and $ab99$. When we complete each such list in Step 3 we end up with

$$1441, 1442, 1443, 1444, 1445, \ldots, 9447, 9448, 9449 \tag{1.2}$$

and

$$1199, 1299, 1399, 1499, 1599, \ldots, 9799, 9899, 9999 \tag{1.3}$$

respectively. This is a problem because lists like 4441 and 4444 appear in both (1.1) and (1.2). A list like 4499 appears in both (1.1) and (1.3). In other words, it is *not* the case that the specifications in Steps 1 and 2 lead to different lists in the end.

The fix

Here is how to fix this. Let

x = # of 4-lists taken from [9]

y = # of 4-lists taken from [9] with at least one pair of adjacent elements equal

z = # of 4-lists taken from [9] with no pair of adjacent elements equal.

We want to find y. By the sum principle $x = y + z$ because any 4-list either has at least one pair of adjacent elements equal or else has no pair of adjacent elements equal. Notice that both x and z are easy to determine. We know $x = 9^4$. For z, there are nine ways to specify the first element, then eight ways to specify the second (anything but the first), then eight ways to specify the third (anything but the second), then eight ways to specify the fourth (anything but the third). By the product principle there are $9 \cdot 8^3$ such lists. Therefore there are

$$y = x - z = 9^4 - 9 \cdot 8^3 = 1953$$

4-lists taken from [9] with at least one pair of adjacent elements equal.

Question 21 *How many 5-lists taken from $\{A, B, \ldots, Z\}$ have no pair of adjacent letters equal?*

Counting the complement

The technique used to fix the last example is known as ***counting the complement***. It is essentially just a particular way to apply the sum principle but it is very powerful.

Counting subsets

How many subsets of [15] have at least two elements?

"At least two elements" could mean any number of elements from 2 to 15. The complement of "at least two" is "at most one" which only means 0 or 1. There are $\binom{15}{0} = 1$ subsets with zero elements and $\binom{15}{1} = 15$ with one element. So there are

$$2^{15} - \left[\binom{15}{0} + \binom{15}{1}\right] = 32{,}752$$

subsets with at least two elements.

Notice that it is not necessary to count the complement, for we could just sum the number of subsets of size k from $k = 2$ to 15 to get the answer:

$$\binom{15}{2} + \binom{15}{3} + \cdots + \binom{15}{15} = \sum_{k=2}^{15} \binom{15}{k}.$$

However, counting the complement makes for a quicker calculation.

Question 22 *How many n-digit binary numbers have at least one 0 and one 1?*

Counting passwords, again

Passwords often must have a minimum number of characters of a certain type. How many eight-character passwords are there if each character is either an uppercase letter A-Z, a lowercase letter a-z, or a digit 0-9, and where at least one letter is used?

The at-least-one-letter requirement eliminates the possibility of an all-number password. All-number passwords are easy to count so we count the complement. We already know that there are 62^8 possible passwords, and of these 10^8 contain only numbers. Therefore, $62^8 - 10^8 = 218{,}340{,}005{,}584{,}896$ contain at least one letter.

Question 23 *Answer the same question, but where at least one letter and at least one number is used.*

Still counting passwords

How many eight-character passwords are there if each character is either an uppercase letter A-Z, a lowercase letter a-z, or a digit 0-9, and where at least one uppercase and at least one lowercase letter are used?

The complement of "at least one uppercase and at least one lowercase letter are used" is "either no uppercase or no lowercase letters are used." We have to be careful about counting objects specified by an "or" statement. Define the following sets:

$$A = \{\text{passwords } p : p \text{ has 8 characters}\}$$
$$B = \{\text{passwords } p : p \text{ has 8 characters and no uppercase letters}\}$$
$$C = \{\text{passwords } p : p \text{ has 8 characters and no lowercase letters}\}.$$

The answer to the question is $|A| - |B \cup C|$ via counting the complement. We know $|A| = 62^8$. For $|B \cup C|$ we use the familiar formula

$$|B \cup C| = |B| + |C| - |B \cap C|.$$

There are $|B| = 36^8$ passwords with no uppercase letters, $|C| = 36^8$ with no lowercase letters, and $|B \cap C| = 10^8$ with neither upper nor lowercase letters (i.e., all numbers). Therefore there are

$$|A| - |B \cup C| = 62^8 - (36^8 + 36^8 - 10^8) = 212{,}697{,}985{,}769{,}984$$

passwords in which at least one uppercase and one lowercase letter are used. This requirement removes $|B \cup C| = 5{,}642{,}119{,}814{,}912$ passwords from consideration.

More examples

Best-of-seven series

Two baseball teams, A and B, play each other in a best-of-seven series, so that the first team to win four games wins the series. The outcome ABAAA means that team A wins game 1, team B wins game 2, and then team A wins games 3-5 and therefore the series. The outcome BBBB means that team B wins games 1-4, and BAABABB means that team B wins in seven games. How many different outcomes are there?

We represent each outcome as a length-4, -5, -6, or -7 list depending on the series' length. That observation dictates how to break this problem into manageable cases. First, let's count the outcomes in which team A wins. There are four cases:

◯◯◯◯◯◯A ◯◯◯◯◯A ◯◯◯◯A ◯◯◯A.

In each case, the blanks stand for any list of As and Bs containing exactly three As. There are $\binom{6}{3}$ in the first case, $\binom{5}{3}$ in the second, and so on. Therefore, there are

$$\binom{6}{3} + \binom{5}{3} + \binom{4}{3} + \binom{3}{3}$$

outcomes in which A wins. The number of outcomes in which B wins is exactly the same, so in all there are

$$2\left[\binom{6}{3} + \binom{5}{3} + \binom{4}{3} + \binom{3}{3}\right] = 70$$

different outcomes.

Poker hands

From a standard 52-card deck, how many different five-card hands are possible? How likely is it that you will be dealt three-of-a-kind?

There are as many five-card hands as there are 5-subsets of a 52-set, about 2.6 million:

$$\binom{52}{5} = \frac{(52)_5}{5!} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 2{,}598{,}960.$$

Counting the three-of-a-kind hands requires some care. One approach encodes each hand as a 5-list (A, B, C, D, E) where

- A is the denomination of the three-of-a-kind
  $\Longrightarrow$ 13 ways to choose A
- B is the 3-set of suits for the three-of-a-kind
  $\Longrightarrow \binom{4}{3}$ ways to choose B
- C is a 2-set of denominations for the other two cards
  $\Longrightarrow \binom{12}{2}$ ways to choose C
- D is the suit of the smaller denomination in C
  $\Longrightarrow$ 4 ways to choose D
- E is the suit of the larger denomination in C
  $\Longrightarrow$ 4 ways to choose E.

For example, the hand $\{4\spadesuit, 4\diamondsuit, 4\heartsuit, 3\diamondsuit, \mathrm{K}\clubsuit\}$ corresponds to the 5-list

$$\big(4,\ \{\spadesuit, \diamondsuit, \heartsuit\},\ \{3, \mathrm{K}\},\ \diamondsuit,\ \clubsuit\big).$$

By the product principle there are $13 \cdot \binom{4}{3} \cdot \binom{12}{2} \cdot 4^2 = 54{,}912$ hands.

Question 24 *Explain what is wrong with the following reasoning: There are 52 ways to select the first card that is a part of the three-of-a-kind. Then there are* $\binom{3}{2}$ *ways to pick the other two cards to make up the three-of-a-kind. Finally, there are* $\binom{48}{2}$ *ways to pick the other two cards (any cards except those of the denomination of the three-of-a-kind). By the product principle there are* $52 \cdot \binom{3}{2} \cdot \binom{48}{2}$ *ways.*

Since the ratio of three-of-a-kind hands to all possible hands is

$$\frac{54{,}912}{2{,}598{,}960} = 0.0211284...,$$

we can expect to receive three-of-a-kind on the initial deal about 2% of the time—about once every 50 hands.

Question 25 *How likely is it that you will be dealt a hand containing a full house? (A full house is three cards of one denomination and two of another denomination.)*

See Exercise 18 for the full story.

At least two

How many 5-lists taken from $\{A, B, C, D, E\}$ have at least two As?

Since "at least two As" could mean two or three or four or five As, a direct count would require several cases and also some care to make sure the cases didn't overlap. The opposite of "at least two" is "at most one" which requires fewer cases. We count the complement. The following question outlines a solution via counting the complement.

Question 26 *How many 5-lists taken from $\{A, B, C, D, E\}$ are possible? How many have no As? How many have exactly one A? What now is the answer to the original question?*

As a check, your answer should be 821.

Summary

Two indispensable principles in combinatorics are the sum principle and the method of counting the complement. The sum principle is used when we divide a counting problem into disjoint and exhaustive cases, count each case, and then add the answers. Counting the complement is useful when the description of the objects to be counted includes phrases like "at least one" or "at least two" or "nonempty."

Exercises

1. Jeopardy! The following are *answers* to counting questions. Your job is to write a *question* for each.
   (a) $n^k - (n)_k$
   (b) $n^n - n!$
   (c) $2^n - 2$
   (d) $3^5 - 2^5$
2. How many different outcomes are there in a best-of-nine series between two teams A and B? Generalize to a best-of-n series where n is odd.
3. Given 20 people, how many ways are there to form a committee containing at least three people?
4. A group consists of 12 men and eight women. How many ways are there to...
   (a) form a committee of size 5?
   (b) form a committee of size 5 containing two men and three women?
   (c) form a committee of size 6 containing at least three women?

(d) form a committee of size 10 containing at least four women?

(e) form an all-male committee of any size?

5. How many eight-character passwords are there if each character is either an uppercase letter A-Z, a lowercase letter a-z, or a digit 0-9, and where at least one character of each of the three types is used?

6. Nate, Ben, Suzy, and Gracie play bridge. In how many ways can the 52-card deck be dealt so that each player receives 13 cards?

7. How many k-multisets taken from $[n]$ are not also (ordinary) subsets of $[n]$?

8. Let k and n be positive integers satisfying $k < n$. How many subsets of $[n]$ are not also subsets of $[k]$?

9. How many nonempty subsets of [10] have the product of their elements even?

10. How many permutations of $[n]$ are possible in which no even numbers and no odd numbers are adjacent?

11. How many five-letter words (uppercase letters only) do not both begin and end with a vowel?

12. Consider the 3-lists taken from [3]. How many are there in which each element of [3] appears at least once? Answer the same question, but for 4-lists and 5-lists taken from [3].

13. A ***Shidoku board*** is a 4×4 grid of numbers where each of the numbers 1–4 appears exactly once in each row, column, and in each of the four 2×2 sub-grids. Here are two different Shidoku boards:

4	3	1	2
2	1	3	4
3	2	4	1
1	4	2	3

1	2	4	3
3	4	1	2
2	1	3	4
4	3	2	1

How many different Shidoku boards are there?

14. In how many different ways can you arrange the numbers 1–9 in a 3×9 grid such that each number appears exactly once in each row; and each number appears exactly once in each of the left, middle, and right 3×3 sub-grids? Here is the grid along with one possible arrangement:

2	7	1	3	5	9	6	4	8
4	3	8	6	7	2	1	5	9
5	6	9	1	4	8	2	3	7

15. You write down all of the integers from 1 to 1,000,000. How many times did you write the digit 4?

16. How many 4-permutations of [10] have maximum element equal to 6? How many have maximum element at most 6?

17. Find the number of 4-lists of the form (x_1, x_2, x_3, x_4), where each x_i is a nonnegative integer and $x_1 + x_2 + x_3 + 4x_4 = 15$.

18. This is an excellent exercise for practicing counting. Find the number of five-card hands, dealt from a standard 52-card deck, that contain:
    (a) a royal flush (A-K-Q-J-10 all in one suit);
    (b) a straight flush (five cards of consecutive denominations all in one suit, but not a royal flush);
    (c) four-of-a-kind (four cards of one denomination and one card of a different denomination);
    (d) a full house (three cards of one denomination and two of a different denomination);
    (e) a flush (five cards all in one suit, but not a straight flush or royal flush);
    (f) a straight (five cards of consecutive denominations, but not all in one suit);
    (g) three-of-a-kind (three cards of one denomination, a fourth card of a different denomination, and a fifth card of a third different denomination);
    (h) two pairs (two cards of one denomination, two cards of a different denomination, and a fifth card of a third different denomination);
    (i) one pair (two cards of one denomination, a third card of a different denomination, a fourth card of a third different denomination, and a fifth card of a fourth different denomination); and
    (j) none of the above.

    Compute the likelihood, or probability, of receiving each type of hand on the initial deal. (As a check, they are listed in increasing order of likelihood.)
19. How many zeros does $n!$ end with? Prove your answer.

1.3 Functions and the bijection principle

It is now time to delve into some of the mathematical underpinnings of combinatorics. The concept of relation plays a central role. Functions, equivalence relations, graphs, and partial orders are the main players that we will encounter in this book, and each is a different kind of relation. We begin with functions because they are the most familiar and they are closely related to the counting methods of Sections 1.1 and 1.2.

Counting via a bijection

In Section 1.1, we counted the possible subsets of the set [3] via the correspondence shown at the left of Figure 1.2. We counted the 5-digit binary numbers with exactly two 1s via the correspondence shown at the right.

In both cases the objects to count appear to the left of the arrows, and objects that we know how to count (because they are instances of standard counting problems) appear to the right. The correspondence on the left shows that there are exactly as many subsets of [3] as there are 3-digit binary numbers, namely 2^3. The correspondence on the right shows that there are exactly as many 5-digit binary numbers with exactly two 1s as there are 2-subsets of [5], namely $\binom{5}{2}$.

Each of these correspondences is a kind of function called a bijection. They are useful in combinatorics because, as the two examples suggest, we can count the elements of a set A that is difficult to count by

$$\begin{aligned}
\emptyset &\longrightarrow 000 \\
\{1\} &\longrightarrow 100 \\
\{2\} &\longrightarrow 010 \\
\{3\} &\longrightarrow 001 \\
\{1,2\} &\longrightarrow 110 \\
\{1,3\} &\longrightarrow 101 \\
\{2,3\} &\longrightarrow 011 \\
\{1,2,3\} &\longrightarrow 111
\end{aligned}
\qquad
\begin{aligned}
11000 &\longrightarrow \{1,2\} \\
10100 &\longrightarrow \{1,3\} \\
10010 &\longrightarrow \{1,4\} \\
10001 &\longrightarrow \{1,5\} \\
01100 &\longrightarrow \{2,3\} \\
01010 &\longrightarrow \{2,4\} \\
01001 &\longrightarrow \{2,5\} \\
00110 &\longrightarrow \{3,4\} \\
00101 &\longrightarrow \{3,5\} \\
00011 &\longrightarrow \{4,5\}
\end{aligned}$$

Figure 1.2. Two correspondences for counting.

- finding another set B which is easier to count, and
- constructing a bijection from A to B.

This allows us to conclude that A and B have the same size. Though the two correspondences shown involve relatively intuitive or straightforward bijections, tougher problems call for more cleverness. As such, we need to understand the theory of functions pertinent to counting.

Relations and functions

In order to define a relation we first define the Cartesian product. For sets A and B, the ***Cartesian product of*** A ***and*** B is that set $A \times B$ given by

$$A \times B = \big\{(a,b) : a \in A \text{ and } b \in B\big\}.$$

For example, if $A = \{1,2\}$ and $B = \{\alpha, \beta, \gamma\}$, then $A \times B$ contains six ordered pairs:

$$A \times B = \big\{(1,\alpha),(1,\beta),(1,\gamma),(2,\alpha),(2,\beta),(2,\gamma)\big\}.$$

Question 27 *What is $B \times A$? In general, if X and Y are finite sets, then are the following statements true or false? (1) $X \times Y = Y \times X$; (2) $|X \times Y| = |Y \times X|$.*

Next we define relation.

Definition 1.3.1 (relation) *Let A and B be sets. A* ***relation from*** A ***to*** B *is a subset of $A \times B$. A* ***relation on*** A *is a subset of $A \times A$.*

A mere relation needn't have very much structure. By imposing the following structure we obtain what we wish to study in this section—a function.

Definition 1.3.2 (function) *Let A and B be sets. A* ***function from*** A ***to*** B *is a relation f from A to B that satisfies the following property: for each $a \in A$, there is exactly one $b \in B$ such that $(a,b) \in f$. We write $f : A \longrightarrow B$ to indicate that f is a function from A to B, and we write $f(a) = b$ to mean $(a,b) \in f$.*

You might consider a function to be an input-output rule like $f(x) = x^2$, not a set of ordered pairs. But this input-output rule means that each input x is associated with the

output x^2. When you graph this function, you plot ordered pairs of the form (x, x^2) such as $(0, 0)$, $(0.5, 0.25)$, $(1, 1)$, and $(1.5, 2.25)$. So from this point of view a function really is a set of ordered pairs as described in the definition.

For example, if $A = \{1, 2, 3, 4, 5\}$ and $\mathbb{Z}$ is the set of integers, then the function $f : A \longrightarrow \mathbb{Z}$ defined by the rule $f(x) = x^2$ is the set of ordered pairs

$$f = \big\{(1, 1), (2, 4), (3, 9), (4, 16), (5, 25)\big\}. \tag{1.4}$$

For example, $(3, 9) \in f$ means $f(3) = 9$.

Question 28 *Define $g : 2^{[2]} \longrightarrow \mathbb{Z}$ by the rule $g(S) = |S|$, where S is any subset of* [2]. *Write g as a set of ordered pairs.*

Domain, codomain, and range

If we have a function $f : A \longrightarrow B$, then the set A is the ***domain of*** f and the set B is the ***codomain of*** f. We write $\mathrm{dom}(f) = A$ and $\mathrm{co}(f) = B$ to indicate this. The ***range of*** f is that subset of B defined by

$$\mathrm{rng}(f) := \{b \in B : f(a) = b \text{ for at least one } a \in A\}.$$

The range could equal the codomain but not necessarily. For example, if we define $f : \mathbb{R} \longrightarrow \mathbb{R}$ by $f(x) = x^2$, then this has $\mathrm{dom}(f) = \mathrm{co}(f) = \mathbb{R}$ while $\mathrm{rng}(f)$ is the set of nonnegative real numbers. The definition of function allows us to be careless with the codomain.

Examples

(a) If f is the function at the left of Figure 1.2, then the domain is the power set of [3] and the codomain is the set of 3-digit binary numbers. For any set S in the domain, the rule is $f(S) = d_1d_2d_3$ where d_i is 1 or 0 according to whether $i \in S$ or $i \notin S$, respectively.

(b) If g is the function at the right of Figure 1.2, then the domain is the set of 5-digit binary numbers containing exactly two 1s and the range is the set of 2-subsets of [5]. For any binary number b in the domain, the rule is $g(b) = \{i, j\}$ where i and j are the positions in which b has a 1.

(c) Let A be the set of 2-subsets of [5] and let B be the set of 3-subsets of [5]. Then the function $h : A \longrightarrow B$ defined by the rule $h(S) = S^c$ is the function that associates each set in A with its complement, which is in B. For example, $h\big(\{3, 4\}\big) = \{1, 2, 5\}$.

See Figure 1.3 for a picture of the function in part (c).

Question 29 *Let $X = 2^{[10]}$ and let Y be the set of nonnegative integers. Define $f : X \longrightarrow Y$ by $f(S) = |S|$. Find $f\big(\{3, 5, 6, 7, 8\}\big)$ and $f(\emptyset)$. Is* $\mathrm{rng}(f) = Y$*?*

One-to-one, onto, and bijective functions

We next identify the properties of functions that are useful for counting. For a function $f : A \longrightarrow B$, it is one-to-one provided that it "uses" every possible output in B at most once. It is onto provided that every possible output in B is "used" at least once. A bijection is a one-to-one and onto function.

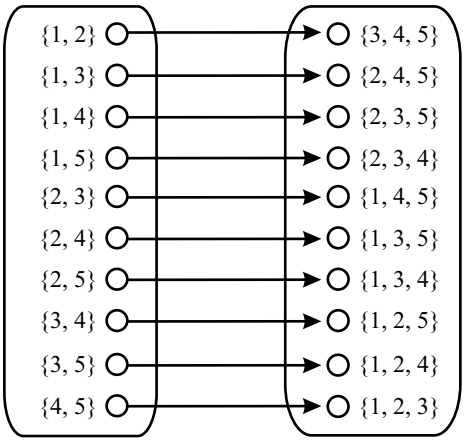


Figure 1.3. Function from the 2-subsets of [5] to the 3-subsets of [5].

Definition 1.3.3 (one-to-one, onto, bijection) *For a function $f : A \longrightarrow B$, we say f is a **bijection** or **one-to-one correspondence** provided f has both of the following properties.*

- ***One-to-one:*** *For each $a_1, a_2 \in A$, if $f(a_1) = f(a_2)$, then $a_1 = a_2$.*
- ***Onto:*** *For each $b \in B$, there exists some $a \in A$ such that $f(a) = b$.*

A one-to-one function is also called an ***injective function*** or an ***injection***. An onto function is also called a ***surjective function*** or a ***surjection***. Another way to define one-to-one function is with the contrapositive of the statement given in the above definition.

- ***One-to-one, alternate version:*** *For each $a_1, a_2 \in A$, if $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.*

This may seem more natural—it says that different inputs produce different outputs—but the original one is sometimes easier to use in proofs.

We have already seen three examples of bijections in Figures 1.2 and 1.3.

Question 30 *Is the function f of Question 29 a bijection?*

The bijection principle

Figure 1.4 shows a basic but important visual representation of four kinds of functions. It appears that when a function is a bijection the domain and codomain are equal in size. In fact, this is the mathematical definition of what it means for two sets to have the same size.

The bijection principle: *Two finite sets A and B have the same size if and only if there exists a bijection from one set to the other.*

Bijective proofs

We now have the theory that allows us to count using the method explained at the beginning of this section. To illustrate, we'll use the bijection principle to prove the following two statements. A proof using the bijection principle is called a ***bijective proof***.

- The number of k-subsets of $[n]$ equals the number of $(n-k)$-subsets of $[n]$.
- The number of subsets of $[n]$ of odd size equals the number of subsets of $[n]$ of even size.

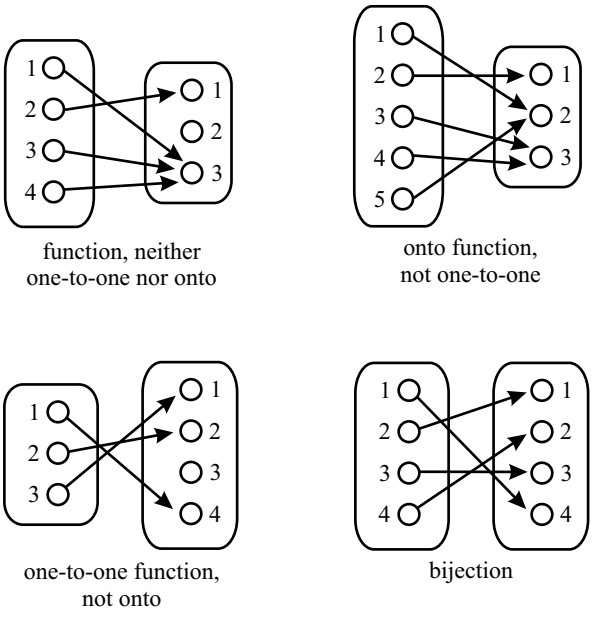


Figure 1.4. Four kinds of functions.

The first statement says $\binom{n}{k} = \binom{n}{n-k}$. This is intuitively clear: to specify a k-subset of $[n]$ we can choose the k elements to include or equivalently choose the $n-k$ elements to exclude. We'll prove it using the bijection principle for the purposes of illustration. The second statement is perhaps less obvious.

Bijective proof #1

Figure 1.3 illustrates how the set complement function gives a bijection between the 2-subsets of [5] and the 3-subsets of [5]. We now generalize this.

Let A be the set of k-subsets of $[n]$ and let B be the set of $(n-k)$-subsets of $[n]$. Define $h : A \longrightarrow B$ by the rule $h(S) = S^c$. Note that S has size k so S^c has size $n-k$, which means that this function is well defined. We prove that h is a bijection.

One-to-one: Assume S_1 and S_2 are two k-subsets of $[n]$ satisfying $S_1 \neq S_2$. It follows that there is some i satisfying $i \in S_1$ and $i \notin S_2$. Since $i \in S_1$, we know that $i \notin h(S_1)$ because h is the set complement function. Also, since $i \notin S_2$, we know that $i \in h(S_2)$. But this means $h(S_1) \neq h(S_2)$ since the element i is in $h(S_2)$ but not $h(S_1)$. Therefore h is one-to-one.

Onto: Let T be an $(n-k)$-subset of $[n]$. Our job is to find some k-subset S of $[n]$ such that $h(S) = T$. Choosing $S = T^c$ works: T has size $n-k$ so T^c has size k, meaning that $T^c \in A$. Moreover,

$$h(S) = h(T^c) = (T^c)^c = T.$$

Therefore, h is onto. This completes the proof that h is a bijection. Therefore $\binom{n}{k} = \binom{n}{n-k}$, because we know $\binom{n}{k}$ is the number of k-subsets of $[n]$ and $\binom{n}{n-k}$ is the number of $(n-k)$-subsets of $[n]$.

Bijective proof #2

Notice that there are as many even-sized subsets of [3] as there are odd-sized:

even size	$\emptyset, \{1,2\}, \{1,3\}, \{2,3\}$
odd size	$\{1\}, \{2\}, \{3\}, \{1,2,3\}$

The same is true for the even- and odd-sized subsets of [4]:

even size	$\emptyset, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \{1,2,3,4\}$
odd size	$\{1\}, \{2\}, \{3\}, \{4\}, \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}$

This looks like it should be true in general. The question is whether there is a natural bijection between the sets. Here is one: if a set contains element 1, remove it; and if a set doesn't contain element 1, add it.

Question 31 *Draw a picture of the correspondence for the subsets of* [3]*, as described in the last sentence.*

In general, let $\mathcal{E}$ and $\mathcal{O}$ be the set of even-sized and odd-sized subsets of $[n]$, respectively. Define $f : \mathcal{E} \longrightarrow \mathcal{O}$ by the rule

$$f(A) = \begin{cases} A - \{1\} & \text{if } 1 \in A \\ A \cup \{1\} & \text{if } 1 \notin A. \end{cases}$$

First we observe that f is indeed well-defined because if A is any even-sized subset, then the size of $f(A)$ is either $|A| - 1$ or $|A| + 1$ and both of these numbers are odd.

One-to-one: Let A_1 and A_2 be even-sized subsets of $[n]$, and assume that $f(A_1) = f(A_2)$. Our goal is to show that $A_1 = A_2$. We use the standard technique of showing that $A_1 \subseteq A_2$ and $A_2 \subseteq A_1$.

To show $A_1 \subseteq A_2$, let $i \in A_1$. We need to show $i \in A_2$, and we do so by considering two cases: $i = 1$ and $i > 1$. First, if $i = 1$ then

$$\begin{array}{rcll} 1 \in A_1 & \Longrightarrow & 1 \notin f(A_1) & \text{since } f \text{ removes element 1} \\ & \Longrightarrow & 1 \notin f(A_2) & \text{since } f(A_1) = f(A_2) \text{ by assumption} \\ & \Longrightarrow & 1 \in A_2 & \text{since } f \text{ removed element 1.} \end{array}$$

On the other hand, if $i > 1$ then

$$\begin{array}{rcll} i \in A_1 & \Longrightarrow & i \in f(A_1) & \text{since } f \text{ does not remove element } i \\ & \Longrightarrow & i \in f(A_2) & \text{since } f(A_1) = f(A_2) \text{ by assumption} \\ & \Longrightarrow & i \in A_2 & \text{since } f \text{ did not remove element } i. \end{array}$$

In either case $i \in A_2$ and therefore $A_1 \subseteq A_2$.

To show $A_2 \subseteq A_1$, the details are similar; see the Question below. Therefore $A_1 = A_2$ and so f is one-to-one.

Question 32 *Provide the details that prove* $A_2 \subseteq A_1$.

Onto: Let B be an odd-sized subset of $[n]$. We must construct an even-sized subset A of $[n]$ such that $f(A) = B$. The idea is simple: if $1 \in B$ then define $A := B - \{1\}$, and if $1 \notin B$ then define $A := B \cup \{1\}$. Notice that in either case A is an even-sized subset. Now, if $1 \in B$ then

$$f(A) = f\big(B - \{1\}\big) = \big(B - \{1\}\big) \cup \{1\} = B,$$

and if $1 \notin B$ then

$$f(A) = f\big(B \cup \{1\}\big) = \big(B \cup \{1\}\big) - \{1\} = B.$$

In either case, $f(A) = B$. Therefore f is onto. This completes the proof that f is a bijection. Therefore the number of even-sized subsets of an n-set equals the number of odd-sized subsets of an n-set.

Function composition

In the remainder of this section we mention two more ideas involving functions that will be useful in our later work. The first is function composition. For example, recall that the function $h(x) = (x^3 - 1)^5$ is the composition of $f(x) = x^3 - 1$ and $g(x) = x^5$ because $(g \circ f)(x) = g\big(f(x)\big) = g\big(x^3 - 1\big) = (x^3 - 1)^5$.

Definition 1.3.4 (composition) *For functions $f : A \longrightarrow B$ and $g : B \longrightarrow C$, the **composition of f with g** is that function $g \circ f : A \longrightarrow C$ defined by $(g \circ f)(a) = g\big(f(a)\big)$.*

For example, let $f : [4] \longrightarrow [3]$ and $g : [3] \longrightarrow [7]$ be defined by

$$f = \big\{(1,2),\ (2,1),\ (3,1),\ (4,2)\big\}$$
$$g = \big\{(1,2),\ (2,6),\ (3,6)\big\}.$$

This means that $g \circ f = \big\{(1,6),\ (2,2),\ (3,2),\ (4,6)\big\}$ because $g\big(f(1)\big) = g(2) = 6$ and $g\big(f(2)\big) = g(1) = 2$ and so forth.

Question 33 *Is the composition $f \circ g$ defined? Explain.*

Inherited properties

The one-to-one and onto properties of functions are preserved under composition.

Theorem 1.3.5 *Let $f : A \longrightarrow B$ and $g : B \longrightarrow C$. If f and g are both one-to-one, then so is $g \circ f$. If f and g are both onto, then so is $g \circ f$. If f and g are both bijective, then so is $g \circ f$.*

Proof: Assume $f : A \longrightarrow B$ and $g : B \longrightarrow C$.

Assume that f and g are both one-to-one. To prove that $g \circ f$ is one-to-one, let $a_1, a_2 \in A$ and assume that $(g \circ f)(a_1) = (g \circ f)(a_2)$, i.e., $g\big(f(a_1)\big) = g\big(f(a_2)\big)$. Since g is one-to-one, this implies $f(a_1) = f(a_2)$. Then since f is one-to-one, this implies $a_1 = a_2$. Therefore $g \circ f$ is one-to-one.

The proof that $g \circ f$ is onto is left to you in the Question after the proof. It then immediately follows that $g \circ f$ is bijective when f and g are bijective. ■

Question 34 *Prove that if f and g are onto, then $g \circ f$ is onto.*

Function composition is associative

That function composition is an associative operation is an important property. In fact, the counting method that we study in Chapter 5 relies on this principle.

Theorem 1.3.6 *Let $f : A \longrightarrow B$, $g : B \longrightarrow C$, and $h : C \longrightarrow D$. Then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Proof: Let $f : A \longrightarrow B$, $g : B \longrightarrow C$, and $h : C \longrightarrow D$. First examine the function $h \circ (g \circ f)$. Definition 1.3.4 shows that $g \circ f : A \longrightarrow C$, and then also that $h \circ (g \circ f) : A \longrightarrow D$. Also by that definition, $h \circ g : B \longrightarrow D$ and so $(h \circ g) \circ f : A \longrightarrow D$. This means that the two functions in question have equal domains and codomains.

Now let $a \in A$. On one hand, apply Definition 1.3.4 twice to show

$$\big(h \circ (g \circ f)\big)(a) = h\big((g \circ f)\big)(a) = h\Big(g\big(f(a)\big)\Big).$$

On the other hand,

$$\big((h \circ g) \circ f)\big)(a) = (h \circ g)\big(f(a)\big) = h\Big(g\big(f(a)\big)\Big).$$

Since $\big(h \circ (g \circ f)\big)(a) = \big((h \circ g) \circ f)\big)(a)$ for each $a \in A$, and since these two functions have the same domain and codomain, they must be equal. ■

Inverse relation, inverse function

The last concept we cover in this section is the inverse of a relation. To obtain the inverse of a relation we simply switch the order of the elements in each 2-list. If R is a relation from A to B, then the ***inverse of*** R is that relation R^{-1} from B to A given by

$$R^{-1} = \big\{(b, a) : (a, b) \in R\big\}.$$

Put another way, $(a, b) \in R$ if and only if $(b, a) \in R^{-1}$. Since every function is a relation, then the ***inverse of a function*** does not need a separate definition. Yet we must make one crucial point: the inverse of a function need not be a function.

Question 35 *Is the inverse relation of the function f shown in (1.4) on page 26 a function? If so, give the domain and codomain of f^{-1} as well as its input-output rule.*

The best we can say is that if $f : A \longrightarrow B$ is a function from A to B, then f^{-1} is a *relation* from B to A. We now give a necessary and sufficient condition for f^{-1} to be a function.

Theorem 1.3.7 *If f is a function, then the inverse relation f^{-1} is a function if and only if f is one-to-one. In that case,* $\mathrm{dom}(f^{-1}) = \mathrm{rng}(f)$ *and* $\mathrm{rng}(f^{-1}) = \mathrm{dom}(f)$.

See Exercise 7 for the proof.

This now gives us two slightly different methods for demonstrating that a function $f : A \longrightarrow B$ is bijective.

- Prove that f is one-to-one and onto.
- Prove that the inverse relation f^{-1} is a function with domain equal to B.

Mathematical convenience dictates which one to use. You can tell when the second method is being used because it is often accompanied by the term "reversible." Exercise 11 asks you to prove it without using Theorem 1.3.7.

Summary

If A is a set of objects that is difficult to count, and you suspect that there are as many objects in A as there are in a different, easy-to-count set B, then the bijection principle might be of use. A bijection is a one-to-one and onto function, and the bijection principle says that two finite sets have the same size exactly when there is a bijection between them. Besides studying these ideas, we also examined function composition and the inverse relation of a function.

Exercises

1. The less-than relation on [4] is the set

$$R = \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}.$$

In other words, $(a,b) \in R$ if and only if $a < b$. It contains six ordered pairs. How many ordered pairs are in the less-than relation on $[n]$? How many are in the less-than-or-equal-to relation on $[n]$?

2. Define a relation R on $[24] \times [24]$ where $(a,b) \in R$ exactly when a is a factor of b. Write R as a set of ordered pairs.

3. How many different functions from [7] to [10] are there?

4. Given a set S, a function $f : S \times S \longrightarrow S$ is called a ***binary operation on*** S. If S is a finite set, then how many different binary operations on S are possible?

5. Give a bijective proof: The number of subsets of $[n]$ equals the number of n-digit binary numbers. (This proves one fact suggested by Figure 1.2 on page 25.)

6. Give a bijective proof: The number of n-digit binary numbers with exactly k 1s equals the number of k-subsets of $[n]$. (This proves the other fact suggested by Figure 1.2 on page 25.)

7. Prove Theorem 1.3.7.

8. Prove: If $f : A \longrightarrow B$ is a bijection, then f^{-1} is a bijection $B \longrightarrow A$.

9. In Bijective Proof #1, prove that the set complement function is one-to-one using the property as stated in Definition 1.3.3 instead. Compare with the proof given in the text.

10. Suppose A and B are finite sets with $|A| = |B|$ and that $f : A \longrightarrow B$ is a function. Prove: f is one-to-one if and only if f is onto.

11. Suppose that A and B are finite sets and that $f : A \longrightarrow B$ is a function. Prove without using Theorem 1.3.7: If the inverse relation f^{-1} is a function with domain B, then f is a bijection. Also, do you need A and B to be finite sets?

12. Let $\mathcal{E}$ and $\mathcal{O}$ be the sets of even- and odd-sized subsets of $[n]$, respectively. If n is odd then the set complement function maps sets in $\mathcal{E}$ to sets in $\mathcal{O}$. Is this a bijection? Prove or disprove.

13. This exercise outlines a bijective proof of the formula $\left(\!\binom{n}{k}\!\right) = \binom{k+n-1}{k}$ from Section 1.1. Let A be the set of k-multisets taken from $[n]$ and let B be the set of k-subsets of $[k+n-1]$. Assume that the k-multiset $\{a_1, a_2, \ldots, a_k\}$ is written in nondecreasing order: $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k$. Define $f : A \longrightarrow B$ by

$$f\big(\{a_1, a_2, \ldots, a_k\}\big) = \{a_1, a_2 + 1, a_3 + 2, \ldots, a_k + k - 1\}.$$

This function, and proof, is originally due to Euler.

   (a) Prove that the outputs of f are indeed k-subsets of $[k+n-1]$. This requires proof since it is not immediately clear from the definition of f.
   (b) Prove that f is a bijection.

1.4 Relations and the equivalence principle

The equivalence principle applies to combinatorial problems that exhibit certain symmetries. Two canonical problems involve counting the possible ways to seat a group of people around a circular table and counting the possible ways to pair off a group of people, say for the first round of a round-robin tournament. Both problems involve subtleties that we have not yet encountered.

Our purposes in this section are first to lay the groundwork for the equivalence principle and second to illustrate how to apply it. In Chapter 5, we study Pólya's enumeration theorem which is a very powerful generalization of the equivalence principle.

Equivalence relation

The equivalence principle rests on the idea of equivalence relation which is one of the most ubiquitous in all of mathematics. Recall that a relation on a set A is a subset of $A \times A$.

Definition 1.4.1 (equivalence relation) *A relation $\mathcal{E}$ on a set A is an **equivalence relation on** A provided that $\mathcal{E}$ has the following three properties.*

- ***Reflexive:*** *For each $a \in A$, $(a, a) \in \mathcal{E}$.*
- ***Symmetric:*** *For each $a, b \in A$, if $(a, b) \in \mathcal{E}$ then $(b, a) \in \mathcal{E}$.*
- ***Transitive:*** *For each $a, b, c \in A$, if $(a, b) \in \mathcal{E}$ and $(b, c) \in \mathcal{E}$, then $(a, c) \in \mathcal{E}$.*

The idea of equivalence relation abstracts three properties that ordinary $=$ (equals) enjoys on any set of numbers. It is reflexive (because $a = a$ for any number a), symmetric (order doesn't matter because $a = b$ and $b = a$ mean the same thing), and transitive (if $a = b$ and $b = c$ then $a = c$).

It's customary to write $a\mathcal{E}b$ to mean $(a, b) \in \mathcal{E}$. With this notation the symmetric property, for example, becomes: for each $a, b \in A$, if $a\mathcal{E}b$ then $b\mathcal{E}a$. We use the two notations interchangeably.

Examples

(a) One important equivalence relation is congruence modulo n on the set $\mathbb{Z}$ of integers. That is, fix a positive integer n and define, for any integers a and b, the relation

$$a \equiv b \pmod{n} \quad \text{if and only if} \quad n \,\big|\, (a - b). \tag{1.5}$$

So for example $5 \equiv 54 \pmod 7$ because $5 - 54 = -49$ and $7 \big| (-49)$. On the other hand, $5 \not\equiv -3 \pmod 7$ because $5 - (-3) = 8$ and 7 is not a factor of 8. (See Exercise 4 for the proof that this is an equivalence relation.)

Question 36 *Is $45 \equiv 106 \pmod 2$? Is $47 \equiv 97 \pmod 2$? Determine exactly when $a \equiv b \pmod 2$ is true.*

(b) Define a relation $\sim$ on the power set of $[3]$ by $S \sim T$ if and only if $|S| = |T|$. In other words, two sets are related when they have the same size. Then for example $\{3\} \sim \{1\}$ because both sets have size 1, and $\{1, 2\} \sim \{2, 3\}$ because both sets have size 2. However, $\emptyset \not\sim \{1\}$ because they do not have the same size. This relation $\sim$ is reflexive because $|S| = |S|$ is true of any set S. It is symmetric because if $|S| = |T|$ then $|T| = |S|$. It is transitive because if $|S| = |T|$ and $|T| = |U|$, then $|S| = |U|$. It is an equivalence relation.

(c) For any set A, the ***identity relation on*** A is the relation

$$\mathcal{I}_A := \{(a, a) : a \in A\}.$$

It is an equivalence relation.

Equivalence class

Given an equivalence relation on a set A and any $a \in A$, the equivalence class containing a is the set of all elements of A that are related to a.

Definition 1.4.2 (equivalence class) *Let $\mathcal{E}$ be an equivalence relation on a set A. For any $a \in A$, the* ***equivalence class containing*** *a is that set*

$$\mathcal{E}(a) := \{x \in A : (a, x) \in \mathcal{E}\}.$$

Examples

(a) If $\mathcal{E}$ is the congruence modulo 3 relation on the integers, then the equivalence class containing the integer 0 is the set of all integers whose remainder is 0 when divided by 3, i.e., the multiples of 3:

$$\mathcal{E}(0) = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}.$$

The equivalence class containing 1 is the set of all integers whose remainder is 1 when divided by 3:

$$\mathcal{E}(1) = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}.$$

Question 37 *Find $\mathcal{E}(2)$ and $\mathcal{E}(40)$.*

(b) If $\sim$ is the has-the-same-size relation on the power set of [3], then the equivalence class containing the set $\{1\}$ is $\big\{\{1\}, \{2\}, \{3\}\big\}$.

Question 38 *For this same relation, find the equivalence class containing $\emptyset$ and the equivalence class containing $\{2, 3\}$.*

Related elements are in the same equivalence class

This next result says that if two elements are related by an equivalence relation, then their equivalence classes are equal.

Theorem 1.4.3 *If $\mathcal{E}$ is an equivalence relation on a set A and $(a, b) \in \mathcal{E}$, then $\mathcal{E}(a) = \mathcal{E}(b)$.*

Proof: Let $\mathcal{E}$ be an equivalence relation on a set A, and let $(a, b) \in \mathcal{E}$. To prove $\mathcal{E}(a) = \mathcal{E}(b)$, we show that each is a subset of the other.

First, let $x \in \mathcal{E}(a)$. This means $(a, x) \in \mathcal{E}$. Since $(b, a) \in \mathcal{E}$ because $\mathcal{E}$ is symmetric, this implies $(b, x) \in \mathcal{E}$ because $\mathcal{E}$ is transitive. But then $x \in \mathcal{E}(b)$. Therefore $\mathcal{E}(a) \subseteq \mathcal{E}(b)$.

The proof that $\mathcal{E}(b) \subseteq \mathcal{E}(a)$ is similar and left to the Question below. This completes the proof that $\mathcal{E}(a) = \mathcal{E}(b)$. ■

Question 39 *Complete the proof by proving that $\mathcal{E}(b) \subseteq \mathcal{E}(a)$.*

Partition

Definition 1.4.4 (partition) *For any set S, a **partition of** S is a set of nonempty, disjoint subsets of S whose union is S.*

For example, here are three possible partitions of [6]:

$$P_1 = \big\{\{1,6\},\ \{2\},\ \{3,4,5\}\big\}$$
$$P_2 = \big\{\{1,2,3,4,5,6\}\big\}$$
$$P_3 = \big\{\{1\},\ \{2\},\ \{3\},\ \{4,5\},\ \{6\}\big\}.$$

The elements of a partition are called the ***blocks*** of the partition. Thus P_1 has three blocks, P_2 has one block, and P_3 has five blocks. (We will learn how to count partitions in Sections 2.3 and 3.1.)

Equivalence relations and partitions

The concepts of equivalence relation and partition are intimately related: there is a natural bijection between the equivalence relations on a given set and the partitions of that same set. We now prove this. The first step is to understand how an equivalence relation induces a partition.

Theorem 1.4.5 *If $\mathcal{E}$ is an equivalence relation on a set A, then the set*

$$P := \big\{\mathcal{E}(a) : a \in A\big\} \tag{1.6}$$

of equivalence classes of $\mathcal{E}$ is a partition of A.

Proof: Let $\mathcal{E}$ be an equivalence relation on a set A. Following Definition 1.4.4, we first verify that each block of P is nonempty. Let $\mathcal{E}(a)$ be a block of P. Since $\mathcal{E}$ is reflexive, we know $(a,a) \in \mathcal{E}$. This means $a \in \mathcal{E}(a)$, so $\mathcal{E}(a)$ is nonempty. Also, since $a \in \mathcal{E}(a)$ for all $a \in A$, we see that the union of the blocks of P equals A.

The last thing to prove is that the blocks of P are disjoint. If P has only one block (namely A itself) then there is nothing to do. So, assume that $\mathcal{E}(a)$ and $\mathcal{E}(b)$ are two different blocks of P. We must show that they are disjoint.

Suppose they are not disjoint. Then there is some $c \in A$ for which $c \in \mathcal{E}(a)$ and $c \in \mathcal{E}(b)$. The first implies that $(a,c) \in \mathcal{E}$ and the second that $(c,b) \in \mathcal{E}$. Transitivity then implies $(a,b) \in \mathcal{E}$. But Theorem 1.4.3 then implies that $\mathcal{E}(a) = \mathcal{E}(b)$, which contradicts our original assumption that these are different blocks of P. Therefore they are disjoint. ■

Next, we show how a partition induces an equivalence relation.

Theorem 1.4.6 *If P is a partition of a set A, then the relation $\mathcal{R}$ on A defined by*

$$\mathcal{R} := \big\{(a,b) \in A \times A : a \text{ is in the same block of } P \text{ as is } b\big\} \tag{1.7}$$

is an equivalence relation on A.

Proof: Let $P = \{P_1, \ldots, P_k\}$ be a partition of the set A. We must prove that the relation $\mathcal{R}$ defined in (1.7) is an equivalence relation.

Reflexive: Let $a \in A$. Since P is a partition of A, the element a belongs to exactly one block P_i. Clearly a is in the same block as itself, so $(a,a) \in \mathcal{R}$. Therefore $\mathcal{R}$ is reflexive.

Symmetric: Suppose $(a, b) \in \mathcal{R}$. This means that a is in the same block of P as b. But then b is in the same block of P as a, so $(b, a) \in \mathcal{R}$. Therefore $\mathcal{R}$ is symmetric.

Transitive: Suppose $(a, b) \in \mathcal{R}$ and $(b, c) \in \mathcal{R}$. This means that a is in the same block of P as b, and also that b is in the same block of P as c. But, since P is a partition and hence each element of A belongs to exactly one block, this means that a is in the same block of P as c, so $(a, c) \in \mathcal{R}$. Therefore $\mathcal{R}$ is transitive. ■

We can now demonstrate the bijection between equivalence relations and partitions.

Theorem 1.4.7 *If A is a finite set, then the number of possible equivalence relations on A equals the number of possible partitions of A.*

Proof: Let A be a finite set. We use the bijection principle. Define the sets

$$\mathbf{E} := \{\mathcal{E} : \mathcal{E} \text{ is an equivalence relation on } A\}$$
$$\mathbf{P} := \{P : P \text{ is a partition of } A\}$$

and the function $f : \mathbf{E} \longrightarrow \mathbf{P}$ by

$$f(\mathcal{E}) = \big\{\mathcal{E}(a) : a \in A\big\}.$$

We must prove that this is a bijection. First note that, by Theorem 1.4.5, that $f(\mathcal{E})$ is indeed a partition of A.

One-to-one: Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be two unequal equivalence relations on A. This means, without loss of generality, that there exists a 2-list (a_1, a_2) in $\mathcal{E}_1$ but not $\mathcal{E}_2$.

Since $(a_1, a_2) \in \mathcal{E}_1$, we know that $a_2 \in \mathcal{E}_1(a_1)$ and hence that a_1 and a_2 are in the same block of the partition $f(\mathcal{E}_1)$. But since $(a_1, a_2) \notin \mathcal{E}_2$, we know that $a_2 \notin \mathcal{E}_2(a_1)$ and hence that a_1 and a_2 are not in the same block of the partition $f(\mathcal{E}_2)$. Therefore these two partitions are not the same: $f(\mathcal{E}_1) \neq f(\mathcal{E}_2)$.

Onto: Let P be a partition of A. Construct the set $\mathcal{E}$ shown in (1.7), which Theorem 1.4.6 guarantees is an equivalence relation. Then it quickly follows that $f(\mathcal{E}) = P$, for the equivalence classes of $\mathcal{E}$ are exactly the blocks of P. ■

The equivalence principle

Now we return to counting and show how to exploit equivalence relations for combinatorial purposes.

Example: counting circular arrangements

In how many ways can we seat a group of four people around a circular table? Consider two seatings the same provided that each person has the same left- and right-neighbors.

Let [4] be the set of people. Begin with the $4! = 24$ permutations of [4], and then consider two permutations equivalent if, when placed around a table, each person has the same left- and right-neighbors. Given a permutation such as $(3, 4, 2, 1)$, it is equivalent to itself and three other permutations, namely

$$(3, 4, 2, 1) \equiv (4, 2, 1, 3) \equiv (2, 1, 3, 4) \equiv (1, 3, 4, 2)$$

where we have used $\equiv$ to denote the equivalence relation. These are obtained by rotating the original seating $(3, 4, 2, 1)$ around the table. They are equivalent because any such

rotation preserves each person's left- and right-neighbors. Each permutation's equivalence class has size 4, so our initial count of 4! must be too large by a factor of 4. The answer is thus $4!/4 = 6$.

It is helpful to arrange all 24 permutations according to their equivalence classes:

class 1:	$(1,2,3,4)$	$(2,3,4,1)$	$(3,4,1,2)$	$(4,1,2,3)$
class 2:	$(1,2,4,3)$	$(2,4,3,1)$	$(4,3,1,2)$	$(3,1,2,4)$
class 3:	$(1,3,2,4)$	$(3,2,4,1)$	$(2,4,1,3)$	$(4,1,3,2)$
class 4:	$(1,3,4,2)$	$(3,4,2,1)$	$(4,2,1,3)$	$(2,1,3,4)$
class 5:	$(1,4,2,3)$	$(4,2,3,1)$	$(2,3,1,4)$	$(3,1,4,2)$
class 6:	$(1,4,3,2)$	$(4,3,2,1)$	$(3,2,1,4)$	$(2,1,4,3)$

Notice that we counted equivalence classes (there are six) and not permutations (24).

Statement of the principle

The previous example typifies the use of the equivalence principle: make an over-count, introduce an equivalence relation, and then divide the over-count by the size of each equivalence class. The equivalence principle only applies when all the equivalence classes have the same size. Chapter 5, on Pólya's theory of counting, extends the equivalence principle to when the equivalence classes have unequal sizes.

Theorem 1.4.8 (equivalence principle) *Let $\mathcal{E}$ be an equivalence relation on a finite set A. If for some positive integer C every equivalence class of $\mathcal{E}$ has size C, then $\mathcal{E}$ has $\frac{|A|}{C}$ equivalence classes.*

Proof: Assume that $\mathcal{E}$ is an equivalence relation on a finite set A, and also that there exists a positive integer C such that every equivalence class of $\mathcal{E}$ has size C. Let k be the number of equivalence classes of $\mathcal{E}$. We need to prove that $k = |A|/C$.

By Theorem 1.4.5, the equivalence classes of $\mathcal{E}$ partition A. Say this partition into equivalence classes is $\{P_1, P_2, \ldots, P_k\}$. This means, in particular, that

$$|P_1| + |P_2| + \cdots + |P_k| = |A|.$$

But $|P_i| = C$ for all i, so the equation reads $kC = |A|$, or $k = |A|/C$. ■

Question 40 *In how many ways can we seat a group of n people around a circular table?*

Example: counting pairings

In how many different ways can we arrange 10 people into five pairs?

Let [10] be the set of people. Consider the 10! permutations of [10], of which one example is $(3, 2, 9, 10, 1, 5, 8, 7, 4, 6)$. Then build an arrangement from each permutation by placing adjacent pairs together. The example permutation leads to the pairing

$$\{3,2\} \quad \{9,10\} \quad \{1,5\} \quad \{8,7\} \quad \{4,6\}.$$

Consider two permutations of [10] equivalent if they result in the same pairing. There are many permutations of [10] that are equivalent to the given permutation. If we swap the position of the elements in positions 1 and 2, and/or those in positions 3 and 4, and so on, we obtain the same pairing. Using $\equiv$ to denote the equivalence relation, one way to do this on the example permutation is

$$(3,2,9,10,1,5,8,7,4,6) \equiv (3,2,\underbrace{10,9,}_{\text{swap}}1,5,\underbrace{7,8,}_{\text{swap}}\underbrace{6,4}_{\text{swap}}).$$

We may also rearrange the positions of the pairs as a unit, as in

$$(\underbrace{3,2,}_{\text{pair 1}}\ \underbrace{9,10,}_{\text{pair 2}}\ \underbrace{1,5,}_{\text{pair 3}}\ \underbrace{8,7,}_{\text{pair 4}}\ \underbrace{4,6}_{\text{pair 5}}) \equiv (\underbrace{8,7,}_{\text{pair 4}}\ \underbrace{3,2,}_{\text{pair 1}}\ \underbrace{9,10,}_{\text{pair 2}}\ \underbrace{4,6,}_{\text{pair 5}}\ \underbrace{1,5}_{\text{pair 3}}).$$

Question 41 *Give two permutations equivalent to* $(10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$ *under* $\equiv$.

In general, any permutation of [10] is equivalent to $2^5 \cdot 5! = 3840$ permutations, corresponding to the 2^5 ways to rearrange the pairs and the 5! ways to order the pairs. By the equivalence principle, there are

$$\frac{10!}{2^5 \cdot 5!} = 945$$

different ways to pair 10 people into five pairs. In fact, we have counted the number of partitions of [10] into five blocks where each block has size 2.

Question 42 *In how many different ways can we arrange* $2n$ *people into* n *pairs?*

Example: formula for $\binom{n}{k}$

Here is how to use the equivalence principle to justify the formula $\binom{n}{k} = \frac{(n)_k}{k!}$ that we mentioned in Section 1.1. First we examine the special case $n = 5$ and $k = 3$. How many 3-subsets does the set [5] have?

First list all of the 3-permutations of [5], of which there are $(5)_3 = 60$. They are shown in Figure 1.5. Recall that order matters in a permutation but not in a set. Let's define the following equivalence relation on the set of 3-permutations: consider two 3-permutations equivalent if they contain exactly the same elements. This an equivalence relation. Also, each equivalence class has size 3! because there are 3! ways to reorder the three elements. (The boxes in Figure 1.5 delineate the equivalence classes.) By the equivalence principle there are $\frac{(5)_3}{3!}$ equivalence classes. Each equivalence class corresponds to a different 3-subset of [5], so the number of 3-subsets of [5] is $\frac{(5)_3}{3!}$.

Question 43 *Now generalize to prove the formula* $\binom{n}{k} = \frac{(n)_k}{k!}$.

Are they equivalence relations?

We didn't formally prove that the notions of equivalence used in the last three examples were indeed equivalence relations. For many examples a justification along informal lines would suffice. In the circular arrangement question, one could do this for "equivalent under rotation" as follows. Is any seating of four people equivalent to itself? Yes, just don't rotate it. Also if seating A is equivalent to seating B via some rotation, then B is equivalent to seating A by reversing the original rotation. Finally, if A is equivalent to B and B to C, then A is equivalent to C by composing the two rotations.

An application of the equivalence principle that requires a relatively complex equivalence relation should include a proof of such. However, many don't.

Summary

An equivalence relation is a relation on a set that is reflexive, symmetric, and transitive. There is a natural correspondence between an equivalence relation on a set and a partition of that set. That an equivalence relation partitions a set leads to the equivalence principle.

(1, 2, 3)	(1, 2, 4)	(1, 2, 5)	(1, 3, 4)	(1, 3, 5)
(1, 3, 2)	(1, 4, 2)	(1, 5, 2)	(1, 4, 3)	(1, 5, 3)
(2, 1, 3)	(2, 1, 4)	(2, 1, 5)	(3, 1, 4)	(3, 1, 5)
(2, 3, 1)	(2, 4, 1)	(2, 5, 1)	(3, 4, 1)	(3, 5, 1)
(3, 1, 2)	(4, 1, 2)	(5, 1, 2)	(4, 1, 3)	(5, 1, 3)
(3, 2, 1)	(4, 2, 1)	(5, 2, 1)	(4, 3, 1)	(5, 3, 1)
(1, 4, 5)	(2, 3, 4)	(2, 3, 5)	(2, 4, 5)	(3, 4, 5)
(1, 5, 4)	(2, 4, 3)	(2, 5, 3)	(2, 5, 4)	(3, 5, 4)
(4, 1, 5)	(3, 2, 4)	(3, 2, 5)	(4, 2, 5)	(4, 3, 5)
(4, 5, 1)	(3, 4, 2)	(3, 5, 2)	(4, 5, 2)	(4, 5, 3)
(5, 1, 4)	(4, 2, 3)	(5, 2, 3)	(5, 2, 4)	(5, 3, 4)
(5, 4, 1)	(4, 3, 2)	(5, 3, 2)	(5, 4, 2)	(5, 4, 3)

{1, 2, 3}	{1, 2, 4}	{1, 2, 5}	{1, 3, 4}	{1, 3, 5}
{1, 4, 5}	{2, 3, 4}	{2, 3, 5}	{2, 4, 5}	{3, 4, 5}

Figure 1.5. The 3-permutations of [5] and their corresponding 3-subsets.

When we use the equivalence principle we re-cast the original problem as one of counting the equivalence classes of a convenient equivalence relation. It applies only when each equivalence class has the same size.

Exercises

1. Consider a small version of the problem solved in this section: How many ways are there to arrange four people into two pairs? Write out all the permutations of [4] and then group them into equivalence classes. What is the size of each equivalence class and what then is the answer to the original question?
2. Let $A = [n]$. What are, respectively, the maximum and minimum possible size of an equivalence relation on A? Prove that you are correct.
3. Let $\mathcal{E}$ be an equivalence relation on a set A. What is $\mathcal{E}^{-1}$? Prove your answer.
4. Prove that congruence modulo n, as defined in (1.5) on page 33, is an equivalence relation on $\mathbb{Z}$.
5. Fill in the blank and then prove the statement: An equivalence relation on A is a function $A \longrightarrow A$ if and only if _____ .
6. Let $f : A \longrightarrow B$. Define a relation $\equiv$ on A by $a_1 \equiv a_2$ if and only if $f(a_1) = f(a_2)$. Give a quick proof that this is an equivalence relation. What are the equivalence classes? Explain intuitively.
7. Solve the circular seating arrangements problem for four people, but with two seatings considered equivalent provided that each person has the same *set* of neighbors. (I.e., we don't distinguish between left- and right-neighbors.)
8. How many ways are there to seat five women and five men around a circular table if the seating alternates man-woman-man-woman, etc.?

9. In how many ways can we arrange 10 chairs of nine different colors (there are two chairs of one color, hence they are indistinguishable) around a circular table?
10. In how many ways can we split a group of 10 people into two groups of size 3 and one group of size 4?
11. How many partitions of $[n]$ into two blocks are there? How many partitions of $[n]$ into $n-1$ blocks are there?
12. Prove that the product of any k consecutive positive integers is divisible by $k!$.
13. Use the equivalence principle to prove the formula $(n)_k = \frac{n!}{(n-k)!}$. In other words, count the k-permutations of $[n]$ by first counting the permutations of n (of which there are $n!$) and then defining an appropriate equivalence relation on the set of permutations of $[n]$.
14. Use the equivalence principle to prove the formula $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$. (This requires a different proof than the one we gave in this section, because the numerator here is $n!$ and not $(n)_k$. That is, your equivalence relation should be on the set of permutations of $[n]$, not on the set of k-permutations of $[n]$.)
15. How many different necklaces can we make from n beads of different colors? Consider two necklaces the same if (like in a circular arrangement) one can be obtained from the other via rotation or if (unlike in a circular arrangement) one can be obtained from the other via flipping the necklace over.
16. Let R_1 and R_2 be equivalence relations on a set A.
    (a) Is $R_1 \cup R_2$ an equivalence relation on A? Prove or disprove.
    (b) Is $R_1 \cap R_2$ an equivalence relation on A? Prove or disprove.

1.5 Existence and the pigeonhole principle

In the final section of this chapter we discuss a principle that concerns existence rather than enumeration.

Theorem 1.5.1 (basic pigeonhole principle) *If more than n objects are distributed among n boxes, then some box must contain at least two objects.*

A proof by contradiction works: if every box contained at most one object, then we must have distributed at most n objects in the first place.

The pigeonhole principle is pure common sense. But, when cleverly applied, it can produce surprising or counterintuitive results. We will make use of the pigeonhole principle on a couple of occasions throughout the book. A highlight is Section 6.4 on Ramsey theory. Ramsey theory concerns generalized versions of the pigeonhole principle and contains some of the toughest research problems in combinatorics today.

First examples

Easy applications of the pigeonhole principle

You attend a major-league baseball game and park your car in the stadium lot. Must there be two cars in the lot for which the last three digits of the odometer are exactly the same?

Also, there are 48,000 people at the baseball game. Must two people share the same birth date (month, day, and year)?

The answer to the first question is probably. There are 1000 possibilities for the last three digits of an odometer: 000 through 999. As long as there are at least 1001 cars in the lot, then the basic pigeonhole principle guarantees that two cars are showing the same last three digits.

Question 44 *Must there be a car in the lot that has the same last three digits showing as* ***your*** *car? Explain.*

The answer to the question about birth dates is yes. Be generous and say the people at the game range in age from 0 to 120 years old and that each year has 366 days. This produces $121 \cdot 366 = 44{,}286$ possible month-day-year birthdays. Since any distribution of 48,000 objects (the people at the game) into 44,286 boxes (the possible birthdays) contains a box with at least two objects, there must be at least two people at the game who share the same birth date.

Others have used the pigeonhole principle to argue that large cities must contain a certain number of people with the same number of hairs on their head. (Apparently a good upper bound on the number of hairs on a human head is 300,000.) Results like these are fascinating to think about. They guarantee the *existence* of something without the hassle of actually finding it.

Points in a square

Place five points anywhere inside a unit square. Prove that there are two points that are at most $1/\sqrt{2}$ units apart.

Divide the unit square into four equal-sized smaller squares, like a windowpane. Since there are five points and four smaller squares, one of the smaller squares contains two points by the pigeonhole principle. This smaller square measures $1/2$ unit by $1/2$, and the farthest away that two points can be in such a square is $1/\sqrt{2}$ which is the length of the diagonal. Figure 1.6 gives a picture.

Question 45 *Apply the same analysis to 10 points placed in a unit square. What distance can you guarantee? Prove it.*

Mutual friends

In a certain group of seven people, each person has at least three friends among the members of the group. If two people in the group are not friends, then must they have a mutual

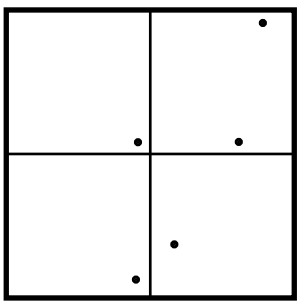


Figure 1.6. Five points in a unit square.

friend in the group? ("Mutual friend" means: If Tommy and Annie both know Billy, then Billy is a mutual friend of Tommy and Annie.)

Take two people that are not friends and call them A and B. Other than A and B, there are five people in the group. Since A's list of friends has at least three names from these five, and so does B's list, the two lists have a total of at least six names. But with only five possible names to choose from, the pigeonhole principle implies that some name must appear twice—a mutual friend of A and B.

If we relax the requirement of "at least three friends" to "at least two friends," does the result necessarily hold? The answer is no.

Question 46 *Give a counterexample. (A helpful visual is to use dots to represent people and to connect two dots to indicate friends.)*

A more general theorem quickly follows from the seven-person example.

Theorem 1.5.2 *Take any group of n people in which each person has at least $\lfloor n/2 \rfloor$ friends among the members of the group. If two people in the group are not friends, then they must have a mutual friend in the group.*

Question 47 *Prove the theorem. First, understand why $\lfloor n/2 \rfloor$ is the right number.*

Exercise 5 asks you to show that $\lfloor n/2 \rfloor$ is best possible. To help you understand any possible distinction that might arise between even and odd values of n, first answer the following question.

Question 48 *Find a counterexample, similar to the one you found for the seven-person instance earlier, to show that the result of the theorem does not necessarily hold with $n = 8$ people and where each person has at least three friends.*

If you are familiar with graph theory (see Chapter 6), then you might recognize the theorem as a disguised form of the following result: in any n-vertex simple graph with minimum degree at least $\lfloor n/2 \rfloor$, any two vertices are either adjacent or have a common neighbor.

Functions and the pigeonhole principle

The pigeonhole principle can be re-stated in the language of functions.

Theorem 1.5.3 (basic pigeonhole principle, function version) *If A and B are finite, nonempty sets with $|A| > |B|$, then no function $A \longrightarrow B$ can be one-to-one.*

The next question is whether we can say something stronger. Consider any function from [10] to [3], say

$$f = \{(1,2),(2,1),(3,2),(4,2),(5,3),(6,1),(7,3),(8,3),(9,2),(10,2)\}.$$

Since [10] is relatively large compared with [3], we should expect that some elements in [3] should have a lot of elements of [10] mapped to them. Indeed if we compute the inverse images of each $b \in [3]$, we see that

$$\begin{aligned} f^{-1}(1) &= \{2,6\} \\ f^{-1}(2) &= \{1,3,4,9,10\} \\ f^{-1}(3) &= \{5,7,8\} \end{aligned}$$

and in particular $|f^{-1}(2)| = 5$ which is relatively large. Remember that the inverse relation f^{-1} is not in general a function, so that $f^{-1}(1)$ is the *set* of elements in [10] that map to 1.

Question 49 *Give an example of a function* $[10] \longrightarrow [3]$ *for which* $f^{-1}(1) = \emptyset$. *For such a function, must either* $f^{-1}(2)$ *or* $f^{-1}(3)$ *be of a certain size? What size?*

Intuitively, we expect each element of [3] to be the image of $\frac{10}{3}$ elements of [10] on the average. We can make this more precise by saying that *some* element of [3] must be the image of at least $\frac{10}{3}$ elements of [10]. For the above function it happens for the element 2, and it also happens for the function you created in Question 49.

To see why, suppose for sake of contradiction that every element of [3] were the image of fewer than $\frac{10}{3}$ elements of [10]; that is, $|f^{-1}(b)| < \frac{10}{3}$ for each $b \in [3]$. This would mean that

$$10 = \sum_{b=1}^{3} |f^{-1}(b)| < \sum_{b=1}^{3} \frac{10}{3} = 3 \cdot \frac{10}{3} = 10,$$

or $10 < 10$, a contradiction. Therefore there is some $b^* \in [3]$ for which $|f^{-1}(b^*)| \geqslant \frac{10}{3}$. Of course, the number $|f^{-1}(b)|$ on the left side of the inequality is an integer, so we can sharpen the right side to $\lceil \frac{10}{3} \rceil = 4$.

The more general result is what we refer to as the pigeonhole principle.

Theorem 1.5.4 (pigeonhole principle) *If A and B are finite, nonempty sets and $f : A \longrightarrow B$ is a function, then there exists some element of B that is the image of at least $\left\lceil \frac{|A|}{|B|} \right\rceil$ elements of A.*

Proof: Assume that A and B are finite, nonempty sets and that f is a function from A to B.

First we prove that there exists some $b^* \in B$ that is the image of at least $\frac{|A|}{|B|}$ elements of A. For sake of contradiction, assume that every $b \in B$ is the image of fewer than $\frac{|A|}{|B|}$ elements of A. Then

$$|A| = \sum_{b \in B} |f^{-1}(b)| < \sum_{b \in B} \frac{|A|}{|B|} = |B| \cdot \frac{|A|}{|B|} = |A|,$$

a contradiction. Therefore some $b^* \in B$ is the image of at least $\frac{|A|}{|B|}$ elements of A. Since the number of elements that map to b^* must be an integer, we can sharpen the bound to $\left\lceil \frac{|A|}{|B|} \right\rceil$. ■

Returning to the odometer example at the beginning of this section, if 5076 cars park in the lot, then the lot contains at least $\lceil \frac{5076}{1000} \rceil = 6$ cars that have the same last three digits showing.

Question 50 *What conclusion results when you apply the pigeonhole principle to a function* $f : [n^2 + 1] \longrightarrow [n]$*? To a function* $g : A \longrightarrow B$ *with* $|A| < |B|$*?*

k-to-one functions

A function is one-to-one provided that each element of its codomain is the image of at most one element of its domain. A function is ***two-to-one*** provided that each element of its codomain is the image of at most two elements of its domain. Here is a general definition.

Definition 1.5.5 (k-to-one) *A function is k-**to-one** provided that each element of its codomain is the image of at most k elements of the domain.*

Pictorially, a k-to-one function has at most k arrows pointing to each element of the codomain.

The function $f : [10] \longrightarrow [3]$ given at the beginning of this subsection has

$$|f^{-1}(1)| = 2, \quad |f^{-1}(2)| = 5, \quad |f^{-1}(3)| = 3,$$

so this function is five-to-one.

Question 51 *Why is any k-to-one function also $(k+1)$-to-one?*

Just as we rephrased the basic pigeonhole principle (Theorem 1.5.1) via the impossibility of a one-to-one function (Theorem 1.5.3), so too can we rephrase Theorem 1.5.4.

Theorem 1.5.6 (pigeonhole principle) *If A and B are finite, nonempty sets, then no function $A \longrightarrow B$ can be k-to-one for any value of k smaller than $\left\lceil \frac{|A|}{|B|} \right\rceil$.*

Exercise 9 asks you to prove the theorem.

Two harder examples

Example: 0s and 1s

For each $n > 0$, prove that there is an integer comprised only of the digits 0 and 1 that is divisible by n.

This requires a very subtle application of the pigeonhole principle! Here is an illustration of the idea when $n = 12$. Take the 13-set

$$A := \{1, 11, 111, \ldots, \underbrace{1111111111111}_{13 \text{ ones}}\}.$$

Divide each number in A by 12 and record the remainder. Since each remainder must be in the 12-set $\{0, 1, 2, \ldots, 11\}$, the pigeonhole principle implies that two of the remainders must be the same. Take any two numbers in A that have the same remainder when divisible by 12 and subtract the smaller from the larger. The result is a number (1) that is divisible by 12, and (2) whose only digits are 0 and 1.

Question 52 *Division algorithm review: Prove that if b and c both have the same remainder when divided by a, then a divides $b - c$.*

If you were to work out the remainders by hand, for concreteness, you'd find that both 11 and 11111 have the same remainder (namely 11) when divided by 12. This means that $11111 - 11 = 11100$ is divisible by 12. (Indeed, $11100/12 = 925$.) There are other pairs that work; for example, 111 and 111111 both have remainder 3.

For a formal proof, consider the $(n+1)$-set

$$A := \{1, 11, 111, 1111, \ldots, \underbrace{111\cdots1}_{n+1 \text{ ones}}\}.$$

The remainder when each element of A is divided by n belongs to the n-set $B := \{0, 1, \ldots, n-1\}$. Let $f : A \longrightarrow B$ be the function that associates each element of A with its remainder when divided by n. Since f cannot be one-to-one, there exist two elements of A that have the same remainder when divided by n. Call them a_1 and a_2 where $a_1 > a_2$. But then $a_1 - a_2$ is divisible by n and its digits are all either 0 or 1.

The Erdős-Szekeres Theorem

You ask a friend to write down a sequence of 10 different real numbers. Before looking at the sequence you spend a moment meditating with your eyes shut and then declare, "I can circle four numbers in your sequence so that when read from left to right, they are either in increasing or decreasing order." Sure enough, it works for your friend's sequence. (Your friend is not impressed. But they should be; read on.)

For example, say your friend wrote down the sequence

$$100,\ 2,\ -17,\ \pi/4,\ -2.3,\ 57,\ 0,\ -2.4,\ -0.2,\ -4.$$

There are no *increasing subsequences* of length 4 because the longest such subsequence has length 3. One is shown in bold below:

$$100,\ 2,\ \mathbf{-17},\ \pi/4,\ \mathbf{-2.3},\ 57,\ 0,\ -2.4,\ \mathbf{-0.2},\ -4.$$

But there is a *decreasing subsequence* of length 4:

$$\mathbf{100},\ 2,\ -17,\ \pi/4,\ -2.3,\ \mathbf{57},\ \mathbf{0},\ -2.4,\ \mathbf{-0.2},\ -4.$$

Actually there is a decreasing subsequence of length 5 if we tack on -4 to the end, but length 4 is all that we will be able to guarantee in general. It is possible that the sequence your friend writes has both kinds of subsequences.

Question 53 *What is an example of a length-10 sequence of distinct real numbers that has both an increasing subsequence of length (at least) 4 and a decreasing subsequence of length (at least) 4?*

If you instead ask your friend for a sequence of 17 distinct real numbers, you can guarantee an increasing or decreasing subsequence of length 5. The general result is known as the Erdős-Szekeres theorem.

Theorem 1.5.7 (Erdős-Szekeres) *For $n \geq 1$, if S is a sequence of $n^2 + 1$ distinct real numbers, then S contains either an increasing subsequence of length $n+1$ or a decreasing subsequence of length $n+1$. Furthermore, this result is best possible in the sense that n^2+1 cannot be replaced by n^2.*

Let's first understand the proof in the context of the length-10 example. To each element x in your friend's sequence, associate a positive integer $\mathrm{LIS}(x)$ that equals the length of the longest increasing subsequence starting with and including x. The LIS function behaves as follows on the example sequence:

element x	100	2	-17	$\pi/4$	-2.3	57	0	-2.4	-0.2	-4
$\mathrm{LIS}(x)$	1	2	3	2	2	1	1	2	1	1

So $\mathrm{LIS}(100) = 1$ because 100 is the largest number in the sequence. But $\mathrm{LIS}(0) = 1$ as well because no number to the right of 0 is larger than 0. And $\mathrm{LIS}(-17) = 3$ because $-17, -2.3, 0$ is a longest increasing subsequence starting with -17.

Question 54 *What are the* LIS *values for the sequence* $3, 8, 5, 2, 7, 1, 10, 9, 4, 6$*?*

Once your friend writes a sequence of 10 different real numbers then you should compute the LIS values for each element. If $\mathrm{LIS}(x) \geq 4$ for any sequence element x then you are home free: there is an increasing subsequence of length 4. This happened in the

sequence of Question 54. But what if that doesn't happen? What if $\mathrm{LIS}(x) \leqslant 3$ for every element x?

This happened with the table given above. Here comes the magic. Since each of the 10 LIS values must be 1, 2, or 3, the pigeonhole principle guarantees the existence of $\lceil \frac{10}{3} \rceil = 4$ elements that share the same LIS value. In fact, $\mathrm{LIS}(x) = 1$ for five (not just four) different values of x:

$$\mathrm{LIS}(100) = \mathrm{LIS}(57) = \mathrm{LIS}(0) = \mathrm{LIS}(-0.2) = \mathrm{LIS}(-4) = 1.$$

Better yet, these values of x form a *decreasing* subsequence.

Will this always work? There are two questions. One, will those elements that share a common LIS value always produce a decreasing subsequence? Two, if so, will the subsequence be long enough? Question one just requires a little reasoning, while question two requires the pigeonhole principle. We tie up both loose ends in the proof.

Proof of Theorem 1.5.7: Let $n \geqslant 1$ and suppose S is a sequence of $n^2 + 1$ distinct real numbers. To each number x in S associate the value $\mathrm{LIS}(x)$ which gives the length of the longest increasing subsequence starting with, and including, x.

If $\mathrm{LIS}(x) \geqslant n + 1$ for some element x of the sequence, then we have found an increasing subsequence of length $n + 1$.

If not, then $\mathrm{LIS}(x) \leqslant n$ for each element x of the sequence. The LIS function maps the sequence (treated as an $(n^2 + 1)$-set) to the set $[n]$ (because $1 \leqslant \mathrm{LIS}(x) \leqslant n$ for all x). By the pigeonhole principle, some element of $[n]$ is the image of at least

$$\left\lceil \frac{n^2 + 1}{n} \right\rceil = \left\lceil n + \frac{1}{n} \right\rceil = n + 1$$

sequence elements. Call these sequence elements $x_1, x_2, \ldots, x_{n+1}$ and assume that they appear in the sequence from left to right in that order. We claim that these elements form a decreasing sequence of length $n + 1$, i.e.,

$$x_1 > x_2 > \cdots > x_{n+1}.$$

To see why, suppose for sake of contradiction that $x_1 < x_2$. We know that the length of the longest increasing subsequence starting with x_2 is $\mathrm{LIS}(x_2)$. Take one such sequence and put x_1 on the front of it. We now have an increasing subsequence starting with x_1 that has length $\mathrm{LIS}(x_2)+1$. But since $\mathrm{LIS}(x_1) = \mathrm{LIS}(x_2)$, we now have an increasing subsequence starting with x_1 of length $\mathrm{LIS}(x_1) + 1$. Impossible! The longest increasing subsequence starting with x_1 has length $\mathrm{LIS}(x_1)$. This contradiction shows that $x_1 > x_2$.

The same argument shows that $x_2 > x_3$, and so forth. Therefore S has a decreasing subsequence of length $n + 1$. Exercise 7 assigns you the task of proving the second part of the theorem. ■

See Exercise 8 for a more general version.

Summary

The various theorems known as the pigeonhole principle ensure the existence of an element of a function's codomain that has a "large" inverse image. A concrete way to state the

pigeonhole principle is: given any distribution of k objects to n boxes, some box receives at least $\lceil \frac{k}{n} \rceil$ objects. The basic pigeonhole principle is intuitive, but clever applications can lead to nonintuitive and deep results.

Exercises

1. A bag contains 97 pennies, 56 nickels, 410 dimes, 102 quarters, and three half-dollars. You reach in and grab some coins. What is the fewest number of coins you must grab in order to guarantee that you have two coins of the same value in your hand?
2. Let n be odd and suppose $(x_1, x_2, \ldots, x_n)$ is any permutation of $[n]$. Prove that the product $(x_1 - 1)(x_2 - 2) \cdots (x_n - n)$ is even. Is the result necessarily true if n is even? Give a proof or counterexample.
3. Let $n \geq 1$, and let S be an $(n + 1)$-subset of $[2n]$. Prove that there exist two numbers in S whose sum is $2n + 1$.
4. Let $n \geq 1$, and let S be an $(n + 1)$-subset of $[2n]$. Prove that there exist two numbers in S such that one divides the other.
5. In Questions 46 and 48, you constructed counterexamples to show that the $\lfloor n/2 \rfloor$ of Theorem 1.5.2 is best possible by showing that it can't be replaced by a smaller number. Construct a general counterexample that works for any value of n.
6. Consider any five points in the plane that have integer coordinates.
   (a) Prove that there are two points such that the midpoint of the line segment joining those two points also has integer coordinates.
   (b) Show that the conclusion in (a) is not necessarily true with only four points.
   (c) Can you conjecture and prove a similar statement involving points in space with integer coordinates?
7. Prove that the result of the Erdős-Szekeres theorem is best possible, in that it is possible for a sequence of n^2 distinct real numbers to have neither an increasing subsequence of length $n + 1$ nor a decreasing subsequence of length $n + 1$.
8. This concerns a more general version of the Erdős-Szekeres theorem.
   (a) Prove: For $m, n \geq 1$, if S is a sequence of $mn + 1$ distinct real numbers, then S contains either an increasing subsequence of length $m + 1$ or a decreasing subsequence of length $n + 1$.
   (b) Prove that this result is best possible by showing that the result doesn't necessarily hold when $mn + 1$ is replaced by mn.
9. Prove Theorem 1.5.6.
10. Prove the following version of the pigeonhole principle. Let $n_1, n_2, \ldots, n_k$ be positive integers. If we distribute $n_1 + n_2 + \cdots + n_k - k + 1$ objects among k boxes, then there is some $i \in [k]$ for which the following is true: box i contains at least n_i objects.
11. Suppose, in the Erdős-Szekeres theorem, we remove the requirement that the numbers in the sequence be distinct. How should you change the statement of the theorem and its proof so that a similar result holds?

12. (This exercise provides an alternative proof of the Erdős-Szekeres theorem.) Let S be a sequence of $n^2 + 1$ distinct real numbers, $n \geq 1$. Suppose, for sake of contradiction, that the conclusion of the theorem does not hold. For each element x of the sequence, define $g : S \longrightarrow [n] \times [n]$ by $g(x) = (i, d)$ where i is the length of the longest increasing subsequence starting with x and d is the length of the longest decreasing subsequence starting with x.

    Explain why g is not one-to-one, and then complete the proof of the Erdős-Szekeres theorem.

Travel Notes

The pigeonhole principle is also known as the Dirichlet drawer principle after Peter Dirichlet (1805–1859), who is generally credited as the first mathematician to make explicit use of it. Theorem 1.5.7 appears in Erdős & Szekeres (1935). The main subject of their paper was a proof of the following result:

> For any positive integer n, there exists some positive integer m (depending on n) so that when any m points are placed in the plane in general position, there exists a subset of n points that are the vertices of a convex n-gon.

Points are in general position when no three of them lie on the same line. When $n = 4$, the smallest value of m that works is $m = 5$. In other words, if you draw any five points in the plane such that no three of them lie on the same line, then there will be four points that are the vertices of a convex quadrilateral, but this is not necessarily true when drawing four points. The importance of their paper lies in the interest it later kindled in Ramsey theory. At the time, Ramsey's theorem was a little-known theorem in mathematical logic. The Hungarian mathematician Paul Erdős (1913–1996) was a major contributer to the field of Ramsey theory. See the accounts in Graham, Rothschild & Spencer (1980) and also Section 6.4 of this book.

CHAPTER 2

Distributions and Combinatorial Proofs

We spent the last chapter practicing basic counting techniques and learning the principles that we will use in the rest of the book. In this chapter we begin our study of combinatorics proper with two key concepts. The first is that of a ***distribution***, which is an assignment of objects to recipients. All of the counting problems in Chapter 1 can be reduced to counting certain distributions. So, distributions provide a unifying framework for counting problems.

The second concept is that of a combinatorial proof. Combinatorialists enjoy the art of constructing combinatorial proofs. These are fun to write and often more memorable or insightful than a proof by, say, mathematical induction. In Section 1.1 we emphasized that it is important to understand the kind of objects that expressions like $(n)_k$ or $\binom{n}{k}$ count. This understanding is essential in writing combinatorial proofs.

2.1 Counting functions

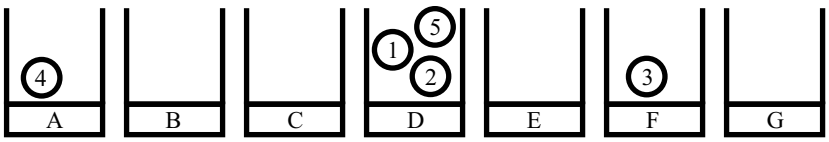
Distribution problems

Let's return to some questions like those we answered in Section 1.1.

1. How many five-letter passwords are there if each letter is A–G?
2. How many of those passwords have no repeated letters?

The answers to these questions are 7^5 and $(7)_5$, respectively.

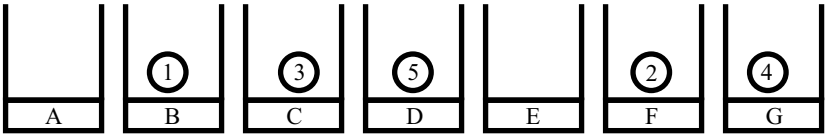
Here is a new way to think about counting passwords. Consider the password DDFAD. The following diagram represents this password as a distribution of five distinct objects (labeled 1–5) to seven distinct recipients (labeled A–G):



The possible letters in the password are the recipients and are represented as bins labeled A–G. The positions of the letters are the objects and are represented as balls numbered 1–5. Object i is placed in bin j if and only if letter j is in position i of the password. For example, bin D contains objects labeled 1, 2, and 5 because DDFAD has a D in the first, second, and fifth positions.

Question 55 *To what distribution does the password GGGAG correspond?*

As another example, the password BFCGD corresponds to the following distribution:



Here, each recipient receives at most one object.

Question 56 *If you rephrase Questions Q1 and Q2 at the beginning of Section 1.1 as distribution problems, how would you label the objects and recipients in each case?*

The idea is that in a counting question for which the answer is n^k, the objects being counted can be thought of as distributions of k distinct objects to n distinct recipients. Also, in a question for which the answer is $(n)_k$, the objects can be thought of as distributions of k distinct objects to n distinct recipients where each recipient receives at most one object.

The 16 distributions

Objects in a distribution problem can be distinct or identical. They are ***distinct*** if they are labeled so that you can tell them apart (think of balls with different numbers on them). They are ***identical*** if they are unlabled and otherwise indistinguishable (think of balls all having the same size and color). Likewise the recipients can be distinct or identical.

Recipients in a distribution problem may also have restrictions on the number of objects they can receive. Typical situations involve no restrictions (like in the first question at the beginning of this section), at most one object (like in the second question), at least one object, or exactly one object. This gives a total of 16 different distributions as shown in the table.

Distributions of		how many objects recipients can receive			
***k* objects**	**to *n* recipients**	no restrictions	$\leqslant 1$	$\geqslant 1$	$= 1$
distinct	distinct	n^k	$(n)_k$	?	$n!$ or 0
identical	distinct	?	?	?	?
distinct	identical	?	?	?	?
identical	identical	?	?	?	?

We discussed the reason for the n^k and $(n)_k$ entries earlier.

Question 57 *Explain the reason for the "$n!$ or 0" entry. Specifically, for what values of k and n is the answer 0?*

By the end of this chapter we will have the full picture. Additional nuances are possible beyond those listed here—for example, a problem involving a mix of distinct and identical objects—but these 16 types go quite far.

Functions as distributions

Here are four questions concerning different types of functions. In each case we rephrase it in terms of distributions.

(a) How many functions $[4] \longrightarrow [3]$ are there?

$\Longrightarrow$ Any such function is a distribution of four distinct objects (the elements of the

domain) to three distinct recipients (the codomain). The answer is 3^4 since each object can be assigned to one of three recipients. See the top of Figure 2.1.

Question 58 *How many functions* $f : [6] \longrightarrow [4]$ *have* $f(3) = 2$*?*

(b) How many functions $[3] \longrightarrow [4]$ are one-to-one?

$\Longrightarrow$ Any such function is a distribution of three distinct objects to four distinct recipients such that each recipient receives at most one object. The answer is $(4)_3$. See the second part of Figure 2.1.

Question 59 *How many one-to-one functions* $f : [4] \longrightarrow [6]$ *have* $5 \notin \mathrm{rng}(f)$*?*

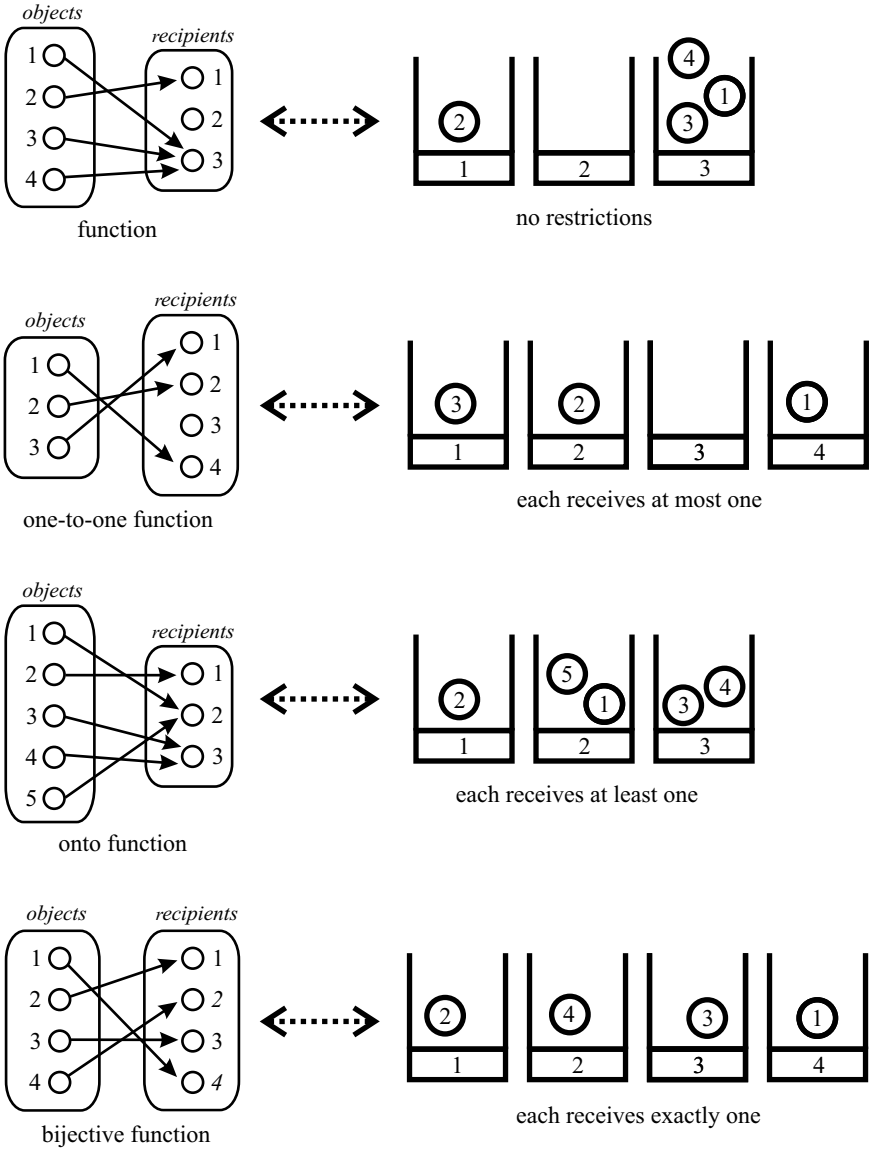


Figure 2.1. Functions and distributions.

(c) How many functions $[5] \longrightarrow [3]$ are onto?

$\Longrightarrow$ Any such function is a distribution of five distinct objects to three distinct recipients such that each recipient receives at least one object. These take more care to count so we postpone the solution until after this example. See the third part of Figure 2.1.

(d) How many functions $[4] \longrightarrow [4]$ are bijective?

$\Longrightarrow$ Any such function is a distribution of four distinct objects to four distinct recipients such that each recipient receives exactly one object. The answer is 4! or $(4)_4$. See the bottom of Figure 2.1.

We now have three canonical problems whose answer is n^k.

n^k equals (1) the number of k-lists taken from an n-set; (2) the number of functions from a k-set to an n-set; and (3) the number of distributions of k distinct objects to n distinct recipients.

Here is the same for $(n)_k$.

$(n)_k$ equals (1) the number of k-lists without repetition taken from an n-set; (2) the number of one-to-one functions from a k-set to an n-set; and (3) the number of distributions of k distinct objects to n distinct recipients such that each recipient receives at most one object.

And here is the same for $n!$.

$n!$ equals (1) the number of permutations of an n-set; (2) the number of bijections from an n-set to an n-set; and (3) the number of distributions of n distinct objects to n distinct recipients such that each recipient receives exactly one object.

Counting onto functions

We postpone the formula for the number of onto functions from a k-set to an n-set until we have introduced Stirling numbers and inclusion-exclusion in Sections 2.3 and 3.1. In the meantime, we tackle the problem of counting the onto functions $[5] \longrightarrow [3]$ in order to understand the issues involved.

We count the complement. There are 3^5 functions from [5] to [3]. Those that fail to be onto fall into two disjoint cases: (1) those that "miss" two elements of [3], and (2) those that miss only one element of [3]. Figure 2.2 shows a picture of a typical function in each case.

In Case 1, there are three functions—those that map everything in [5] to a single element of [3]. For Case 2, there are $3(2^5 - 2)$ functions. This is because there are three ways

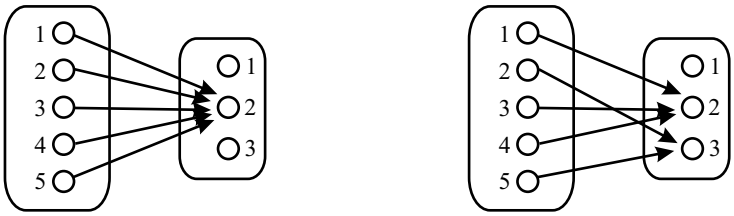


Figure 2.2. Two functions $[5] \longrightarrow [3]$ that are not onto.

to specify the element of [3] that the function misses. Then there are $2^5 - 2$ ways to specify an onto function from [5] to the 2-subset of [3] that the function doesn't miss. (Of the 2^5 functions from a 5-set to a 2-set, only two fail to be onto.) The number of onto functions $[5] \longrightarrow [3]$ is therefore

$$3^5 - \big(3 + 3(2^5 - 2)\big) = 150.$$

Question 60 *Find the number of onto functions* $[k] \longrightarrow [3]$.

Exercise 7 asks to take this one step further by finding the number of onto functions $[k] \longrightarrow [4]$.

Combinatorial proofs

A combinatorial proof of an identity $X = Y$ begins by asking a question and then answers it using two different but correct approaches. One approach produces the answer X and the other the answer Y. As long as we have answered correctly in both cases, we can then conclude $X = Y$. We now give two examples of combinatorial proofs. You'll notice that the key step is in asking the right question.

Combinatorial proof #1

In this first proof we are given an identity and must come up with the combinatorial proof. The identity is

$$(n)_k = (n-1)_k + k \cdot (n-1)_{k-1} \qquad \text{when } n, k \geqslant 1. \tag{2.1}$$

First we examine the special case and attach a concrete counting problem to it.

Question 61 *How should you define* $(n)_k$ *when either n or k (or both) equals 0 so that the formula (2.1) still holds?*

Consider the identity (2.1) when $k = 4$ and $n = 6$, namely

$$(6)_4 = (5)_4 + 4 \cdot (5)_3.$$

We know that, among other things, $(6)_4$ equals the number of ways to distribute four distinct objects to six distinct recipients. Let's say the objects are concert tickets (with seat assignments, so they are distinct) and the recipients are six of our friends.

We begin the proof by asking a question.

Question: How many ways are there to distribute four different concert tickets among six friends such that each friend receives at most one ticket?

We already know one answer.

Answer 1: There are $(6)_4$ ways.

Now we have to use a different method to count these distributions and obtain the answer $(5)_4 + 4 \cdot (5)_3$. The presence of the $+$ in this answer suggests breaking into cases and using the sum principle. The idea is to identify a particular friend and "condition on" (i.e., divide into cases) whether that friend receives a ticket. Figure 2.3 shows the two cases and the analysis for each.

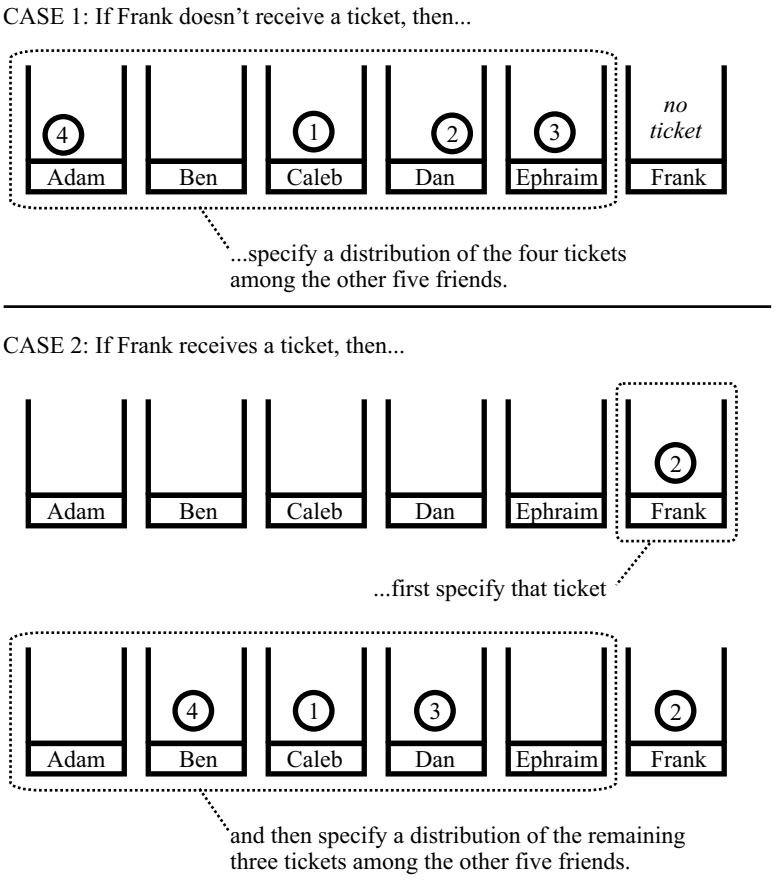


Figure 2.3. The reason why $(6)_4 = (5)_4 + 4 \cdot (5)_3$.

Answer 2: Say your friends are Adam, Ben, Caleb, Dan, Ephraim, and Frank. Divide the distributions into two cases depending on whether Frank receives a ticket. If Frank does not receive a ticket, then there are $(5)_4$ ways to distribute the four tickets among the other five friends.

If Frank does receive a ticket, then there are four ways to specify that ticket, and then there are $(5)_3$ ways to distribute the three remaining tickets among the other five friends. There are $4 \cdot (5)_3$ distributions in this case.

By the sum principle there are $(5)_4 + 4 \cdot (5)_3$ distributions altogether.

This completes the combinatorial proof that $(6)_4 = (5)_4 + 4 \cdot (5)_3$. It is no harder to prove in general.

Theorem 2.1.1 *For any $n \geq 1$ and $k \geq 1$, $(n)_k = (n-1)_k + k \cdot (n-1)_{k-1}$.*

Combinatorial proof: How many ways are there to distribute k different concert tickets among n friends such that each friend receives at most one ticket?

Answer 1: There are $(n)_k$ ways.

Answer 2: One of your friends is Frank. Condition on whether he receives a ticket. If Frank does not receive a ticket, then there are $(n-1)_k$ ways to distribute all k tickets among the $n-1$ friends besides Frank. If Frank does receive a ticket, then there are k ways

to specify that ticket and then $(n-1)_{k-1}$ ways to distribute the remaining $k-1$ tickets among the $n-1$ friends besides Frank. Thus there are $k \cdot (n-1)_{k-1}$ distributions in this case. There are $(n-1)_k + k \cdot (n-1)_{k-1}$ distributions in all. ■

Combinatorial proof #2

If you are handed an identity to prove, as we just did with equation (2.1), you can try to come up with the right question to ask to reverse engineer the proof. But one advantage of combinatorial proofs is that you can discover new identities "on the fly." Here is an example.

First let's create a counting question, this time involving the answer $n!$. As we did the last time we'll experiment with a specific value of n.

Question: Given five blocks each having a different height, how many ways are there to line them up from left to right in a row?

Again, one answer is easy.

Answer 1: There are 5! ways.

In the end our identity will look like $5! = Y$ where Y is Answer 2.

Now we get to be creative with Answer 2. There are a lot of things we could do but here is one idea that can be adapted to prove other combinatorial identities. Any arrangement of the blocks must either be in increasing order of height from left to right or else is not. Label the blocks 1-5 in order of increasing height. We condition on the location of the first mistake that ruins the perfect increasing order 1-2-3-4-5. Figure 2.4 shows the analysis.

Answer 2: Condition on the first position in which a mistake is made in the increasing order 1-2-3-4-5.

Case 1: No mistake is made. The blocks are in increasing order and there is only one such way to arrange them.

Case 2: A mistake is made with the first block. There are four ways to specify the first block—any except block 1—and then 4! ways to line up the remaining blocks. By the product principle there are 4(4!) ways to line them up in this case.

Case 3: A mistake is made with the second block. This means that block 1 is first, followed by any block except block 2. Thus there are three ways to specify the second block, and then 3! ways to line up the remaining blocks. By the product principle there are $3 \cdot 3!$ ways in this case.

Cases 4 and 5 are similar and their answers are $2 \cdot 2!$ and $1 \cdot 1!$, respectively.

By the sum principle there are $1 + 1(1!) + 2(2!) + 3(3!) + 4(4!)$ ways to line up the blocks.

Question 62 *Why can't the first mistake occur with the fifth block?*

We're now ready for the general version.

Theorem 2.1.2 *For any $n \geq 1$, $n! = 1 + \sum_{j=1}^{n-1} j(j!)$.*

Question 63 *Give a combinatorial proof of the theorem by modifying the argument we used for $n = 5$.*

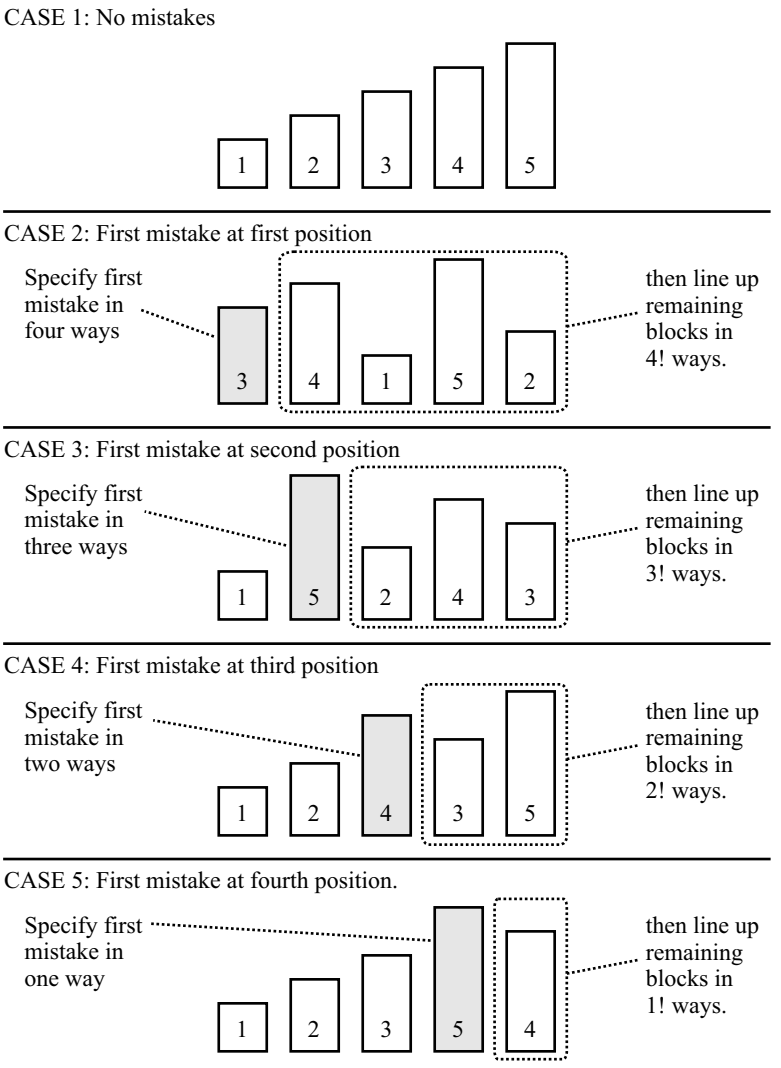


Figure 2.4. The reason why $5! = 1 + 1(1!) + 2(2!) + 3(3!) + 4(4!)$.

Discussion

To reconstruct the proof of Theorem 2.1.1, we can just remember the concert ticket question and condition on whether Frank gets a ticket. To reconstruct the proof of Theorem 2.1.2, we can remember the block line-up question and condition on the first position in which increasing order is ruined. The so-called "conditioning" idea divides the problem into disjoint and exhaustive cases so that we can apply the sum principle. You might prefer these ideas as an alternative to memorizing a formula like $(n)_k = (n-1)_k + k \cdot (n-1)_{k-1}$.

Summary

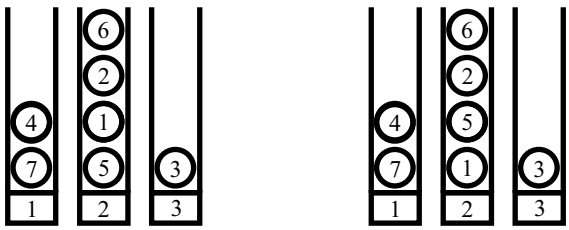
Many counting questions can be re-cast as distribution questions. In this section we counted distributions of k distinct objects to n distinct recipients under three different conditions: each recipient receives any number of objects, at most one object, and exactly one object.

We then introduced combinatorial proofs via two examples. A combinatorial proof begins with a question and then describes two different but correct approaches for answering that question.

Exercises

1. Jeopardy! For each answer, create an accompanying counting question.
   (a) $n! - 1$
   (b) $20^4 - (20)_4$
   (c) $(10)_5 + 5 \cdot (10)_4$
2. You have 10 concert tickets to distribute among 15 friends. Of the 10 tickets, six have assigned seating (so they are distinct) while four are general admission (so they are identical). Each friend gets at most one ticket. How many ways are there to distribute them?
3. How many eight-letter passwords using the letters A-Z are there in which up to one letter is allowed to be used more than once? This means HVCKEWFX and FOWFLQAZ and FBHHHRHT are allowed, but VSSLVRTF and LLLWWWFW are not.
4. Consider the possible functions $f : [7] \longrightarrow [9]$.
   (a) How many have $f(3) = 8$? How many have $f(3) \neq 8$?
   (b) How many have $f(1) \neq 5$ and are one-to-one?
   (c) How many have $f(i)$ even, for all i?
   (d) How many have $\text{rng}(f) = \{5, 6\}$?
   (e) How many in which f^{-1} is not a function?
5. How many one-to-one functions $f : [5] \longrightarrow [9]$ have 7 as the largest element of $\text{rng}(f)$?
6. If f is a function and $f(i) = i$ then we call i a ***fixed point*** of f.
   (a) How many functions $[5] \longrightarrow [5]$ have at least one fixed point?
   (b) How many functions $[n] \longrightarrow [n]$ have no fixed points?
   (c) How many bijections $[4] \longrightarrow [4]$ have no fixed points?
7. Find the number of onto functions $[k] \longrightarrow [4]$.
8. Give a non-combinatorial, algebraic proof of Theorem 2.1.1 that uses the formula $(n)_k = \frac{n!}{(n-k)!}$.
9. Give a combinatorial proof: For $n \geqslant 1$, $n! = n \cdot (n-1)!$.
10. Give a combinatorial proof: For $n \geqslant 1$ and $k \geqslant 1$, $(n)_k = n \cdot (n-1)_{k-1}$.
11. Give a combinatorial proof: For $n \geqslant 1$ and $k \geqslant 1$, $2^{kn} > \max\{n^k, k^n\}$. (Hint: Compare relations to functions.)
12. Define
$$F := \{\text{functions } f : f \text{ is a function } [k] \longrightarrow [n]\}$$
$$L := \{\text{lists } (x_1, x_2, \ldots, x_k) : \text{each } x_i \text{ is taken from } [n]\}$$
and define $G : F \longrightarrow L$ by $G(f) = \big(f(1), f(2), \ldots, f(k)\big)$. Prove that G is a bijection. What combinatorial result does this establish?

13. In the previous exercise, how does the set L change if the set F is changed to the set of one-to-one, onto, or bijective functions, respectively?
14. Give a combinatorial proof: For n and k satisfying $1 \leqslant k \leqslant n$,
$$(n)_k = \sum_{j=k}^{n} k \cdot (j-1)_{k-1}.$$
15. Let π_n equal the number of permutations of $[n]$ having any length, including length 0 (the "empty permutation"). Then $\pi_1 = 2$ because the permutations of [1] having any length are ( ) and (1). The permutations of [2] having any length are
$$(), \qquad (1), \qquad (2), \qquad (1,2), \qquad \text{and} \qquad (2,1),$$
so $\pi_2 = 5$. Set $\pi_0 = 1$.
    (a) Find π_3 by complete enumeration.
    (b) Give a combinatorial proof: For $n \geqslant 1$, $\pi_n = n\pi_{n-1} + 1$.
    (c) Use the identity in part (b) to find π_{10}.
16. (ordered distributions) This exercise and others throughout this chapter that are labeled "ordered distributions" concern distributions wherein the order in which the recipients receive the objects matters. Here are two examples of ordered distributions of seven distinct objects to three distinct recipients:



By convention, objects near the bottom are received first (think of recipients 1–3 as cashiers and the objects as customers in each cashier's line). This means that the two ordered distributions shown are different, even though they would be the same when considered as ordinary distributions.

Let $(n)^{(k)}$ equal the number of ordered distributions of k distinct objects to n distinct recipients.

    (a) Prove $(n)^{(k)} = n(n+1)(n+2)\cdots(n+k-1)$.
    (b) Explain why there are $(k)_n \cdot (n)^{(k-n)}$ ordered distributions of k distinct objects to n distinct recipients such that each receives at least one object.
    (c) Explain combinatorially why $k!\binom{k-1}{n-1}$ is also the answer to part (b).

Travel Notes

The book by Benjamin & Quinn (2003) entitled *Proofs that Really Count: The Art of Combinatorial Proof* is an engaging, one-of-a-kind introduction to combinatorial proofs in a lot of different areas of mathematics. Other good sources are the journals *Mathematics Magazine* and *The College Mathematics Journal*, both published by the Mathematical Association of America.

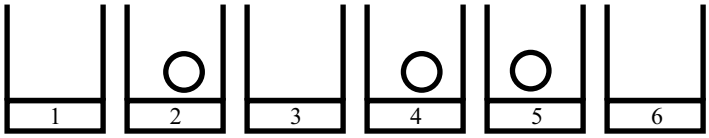
2.2 Counting subsets and multisets

Subsets and multisets as distributions

Here are three questions like those we answered in Section 1.1.

1. In a pick-three lottery involving the numbers 1–6, how many tickets are there?
2. If a store offers four donut varieties, how many orders for seven donuts are there?
3. How many orders in the previous question contain at least one donut of each variety?

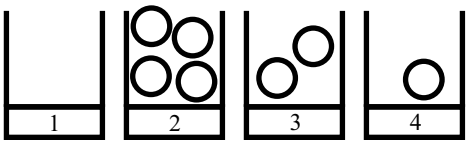
In the first question, a ticket consists of a 3-subset of [6] so the answer is $\binom{6}{3}$. Here is a distribution corresponding to the ticket $\{2, 4, 5\}$.



This is a distribution of three identical objects to six distinct recipients such that each receives at most one object. We throw a ball into bin j whenever j is an element of $\{2, 4, 5\}$.

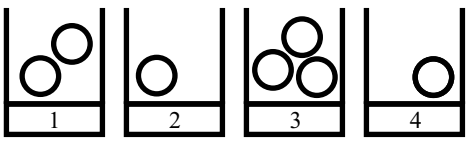
Question 64 *There are $\binom{n}{k}$ ways to form a k-person committee from a group of n people. Rephrase this as a distribution problem.*

In the second question, a donut order is a 7-multiset taken from [4] so the answer is $\left(\!\binom{4}{7}\!\right)$. Here is a distribution corresponding to the multiset $\{2, 2, 2, 2, 3, 3, 4\}$.



This is a distribution of seven identical objects to four distinct recipients under no restrictions on the number of objects each can receive. We throw one ball into bin j per donut of variety j that we order.

A donut order in the third question is a 7-multiset taken from [4] in which each element of [4] appears at least once. There are $\left(\!\binom{4}{7-4}\!\right)$ or $\left(\!\binom{4}{3}\!\right)$ such orders because once we place one donut of each variety in our bag, the rest of the order can be any 3-multiset taken from [4]. Here is a distribution corresponding to the multiset $\{1, 1, 2, 3, 3, 3, 4\}$.



This is a distribution of seven identical objects to four distinct recipients such that each receives at least one.

These examples show that subsets and multisets are equivalent to certain distributions of identical objects to distinct recipients. Here are three canonical problems whose answer is $\binom{n}{k}$.

$\binom{n}{k}$ *equals* (1) *the number of k-subsets of an n-set;* (2) *the number of ways to form a k-person committee from a group of n people; and* (3) *the number of distributions of k identical objects to n distinct recipients such that each receives at most one object.*

Here are the same for $\left(\!\binom{n}{k}\!\right)$.

$\left(\!\binom{n}{k}\!\right)$ *equals* (1) *the number of* k*-multisets taken from an* n*-set;* (2) *the number of ways to order* k *donuts if a store sells* n *varieties; and* (3) *the number of distributions of* k *identical objects to* n *distinct recipients.*

These allow us to fill in the next line of our table of distribution problems.

Distributions of		how many objects recipients can receive			
***k* objects**	**to *n* recipients**	no restrictions	$\leqslant 1$	$\geqslant 1$	$= 1$
distinct	distinct	n^k	$(n)_k$	?	$n!$ or 0
identical	distinct	$\left(\!\binom{n}{k}\!\right)$	$\binom{n}{k}$	$\left(\!\binom{n}{k-n}\!\right)$	1 or 0
distinct	identical	?	?	?	?
identical	identical	?	?	?	?

Question 65 *Explain the reason for the last two answers on the second line of the table.*

Pascal's identity and Pascal's triangle

Let's discover and prove an identity for $\binom{n}{k}$ on the fly. We begin with a special case. In how many ways can we form a three-person committee from a group of five people?

For Answer 1 we know that there are $\binom{5}{3}$ ways. To get another answer, let's say the five people are our friends Adam, Ben, Caleb, Dan, and Ephraim from Section 2.1. Divide the possible committees into two types according to whether Ephraim is on the committee.

All possible committees	
Committees with Ephraim	**Committees without Ephraim**
{Adam, Ben, Ephraim}	{Adam, Ben, Caleb}
{Adam, Caleb, Ephraim}	{Adam, Ben, Dan}
{Adam, Dan, Ephraim}	{Adam, Caleb, Dan}
{Ben, Caleb, Ephraim}	{Ben, Caleb, Dan}
{Ben, Dan, Ephraim}	
{Caleb, Dan, Ephraim}	
$\binom{4}{2}$ with Ephraim	$\binom{4}{3}$ without Ephraim
$\binom{4}{2} + \binom{4}{3}$ total	

There are $\binom{4}{2}$ committees with Ephraim because once he is on the committee we can specify the remaining two people in $\binom{4}{2}$ ways. There are $\binom{4}{3}$ committees without Ephraim because any such committee is just a three-person committee chosen from Adam, Ben, Caleb, and Dan. Therefore by the sum principle, Answer 2 is $\binom{4}{2} + \binom{4}{3}$.

We have proved $\binom{5}{3} = \binom{4}{2} + \binom{4}{3}$. The same reasoning proves the following theorem known as Pascal's identity.

Theorem 2.2.1 (Pascal's identity) *For any* $n \geqslant 1$ *and* $k \geqslant 1$,

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Question 66 *Prove Pascal's identity. Then adapt the same idea to give a combinatorial proof of a related identity: For any $n \geq 1$ and $k \geq 1$,*

$$\left(\!\!\binom{n}{k}\!\!\right) = \left(\!\!\binom{n-1}{k}\!\!\right) + \left(\!\!\binom{n}{k-1}\!\!\right).$$

Pascal's identity leads to ***Pascal's triangle***, a triangular array of the nonzero numbers $\binom{n}{k}$ for n and k satisfying $0 \leqslant k \leqslant n$. Its first eight rows are as follows:

$n\downarrow\ k\rightarrow$	0	1	2	3	4	5	6	7
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1

The entry in row n and column k is $\binom{n}{k}$. Pascal's formula allows for easy computation of this array: each entry equals its "northwestern" neighbor plus its "northern" neighbor. For the first row and column, which have no such neighbors, we rely on the following boundary conditions: $\binom{n}{0} = 1$ for $n \geqslant 0$ and $\binom{0}{k} = 0$ for $k \geqslant 1$. These make combinatorial sense. The number of 0-subsets of an n-set is 1 because $\emptyset$ is the only such subset. Also, there are no k-subsets of a 0-set for any value of $k \geqslant 1$.

Question 67 *Use Pascal's identity to find the ninth (i.e., $n = 9$) row of the table.*

Combinatorial proofs

Quick ones

Two basic identities involving the numbers $\binom{n}{k}$ are

$$\binom{n}{k} = \binom{n}{n-k} \qquad \text{for all } n \text{ and } k \text{ satisfying } 0 \leqslant k \leqslant n \tag{2.2}$$

and

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \qquad \text{for all } n \geqslant 0. \tag{2.3}$$

Both have quick combinatorial proofs. To prove equation (2.2), observe that you can specify a k-person committee by either specifying those k people who are on it or equivalently by specifying those $n-k$ people that are *not* on it.

To prove equation (2.3), recall that there are 2^n possible subsets of an n-set. We can alternately count these subsets by organizing them into piles according to their size. There are $\binom{n}{k}$ subsets of size k, and summing this quantity over all k from 0 to n gives the right-hand side of the equation.

Question 68 *What is the sum of the numbers in row 15 (i.e., $n = 15$) of Pascal's triangle? (Answer this without computing row 15.)*

Committee-counting

We'll use the committee-counting interpretation of $\binom{n}{k}$ to prove two more identities. Here is the first:

$$\binom{n}{k}k = n\binom{n-1}{k-1}. \tag{2.4}$$

Question: From a group of n people, in how many ways can we select a committee of size k and also specify one of the people on the committee as the chair?

Answer 1: Count the 2-lists of the form (committee, chair). We may choose the committee in $\binom{n}{k}$ ways, and then choose the chair from among those k people in one of k ways. By the product principle, there are $\binom{n}{k}k$ total ways.

Answer 2: Count the 2-lists of the form (chair, committee). We may first choose the chair from among the n people in one of n ways. Then, from the $n-1$ people that remain, we may complete the committee by choosing $k-1$ of them in $\binom{n-1}{k-1}$ ways. By the product principle, there are $n\binom{n-1}{k-1}$ total ways.

Vandermonde's formula

The following identity is known as Vandermonde's formula:

$$\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j} = \binom{m+n}{k}. \tag{2.5}$$

To come up with a good question, observe that the right side counts the k-person committees we can form from a group of $m+n$ people. The terms in the sum on the left suggest that there are two types of people—say m men and n women—and that we can break into cases according to the number of men on the committee.

Question: From a group of m men and n women, how many k-person committees can we form?

Answer 1: There are $\binom{m+n}{k}$ committees.

Answer 2: Condition on the number of men on the committee. If this number is j, where $0 \leqslant j \leqslant k$, then there are $\binom{m}{j}$ ways to specify the men. For each such specification, there are $\binom{n}{k-j}$ ways to specify the women so that the committee then contains k people. By the product principle there are $\binom{m}{j}\binom{n}{k-j}$ committees having j men. By the sum principle there are

$$\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}$$

committees.

Donut orders

Let's go back to donut orders. Suppose a store sells 10 varieties and we want to order a half-dozen. There are $\left(\!\!\binom{10}{6}\!\!\right)$ different orders. Focus on one particular variety, say glazed. Any order for a half-dozen must contain between zero and six glazed donuts. There are $\left(\!\!\binom{9}{6}\!\!\right)$ orders containing zero glazed, $\left(\!\!\binom{9}{5}\!\!\right)$ orders containing one glazed, and so on up to $\left(\!\!\binom{9}{0}\!\!\right)$

orders containing six glazed. We just proved that

$$\left(\!\!\binom{10}{6}\!\!\right) = \left(\!\!\binom{9}{6}\!\!\right) + \left(\!\!\binom{9}{5}\!\!\right) + \left(\!\!\binom{9}{4}\!\!\right) + \left(\!\!\binom{9}{3}\!\!\right) + \left(\!\!\binom{9}{2}\!\!\right) + \left(\!\!\binom{9}{1}\!\!\right) + \left(\!\!\binom{9}{0}\!\!\right).$$

Question 69 *Generalize and prove a version involving* $\left(\!\!\binom{n}{k}\!\!\right)$ *instead of* $\left(\!\!\binom{10}{6}\!\!\right)$.

The binomial theorem

The rows of Pascal's triangle give the coefficients on each term when $(x+y)^n$ is expanded and simplified. For example,

$$\begin{aligned}(x+y)^4 &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \\ &= \binom{4}{0}x^4y^0 + \binom{4}{1}x^3y^1 + \binom{4}{2}x^2y^2 + \binom{4}{3}x^1y^3 + \binom{4}{4}x^0y^4.\end{aligned}$$

This is the subject of the binomial theorem.

Theorem 2.2.2 (binomial) *For any integer* $n \geqslant 0$ *and any real numbers* x *and* y,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Since x and y are real numbers, not necessarily positive integers, it seems that a combinatorial proof would be out of the question. We finesse this by first giving a combinatorial proof that it is true for all positive integers x and y, and then explaining why that's sufficient.

Suppose x and y are positive integers. How many n-letter passwords can we make where there are $x+y$ choices for each letter?

There are $(x+y)^n$ such passwords. For another approach, imagine that the letters come from two completely different alphabets: Alphabet 1 which has x characters and Alphabet 2 which has y characters. Arrange the passwords into piles according to the number of characters from Alphabet 2 they contain. If this number is k, where $0 \leqslant k \leqslant n$, then there are $\binom{n}{k}$ ways to specify the positions of the characters from Alphabet 2, then y^k ways to specify those characters, and finally x^{n-k} ways to specify the characters from Alphabet 1 for the remaining $n-k$ positions. Since k can range from 0 to n, by the sum principle there are

$$\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

passwords. This proves the binomial theorem when x and y are positive integers.

To extend the result to all *real numbers* x *and* y, note that the expression $(x+y)^n$ is a polynomial in x and y. If a polynomial equation like that of the binomial theorem is true for infinitely many values of x and y (here, all positive integers), then it is true for all real numbers x and y. This result is known as the uniqueness of polynomials theorem. See Exercise 13.

Counting integral solutions

We close with some examples illustrating another type of counting question that $\left(\!\!\binom{n}{k}\!\!\right)$ answers. The idea will prove useful when we study generating functions in Chapter 3.

Examples

(a) How many solutions does $z_1 + z_2 + z_3 + z_4 = 7$ have, where each z_i is a nonnegative integer?

$\Longrightarrow$ A solution is a 4-list of the form (z_1, z_2, z_3, z_4) that satisfies the conditions in the question. For example both $(0, 4, 2, 1)$ and $(1, 0, 0, 6)$ are solutions, but neither $(4, 2, 1, 2)$ nor $(-1, 0, 0, 8)$ are.

Observe that the solutions are in one-to-one correspondence with the 7-multisets taken from [4]: z_1 is the number of 1s in the multiset, z_2 is the number of 2s, and so on. For example, the solution $(0, 4, 2, 1)$ corresponds to the multiset $\{2, 2, 2, 2, 3, 3, 4\}$. Therefore there are $\left(\!\binom{4}{7}\!\right) = \binom{10}{7} = 120$ solutions.

(b) How many solutions does $z_1 + z_2 + z_3 = 15$ have, where each z_i is a positive integer?

$\Longrightarrow$ Since each $z_i \geqslant 1$, these solutions correspond to 15-multisets taken from [3] where each element of [3] appears at least once. Therefore there are $\left(\!\binom{3}{15-3}\!\right) = \left(\!\binom{3}{12}\!\right) = \binom{14}{12} = 91$ solutions.

Notice that this problem is equivalent to counting the solutions to $y_1 + y_2 + y_3 = 15 - 3$ where each y_i is a *nonnegative* integer.

(c) How many solutions does $z_1 + z_2 + z_3 + 4z_4 = 11$ have, where each z_i is a nonnegative integer?

$\Longrightarrow$ The $4z_4$ term throws a bit of a wrench into the works.

Question 70 *Solve this problem by breaking into cases based on the value of* z_4.

The general idea is that $\left(\!\binom{n}{k}\!\right)$ equals the number of solutions to $z_1 + z_2 + \cdots + z_n = k$ in nonnegative integers z_i, and that $\left(\!\binom{n}{k-n}\!\right)$ equals the number of solutions to the same equation in positive integers z_i.

Question 71 *How many solutions does* $z_1 + z_2 + \cdots + z_n = k$ *have where each* z_i *is either* 0 *or* 1*?*

Summary

Subsets and multisets correspond to distributions of identical objects to distinct recipients. In this section we provided combinatorial proofs of many important results involving the binomial coefficients $\binom{n}{k}$ among them Pascal's identity and the binomial theorem. We also examined how $\left(\!\binom{n}{k}\!\right)$ counts the integer-valued solutions to certain equations.

Exercises

1. Jeopardy! For each answer, create an accompanying counting question.

   (a) $\binom{n}{0} + \binom{n}{1} + \binom{n}{2}$

   (b) $\dfrac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}$

   (c) $\binom{20}{10}\binom{10}{5}$

(d) $\displaystyle\sum_{j=0}^{\lfloor n/2 \rfloor} \left(\!\!\binom{n}{2j+1}\!\!\right)$

2. Justify combinatorially: $\binom{20}{8}\binom{8}{5}\binom{5}{3} = \binom{20}{3}\binom{17}{2}\binom{15}{3}$.

3. Give a bijective proof of Pascal's identity by defining

$$A := \{\text{sets } S : S \subseteq [n] \text{ and } |S| = k\}$$
$$B := \{\text{sets } T : T \subseteq [n-1] \text{ and } |T| = k-1\}$$
$$C := \{\text{sets } U : U \subseteq [n-1] \text{ and } |U| = k\}$$

and then finding a bijection $f : A \longrightarrow B \cup C$.

4. Give combinatorial or bijective proofs of the following. Part of your job is to determine all values of n, k, and/or m for which the identities are valid.

(a) $3^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} 2^{n-k}$.

(b) $\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$.

(c) $\binom{0}{m} + \binom{1}{m} + \binom{2}{m} + \cdots + \binom{n}{m} = \binom{n+1}{m+1}$.

(d) $\left(\!\!\binom{n}{k}\!\!\right) = \left(\!\!\binom{k+1}{n-1}\!\!\right)$.

(e) $\left(\!\!\binom{n}{k-n}\!\!\right) = \binom{k-1}{k-n}$.

(f) $\left(\!\!\binom{1}{k-1}\!\!\right) + \left(\!\!\binom{2}{k-1}\!\!\right) + \left(\!\!\binom{3}{k-1}\!\!\right) + \cdots + \left(\!\!\binom{n}{k-1}\!\!\right) = \left(\!\!\binom{n}{k}\!\!\right)$.

5. What does $\binom{n-1}{k-1} + \binom{n-2}{k-1} + \binom{n-3}{k-1} + \cdots + \binom{k-1}{k-1}$ equal? Make a conjecture and then give a combinatorial proof.

6. Give a combinatorial proof: If x and y are real numbers and n is a nonnegative integer, then

$$(x+y)_n = \sum_{k=0}^{n} \binom{n}{k} (x)_k (y)_{n-k}.$$

(As in the proof of the binomial theorem, you'll need to invoke uniqueness of polynomials.)

7. Determine the number of solutions to each of the following equations. Assume all z_i are nonnegative integers unless stated otherwise.

(a) $z_1 + z_2 + z_3 + z_4 = 1$.

(b) $z_1 + z_2 + 10z_3 = 8$.

(c) $z_1 + z_2 + \cdots + z_{20} = 401$ where each $z_i \geqslant 1$.

(d) $z_1 + z_2 + z_3 + z_4 = 12$ where $z_1, z_2 \geqslant 1$ and $z_3, z_4 \geqslant 2$.

(e) $z_1 + z_2 + z_3 + 3z_4 + 5z_5 = 7$.

(f) $z_1 + z_2 + z_3 + \frac{1}{2}z_4 = \frac{11}{2}$.

8. After expanding $(a + b + c)^9$ and combining like terms, how many terms are there?

9. Fix n to be a positive integer. Find, with proof, the value of k (where $0 \leqslant k \leqslant n$) that maximizes $\binom{n}{k}$.

10. When is $\binom{n}{k}$ even? Give as complete an answer, with proof, as you can.

11. How many k-lists $(x_1, x_2, \ldots, x_k)$ are possible, such that each x_i is a positive integer and $1 \leqslant x_1 \leqslant x_2 \leqslant \cdots \leqslant x_k \leqslant n$? Prove your answer.

12. How many k-subsets of $[n]$ are possible such that no two consecutive integers appear in the subset?

13. (uniqueness of polynomials) Let $f(x) = \sum_{k=0}^{n} a_k x^k$ and $g(x) = \sum_{k=0}^{n} b_k x^k$ be polynomials of degree n, and suppose that $x_0, x_1, \ldots, x_n$ are distinct real numbers for which $f(x_i) = g(x_i)$, for all i. Prove that $f = g$.

Travel Notes

Though it is quite common to attach the French mathematician Blaise Pascal's (1623–1662) name to the triangular array of numbers mentioned in this section, the triangle and many of its properties were known well before Pascal's time. Mathematicians from Asia, the Middle East, Northern Africa, and Southern Europe had studied it as early as the year 1000. See the article by Katz (1996).

The binomial coefficients provide a seemingly endless supply of interesting identities and properties. We will see more throughout the book, especially in Section 4.1. Again, the book by Benjamin & Quinn (2003) is an excellent reference. On a related note, there has been considerable research in recent years into the prospect of identity-proving algorithms for computers. This is a well-solved problem for many important classes of identities including those involving binomial coefficients. See the book entitled $A = B$ by Petkovšek, Wilf & Zeilberger (1996).

The Fermat-Wiles theorem (formerly, Fermat's last theorem) says that there are no nontrivial solutions to $x^n + y^n = z^n$ in integers x, y, z, and n when $n \geqslant 3$. In an article about his father ("Roger Apéry, 1916–1994: A Radical Mathematician," *The Mathematical Intelligencer*, volume 18 number 2, 1996), François Apéry relates the following anecdote.

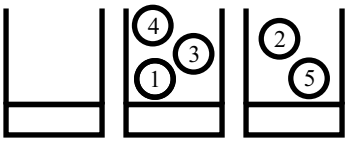
> During a mathematician's dinner in Kingston, Canada, in 1979, the conversation turned to Fermat's last theorem, and Enrico Bombieri proposed a problem: to show that the equation
>
> $$\binom{x}{n} + \binom{y}{n} = \binom{z}{n} \quad \text{where } n \geqslant 3$$
>
> has no nontrivial solution. Apéry left the table and came back at breakfast with the solution $n = 3$, $x = 10$, $y = 16$, $z = 17$. Bombieri replied stiffly, "I said nontrivial."

2.3 Counting set partitions

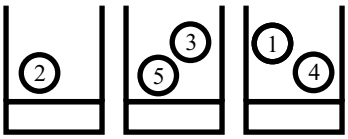
We have two types of distributions left to study: distinct objects to identical recipients, and identical objects to identical recipients. We study the former in this section and in doing so introduce the Stirling numbers of the second kind. We shall study this important family of numbers in more detail in Section 4.3.

Set partitions as distributions

We now consider distributions of distinct objects to identical recipients. Here is a distribution of five distinct objects to three identical recipients.



Here is another such distribution.



We can express the first distribution as $\big\{\{1,3,4\},\{2,5\}\big\}$ which is a partition of the set [5] into two blocks. The second can be expressed as $\big\{\{1,4\},\{2\},\{3,5\}\big\}$ which is a partition of [5] into three blocks. Notice that in the second distribution each recipient receives at least one object. (Recall that we encountered partitions in Section 1.4.)

Question 72 *What distribution corresponds to the partition* $\big\{\{1,2,3,4,5\}\big\}$*?*

For any set S, an ***r-partition of*** S is a set of r nonempty, disjoint sets whose union is S. The elements of the partition are called the ***blocks*** of the partition. The 2-partition of [5] corresponding to the first distribution shown in the previous paragraph consists of the blocks $\{1,3,4\}$ and $\{2,5\}$. If we can do so without confusion, it is sometimes convenient to exclude the inner braces and commas and instead write $\{134,25\}$.

The two salient features of a partition of a set S are: (1) each element of S appears in *exactly one* block of the partition, and (2) the order in which we list the blocks makes no difference.

Stirling numbers of the second kind

To count set partitions we define $S(n,k)$ as the number of partitions of an n-set into k blocks, i.e., the number of k-partitions of an n-set. As such,

> $S(n,k)$ *equals (1) the number of partitions of an* n*-set into* k *blocks; and (2) the number of distributions of* n *distinct objects to* k *identical recipients such that each receives at least one object.*

Take note that the number of distributions of k distinct objects to n identical recipients such that each receives at least one object is $S(k,n)$ not $S(n,k)$. The first parameter denotes the size of the set being partitioned and the second denotes the number of blocks. We define $S(0,0)=1$.

Question 73 *In the context of partitions or distributions (your choice), explain why* $S(0,k) = 0$ *for* $k \geqslant 1$ *and* $S(n,0) = 0$ *for* $n \geqslant 1$.

The numbers $S(n,k)$ are the ***Stirling numbers of the second kind***.

Stirling numbers by complete enumeration

Let's compute $S(4,k)$ for $k = 1,2,3,4$ by complete enumeration. In general, for a given positive integer n the only nonzero values of $S(n,k)$ are for those k satisfying $1 \leqslant k \leqslant n$.

First, $S(4,1)$ equals the number of partitions of [4] into one block. The only such partition is $\big\{\{1,2,3,4\}\big\}$ and so $S(4,1) = 1$.

Next $S(4,2)$ equals the number of partitions of [4] into two blocks. There are seven, namely

$$\begin{array}{llll} \big\{\{1\},\{2,3,4\}\big\} & \big\{\{2\},\{1,3,4\}\big\} & \big\{\{3\},\{1,2,4\}\big\} & \big\{\{4\},\{1,2,3\}\big\} \\ \big\{\{1,2\},\{3,4\}\big\} & \big\{\{1,3\},\{2,4\}\big\} & \big\{\{1,4\},\{2,3\}\big\}, & \end{array}$$

so $S(4,2) = 7$.

Question 74 *Use complete enumeration to show that* $S(4,3) = 6$ *and* $S(4,4) = 1$. *Also, find* $S(3,k)$ *for* $k = 1,2,3$.

Bell numbers

We define $B(n)$ as the number of partitions of an n-set. This means partitions of *any* size. For example, $B(4) = 15$ because there are 15 partitions of [4], namely (using abbreviated form)

$$\begin{array}{lllll} \{1234\} & \{1,234\} & \{2,134\} & \{3,124\} & \{4,123\} \\ \{12,34\} & \{13,24\} & \{14,23\} & \{1,2,34\} & \{1,3,24\} \\ \{1,4,23\} & \{2,3,14\} & \{2,4,13\} & \{3,4,12\} & \{1,2,3,4\}. \end{array}$$

We could have done this without complete enumeration by just adding the Stirling numbers that we found earlier:

$$B(4) = S(4,1) + S(4,2) + S(4,3) + S(4,4) = 1 + 7 + 6 + 1 = 15.$$

Question 75 *Determine* $B(3)$.

The numbers $B(n)$ are called the ***Bell numbers***. Their relationship to the Stirling numbers of the second kind is

$$B(n) = \sum_{k=1}^{n} S(n,k) \qquad \text{for all } n \geqslant 1. \tag{2.6}$$

How about the formulas?

We have good formulas for calculating $(n)_k$, $\binom{n}{k}$, and $\left(\!\binom{n}{k}\!\right)$. The derivation of formulas for $S(n,k)$ and $B(n)$ represent more of a challenge and need more advanced techniques. In Section 3.1, we derive the formula

$$S(n,k) = \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} (-1)^j (k-j)^n.$$

In light of the relationship between the Bell and Stirling numbers shown in equation (2.6) it is then possible to get a formula for $B(n)$. But in Section 4.3 we prove the alternate

formula

$$B(n) = \frac{1}{e}\sum_{j=0}^{\infty}\frac{j^n}{j!}.$$

This is really a remarkable formula because it expresses the integer $B(n)$ that has a combinatorial interpretation as a product of the irrational number $\frac{1}{e}$ and an infinite series.

Question 76 *Find $S(7,3)$ and $B(5)$ using the formulas just given.*

Formulas for special cases

Instead of finding one all-purpose formula for $S(n,k)$, let's set our sights on finding formulas for some specific values of k. These formulas are

$$S(n,1) = S(n,n) = 1 \qquad S(n,2) = 2^{n-1} - 1 \qquad S(n,n-1) = \binom{n}{2}.$$

That $S(n,1) = 1$ and $S(n,n) = 1$ should be clear since the only way to partition an n-set into one block is to have one block consisting of the entire n-set, and the only way to partition an n-set into n blocks is to have each element in its own block.

To calculate $S(n,2)$, observe that the blocks in any 2-partition of $[n]$ consist of some nonempty subset of $[n]$ and its complement. This means we need to count sets of the form $\{A, A^c\}$ where both A and A^c are nonempty subsets of $[n]$.

First let's count the 2-lists (A, A^c) with the same properties. We may choose A from any of the $2^n - 2$ subsets of $[n]$ other than $\emptyset$ and $[n]$ itself. Then A^c is automatically determined, and moreover it is guaranteed to be nonempty. Therefore, there are $2^n - 2$ such 2-lists.

Now, consider two 2-lists equivalent if they represent the same partition of $[n]$. Each equivalence class has size 2, corresponding to the two ways the blocks may be ordered in the 2-list. By the equivalence principle, then, there are $(2^n - 2)/2 = 2^{n-1} - 1$ equivalence classes. Therefore $S(n,2) = 2^{n-1} - 1$.

Question 77 *Now, justify the formula $S(n,n-1) = \binom{n}{2}$.*

Combinatorial proofs

Stirling's triangle of the second kind

We first derive an identity for $S(n,k)$ that is similar to Pascal's identity (Theorem 2.2.1) for the binomial coefficients $\binom{n}{k}$. Examine the following illustration for the special case of $S(5,3)$. Any partition of [5] into three blocks must have element 5 either (1) in a block by itself, or (2) not in a block by itself. Here are the partitions of the first type using abbreviated notation:

$$\begin{array}{llll} \{5,1,234\} & \{5,2,134\} & \{5,3,124\} & \{5,4,123\} \\ \{5,12,34\} & \{5,13,24\} & \{5,14,23\} & \end{array}$$

But these are in one-to-one correspondence with the $S(4,2) = 7$ partitions of [4] into two blocks: removing the block $\{5\}$ from each partition results in a 2-partition of [4]. This operation is a bijection; it's illustrated in the top half of Figure 2.5.

To count the partitions of the second type, first choose one of the $S(4,3)$ partitions of [4] into three blocks. Next, choose one of the three blocks to contain the element 5. This guarantees that 5 will not be in a block by itself; moreover, each selection results in

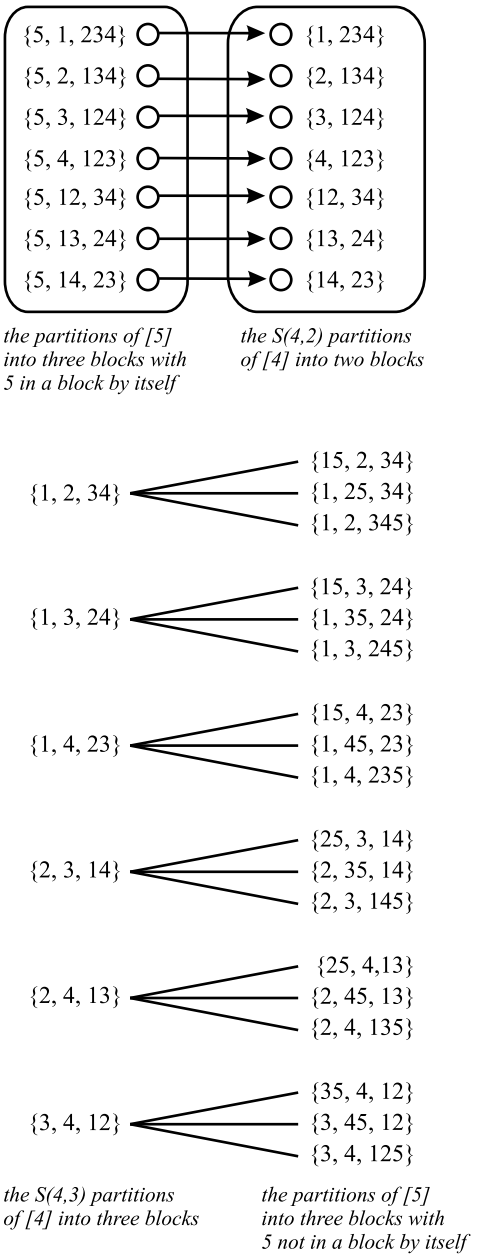


Figure 2.5. Counting partitions of [5] into three blocks.

a different partition. This operation is illustrated in the bottom half of Figure 2.5. By the product principle, there are $3 \cdot S(4,3)$ partitions of the second type.

The sum principle implies that there are $S(4,2) + 3 \cdot S(4,3)$ total partitions. We have proved the identity $S(5,3) = S(4,2) + 3 \cdot S(4,3)$. The following theorem uses this idea.

Theorem 2.3.1 *If $n \geq 1$ and $k \geq 1$, then*

$$S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k).$$

Combinatorial Proof: How many partitions of $[n]$ into k blocks are possible?

Answer 1: There are $S(n,k)$.

Answer 2: Condition on whether the element n is in a block by itself. If it is, then all such partitions can be constructed by first specifying a $(k-1)$-partition of $[n-1]$ and then adding the block $\{n\}$. There are $S(n-1,k-1)$ such partitions.

If n is not in a block by itself, then all such partitions can be constructed by first specifying a k-partition of $[n-1]$ and then putting n in one of the k blocks. By the product principle, there are $S(n-1,k)\cdot k$ such partitions.

Finally, by the sum principle, there are $S(n-1,k-1)+k\cdot S(n-1,k)$ total partitions.

■

This identity allows computation of ***Stirling's triangle of the second kind***, a triangular array of the nonzero numbers $S(n,k)$ for $0 \leqslant k \leqslant n$. Its first eight rows are as follows:

$n\downarrow\ k\rightarrow$	0	1	2	3	4	5	6	7
0	1							
1	0	1						
2	0	1	1					
3	0	1	3	1				
4	0	1	7	6	1			
5	0	1	15	25	10	1		
6	0	1	31	90	65	15	1	
7	0	1	63	301	350	140	21	1

(2.7)

The entry in row n and column k is $S(n,k)$. Its computation is similar to that in Pascal's triangle, but each entry equals its "northwestern" neighbor plus k times its "northern" neighbor, where k is the column index.

Question 78 *Using the identity of Theorem 2.3.1, what is the eighth (i.e., $n=8$) row of Stirling's triangle? What are the Bell numbers $B(5)$ and $B(6)$?*

Another identity involving Stirling numbers

To derive another identity, consider building a partition of $[n]$ into k blocks as follows. The element n must be in some block of the partition, so condition on the number of elements other than n in this block. If this number is j (where $0 \leqslant j \leqslant n-1$) we can specify those elements in $\binom{n-1}{j}$ ways. For each way to do this, we can partition the remaining $n-j-1$ elements into $k-1$ blocks in $S(n-j-1,k-1)$ ways. By the product principle there are $\binom{n-1}{j}S(n-j-1,k-1)$ partitions corresponding to that value of j. Summing over all j proves the following theorem.

Theorem 2.3.2 *If $n \geqslant 1$ and $k \geqslant 1$, then* $S(n,k)=\displaystyle\sum_{j=0}^{n-1}\binom{n-1}{j}S(n-j-1,k-1)$.

Question 79 *Use the theorem and Stirling's triangle to verify that $S(7,5)=140$.*

A Bell number identity

Applying the idea of the previous theorem results in an identity for the Bell numbers.

Theorem 2.3.3 *If $n \geqslant 1$, then* $B(n)=\displaystyle\sum_{j=0}^{n-1}\binom{n-1}{j}B(j)$.

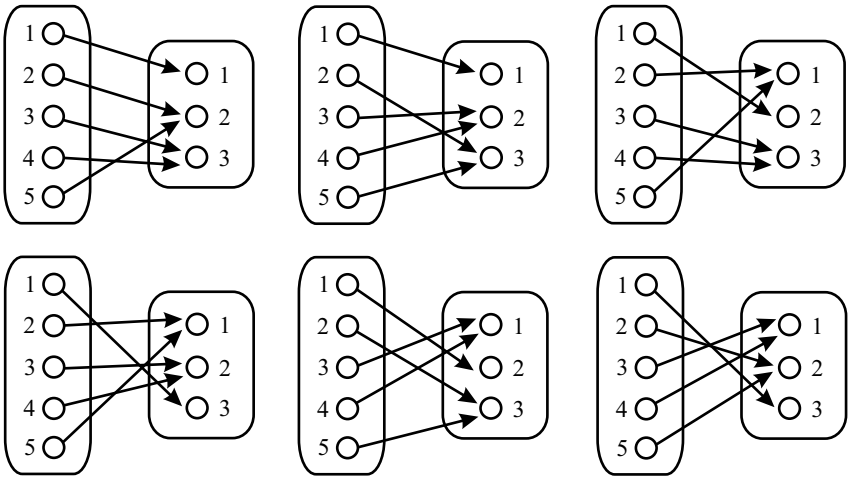


Figure 2.6. The 3! onto functions derived from the partition $\{\{1\},\{2,5\},\{3,4\}\}$.

Combinatorial proof: How many partitions of $[n]$ are there?

Answer 1: There are $B(n)$.

Answer 2: Arrange the partitions of $[n]$ into piles according to the number of elements that are *not* in n's block. Suppose that this number is j, where $0 \leqslant j \leqslant n-1$. There are $\binom{n-1}{j}$ ways to specify those j elements, and then $B(j)$ ways to specify a partition of the set of those j elements. The remaining elements go in the block with n. By the product principle there are $\binom{n-1}{j}B(j)$ partitions in this pile. Summing over all j produces the result. ■

Question 80 *Use Theorem 2.3.3 to calculate* $B(9)$.

Counting onto functions

With the Stirling numbers we can tie up a loose end from Section 2.1, namely that of a formula for the number of onto functions. We begin with the special case of counting onto functions $[5] \longrightarrow [3]$.

First, partition $[5]$ into three blocks in $S(5,3) = 25$ ways. Examine one such partition, say $\{1, 25, 34\}$. Build onto functions from this partition as follows: pick a value for $f(1)$ in three ways, then pick a common value for $f(2)$ and $f(5)$ in two ways, then pick a common value for $f(3)$ and $f(4)$ in one way. The $3! = 6$ functions derived from the partition appear in Figure 2.6. In this case, there are

$$S(5,3) \cdot 3! = 6 \cdot 25 = 150$$

onto functions $[5] \longrightarrow [3]$.

Question 81 *How many onto functions* $[7] \longrightarrow [4]$ *are there?*

In general, to count onto functions $[k] \longrightarrow [n]$, we first partition $[k]$ into n blocks in $S(k,n)$ ways. Then we assign a different output value to each of the n blocks in $n!$ ways. The product principle implies that there are $S(k,n) \cdot n!$ onto functions.

Theorem 2.3.4 *If* $k \geqslant 1$ *and* $n \geqslant 1$, *then the number of onto functions* $[k] \longrightarrow [n]$ *equals* $S(k,n) \cdot n!$.

Back to Distributions

We can now fill in all but the last line of our table of distribution problems. The number of distributions of k distinct objects to n distinct recipients such that each receives at least one equals the number of onto functions $[k] \longrightarrow [n]$, and this is $S(k,n) \cdot n!$.

There are $S(k,n)$ distributions of k distinct objects to n identical recipients such that each recipient receives at least one object. If we drop the requirement that each receives at least one object, then there are $\sum_{i=1}^{n} S(k,i)$ distributions. The other two answers in the third row are trivial. For example, consider distributing k distinct objects to n identical recipients such that each receives at most one object. If $k \leqslant n$ then this is possible but there is only one way to do it—throw each of the k balls in a different bin. If $k > n$ then it is not possible.

Distributions of		how many objects recipients can receive			
***k* objects**	**to *n* recipients**	no restrictions	$\leqslant 1$	$\geqslant 1$	$= 1$
distinct	distinct	n^k	$(n)_k$	$S(k,n) \cdot n!$	$n!$ or 0
identical	distinct	$\left(\!\binom{n}{k}\!\right)$	$\binom{n}{k}$	$\left(\!\binom{n}{k-n}\!\right)$	1 or 0
distinct	identical	$\sum_{i=1}^{n} S(k,i)$	1 or 0	$S(k,n)$	1 or 0
identical	identical	?	?	?	?

Summary

In this section we studied distributions of distinct objects to identical recipients. These are equivalent to set partitions, and the Stirling number of the second kind $S(n,k)$ equals the number of partitions of an n-set into k blocks. The related Bell number $B(n)$ equals the total number of partitions of an n set. We gave several examples of combinatorial proofs involving the Stirling and Bell numbers and we also found a formula for the number of onto functions in terms of the Stirling numbers.

Exercises

1. How many ways are there to arrange 20 different books into three piles? Into at most three piles? Get exact numerical answers.
2. For any integer $n \geqslant 2$, how many onto functions $[n] \longrightarrow [n-1]$ are possible? Give a formula that doesn't involve Stirling numbers.
3. How many onto functions $[8] \longrightarrow [5]$ are possible? Get an exact numerical answer.
4. How many onto functions $[9] \longrightarrow [7]$ have only one element mapped to 7? Get an exact numerical answer.
5. Call a function *almost onto* if it "misses" exactly one element of its codomain. (That is, $f : A \longrightarrow B$ is almost onto if there exists exactly one $b \in B$ for which $f^{-1}(b) = \emptyset$.) How many almost onto functions $[k] \longrightarrow [n]$ are possible?
6. How many partitions of $[10]$ have exactly one block of size five? Get an exact numerical answer.
7. Find the number of equivalence relations on an n-set.

8. Give a bijective proof: If $n \geq 1$, then $S(n,2) = 2^{n-1}-1$. Do so by creating a bijection between the 2-partitions of $[n]$ and the nonempty subsets of $[n-1]$.
9. Give a bijective proof: If $n \geq 1$, then $S(n,n-1) = \binom{n}{2}$. Do so by creating a bijection between the $(n-1)$-partitions of $[n]$ and the 2-subsets of $[n]$.
10. Let $f : A \longrightarrow B$ be a function. Prove that the set $\{f^{-1}(b) : b \in \text{rng}(f)\}$ is a partition of A. (Recall: $f^{-1}(b) = \{a \in A : f(a) = b\}$ is the inverse image of b.)
11. Give a combinatorial proof: If $n \geq 1$ and $k \geq 1$, then
$$S(n,k) = \sum_{i=0}^{n-1} \binom{n-1}{i} S(i,k-1).$$
12. Explain how
$$S(n,k) = S(n-2,k-2) + (2k-1)S(n-2,k-1) + k^2 S(n-2,k)$$
can be derived algebraically from the identity of Theorem 2.3.1. Then give a combinatorial proof.
13. Give a combinatorial proof: If $n \geq 1$ and $k \geq 1$, then
$$S(n,k) = \sum_{j=1}^{n} \binom{n-1}{j-1} S(n-j,k-1).$$
14. Here is a simple recursive C program for computing $S(n,k)$, based on Theorem 2.3.1. The program assumes $n, k \geq 0$.
```
unsigned long S(int n, int k)
{
   if (n == k) return 1;
   else if (n < k) return 0;
   else if (n > 0 && k == 0) return 0;
   else return S(n-1,k-1) + k*S(n-1,k);
}
```
It works, but it is extremely wasteful. Why? Design a more efficient algorithm.
15. Derive the formula $B(n) = \sum_{j=0}^{n-1} \binom{n-1}{j} B(j)$ algebraically from equation (2.6) and Exercise 11.
16. Prove that the infinite series $\displaystyle\sum_{j=0}^{\infty} \frac{j^n}{j!}$ converges, for any positive integer n. Then, explain why it converges to an irrational number.
17. (linear algebra) Solve a linear system to find numbers a, b, c, d, e so that the following polynomial equation is true:
$$x^4 = a \cdot (x)_0 + b \cdot (x)_1 + c \cdot (x)_2 + d \cdot (x)_3 + e \cdot (x)_4.$$
Here, $(x)_4 = x(x-1)(x-2)(x-3) = x^4 - 6x^3 + 11x^2 - 6x$ and $(x)_3 = x(x-1)(x-2) = x^3 - 3x^2 + 2x$, and so on, where $(x)_0 = 1$. Express the solution a, b, c, d, e in terms of numbers studied in this section.

18. (ordered distributions) This continues Exercise 16 of Section 2.1. Let S be an n-set. An ***ordered partition of S into k blocks*** is a partition of S into k blocks but where the order of the elements matters in each block. For example, $\{(4,1),(3,6,2),(5)\}$ is an ordered partition of [6] into 3 blocks. It is the same as $\{(3,6,2),(5),(4,1)\}$ but different than $\{(4,1),(3,2,6),(5)\}$. Also, $\{(4,1),(3,2,4,6),(5)\}$ is *not* a ordered partition of [6] because the blocks are not disjoint.

    Let $\beta(k,n)$ equal the number of ordered partitions of a k-set into n blocks.

    (a) Explain why $\beta(k,n)$ equals the number of ordered distributions of k distinct objects to n identical recipients such that each receives at least one object.

    (b) How many ordered distributions of k distinct objects to n identical recipients are there?

    (c) Prove that $\beta(k,n) = \frac{k!}{n!}\binom{k-1}{n-1}$.

19. (ordered distributions) Give combinatorial proofs of the following identities.

    (a) $\beta(k,n) = \binom{k}{n}(k-1)_{k-n}$

    (b) $\beta(k,n) = \beta(k-1,n-1) + (k+n-1)\cdot\beta(k-1,n)$

Travel Notes

James Stirling (1692–1770) first studied the numbers $S(k,n)$ though not in the context of set partitions. Stirling's interest was in the algebraic rather than combinatorial properties of the numbers and we explore some of these properties in Section 4.3. The name "Stirling numbers of the second kind" suggests that there are Stirling numbers of the first kind. We shall also see these in Section 4.3. Stirling is well-known for the following result he produced in 1730 known as ***Stirling's approximation*** or ***Stirling's formula***:

$$n! \approx n^n e^{-n}\sqrt{2\pi n}.$$

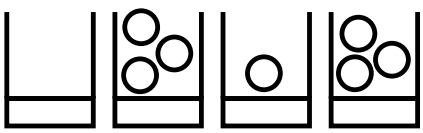
The Bell numbers are named in honor of Eric Temple Bell (1883–1960) who called them the "exponential numbers."

2.4 Counting integer partitions

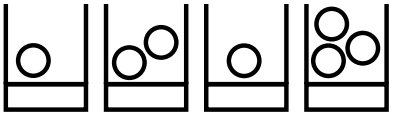
The last type of distribution problem we study is that of distributing identical objects to identical recipients. Among the 16 different types of distribution problems that we consider, these are the hardest for which to obtain closed-form formulas. Such distributions correspond to a different kind of partition than we studied in the last section, namely a partition of an integer. In this section we'll study some combinatorial properties of the integer partition numbers. In Section 4.4 we'll visit them again.

Integer partitions as distributions

Here is a distribution of seven identical objects to four identical recipients.



We can record this as the multiset $\{1, 3, 3\}$. Notice that it doesn't matter the order in which we list the elements because both the objects and recipients are identical. Here is a distribution of seven identical objects to four identical recipients such that each receives at least one object.



This corresponds to the multiset $\{1, 1, 2, 3\}$.

In either distribution, the corresponding multiset consists of positive integers which sum to 7. Given positive integers n and k, a ***partition of*** n ***into*** k ***parts*** is a k-multiset of positive integers that sum to n. The elements of the multiset are the ***parts*** of the partition. Therefore $\{1, 3, 3\}$ is a partition of 7 into three parts and $\{1, 1, 2, 3\}$ is a partition of 7 into four parts. It is customary and convenient to write these as

$$3 + 3 + 1 \qquad \text{and} \qquad 3 + 2 + 1 + 1$$

to emphasize that the sum of the parts equals the integer being partitioned. Generally the parts are arranged in nonincreasing order from left to right but this is not necessary. For example, $3 + 3 + 1$ and $3 + 1 + 3$ and $1 + 3 + 3$ all represent the same partition of 7 into three parts.

Question 82 *Give five different partitions of 10 into four parts.*

It is common to refer to both set partitions and integer partitions as simply partitions since the type should be clear from context.

Integer partition numbers

To count integer partitions, we define $P(n, k)$ as the number of partitions of the integer n into k parts. Based on our observations about distributions earlier,

> *$P(n, k)$ equals (1) the number of partitions of n into k parts; and (2) the number of distributions of n identical objects to k identical recipients such that each receives at least one object.*

Note that the number of distributions of k identical objects to n identical recipients such that each receives at least one object is $P(k, n)$ not $P(n, k)$. We define $P(0, 0) = 1$.

Question 83 *Using partitions or distributions (your choice), explain why $P(0, k) = 0$ for $k \geqslant 1$ and $P(n, 0) = 0$ for $n \geqslant 1$.*

Another method used to record a partition is as a type vector. For example, the type vector of the partition $6 + 5 + 4 + 3 + 3$ of the integer 21 is

$$\left[1^0\, 2^0\, 3^2\, 4^1\, 5^1\, 6^1\right].$$

In general, the ***type vector*** $[1^{p_1}\, 2^{p_2} \cdots m^{p_m}]$ corresponds to the partition that has p_1 parts of size 1, p_2 parts of size 2, and so forth. (The exponents indicate repeated addition rather than multiplication!) The integer being partitioned is $\sum_{j=1}^{m} j \cdot p_j$ and the number of parts in the partition is $\sum_{j=1}^{m} p_j$. It is customary to make the type vector only as long as the largest part in the partition, say m, or else as long as the integer being partitioned.

Question 84 *For the type vector $[1^5\, 2^1\, 3^0\, 4^2\, 5^0\, 6^0\, 7^3]$, what integer is being partitioned? How many parts are in this partition?*

Integer partition numbers by complete enumeration

Let's compute $P(6,k)$ for $k = 1,2,3,4,5,6$. Here are all the partitions of 6 into k parts for $k = 1,2,3,4$:

$k=1$	$k=2$	$k=3$	$k=4$
6	$5+1$	$4+1+1$	$3+1+1+1$
	$4+2$	$3+2+1$	$2+2+1+1$
	$3+3$	$2+2+2$	

Therefore $P(6,1) = 1$, $P(6,2) = P(6,3) = 3$, and $P(6,4) = 2$. The only partition of 6 into five parts is $2+1+1+1+1$ and the only partition of 6 into six parts is $1+1+1+1+1+1$, so $P(6,5) = P(6,6) = 1$. Notice that there is no relation between the number of partitions of the integer 6 into two parts (which is 3) and the number of partitions of the set [6] into two parts (which is $S(6,2) = 31$).

Question 85 *Find $P(7,k)$ for $k = 1,2,3,4,5,6,7$ by complete enumeration.*

All partitions of an integer

We define $P(n)$ to be the number of partitions of the integer n. This means partitions of *any* size. For example, we can find $P(6)$ as follows:

$$\begin{aligned} P(6) &= P(6,1) + P(6,2) + P(6,3) + P(6,4) + P(6,5) + P(6,6) \\ &= 1 + 3 + 3 + 2 + 1 + 1, \end{aligned}$$

so $P(6) = 11$. In general, we have

$$P(n) = \sum_{k=1}^{n} P(n,k) \qquad \text{for all } n \geqslant 1. \tag{2.8}$$

Question 86 *What is $P(7)$?*

How about the formulas?

Formulas for $P(n,k)$ or $P(n)$ are much harder to come by than those for $S(n,k)$ or $B(n)$. In Section 4.4 we will prove that $P(n,3)$ equals the closest integer to $n^2/12$. Formulas for $P(n,4)$ and $P(n,5)$ are possible but more difficult to derive. Many of the known results about $P(n,k)$ or $P(n)$ involve bounds or asymptotic formulas.

Formulas for special cases

First we observe that $P(n,1) = P(n,n-1) = P(n,n) = 1$.

Question 87 *Give a brief justification.*

For $P(n,2)$ let's look at the partitions of n into two parts for $n = 6,7,8,9,10,11$:

$n=6$	$n=7$	$n=8$	$n=9$	$n=10$	$n=11$
$5+1$	$6+1$	$7+1$	$8+1$	$9+1$	$10+1$
$4+2$	$5+2$	$6+2$	$7+2$	$8+2$	$9+2$
$3+3$	$4+3$	$5+3$	$6+3$	$7+3$	$8+3$
		$4+4$	$5+4$	$6+4$	$7+4$
				$5+5$	$6+5$

This suggests that $P(n,2)$ is about $n/2$. More precisely, we have

$$P(n,2) = \left\lfloor \frac{n}{2} \right\rfloor.$$

Combinatorial proofs

Like the Stirling numbers of the second kind $S(n,k)$, the numbers $P(n,k)$ satisfy many identities supported by interesting combinatorial or bijective proofs.

One Identity

Consider the partitions of n into k parts. Each partition either has (1) its smallest part equal to 1, or else (2) its smallest part equal to some number greater than 1. By counting the partitions of each type and adding we can prove an identity involving $P(n,k)$.

For example, consider the $P(10,3)$ partitions of 10 into three parts. Among the four partitions with smallest part equal to 1, we can delete one of the 1s to obtain a partition of 9 into two parts. This operation is a bijection, as follows.

$$\begin{aligned} 8+1+1 &\longrightarrow 8+1 \\ 7+2+1 &\longrightarrow 7+2 \\ 6+3+1 &\longrightarrow 6+3 \\ 5+4+1 &\longrightarrow 5+4 \end{aligned}$$

There are $P(9,2)$ such partitions. On the other hand, if the smallest part is at least 2, we can subtract 1 from each part to obtain a partition of $10-3=7$ into three parts. Again, this operation is a bijection and is illustrated below.

$$\begin{aligned} 6+2+2 &\longrightarrow 5+1+1 \\ 5+3+2 &\longrightarrow 4+2+1 \\ 4+4+2 &\longrightarrow 3+3+1 \\ 4+3+3 &\longrightarrow 3+2+2 \end{aligned}$$

There are $P(7,3)$ such partitions. We have proved that $P(10,3) = P(9,2) + P(7,3)$. The following theorem gives the general result.

Theorem 2.4.1 *If $n \geq 1$ and $k \geq 1$, then $P(n,k) = P(n-1,k-1) + P(n-k,k)$.*

Combinatorial proof: How many partitions of n into k parts are there?

Answer 1: There are $P(n,k)$.

Answer 2: Each partition has either (1) smallest part equal to 1, or (2) smallest part at least 2. For those of the first type, deleting a part of size 1 leaves a partition of $n-1$ into $k-1$ parts. This is a bijection, so there are $P(n-1,k-1)$ such partitions. For those of the second type, subtracting 1 from each part leaves a partition of $n-k$ into k parts, for no part vanishes if each originally had size at least 2. This is also a bijection, so there are $P(n-k,k)$ partitions of the second type. In total there are $P(n-1,k-1) + P(n-k,k)$ partitions. ■

For example, we can use our earlier work to calculate

$$P(7,3) = P(6,2) + P(4,3) = 3 + 1 = 4$$

and

$$P(7,4) = P(6,3) + P(3,4) = 3 + 0 = 3.$$

Question 88 *Using the identity, what is $P(9,3)$? What is $P(9,4)$?*

A related identity

The inspiration for another identity comes from this observation: given a partition of n into k parts, if we subtract 1 from each part then a partition of $n-k$ into *at most* k parts remains.

For example, consider subtracting 1 from each of the $P(10,3) = 8$ partitions of 10 into three parts, and ignore resulting "parts" of size 0. The correspondence is illustrated below.

$$\begin{array}{lcl} 8+1+1 & \longrightarrow & 7 \\ 7+2+1 & \longrightarrow & 6+1 \\ 6+3+1 & \longrightarrow & 5+2 \\ 6+2+2 & \longrightarrow & 5+1+1 \\ 5+4+1 & \longrightarrow & 4+3 \\ 5+3+2 & \longrightarrow & 4+2+1 \\ 4+4+2 & \longrightarrow & 3+3+1 \\ 4+3+3 & \longrightarrow & 3+2+2 \end{array}$$

On the right appear partitions of 7 into at most three parts. In fact, all such partitions appear: there are $P(7,1) + P(7,2) + P(7,3)$ of them. We have shown that

$$P(10,3) = P(7,1) + P(7,2) + P(7,3).$$

Now for the theorem.

Theorem 2.4.2 *If $n \geqslant 1$ and $k \geqslant 1$, then* $P(n,k) = \sum_{j=1}^{k} P(n-k, j)$.

Bijective proof: Define a function from the set of partitions of n into k parts and the set of partitions of $n-k$ into at most k parts by the operation: subtract 1 from each part and ignore any resulting "parts" of 0. This function is a bijection, hence the two sets have the same size by the bijection principle. The first set has size $P(n,k)$ and the second has size

$$P(n-k,1) + P(n-k,2) + \cdots + P(n-k,k) = \sum_{j=1}^{k} P(n-k, j)$$

by the sum principle. ■

Question 89 *Compute $P(9,3)$ using the theorem and previous work.*

The theorem allows for calculation of a partition number triangle as shown below.

$n\downarrow\ k\rightarrow$	0	1	2	3	4	5	6	7	8
0	1								
1	0	1							
2	0	1	1						
3	0	1	1	1					
4	0	1	2	1	1				
5	0	1	2	2	1	1			
6	0	1	3	3	2	1	1		
7	0	1	3	4	3	2	1	1	
8	0	1	4	5	5	3	2	1	1

The entry in row n and column k is $P(n,k)$.

It is also possible to derive algebraically the identity of Theorem 2.4.1 from that of Theorem 2.4.2. That is,

$$\begin{aligned} P(n,k) - P(n-1,k-1) &= \sum_{j=1}^{k} P(n-k,j) - \sum_{j=1}^{k-1} P\big((n-1)-(k-1),j\big) \\ &= \sum_{j=1}^{k} P(n-k,j) - \sum_{j=1}^{k-1} P(n-k,j) \\ &= P(n-k,k), \end{aligned}$$

and so $P(n,k) = P(n-1,k-1) + P(n-k,k)$.

Using type vectors

The type vector concept can help make a bijective proof rigorous. In the following theorem, the bijection is the function that adds a part of size 1 to the partition.

Theorem 2.4.3 *If $n \geqslant 1$, then the number of partitions of n equals the number of partitions of $n+1$ having smallest part 1.*

Bijective proof: Define A as the set of partitions of n and B as the set of partitions of $n+1$ with smallest part 1. Define the function $f : A \longrightarrow B$ by

$$f\left(\left[1^{p_1}\, 2^{p_2} \cdots n^{p_n}\right]\right) = \left[1^{p_1+1}\, 2^{p_2} \cdots n^{p_n}\right].$$

That is, f takes a partition of n and adds a part of size 1.

One-to-one: Let $\left[1^{p_1}\, 2^{p_2} \cdots n^{p_n}\right]$ and $\left[1^{q_1}\, 2^{q_2} \cdots n^{q_n}\right]$ be partitions in A, and assume that

$$f\left(\left[1^{p_1}\, 2^{p_2} \cdots n^{p_n}\right]\right) = f\left(\left[1^{q_1}\, 2^{q_2} \cdots n^{q_n}\right]\right).$$

This means that $\left[1^{p_1+1}\, 2^{p_2} \cdots n^{p_n}\right] = \left[1^{q_1+1}\, 2^{q_2} \cdots n^{q_n}\right]$ and hence (equate the exponents) that $p_i = q_i$ for all i. Therefore $\left[1^{p_1}\, 2^{p_2} \cdots n^{p_n}\right] = \left[1^{q_1}\, 2^{q_2} \cdots n^{q_n}\right]$.

Onto: Let $\left[1^{q_1}\, 2^{q_2} \cdots n^{q_n}\right]$ be in B. Notice that it is a partition of $n+1$ with at least one part of size 1, so it can't have any parts of size $n+1$. (That is, we are justified in stopping the type vector at n^{q_n}.) Since $q_1 \geqslant 1$, the type vector $\left[1^{q_1-1}\, 2^{q_2} \cdots n^{q_n}\right]$ corresponds to a partition of n, so it is in A. Moreover

$$f\left(\left[1^{q_1-1}\, 2^{q_2} \cdots n^{q_n}\right]\right) = \left[1^{(q_1-1)+1}\, 2^{q_2} \cdots n^{q_n}\right] = \left[1^{q_1}\, 2^{q_2} \cdots n^{q_n}\right],$$

so f is onto. ■

Back to distributions

We can now complete our table of distribution problems. There are $P(k,n)$ distributions of k identical objects to n identical recipients such that each receives at least one object. If we drop the "at least one object" requirement, then there are $\sum_{i=1}^{n} P(k,i)$ distributions. The remaining two distributions in the last row are trivial.

Distributions of		how many objects recipients can receive			
***k* objects**	**to *n* recipients**	no restrictions	$\leqslant 1$	$\geqslant 1$	$= 1$
distinct	distinct	n^k	$(n)_k$	$S(k,n)\cdot n!$	$n!$ or 0
identical	distinct	$\left(\!\binom{n}{k}\!\right)$	$\binom{n}{k}$	$\left(\!\binom{n}{k-n}\!\right)$	1 or 0
distinct	identical	$\sum_{i=1}^{n} S(k,i)$	1 or 0	$S(k,n)$	1 or 0
identical	identical	$\sum_{i=1}^{n} P(k,i)$	1 or 0	$P(k,n)$	1 or 0

Summary

In this section we completed our classification and study of distribution problems by considering distributions of identical objects to identical recipients. These are counted with the integer partition numbers. The number $P(n,k)$ equals the number of partitions of the integer n into k parts, where such a partition is a multiset of k positive integers that sum to n. A closed-form formula for $P(n,k)$ is difficult to obtain but we found formulas for special cases and used combinatorial proofs to establish some identities.

Exercises

1. You have 40 pieces of candy to distribute among 10 children. Find the number of ways to do this in each of the following situations. Leave your answers in standard notation.
   (a) The pieces of candy are different and each child gets at least one piece.
   (b) The pieces of candy are indistinguishable and each child can get any number of pieces.
   (c) The pieces of candy are different but you distribute them among 10 indistinguishable paper bags.
   (d) The pieces of candy are indistinguishable but you distribute them among 10 indistinguishable paper bags and each bag contains at least one piece.
   (e) The pieces of candy are different and each child gets exactly one piece, so there are some pieces left over.
   (f) The pieces of candy are different and Frank receives four pieces.
2. Use type vectors to establish the bijection (mentioned in the proof of Theorem 2.4.1) between partitions of n into k parts with smallest part equal to 1 and partitions of $n-1$ into $k-1$ parts.
3. Use type vectors to establish the bijection (mentioned in the proof of Theorem 2.4.1) between partitions of n into k parts with smallest part at least 2 and partitions of $n-k$ into k parts.
4. Use type vectors to establish the bijection in Theorem 2.4.2.
5. Find and prove a formula for $P(n,n-2)$, for $n \geqslant 3$.
6. Explain how to algebraically derive the identity $P(n,2) = \lfloor \frac{n}{2} \rfloor$ from the identity of Theorem 2.4.1.
7. Under what conditions on n and k is the statement $P(n,k) = P(n-1,k-1)$ true?

8. Give a bijective proof of the following: The number of partitions of n is equal to the number of partitions of $2n$ into n parts.
9. We showed how to use Theorem 2.4.2 to prove Theorem 2.4.1. Now use Theorem 2.4.1 to prove Theorem 2.4.2.
10. Prove using type vectors: The number of partitions of n into k parts is equal to the number of partitions of n with largest part equal to k.
11. What counting question does $P(n) - P(n-1)$ answer?
12. Prove that $P(n+2) + P(n) \geqslant 2P(n+1)$.
13. Let $Q(n,k)$ denote the number of partitions of n into k distinct parts. For example, $Q(8,3) = 2$ because the relevant partitions are $5+2+1$ and $4+3+1$.
    (a) Derive and prove an identity for $Q(n,k)$, similar to that of Theorem 2.4.1 on page 78.
    (b) Compute $Q(n,k)$ for $0 \leqslant n,k \leqslant 8$ using the identity of part (a).
    (c) Derive and prove a formula for $P(n,k)$ in terms of the numbers $Q(\cdot,\cdot)$.

Travel Notes

As with many areas of mathematics, some of the first important results can be traced back to Leonhard Euler (1707-1783). Euler's famous 1740 proof that the number of partitions of n into distinct parts equals the number of partitions of n into odd parts established integer partitions as worthy of study. More importantly, however, Euler essentially invented the concept of generating function while doing so. We will study generating functions in Chapter 3 and they are one of the most important tools in combinatorics. We present Euler's proof in Section 3.4. See Dunham (1999) for an exciting account of Euler's discovery.

Ferrer's diagrams are useful visual representations of integer partitions. We explore them in Section 4.4.

CHAPTER 3

Algebraic Tools

In this chapter we cover three important tools: inclusion-exclusion, mathematical induction, and generating functions. We call these algebraic tools because, in contrast with combinatorial or bijective methods of proof, they can reduce a combinatorial problem to a relatively routine algebraic calculation.

3.1 Inclusion-exclusion

The principle of inclusion-exclusion is the big brother of set-union formulas like

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

and

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| = {} & |A_1| + |A_2| + |A_3| \\ & - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ & + |A_1 \cap A_2 \cap A_3|. \end{aligned}$$

In this section we show how to apply inclusion-exclusion to some classic combinatorial problems—counting divisors, counting so-called "derangements," and counting onto functions—that are difficult to handle with the tools we've learned so far.

Framework for inclusion-exclusion

Any use of inclusion-exclusion needs, implicitly or explicitly, two things: a universe of objects and a set of properties. The universe of objects, denoted $\mathcal{U}$, is really just a set. The term "universe" suggests that it typically contains more than just those objects we wish to count. The set of properties, denoted P, describes traits that the objects in the universe may or may not possess. If there are n properties, we usually write $P = \{p_1, p_2, \ldots, p_n\}$ to indicate the set of properties.

A typical application of inclusion-exclusion involves the question, "How many objects in the universe have none of the properties?" The following examples should help you understand both the types of questions to which inclusion-exclusion naturally applies and also how to define the universe and properties. We will solve these examples in parallel during the course of this section.

Example: counting integers in [100] not divisible by 2, 3, or 5

How many integers in [100] are not divisible by 2, 3, or 5?

A complete enumeration appears time-consuming. You could write the integers from 1 to 100, cross off all the multiples of 2, 3, and 5, and then count those remaining. Doable, but perhaps not efficient.

Define the universe as [100], and the properties as those traits we wish to avoid:

$$\begin{aligned}\mathcal{U} &:= [100]\\ d_2 &:= \text{“the integer is divisible by 2”}\\ d_3 &:= \text{“the integer is divisible by 3”}\\ d_5 &:= \text{“the integer is divisible by 5.”}\end{aligned}$$

The number of integers not divisible by 2, 3, or 5 then equals the number of integers in $\mathcal{U}$ that have *none* of the three properties.

Question 90 *How many integers in $\mathcal{U}$ have property d_2 (and possibly others)? How many have both properties d_3 and d_5 (and possibly d_2)?*

Example: counting ciphers

In coding theory, a *monoalphabetic substitution cipher* creates a coded message by replacing each character of the original message with a unique alternate character in order to obtain the coded message. For example, if the cipher is

```
Original letter: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 Encoded letter: W X B D A H J K P R Y Z M L F I S Q C U E G O N V T
```

then `MEET ME AT MIDNIGHT` is encoded as `MAAU MA WU MPDLPJKU`. The permutation (`W`, `X`, `B`, ..., `V`, `T`) of the 26 letters `A`–`Z` does a good job of storing this cipher.

In such a cipher, it might be desirable to have no letter “fixed,” i.e., replaced by itself. The above cipher does not have such a property because both `D` and `M` are fixed. How many monoalphabetic substitution ciphers are possible in which no letter is fixed?

Define the universe and properties as follows:

$$\begin{aligned}\mathcal{U} &:= \text{set of all possible permutations of the letters } \texttt{A}\text{–}\texttt{Z}\\ f_{\texttt{A}} &:= \text{“the permutation fixes the letter } \texttt{A}\text{”}\\ f_{\texttt{B}} &:= \text{“the permutation fixes the letter } \texttt{B}\text{”}\\ &\vdots\\ f_{\texttt{Z}} &:= \text{“the permutation fixes the letter } \texttt{Z}\text{.”}\end{aligned}$$

The number of ciphers with no letters fixed then equals the number of permutations in $\mathcal{U}$ that have *none* of the 26 properties.

Question 91 *What is the size of $\mathcal{U}$? How many permutations leave the letters `D` and `M` fixed (and possibly others)?*

Example: counting onto functions $[k] \longrightarrow [n]$

How many onto functions $[k] \longrightarrow [n]$ are possible? We know that an onto function f does not “miss” any of the elements in the codomain $[n]$. That is, no matter what $j \in [n]$ we pick, there is always at least one $i \in [k]$ for which $f(i) = j$.

To count onto functions, define the universe and properties as such:

$$\begin{aligned}
\mathcal{U} &:= \text{set of all possible functions } [k] \longrightarrow [n] \\
m_1 &:= \text{“the function misses element } 1 \in [n]\text{”} \\
m_2 &:= \text{“the function misses element } 2 \in [n]\text{”} \\
&\vdots \\
m_n &:= \text{“the function misses element } n \in [n].\text{”}
\end{aligned}$$

The number of onto functions $[k] \longrightarrow [n]$ then equals the number of functions in $\mathcal{U}$ that have *none* of the n properties.

Question 92 *What is the size of $\mathcal{U}$? How many functions miss elements 1, 2, and 3 (and possibly others)?*

In each of these examples you should make note of two things. One, the universe contains more objects than we wish to count. Two, the properties describe features that the objects we wish to count *do not* possess.

The functions $N_{\geqslant}(J)$ and $N_{=}(J)$

Now that we can put counting problems in the inclusion-exclusion framework, we examine how to answer them. The key is to be able to count the objects that possess any given subset of properties.

In Question 90, you counted the integers in [100] that are divisible by 2. There are $\lfloor \frac{100}{2} \rfloor = 50$ of them, namely

$$2, 4, 6, 8, 10, 12, \ldots, 98, 100.$$

Some of those integers are also divisible by 3 or 5 or both, and so they satisfy additional properties. We needn't worry about this, though, since we only wanted to count those with property d_2 *and possibly others*. Similarly, there are $\lfloor \frac{100}{3 \cdot 5} \rfloor = 6$ integers that are divisible by both 3 and 5, namely

$$15, 30, 45, 60, 75, 90.$$

Again, some are also divisible by 2 but that is of no concern.

Question 93 *How many are divisible by 2 and 5? By 2, 3, and 5?*

In Question 91, you counted the ciphers that leave at least the letters `D` and `M` fixed. Your answer should have been 24!, because with those two letters fixed any permutation of the remaining 24 letters will possess both property $f_{\mathtt{D}}$ and property $f_{\mathtt{M}}$. Of course, some of those 24! ciphers will fix other letters and thus possess additional properties. The crucial point is that we have counted the ciphers that leave `D` and `M` fixed *and possibly others*.

Question 94 *Suppose you're given a j-subset of the letters `A-Z`. How many ciphers leave at least those j letters fixed?*

In Question 92, you counted the onto functions that miss at least elements 1, 2, and 3 of $[n]$. Your answer should have been $(n-3)^k$ because any function from $[k]$ to $\{4, 5, \ldots, n\}$ will miss elements 1, 2, and 3. Some of those $(n-3)^k$ functions miss other elements of $[n]$, but again we counted the functions that miss *at least* elements 1, 2, and 3.

Question 95 *Suppose you're given a j-subset of $[n]$. How many functions miss at least those j elements?*

In these examples, the phrase "at least" makes a terribly important difference. If we wanted to count the functions that miss *exactly* elements 1, 2, and 3, we would need to count onto functions $[k] \longrightarrow \{4, 5, \ldots, n\}$. But that is just as hard as our original question of counting onto functions $[k] \longrightarrow [n]$! A similar comment applies to the other two examples.

We now define counting functions to handle the "at least" and "exactly" ideas.

Definition 3.1.1 *Let $\mathcal{U}$ be a universe of objects and let P be a set of properties that the objects may or may not have. For any subset J of P, define the following expressions:*

- $N_{\geqslant}(J)$ *equals the number of objects in $\mathcal{U}$ that have the properties in J and* possibly others*, and*
- $N_{=}(J)$ *equals the number of objects in $\mathcal{U}$ that have the properties in J and* no others.

Of course, the "$\geqslant$" suggests "at least" and "=" suggests "exactly."

We have already computed some values of the $N_{\geqslant}$ function in our three examples, namely

$$\begin{aligned} N_{\geqslant}\Big(\{d_2\}\Big) &= 50 && \text{counting integers example,} \\ N_{\geqslant}\Big(\{f_{\mathrm{D}}, f_{\mathrm{M}}\}\Big) &= 24! && \text{cipher example,} \\ N_{\geqslant}\Big(\{m_1, m_2, m_3\}\Big) &= (n-3)^k && \text{onto function example.} \end{aligned}$$

From now on, write these as $N_{\geqslant}(d_2)$, $N_{\geqslant}(f_{\mathrm{D}} f_{\mathrm{M}})$, and $N_{\geqslant}(m_1 m_2 m_3)$ to streamline the notation. In all three examples we seek the number of objects with none of the properties, otherwise known as $N_{=}(\emptyset)$.

Question 96 *What is $N_{\geqslant}(\emptyset)$, in any inclusion-exclusion problem?*

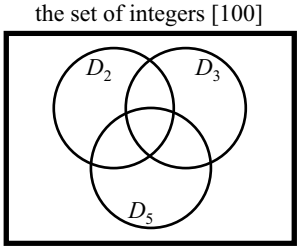
The idea behind the inclusion-exclusion formula

The inclusion-exclusion formula, which we now derive, is nothing more than the same accounting trick you have seen in counting the size of a union of two or three sets using a Venn diagram. Those formulas appeared at the beginning of this section.

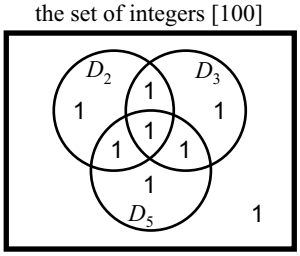
To illustrate the idea, return to the example of counting the integers in [100] not divisible by 2, 3, or 5. Here are the subsets of [100] described by the three properties:

$$\begin{aligned} D_2 &:= \{2, 4, 6, 8, 10, \ldots, 100\} \\ D_3 &:= \{3, 6, 9, 12, 15, \ldots, 99\} \\ D_5 &:= \{5, 10, 15, 20, 25, \ldots, 100\}. \end{aligned}$$

The reason for the capital D_i is to distinguish the actual sets from the properties d_i that describe them. Here are the sets in a Venn diagram:



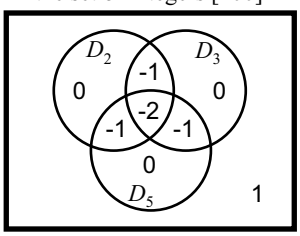
Our goal (remember!) is to count the integers in none of the sets, using the $N_{\geqslant}(\cdot)$ values. Begin by including in the count everything in [100], which $N_{\geqslant}(\emptyset)$ does for us:



$N_{\geqslant}(\emptyset)$

The 1s indicate we have counted each integer in the eight disjoint regions of the Venn diagram exactly once. We have included too much since our goal is to get a 1 in the region outside the circles (which contains the integers in [100] that have none of the properties) and 0s in the other seven regions (each of which contains integers that have at least one of the properties).

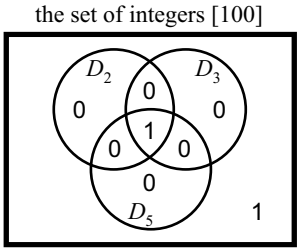
To remedy this over-count, exclude the integers with property d_2, with d_3, and with d_5. Subtracting each of $N_{\geqslant}(d_2)$, $N_{\geqslant}(d_3)$, and $N_{\geqslant}(d_5)$ accomplishes this:



$N_{\geqslant}(\emptyset) - (N_{\geqslant}(d_2) + N_{\geqslant}(d_3) + N_{\geqslant}(d_5))$

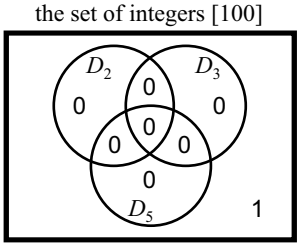
We're getting there, but we have "counted -1 times" (in a net sense) those integers with exactly two of the properties. Worse, we have "counted -2 times" those integers with all three properties. The -2 comes from the $+1$ contributed by $N_{\geqslant}(\emptyset)$ and the three -1s contributed by subtracting $N_{\geqslant}(d_2)$, $N_{\geqslant}(d_3)$, and $N_{\geqslant}(d_5)$.

Now include the integers that share any two of the properties, which adding each of $N_{\geqslant}(d_2d_3)$, $N_{\geqslant}(d_3d_5)$, and $N_{\geqslant}(d_2d_5)$ accomplishes:



$N_{\geqslant}(\emptyset) - (N_{\geqslant}(d_2) + N_{\geqslant}(d_3) + N_{\geqslant}(d_5)) + (N_{\geqslant}(d_2d_3) + N_{\geqslant}(d_3d_5) + N_{\geqslant}(d_2d_5))$

Make the final adjustment by subtracting $N_{\geqslant}(d_2d_3d_5)$:



$N_{\geqslant}(\emptyset) - (N_{\geqslant}(d_2) + N_{\geqslant}(d_3) + N_{\geqslant}(d_5)) + (N_{\geqslant}(d_2d_3) + N_{\geqslant}(d_3d_5) + N_{\geqslant}(d_2d_5)) - N_{\geqslant}(d_2d_3d_5)$

We accomplished our goal and in doing so proved the formula

$$\begin{aligned} N_{=}(\emptyset) = N_{\geqslant}(\emptyset) &- \Big(N_{\geqslant}(d_2) + N_{\geqslant}(d_3) + N_{\geqslant}(d_5)\Big) \\ &+ \Big(N_{\geqslant}(d_2d_3) + N_{\geqslant}(d_3d_5) + N_{\geqslant}(d_2d_5)\Big) - N_{\geqslant}(d_2d_3d_5). \end{aligned} \tag{3.1}$$

Notice that there are eight terms, one for each possible subset of $P = \{d_2, d_3, d_5\}$. In addition, those terms corresponding to even-sized subsets are positive and those corresponding to odd-sized subsets are negative.

Finishing the first example

To finish the example we just need the eight values of $N_{\geqslant}(\cdot)$. Some of these you have already computed in Question 90.

$$N_{\geqslant}(\emptyset) = 100 \qquad N_{\geqslant}(d_2d_3) = \left\lfloor \frac{100}{2 \cdot 3} \right\rfloor = 16$$

$$N_{\geqslant}(d_2) = \left\lfloor \frac{100}{2} \right\rfloor = 50 \qquad N_{\geqslant}(d_3d_5) = \left\lfloor \frac{100}{3 \cdot 5} \right\rfloor = 6$$

$$N_{\geqslant}(d_3) = \left\lfloor \frac{100}{3} \right\rfloor = 33 \qquad N_{\geqslant}(d_2d_5) = \left\lfloor \frac{100}{2 \cdot 5} \right\rfloor = 10$$

$$N_{\geqslant}(d_5) = \left\lfloor \frac{100}{5} \right\rfloor = 20 \qquad N_{\geqslant}(d_2d_3d_5) = \left\lfloor \frac{100}{2 \cdot 3 \cdot 5} \right\rfloor = 3$$

The answer is $100 - (50 + 33 + 20) + (16 + 6 + 10) - 3 = 26$.

Proof of the inclusion-exclusion formula

Before completing the other two examples, we prove an inclusion-exclusion formula which generalizes the formula we derived with the aid of the Venn diagram. The only surprise in the proof comes when the sum in the following Question appears.

Question 97 *Find the value of* $\displaystyle\sum_{j=0}^{m} \binom{m}{j} (-1)^j$. *(Hint: binomial theorem)*

Before proving the general version of the principle we address a matter of notation. The sum that appears in the inclusion-exclusion formula is a *subset sum*. Writing $\sum_{J:J\subseteq P}$ means that the sum is over all possible subsets J of the set P, from the empty set to P itself. For example, the right-hand side of equation (3.1) can be written

$$\sum_{J:J\subseteq P} (-1)^{|J|} N_{\geqslant}(J)$$

where $P = \{d_2, d_3, d_5\}$ is the set of properties.

Theorem 3.1.2 (basic principle of inclusion-exclusion) *Let $\mathcal{U}$ be a universe of objects and let P be a set of properties that the objects may or may not have. Then the number of objects in $\mathcal{U}$ with none of the properties is*

$$N_{=}(\emptyset) = \sum_{J:J\subseteq P} (-1)^{|J|} N_{\geqslant}(J).$$

Proof: Let $\mathcal{U}$ be a universe of objects and let P be a set of properties that the objects may or may not have. We prove that the number of times the right-hand side of the formula includes each object in $\mathcal{U}$ is 1 when the object has none of the properties and 0 when the object has at least one property. Arrange the sum according to the size of the subset J of the n-set P:

$$\begin{aligned}\sum_{J:J\subseteq P} (-1)^{|J|} N_{\geqslant}(J) = \sum_{|J|=0} (-1)^0 N_{\geqslant}(J) + \sum_{|J|=1} (-1)^1 N_{\geqslant}(J) \\ + \sum_{|J|=2} (-1)^2 N_{\geqslant}(J) + \cdots + \sum_{|J|=n} (-1)^n N_{\geqslant}(J).\end{aligned} \tag{3.2}$$

There are $\binom{n}{0}$ terms in the first sum, $\binom{n}{1}$ in the second, $\binom{n}{2}$ in the third, and so on.

First consider an object in $\mathcal{U}$ with none of the properties. In which terms of the formula (3.2) does it get counted? Since it has none of the properties, the formula only counts it in the $|J| = 0$ sum, which equals $N_{\geqslant}(\emptyset)$ since there is only $\binom{n}{0} = 1$ subset of size 0 of P. Therefore it is counted exactly once. We are halfway there.

Now consider an object in $\mathcal{U}$ with at least one of the properties. Let's say it has exactly m of the n properties, where $1 \leqslant m \leqslant n$. In which terms of the formula (3.2) does it get counted?

The answer is that it will be counted in the terms with $|J| = 0$, $|J| = 1$, and so on up to $|J| = m$. It will not be counted when $|J| > m$ because the object has exactly m properties and no others. So when $|J| = j$, where $0 \leqslant j \leqslant m$, there are $\binom{m}{j}$ ways to pick a j-subset of the m properties that the object has, and each time it is counted it contributes $(-1)^j$ to the sum. The total contribution when $|J| = j$ is then $\binom{m}{j}(-1)^j$. Therefore in a net sense the formula counts this object

$$\sum_{j=0}^{m} \binom{m}{j} (-1)^j$$

times. That sum equals 0 from Question 97, and this completes the proof. ■

Finishing the other two examples

Example: counting ciphers

To finish this question, we need $N_{\geqslant}(J)$ for each subset J of the 26-set of properties P. The key is to divide the work according to the size of J.

In Question 94, you found that given *any* j-subset of the letters `A-Z`, the number of ciphers that leave those j letters fixed is $(26 - j)!$. This means

$$N_{\geqslant}(J) = (26 - j)! \qquad \text{for all } J \subseteq P \text{ with } |J| = j.$$

There are $\binom{26}{j}$ such subsets J, and so the contribution to that part of the formula is $\binom{26}{j}(-1)^j(26-j)!$. Summing this quantity over all possible values of j gives us the answer of

$$N_=(\emptyset) = \sum_{j=0}^{26} \binom{26}{j}(-1)^j(26-j)!. \tag{3.3}$$

This sum equals 148,362,637,348,470,135,821,287,825. Compare this with the

$$26! = 403{,}291{,}461{,}126{,}605{,}635{,}584{,}000{,}000$$

possible ciphers in which letters are allowed to be fixed. About 37% of these have no letters fixed:

$$\frac{148{,}362{,}637{,}348{,}470{,}135{,}821{,}287{,}825}{403{,}291{,}461{,}126{,}605{,}635{,}584{,}000{,}000} = 0.367879\ldots$$

This number is essentially $1/e$. See Exercise 7.

Question 98 *Show that the sum (3.3) simplifies algebraically to* $26!\sum_{j=0}^{26}\frac{(-1)^j}{j!}$.

Example: counting onto functions $[k] \longrightarrow [n]$

To answer the question of counting onto functions, again divide the work according to the size of the subset J. In Question 94, you found that given *any* j-subset of $[n]$, the number of functions that miss those j elements is $(n-j)^k$. This means

$$N_{\geqslant}(J) = (n-j)^k \qquad \text{for all } J \subseteq P \text{ with } |J| = j.$$

There are $\binom{n}{j}$ such subsets J, and so the contribution to that part of the formula is $\binom{n}{j}(-1)^j(n-j)^k$. Summing this quantity over all possible values of j gives us the answer

$$N_=(\emptyset) = \sum_{j=0}^{n}\binom{n}{j}(-1)^j(n-j)^k.$$

Onto functions and Stirling numbers of the second kind

In Chapter 2, we derived $S(k,n)\cdot n!$ as a formula for the number of onto functions from a k-set to an n-set. This was not so satisfactory because we lacked a formula for $S(k,n)$. But now we have one.

Theorem 3.1.3 (number of onto functions) *Let k and n be positive integers. The number of onto functions from a k-set to an n-set is*

$$\sum_{j=0}^{n}\binom{n}{j}(-1)^j(n-j)^k.$$

The formula for the Stirling number of the second kind $S(n,k)$ then follows immediately. Beware that n and k have now switched places.

Theorem 3.1.4 (number of set partitions) *Let n and k be nonnegative integers. The number of partitions of an n-set into k parts is*

$$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1)^j(k-j)^n.$$

Proof: Since the formula of Theorem 3.1.3 only applies to *positive* values of n and k, we need to check that the formula works when at least one of n and k equals 0.

When $n = k = 0$, the formula gives

$$S(0,0) = \frac{1}{0!}\sum_{j=0}^{0}\binom{0}{j}(-1)^j(0-j)^0 = 1\cdot\binom{0}{0}(-1)^0 0^0 = 1$$

with the convention $0^0 = 1$. This is correct since the number of partitions of the empty set into zero parts equals 1 (the empty partition). The other two cases are left for you to check in the following Question. ■

Question 99 *For $n > 1$, what value should $S(n,0)$ take? Does the formula agree? For $k > 1$, what value should $S(0,k)$ take? Does the formula agree?*

Another example and a warning

The problem of counting ciphers is more commonly known as the ***problem of derangements***: How many permutations of $[n]$ have no fixed points? (A fixed point of a function f is a value i for which $f(i) = i$.) It is also known as the ***hat-check problem***: in how many ways can the hats of n people be re-distributed so that each person receives exactly one hat but no person receives their own hat? The cipher problem is equivalent to either of these problems with $n = 26$.

Consider modifying the hat-check problem by removing the requirement that each person receives exactly one hat. That is, allow any person to receive any number of hats but still require that no person receives their own hat. This involves counting functions rather than permutations, and an application of inclusion-exclusion might use

$$\begin{aligned}\mathcal{U} &:= \text{set of all possible functions } [n] \longrightarrow [n]\\ f_i &:= \text{“the function fixes element } i\text{”, for all } i \in [n].\end{aligned}$$

As usual we want $N_=(\emptyset)$. For any j-subset J of the properties it follows that $N_{\geqslant}(J) = n^{n-j}$. This means that the answer is

$$N_=(\emptyset) = \sum_{j=0}^{n}\binom{n}{j}(-1)^j n^{n-j}.$$

This is correct but if we apply the binomial theorem to this sum we get

$$\sum_{j=0}^{n}\binom{n}{j}(-1)^j n^{n-j} = (-1+n)^n = (n-1)^n.$$

There should be a simple explanation for this simple answer, and there is: for every $i \in [n]$, there are $n-1$ choices (anything except i) for the value of $f(i)$.

This problem warns us to seek the simplest solutions first before trying more complicated methods!

The more general formula

The basic principle of inclusion-exclusion applies to counting objects that satisfy none of the properties. How might we count the objects that satisfy *some* of the properties?

Theorem 3.1.5 (general principle of inclusion-exclusion) *Let $\mathcal{U}$ be a universe of objects, and let $P = \{p_1, p_2, \ldots, p_n\}$ be a set of properties that the objects may or may not have. If S is any subset of P, then the number of objects in $\mathcal{U}$ with the properties in S and no others is*

$$N_{=}(S) = \sum_{J:S\subseteq J\subseteq P} (-1)^{|J|-|S|} N_{\geqslant}(J).$$

In this case, the sum is over all subsets of P that contain the elements of S. The proof of the general principle is in Exercise 16 and uses essentially the same technique as the proof of the basic principle.

Example: counting divisors again

How many integers in [100] are divisible by 2 but *not* by 3 or 5?

This question still has $\mathcal{U} = [100]$ and $P = \{d_2, d_3, d_5\}$ as defined earlier, but now we seek $N_{=}(d_2)$. So we apply the formula in the theorem with $S = \{d_2\}$. The sum will then be over the four subsets

$$\{d_2\},\ \{d_2, d_3\},\ \{d_2, d_5\},\ \{d_2, d_3, d_5\}.$$

The formula gives

$$N_{=}(d_2) = N_{\geqslant}(d_2) - \Big(N_{\geqslant}(d_2d_3) + N_{\geqslant}(d_2d_5)\Big) + N_{\geqslant}(d_2d_3d_5).$$

We have already computed these values. The answer is $50 - (16 + 10) + 3 = 27$.

Question 100 *How many integers in* [100] *are divisible by 3 but not by 2 or 5? How many are divisible by 2 and 3 but not by 5?*

Summary

Inclusion-exclusion is tailor-made for counting problems that fit the universe/properties framework. The properties generally describe "bad" traits, and the inclusion-exclusion formula counts those objects with none of the bad traits. In applying the formula, some problems allow shortcuts because the value of $N_{\geqslant}(J)$ only depends on the size of J. This was the case in both the cipher and onto function examples. Other problems, such as the one involving counting integers not divisible by 2, 3, or 5, do not allow such shortcuts. In that example we had to compute each value of $N_{\geqslant}(J)$ separately.

Exercises

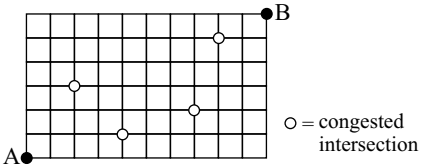
1. How many integers in [10000] are not divisible by 2, 3, or 5? How many are not divisible by 2, 3, 5, or 13?
2. How many integers in [100] are not divisible by 4, 6 or 7?
3. Use inclusion-exclusion to prove the formula

$$\begin{aligned}|A_1 \cup A_2 \cup A_3| = {} & |A_1| + |A_2| + |A_3| \\ & - |A_1A_2| - |A_1A_3| - |A_2A_3| \\ & + |A_1A_2A_3|.\end{aligned}$$

(The notation A_1A_2 means $A_1 \cap A_2$.)

4. Find the number of 13-card hands drawn from a 52-card deck that...
   (a) have at least one card in each suit.
   (b) are void in exactly one suit. ("Void in spades" means there are no spades in the hand.)
5. After a day of skiing a family of six washes all of their ski-wear including their gloves. The next day, each family member grabs two gloves from the pile.
   (a) Assume that everyone grabs one left-hand and one right-hand glove. In how many ways can they do this so that no one has both of their own gloves?
   (b) Answer part (a) assuming instead that each family member grabs any two gloves.
6. Answer the hat-check problem (i.e., the problem of derangements) for general n. This number is known as D_n.
7. Let D_n be as defined in the previous exercise.
   (a) Calculate $\lim_{n\longrightarrow\infty} \frac{D_n}{n!}$. Interpret your result.
   (b) Prove that for any n, D_n equals the closest integer to $n!/e$.
8. In how many ways can you distribute 20 identical objects to 10 distinct recipients so that each recipient receives at most five objects? How many ways if each receives at least one but at most five objects?
9. Generalize the previous problem: In how many ways can you distribute k identical objects to n distinct recipients so that each recipient receives at most r objects?
10. How many functions $[6] \longrightarrow [7]$ have at most two arrows pointing to each element of the codomain?
11. When $k < n$, what is the value of the sum $\sum_{j=0}^{n} \binom{n}{j} (-1)^j (n-j)^k$? Explain combinatorially.
12. Derive an identity for $\binom{n}{k}$ via inclusion-exclusion by counting the k-multisets of $[n]$ in which each element of $[n]$ appears at most once. Use p_i = "element i appears more than once in the multiset" as the i-th property, for $1 \leqslant i \leqslant n$.
13. Suppose that in an inclusion-exclusion problem, there exists a function f such that $N_{\geqslant}(J) = f\big(|J|\big)$ for any subset J of P. Prove:
$$N_{=}(\emptyset) = \sum_{j=0}^{n} \binom{n}{j} (-1)^j f(j).$$
14. Give a combinatorial proof of the identity $\sum_{k=0}^{n} \binom{n}{j} (-1)^j = 0$ wherein the left side is computed using inclusion-exclusion.
15. Prove combinatorially, using inclusion-exclusion, the identity that results from letting $x = -1$ and $y = 2$ in the binomial theorem (Theorem 2.2.2, p. 63).
16. Prove Theorem 3.1.5 by adapting the technique we used to prove Theorem 3.1.2.

17. A taxi drives from the intersection labeled A to the intersection labeled B in the grid of streets shown below. The driver only drives north (up) or east (right).



Traffic reports indicate that there is heavy congestion at the intersections identified. How many routes from A to B can the driver take that...

(a) avoid all congested intersections?

(b) pass through at most one congested intersection?

18. A 4-by-4 word search puzzle is a 4-by-4 array of capital letters. How many 4-by-4 word searches have the word MATH appearing at least once either horizontally, vertically, or diagonally? Here are examples of four different such puzzles:

```
F H M A     M A T H     M M M M     M A T H
M A T H     A T H M     G A A P     M A T H
G Z Z Q     T S M E     Z R T Y     M A T H
F A Y U     H E E N     K L H H     M A T P
```

Assume MATH appears left-to-right, top-to-bottom, or top-left-to-bottom-right only.

Travel Notes

Several 19th century mathematicians have been associated with discovering the inclusion-exclusion formula, including Daniel da Silva, Abraham de Moivre, and J. J. Sylvester, but it was da Silva who first published it in 1854.

The hardest part about inclusion-exclusion is the notation. The use of $N_{\geqslant}$ and $N_{=}$ is fairly common but not universal. The use of the subset sum $\sum_{J:J\subseteq P}$ avoids undue use of "$\cdots$" in something like

$$N_{=}(\emptyset) = N_{\geqslant}(\emptyset) - \sum_{i} N_{\geqslant}(p_i) + \sum_{i\neq j} N_{\geqslant}(p_i\,p_j) - \sum_{i,j,k \text{ different}} N_{\geqslant}(p_i\,p_j\,p_k) + \cdots + (-1)^n N_{\geqslant}(p_1\,p_2\cdots p_n).$$

In Sections 8.5 and 8.6, we study a powerful generalization of inclusion-exclusion called the principle of Möbius inversion. In the foundational paper concerning Möbius inversion, Rota (1964) begins by declaring that "One of the most useful principles of enumeration in discrete probability and combinatorial theory is the celebrated principle of inclusion-exclusion. When skillfully applied, this principle has yielded the solution to many a combinatorial problem."

3.2 Mathematical induction

The reader familiar with induction can either omit this section or skim the examples.

In this section we highlight how to use induction to complement our combinatorial proof techniques. Sometimes you might first discover the truth of an identity using induction, and then later realize a combinatorial proof. Other times, induction ends up being the only thing that works.

The principle of mathematical induction

The principle of mathematical induction provides a sufficient condition to guarantee the truth of a statement that depends on an integer.

Theorem 3.2.1 (mathematical induction) *Let n_0 be an integer, and suppose $S(n)$ is a statement involving an integer n. If the following two conditions are true, then $S(n)$ is true for all $n \geqslant n_0$.*

- ***Base case:*** *$S(n_0)$ is true.*
- ***Inductive step:*** *If k is an integer, $k \geqslant n_0$, and $S(k)$ is true, then $S(k+1)$ is true.*

The proof appears at the end of this section.

To use mathematical induction you must verify the base case and the inductive step of the theorem. The base case must involve a demonstration that $S(n_0)$ is true. The inductive step is an if-then proof in itself. You must (1) assume k is an integer, $k \geqslant n_0$, (2) assume that $S(k)$ is true, and then (3) prove that $S(k+1)$ is true.

It is step (3) where all the work and creativity occur. The truth of $S(k)$ in step (2) is known as the ***inductive hypothesis***. Every proof by induction must use the inductive hypothesis (abbreviated IHYP in the examples to follow) at some point. If it doesn't then it's mostly likely an incorrect proof.

Example #1: partial geometric series

In the sections on generating functions soon to follow we make good use of the identity

$$1 + x + x^2 + \cdots + x^n = \frac{1 - x^{n+1}}{1 - x}$$

which holds for any real number $x \neq 1$ and for any integer $n \geqslant 0$. You have used this formula in calculus to find the partial sum of a geometric series.

Question 101 *Compute* $1 - 2 + 4 - 8 + 16 - 32 + 64 - 128$ *using the formula.*

We'll prove the theorem by induction on n.

Theorem 3.2.2 *If x is a real number, $x \neq 1$, then for all $n \geqslant 0$,*

$$\sum_{j=0}^{n} x^j = \frac{1 - x^{n+1}}{1 - x}.$$

Proof by induction on *n:* Assume that x is a real number, $x \neq 1$. For $n \geqslant 0$, define $S(n)$ to be the statement

$$S(n): \quad \sum_{j=0}^{n} x^j = \frac{1 - x^{n+1}}{1 - x}.$$

When $n = 0$, the left-hand side of the equation $S(0)$ is $\sum_{j=0}^{0} x^j = x^0 = 1$ since x^0 is defined to be 1 for all real numbers x (including 0). The right-hand side of $S(0)$ is $\frac{1-x^{0+1}}{1-x} = \frac{1-x}{1-x} = 1$ since $x \neq 1$. They are equal, so $S(0)$ is true.

Now assume k is an integer, $k \geqslant 0$, and that $S(k)$ is true, namely

$$\text{IHYP:} \quad \sum_{j=0}^{k} x^j = \frac{1-x^{k+1}}{1-x}.$$

We must prove that $S(k+1)$ is true, namely

$$\sum_{j=0}^{k+1} x^j = \frac{1-x^{k+2}}{1-x}.$$

To do so, start with the left-hand side:

$$\begin{aligned}
\sum_{j=0}^{k+1} x^j &= \left(\sum_{j=0}^{k} x^j\right) + x^{k+1} && \text{peel off last term} \\
&= \frac{1-x^{k+1}}{1-x} + x^{k+1} && \text{use IHYP} \\
&= \frac{1-x^{k+1}+x^{k+1}(1-x)}{1-x} && \text{common denominator} \\
&= \frac{1-x^{k+1}+x^{k+1}-x^{k+2}}{1-x} \\
&= \frac{1-x^{k+2}}{1-x}.
\end{aligned}$$

Therefore $S(k+1)$ is true. Therefore $S(n)$ is true for $n \geqslant 0$. ■

Example #2: proving an inequality

It appears that the inequality

$$\sum_{j=1}^{n} j! < (n+1)!$$

might be true for any integer $n \geqslant 1$ because

$$\begin{aligned}
1! &= 1 < 2 = 2! \\
1!+2! &= 3 < 6 = 3! \\
1!+2!+3! &= 9 < 24 = 4! \\
1!+2!+3!+4! &= 33 < 120 = 5! \\
1!+2!+3!+4!+5! &= 153 < 720 = 6!
\end{aligned} \tag{3.4}$$

is a promising start.

Define $S(n)$ to be the statement

$$S(n): \quad \sum_{j=1}^{n} j! < (n+1)!.$$

To prove by induction, note that the first line of inequalities (3.4) shows that $S(1)$ is true. Now assume that k is an integer, $k \geqslant 1$, and that $S(k)$ is true, namely

$$\text{IHYP:} \quad \sum_{j=1}^{k} j\,! < (k+1)!.$$

We must show that $\sum_{j=1}^{k+1} j\,! < (k+2)!$. The following calculations do the job:

$$\begin{aligned}
\sum_{j=1}^{k+1} j\,! &= \left(\sum_{j=1}^{k} j\,!\right) + (k+1)! && \text{peel off last term} \\
&< (k+1)! + (k+1)! && \text{by IHYP} \\
&= 2(k+1)! \\
&< (k+2)(k+1)! && 2 < k+2 \text{ since } k \geqslant 1 \\
&= (k+2)!\,.
\end{aligned}$$

Therefore $S(k+1)$ is true, so $S(n)$ is true for all $n \geqslant 1$.

Example #3: solving a recurrence relation

An example of a *recurrence relation* is

$$\begin{aligned}
a_0 &= 1 \\
a_n &= 2a_{n-1} + n - 1 \qquad \text{for } n \geqslant 1.
\end{aligned} \tag{3.5}$$

It governs the iterative computation of the numbers $a_0, a_1, a_2, a_3, \ldots$. The value $a_0 = 1$ is the *initial condition*, and then to get the successive values $a_1, a_2, a_3, \ldots$ you just apply the rule $a_n = 2a_{n-1} + n - 1$ repeatedly:

$$\begin{aligned}
a_0 &= 1 \\
a_1 &= 2a_0 + 1 - 1 = 2(1) + 0 = 2 \\
a_2 &= 2a_1 + 2 - 1 = 2(2) + 1 = 5 \\
a_3 &= 2a_2 + 3 - 1 = 2(5) + 2 = 12 \\
&\vdots
\end{aligned}$$

Question 102 *What is a_6?*

To find a_{100} and a_{1000} and so forth, we would like a formula that allows us to jump right to a_{1000} without computing the previous terms. Compute a few more terms and look for a pattern:

n	0	1	2	3	4	5	6	7
a_n	1	2	5	12	27	58	121	248

They seem to have something to do with powers of 2, specifically

$$\begin{aligned} a_0 &= 1 = 2^1 - 1 \\ a_1 &= 2 = 2^2 - 2 \\ a_2 &= 5 = 2^3 - 3 \\ a_3 &= 12 = 2^4 - 4 \\ a_4 &= 27 = 2^5 - 5 \\ a_5 &= 58 = 2^6 - 6 \\ a_6 &= 121 = 2^7 - 7 \\ a_7 &= 248 = 2^8 - 8. \end{aligned}$$

Our guess is that $a_n = 2^{n+1} - n - 1$ holds for all $n \geqslant 0$.

To prove this by induction on n, first verify the formula when $n = 0$. The formula says $a_0 = 2^{0+1} - 0 - 1 = 1$. The recurrence defines $a_0 = 1$, so it is correct in this case.

Now assume k is an integer, $k \geqslant 0$, and that $a_k = 2^{k+1} - k - 1$; this is IHYP. We must prove that $a_{k+1} = 2^{k+2} - (k+1) - 1$, or equivalently that $a_{k+1} = 2^{k+2} - k - 2$. Here it is:

$$\begin{aligned} a_{k+1} &= 2a_k + k && \text{by the recurrence relation} \\ &= 2(2^{k+1} - k - 1) + k && \text{by IHYP} \\ &= 2^{k+2} - 2k - 2 + k \\ &= 2^{k+2} - k - 2. \end{aligned}$$

This proves that $S(k+1)$ is true. Therefore $a_n = 2^{n+1} - n - 1$ is true for all $n \geqslant 0$.

Example #4: solving a counting problem

Here's a straightforward yet typical example of how you might use induction in combinatorics. You are trying to count the partitions of $[n]$ into two blocks but don't see how to jump directly to a formula. Instead, you define p_n to be the number of partitions of $[n]$ into two blocks, for $n \geqslant 2$. Using complete enumeration, you find $p_2 = 1$, $p_3 = 3$, $p_4 = 7$, and $p_5 = 15$. For example, the partitions of [3] into two blocks are

$$\big\{\{1\},\{2,3\}\big\}, \qquad \big\{\{2\},\{1,3\}\big\}, \qquad \text{and} \qquad \big\{\{3\},\{1,2\}\big\}.$$

Then you discover a combinatorial proof of the identity $p_n = 2p_{n-1} + 1$, for $n \geqslant 3$.

Question 103 *Give the combinatorial proof.*

Starting with $p_2 = 1$, you do some computation:

$$\begin{aligned} p_2 &= 1 \\ p_3 &= 2p_2 + 1 = 3 \\ p_4 &= 2p_3 + 1 = 7 \\ p_5 &= 2p_4 + 1 = 15 \\ p_6 &= 2p_5 + 1 = 31 \\ p_7 &= 2p_6 + 1 = 63. \end{aligned}$$

The first four values agree with those you found by complete enumeration—good. Also, the pattern looks pretty clear:

$$p_n = 2^{n-1} - 1 \qquad \text{for } n \geqslant 2.$$

In other words, you need to prove that the numbers defined by the recurrence relation

$$\begin{aligned} p_2 &= 1 \\ p_n &= 2p_{n-1} + 1 \qquad \text{for } n \geqslant 3 \end{aligned}$$

are really just the numbers $p_n = 2^{n-1} - 1$, for $n \geqslant 2$.

Question 104 *Give a proof by induction, like that of Example #3.*

Strong mathematical induction

When using induction, sometimes the truth of $S(k)$ alone is not strong enough to imply the truth of $S(k+1)$. In such cases we can try strong induction. In the induction hypothesis of strong induction, we assume the truth of $S(j)$ for all j between the base value n_0 and the arbitrary integer k.

Theorem 3.2.3 (strong mathematical induction) *Let n_0 and n_1 be integers, $n_0 \leqslant n_1$, and suppose that $S(n)$ is a statement involving the integer n. If the following two conditions are true, then $S(n)$ is true for all $n \geqslant n_0$:*

- ***Base case(s):*** *$S(n_0), \ldots, S(n_1)$ are true.*
- ***Inductive step:*** *If k is an integer, $k \geqslant n_1$, and $S(j)$ is true for all j satisfying $n_0 \leqslant j \leqslant k$, then $S(k+1)$ is true.*

Notice that it may be necessary to verify that more than one statement is true in the base case. Since the assumptions are stronger than those of Theorem 3.2.1, essentially the same proof works. (The proof of Theorem 3.2.1 appears at the end of the section.)

Example #5: bounding terms of a recurrence relation

Consider another recurrence relation:

$$\begin{aligned} L_0 &= 2 \\ L_1 &= 1 \\ L_n &= L_{n-1} + L_{n-2} \qquad \text{for } n \geqslant 2. \end{aligned} \tag{3.6}$$

This means $L_2 = L_1 + L_0 = 3$ and $L_3 = L_2 + L_1 = 4$ and so forth:

n	0	1	2	3	4	5	6	7	$\cdots$
L_n	2	1	3	4	7	11	18	29	$\cdots$

This is the well-known sequence of *Lucas numbers* which we will revisit a couple of times in the text. A formula for L_n is not obvious. Later in this chapter we develop a systematic technique that allows us to derive a formula.

But if at first you don't succeed then lower your standards: sometimes just having an upper bound on the n-th term of a sequence is a useful thing. In this case, one easy upper bound is $L_n < 2^n$ which appears to hold for all $n \geqslant 1$. At least it is true for $1 \leqslant n \leqslant 7$:

n	0	1	2	3	4	5	6	7
L_n	2	1	3	4	7	11	18	29
2^n	1	2	4	8	16	32	64	128

(In fact the bound appears too generous. Exercise 9 asks you to prove a tighter bound.)

To prove the upper bound, define the statement

$$S(n): \qquad L_n < 2^n.$$

Our proof is by strong induction. When $n = 1$, we have $L_1 = 1$ by definition. Also, $2^1 = 2$. It follows that $L_1 < 2^1$ and so $S(1)$ is true. When $n = 2$, we have $L_2 = 3$ and $2^2 = 4$. It follows that $L_2 < 2^2$ and so $S(2)$ is true. (In applying Theorem 3.2.3 we chose $n_0 = 1$ and $n_1 = 2$. The base case(s) portion requires us to show that $S(1)$ and $S(2)$ are true, which we just did.)

Now assume that k is an integer, $k \geqslant 2$, and that $S(j)$ is true for all j satisfying $1 \leqslant j \leqslant k$, namely

$$\text{IHYP:} \qquad L_j < 2^j \text{ for all } j \text{ with } 1 \leqslant j \leqslant k.$$

We must show that $S(k+1)$ is true, namely $L_{k+1} < 2^{k+1}$. Now,

$$\begin{aligned} L_{k+1} &= L_k + L_{k-1} && \text{by the recurrence relation} \\ &< 2^k + 2^{k-1} && \text{use IHYP} \\ &= 2^{k-1}(2+1) \\ &= 2^{k-1} \cdot 3 \\ &< 2^{k-1} \cdot 2^2 \\ &= 2^{k+1}. \end{aligned}$$

Therefore $L_{k+1} < 2^{k+1}$, and so $S(k+1)$ is true. Therefore $L_n < 2^n$ for all integers $n \geqslant 1$.

It is very important to understand why we could apply the inductive hypothesis to both L_k and L_{k-1} in the second line of the calculation above. The reason is that because k is at least 2, then $k-1$ is at least 1. Since the induction hypothesis assumes that $S(j)$ is true for all j satisfying $1 \leqslant j \leqslant k$, we are safe in using both $L_k < 2^k$ and $L_{k-1} < 2^{k-1}$.

Question 105 *What happens if you try to prove $L_n < 2^n$ for all $n \geqslant 0$ and do not verify the base cases?*

Proof of the principle of mathematical induction

The proof of Theorem 3.2.1 uses an axiom called the well-ordering principle.

Axiom 3.2.4 (the well-ordering principle) *A nonempty subset of integers that is bounded below contains a least element.*

"Bounded below" means that there is some number L such that $L \leqslant x$ for every integer x in the set. The well-ordering principle does not apply to, say, the set of even integers $\{0, \pm 2, \pm 4, \ldots\}$ because it is not bounded below.

Proof of Theorem 3.2.1: We prove by contradiction. Assume that the two conditions of the theorem are true and yet it is not the case that $S(n)$ is true for all $n \geq n_0$. Consider the set of integers

$$\{n_0, n_0 + 1, n_0 + 2, \ldots\}.$$

There is at least one integer in this set for which the statement S is false. Collect all such integers into a set called $\mathcal{F}$, and notice that each element of $\mathcal{F}$ is at least $n_0 + 1$. This is because $S(n_0)$ is true by the base case assumption.

This set $\mathcal{F}$ of integers is then nonempty and bounded below, and so the well-ordering principle tells us that it has a least element. Call it m, and notice that $m \geq n_0 + 1$. Then $S(m)$ is certainly false but $S(m-1)$ must be true. This is because m is the *least* integer in $\{n_0, n_0 + 1, n_0 + 2, \ldots\}$ that makes the statement false, and also because $m - 1 \geq n_0$.

But the hypothesis of the theorem says then that $S\big((m-1)+1\big) = S(m)$ is true, contradicting the fact that $S(m)$ is false! Therefore $S(n)$ is true for all $n \geq n_0$. ■

Summary

Mathematical induction is a technique for proving a statement $S(n)$ that depends on an integer n. It requires two parts: verification of the base case and a proof of the inductive step. In the inductive step we prove that the truth of $S(k)$ implies the truth of $S(k+1)$. Sometimes the truth of $S(k)$ alone does not imply the truth of $S(k+1)$, and so the principle of strong mathematical induction might work. In its inductive step, one assumes the truth of $S(j)$ for all values of j satisfying $j \leq k$ and then proves that $S(k+1)$ is true.

Exercises

1. (a) Prove: for $n \geq 0$, $3^n - 1$ is divisible by 2.
   (b) Prove: for $n \geq 0$, $4^n - 1$ is divisible by 3.
   (c) Find a general theorem and prove it.
2. Let a and b be unequal integers. Prove: for $n \geq 0$, $a^n - b^n$ is divisible by $a - b$.
3. Prove: for $n \geq 2$, $\displaystyle\prod_{j=2}^{n}\left(1 - \frac{1}{j^2}\right) = \frac{n+1}{2n}$. The product notation means

$$\prod_{j=2}^{n}\left(1 - \frac{1}{j^2}\right) = \left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{4^2}\right)\cdots\left(1 - \frac{1}{n^2}\right).$$

4. Discover and prove formulas for each of the following products.
   (a) $\displaystyle\prod_{j=1}^{n}\left(1 + \frac{1}{j}\right)$
   (b) $\displaystyle\prod_{j=2}^{n}\left(1 - \frac{1}{j}\right)$
5. Discover and prove a formula for the sum $\displaystyle\sum_{j=1}^{n}(-1)^j j^2$.

6. Conjecture and prove a formula for $\sum_{i=1}^{n}\sum_{j=1}^{i} j$. (You can call this the "Twelve Days of Christmas" formula because when $n = 12$ the sum equals the total number of gifts given in the song.)

7. Give a combinatorial proof: for $n \geqslant 1$, $\sum_{j=1}^{n} j! < (n+1)!$.
   Do so by asking a question and then performing a deliberate under- or over-count with one of the answers.

8. The work in (3.4), page 96, suggests that $\sum_{j=1}^{n} j! \leqslant \frac{1}{2}(n+1)!$ might be true.
   (a) Prove this sharper inequality by induction.
   (b) Give a combinatorial proof.

9. For the recurrence relation shown in (3.6), page 99, we proved $L_n < 2^n$ for $n \geqslant 1$.
   (a) Prove the tighter inequality $L_n \leqslant 1.7^n$. At what value of n should you start the induction?
   (b) What is so special about the number 1.7? Adjust your work in part (a) to create the tightest bound that you can.

10. Define a recurrence relation by $a_0 = a_1 = a_2 = 1$, and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for $n \geqslant 3$. Prove: $a_n \leqslant 1.9^n$ for all $n \geqslant 0$. Also, can you prove a tighter bound?

11. Define $a_0 = 1$ and for $n \geqslant 1$, define $a_n = na_{n-1} + 1$. Prove: For $n \geqslant 0$, $a_n = \sum_{j=0}^{n}(n)_j$.

12. Prove: If n is an integer, $n \geqslant 2$, then either n is prime or else can be factored into a product of primes. (This is the fundamental theorem of arithmetic.)

13. Assume the truth of the following statement: if A and B are disjoint, finite sets, then $|A \cup B| = |A| + |B|$. Prove the following by induction on n: for $n \geqslant 2$, if $A_1, A_2, \ldots, A_n$ are finite, pairwise disjoint sets, then
$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i|.$$

14. Let $n \geqslant 1$. Prove that any $2^n \times 2^n$ checkerboard with any one square removed can be completely tiled with L-shaped tiles. (The tiles take up three adjacent squares of the checkerboard in an L shape.)

3.3 Using generating functions, part I

Our job for the remainder of this chapter is to introduce and use generating functions to solve combinatorial problems. Generating functions exploit algebra to mimic calculations involving the sum and product principles. The amount of information that can be squeezed out of a generating function is surprisingly great. Their use often leads to new insights and clever proofs.

The magic of algebra

In how many ways can a team score a total of six points in basketball? (In basketball, any single shot is worth either one, two, or three points. And we're only interested in the number of each type of shot made, not the order in which they were made.)

Admittedly this is a problem small enough to solve by brute force because six is not a large number. In fact, we just need to count the partitions of 6 into parts of size at most 3. There are seven, namely

$$\begin{array}{lll} 3+3 & 2+2+2 & 1+1+1+1+1+1 \\ 3+2+1 & 2+2+1+1 & \\ 3+1+1+1 & 2+1+1+1+1. & \end{array}$$

But this becomes unreasonable to do when we ask the same question of 98 points—a more realistic total for an NBA game—instead of six points.

Question 106 *How many ways are there to score seven points?*

Generating functions can answer both the six-point question and the 98-point question with the same effort, and therein lies the advantage. Let's tackle the six-point question first.

- In scoring six points, the contribution from one-point shots to that score is

  $$0 \text{ pts} \oplus 1 \text{ pt} \oplus 2 \text{ pts} \oplus 3 \text{ pts} \oplus 4 \text{ pts} \oplus 5 \text{ pts} \oplus 6 \text{ pts}$$

  where $\oplus$ means exclusive-or. Symbolize this algebraically as

  $$x^0 + x^1 + x^2 + x^3 + x^4 + x^5 + x^6$$

  where the $\oplus$ signs have been replaced by ordinary addition and where the total contribution appears in the exponents.

- The contribution from two-point shots to the score of six points is

  $$0 \text{ pts} \oplus 2 \text{ pts} \oplus 4 \text{ pts} \oplus 6 \text{ pts}.$$

  Symbolize this algebraically as $x^0 + x^2 + x^4 + x^6$.

- Finally, the contribution from three-point shots is

  $$0 \text{ pts} \oplus 3 \text{ pts} \oplus 6 \text{ pts},$$

  which we symbolize algebraically as $x^0 + x^3 + x^6$.

Multiply these three algebraic expressions together in a product-principle-type of calculation to get the *generating function*

$$\underbrace{(1+x+x^2+x^3+x^4+x^5+x^6)}_{\text{contribution from 1-pt shots}}\underbrace{(1+x^2+x^4+x^6)}_{\text{...from 2-pt shots}}\underbrace{(1+x^3+x^6)}_{\text{...from 3-pt shots}}. \tag{3.7}$$

Then distribute and gather like terms (which is best done with a symbolic manipulator like Maple) to rewrite it as

$$\begin{aligned} &1 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 7x^6 + 7x^7 + 8x^8 + 8x^9 \\ &\quad + 8x^{10} + 7x^{11} + 7x^{12} + 5x^{13} + 4x^{14} + 3x^{15} + 2x^{16} + x^{17} + x^{18}. \end{aligned} \tag{3.8}$$

To answer the original question, we just find the coefficient of the x^6 term, which is 7.

$$
\begin{aligned}
&(x^0+x+x^2+x^3+x^4+x^5+x^6)(x^0+x^2+x^4+x^6)(x^0+x^3+x^6)\\
&\quad= x^{0+0+0}+x^{1+0+0}+x^{2+0+0}+x^{3+0+0}+x^{4+0+0}+x^{5+0+0}+x^{6+0+0}\\
&\qquad+x^{0+2+0}+x^{1+2+0}+x^{2+2+0}+x^{3+2+0}+x^{4+2+0}+x^{5+2+0}+x^{6+2+0}\\
&\qquad+x^{0+4+0}+x^{1+4+0}+x^{2+4+0}+x^{3+4+0}+x^{4+4+0}+x^{5+4+0}+x^{6+4+0}\\
&\qquad+x^{0+6+0}+x^{1+6+0}+x^{2+6+0}+x^{3+6+0}+x^{4+6+0}+x^{5+6+0}+x^{6+6+0}\\
&\qquad+x^{0+0+3}+x^{1+0+3}+x^{2+0+3}+x^{3+0+3}+x^{4+0+3}+x^{5+0+3}+x^{6+0+3}\\
&\qquad+x^{0+2+3}+x^{1+2+3}+x^{2+2+3}+x^{3+2+3}+x^{4+2+3}+x^{5+2+3}+x^{6+2+3}\\
&\qquad+x^{0+4+3}+x^{1+4+3}+x^{2+4+3}+x^{3+4+3}+x^{4+4+3}+x^{5+4+3}+x^{6+4+3}\\
&\qquad+x^{0+6+3}+x^{1+6+3}+x^{2+6+3}+x^{3+6+3}+x^{4+6+3}+x^{5+6+3}+x^{6+6+3}\\
&\qquad+x^{0+0+6}+x^{1+0+6}+x^{2+0+6}+x^{3+0+6}+x^{4+0+6}+x^{5+0+6}+x^{6+0+6}\\
&\qquad+x^{0+2+6}+x^{1+2+6}+x^{2+2+6}+x^{3+2+6}+x^{4+2+6}+x^{5+2+6}+x^{6+2+6}\\
&\qquad+x^{0+4+6}+x^{1+4+6}+x^{2+4+6}+x^{3+4+6}+x^{4+4+6}+x^{5+4+6}+x^{6+4+6}\\
&\qquad+x^{0+6+6}+x^{1+6+6}+x^{2+6+6}+x^{3+6+6}+x^{4+6+6}+x^{5+6+6}+x^{6+6+6}\\
&\quad= x^0+x^1+x^2+x^3+x^4+x^5+x^6+x^2+x^3+x^4+x^5+x^6+x^7+x^8\\
&\qquad+x^4+x^5+x^6+x^7+x^8+x^9+x^{10}+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}\\
&\qquad+x^3+x^4+x^5+x^6+x^7+x^8+x^9+x^5+x^6+x^7+x^8+x^9+x^{10}+x^{11}\\
&\qquad+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}\\
&\qquad+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}\\
&\qquad+x^6+x^7+x^8+x^9+x^{10}+x^{11}+x^{12}\\
&\qquad+x^8+x^9+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}\\
&\qquad+x^{10}+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}\\
&\qquad+x^{12}+x^{13}+x^{14}+x^{15}+x^{16}+x^{17}+x^{18}\\
&\quad= 1+x+2x^2+3x^3+4x^4+5x^5+7x^6+7x^7+8x^8+8x^9\\
&\qquad+8x^{10}+7x^{11}+7x^{12}+5x^{13}+4x^{14}+3x^{15}+2x^{16}+x^{17}+x^{18}.
\end{aligned}
$$

Figure 3.1. The 84 terms in the expanded generating function.

Why does this work? Figure 3.1 reveals the hidden algebraic details. There are $7\cdot4\cdot3 = 84$ terms when the generating function (3.7) is multiplied out, and each appears before simplification in the form x^{a+b+c} where a is the total contribution from one-point shots, b from two-point shots, and c from three-point shots. After simplifying the exponents, each exponent stores the point totals. Then *combining like terms*—the key step!—makes the *coefficient* of x^6 equal the number of ways the team can score exactly k points.

Answering other questions

The generating function (3.8) actually answers more than just the original question. In how many ways can a team score a total of five points? The answer is the coefficient of x^5, which is 5. How about three points? The answer is the coefficient of x^3, which is 3.

Although the coefficient of x^{10} is 8, there are *not* eight ways to score 10 points in

basketball. This is because the generating function

$$(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)(1 + x^2 + x^4 + x^6)(1 + x^3 + x^6)$$

limits the contribution from each type of shot to be at most six points. So eight is the answer to the question, In how many ways can a team score a total of 10 points if they make at most six one-point shots, at most three two-point shots, and at most two three-point shots?

Question 107 *Does the coefficient of x^7 in the generating function equal the number of ways that a team can score seven points or does the same issue arise?*

To answer the question of how many ways a team can score a total of 10 points, we would find the coefficient of x^{10} in

$$(1 + x + x^2 + \cdots + x^{10})(1 + x^2 + x^4 + \cdots + x^{10})(1 + x^3 + x^6 + x^9).$$

Using Maple, the answer is 14. And to go back to our original question of how many ways the team can score a total of 98 points, we need to find the coefficient of x^{98} in

$$(1 + x + x^2 + \cdots + x^{98})(1 + x^2 + x^4 + \cdots + x^{98})(1 + x^3 + x^6 + \cdots + x^{96}).$$

With the help of Maple this is 850.

Generating functions are capable of answering many questions at once. Might there be one generating function that answers the question of how many ways can a team score a total of k points for any value of k? There is:

$$(1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots). \quad (3.9)$$

The answer to the question equals the coefficient of x^k in the above generating function.

This last generating function should raise some eyebrows. How can we make sense of a product where each term is an infinite sum? Is it really true that the six-point and 98-point questions can be answered with the same effort? Stay tuned.

The magic of calculus

Each term of the product shown in (3.9) is a power series. The well-known geometric series formula from calculus is

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots \qquad \text{for } |x| < 1.$$

If you replace x by x^2 you get

$$\begin{aligned}\frac{1}{1-x^2} &= 1 + x^2 + (x^2)^2 + (x^2)^3 + \cdots \\ &= 1 + x^2 + x^4 + x^6 + \cdots\end{aligned}$$

and if you replace x by x^3 you get

$$\begin{aligned}\frac{1}{1-x^3} &= 1 + x^3 + (x^3)^2 + (x^3)^3 + \cdots \\ &= 1 + x^3 + x^6 + x^9 + \cdots.\end{aligned}$$

Thus there is a concise way to write the generating function (3.9) for the number of ways that a team can score any number of points:

$$\frac{1}{(1-x)(1-x^2)(1-x^3)}.$$

Is such an expression a satisfactory answer to the original question? That is, if you ask how many ways that a basketball team can score a total of k points and someone tells you that the answer is the coefficient of x^k in the given generating function, then is that a good answer? This section and the next should convince you that it is.

More magic

The six-point problem is equivalent to: How many 3-lists (z_1, z_2, z_3) satisfy $z_1+z_2+z_3 = 6$ where $z_1 \in \{0,1,2,3,4,5,6\}$, $z_2 \in \{0,2,4,6\}$, and $z_3 \in \{0,3,6\}$? Here, z_1 is the contribution from one-point shots, z_2 from two-point shots, and z_3 from three-point shots. Problems that fit into this form are tailor-made for generating functions. We introduced such problems in Section 2.2.

Example: postage

In how many ways can we construct a postage of 39 cents using only three- and five-cent stamps?

The contribution from three-cent stamps can be symbolized algebraically as

$$x^0 + x^3 + x^6 + \cdots + x^{36} + x^{39}$$

and for five-cent stamps as

$$x^0 + x^5 + x^{10} + \cdots + x^{30} + x^{35}.$$

The answer is the coefficient of x^{39} in

$$(1 + x^3 + x^6 + \cdots + x^{36} + x^{39})(1 + x^5 + x^{10} + \cdots + x^{30} + x^{35})$$

which, using Maple, is 3.

Question 108 *How many ways are there to make change for 14 cents using five pennies, three nickels, and one dime? Write down a generating function and find a coefficient.*

Just like the basketball question, the question of the number of ways to make a postage of k cents using only three- and five-cent stamps can be answered by finding the coefficient of x^k in the "extended" generating function

$$(1 + x^3 + x^6 + x^9 + \cdots)(1 + x^5 + x^{10} + x^{15} + \cdots)$$

or its equivalent, concise form

$$\frac{1}{(1-x^3)(1-x^5)}. \tag{3.10}$$

And this problem is equivalent to counting the 2-lists (z_1, z_2) of integers satisfying

$$\begin{aligned} z_1 + z_2 &= 39 \\ z_1 &\in \{0, 3, 6, 9, \ldots, \} \\ z_2 &\in \{0, 5, 10, 15, \ldots\}, \end{aligned}$$

because z_1 equals the contribution from three-cent stamps to the total postage, and z_2 equals the contribution from five-cent stamps.

Question 109 *How would the concise generating function change if you could also use up to two 12-cent stamps?*

Example: integer partitions

How many partitions of 12 have parts of size at most 5?

There are as many such partitions as there are 5-lists $(z_1, z_2, z_3, z_4, z_5)$ satisfying

$$\begin{aligned} z_1 + z_2 + z_3 + z_4 + z_5 &= 12 \\ z_1 &\in \{0, 1, 2, 3, \ldots\} \\ z_2 &\in \{0, 2, 4, 6, \ldots\} \\ &\vdots \\ z_5 &\in \{0, 5, 10, 15, \ldots\}. \end{aligned}$$

The answer is the coefficient of x^{12} in

$$(1 + x + x^2 + x^3 + \cdots)(1 + x^2 + x^4 + x^6 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots)$$
$$(1 + x^4 + x^8 + x^{12} + \cdots)(1 + x^5 + x^{10} + x^{15} + \cdots),$$

or in concise form,

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)}.$$

The solution, with Maple, is 47.

Question 110 *How would the concise form of the generating function change if we wanted to know the number of partitions of 12 that have parts of size at most 5 but no parts of size 4?*

Ordinary generating functions

Now that we know a little about what generating functions do, it's time to learn what they are. Informally, a generating function is a power series that organizes a number sequence for display. The ordinary generating function (OGF) of the sequence $a_0, a_1, a_2, a_3, \ldots$ is

$$\sum_{k \geq 0} a_k x^k = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

and a handy way to abbreviate the sequence $a_0, a_1, a_2, a_3, \ldots$ is $\{a_k\}_{k \geq 0}$. Take note that the sum is from $k = 0$ to ∞.

Definition 3.3.1 (OGF) *The **ordinary generating function (OGF)** of the number sequence $\{a_k\}_{k \geq 0}$ is defined as* $\sum_{k \geq 0} a_k x^k$.

The key feature is that a_k is the coefficient of x^k. In that way the OGF is like a file cabinet and x^k is the label on the file that contains the term a_k. The term "ordinary" distinguishes this generating function from other types. More on that in Section 3.4.

Semi-formal power series: a necessary conversation

Generating functions are power series, so it appears that we need to rely on calculus to work with them. This is partly true. We already mentioned that one of the more memorable power series you studied in calculus was the geometric series

$$\begin{aligned} f(x) &= \sum_{k\geq 0} x^k \\ &= 1 + x + x^2 + x^3 + \cdots . \end{aligned}$$

This converges if and only if $|x| < 1$ (its *radius of convergence*), and if so, then it converges to $\frac{1}{1-x}$. This means that from an *analytical* perspective, it is correct to say that these two functions of x are the same as long as $|x| < 1$, i.e.,

$$\sum_{k\geq 0} x^k = \frac{1}{1-x} \qquad \text{for } |x| < 1.$$

Question 111 *What is the value of the series* $\sum_{k\geq 0}(-\frac{1}{3})^k$*? Of* $\sum_{k\geq 1} 4^k 5^{-k}$*? Of* $\sum_{k\geq 0} 3^k$*?*

We can also do things like replace x by $2x$ and get a power series representation for the function $\frac{1}{1-2x}$, i.e.,

$$\sum_{k\geq 0}(2x)^k = \sum_{k\geq 0} 2^k x^k = \frac{1}{1-2x} \qquad \text{for } |x| < \tfrac{1}{2}.$$

Question 112 *Why is the radius of convergence* $|x| < \frac{1}{2}$ *instead of* $|x| < 1$*?*

In fact, we already did something like this when we replaced x by x^2 in getting the concise form for the generating function (3.9).

In combinatorics our perspective mostly is *algebraic*, not analytical. The power series $1 + x + x^2 + x^3 + \cdots$ puts the sequence $1, 1, 1, 1, \ldots$ on display because the coefficient of x^k is always 1. In that way we consider $\sum_{k\geq 0} x^k$ to be the OGF of the sequence $\{1\}_{k\geq 0}$. But we will also borrow the more concise form $\frac{1}{1-x}$ from calculus and write

$$\sum_{k\geq 0} x^k = \frac{1}{1-x}, \tag{3.11}$$

and then carry on all sorts of operations on these two expressions as if they were completely interchangeable. We won't even mention convergence. In the same way we will say that the expressions on each side of the $=$ sign in

$$\sum_{k\geq 0} 2^k x^k = \frac{1}{1-2x} \tag{3.12}$$

are each OGFs for $\{2^k\}_{k\geq 0}$. The left-hand side is in explicit form (the coefficient of x^k is available at a glance) and the right-hand side is in concise form.

The algebraic theory of *formal power series* allows us to get away with such blasphemy. All of the algebraic operations that we will need to perform on generating functions, like addition, multiplication, and partial fraction decomposition, are covered. Even differentiation and antidifferentiation can be thought of as formal operations. We will not develop

this theory but instead make free use of it. See the exercises in Section 3.4 for some basic results.

In that sense the symbol x in a generating function is an *indeterminate* rather than a *variable*. Very useful information can be had by evaluating generating functions at certain values of x. But keep in mind that doing so requires a return to analytic theory and the examination of convergence issues.

Bread-and-butter OGFs

Users of generating functions need fluency in the translation of a sequence into a concise generating function and vice-versa. Illustrations of these techniques on three of the most important classes of OGFs follow.

OGFs and geometric series

We have already observed that $\frac{1}{1-x}$ is the concise form of the OGF for the all-1s sequence $\{1\}_{k\geq 0}$ because

$$\frac{1}{1-x} = \sum_{k\geq 0} x^k.$$

More generally, if c is any real number, then the OGF for $\{c^k\}_{k\geq 0}$ is $\frac{1}{1-cx}$ because

$$\frac{1}{1-cx} = \sum_{k\geq 0} (cx)^k = \sum_{k\geq 0} c^k x^k.$$

The $c = -1$ special case gets used quite often:

$$\frac{1}{1+x} = \frac{1}{1-(-x)} = \sum_{k\geq 0} (-1)^k x^k.$$

Therefore $\frac{1}{1+x}$ is the OGF of the alternating sequence $\left\{(-1)^k\right\}_{k\geq 0}$.

Question 113 *Of what sequence is* $\dfrac{1}{1+3x}$ *the OGF?*

OGFs and the binomial theorem

Set $y = 1$ in the the binomial theorem (Theorem 2.2.2, page 63) to obtain

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k = \sum_{k\geq 0} \binom{n}{k} x^k.$$

This means that for fixed n, $(1+x)^n$ is the OGF for the binomial coefficients $\left\{\binom{n}{k}\right\}_{k\geq 0}$. Notice that the first sum stops at n while the second is infinite. Writing equality between the two is fine because $\binom{n}{k} = 0$ for $k > n$. In that sense we justify saying that $(1+x)^n$ is the OGF for the infinite sequence

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}, \underbrace{\binom{n}{n+1}}_{=0}, \underbrace{\binom{n}{n+2}}_{=0}, \ldots$$

rather than just for the finite sequence $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$.

Question 114 *What is the coefficient of* x^5 *in* $(1-x)^9$*?*

OGFs and multisets

We could use our symbolic series technique to derive the OGF for the binomial coefficients $\binom{n}{k}$ in the following way without using the binomial theorem. The binomial coefficient $\binom{n}{k}$ equals the number of n-lists that solve the equation $z_1 + z_2 + \cdots + z_n = k$ where each z_i is either 0 or 1. We symbolize the choice for each z_i with the term $x^0 + x^1$, or $1 + x$. Multiplying n copies of this term together gives the OGF for the number of n-lists that solve the equation:

$$\underbrace{(1+x)}_{z_1\in\{0,1\}}\ \underbrace{(1+x)}_{z_2\in\{0,1\}}\ \cdots\ \underbrace{(1+x)}_{z_n\in\{0,1\}} = (1+x)^n.$$

That's it, since we know the number of n-lists that solve the equation is $\binom{n}{k}$.

The same idea works to get the concise form for the OGF of the sequence of multichoose coefficients $\left\{\left(\!\binom{n}{k}\!\right)\right\}_{k\geq 0}$. For a fixed positive integer n, we know that $\left(\!\binom{n}{k}\!\right)$ is the number of n-lists $(z_1, z_2, \ldots, z_n)$ that solve the equation $z_1 + z_2 + \cdots + z_n = k$ where each z_i is a nonnegative integer. Proceeding as before, the symbolic series for each z_i is $1 + x + x^2 + x^3 + \cdots$. We already have a concise form for this: $\frac{1}{1-x}$. Multiplying n copies of this together gives the OGF for the multichoose coefficients:

$$\left(\frac{1}{1-x}\right)^n = \frac{1}{(1-x)^n}.$$

There is a nice duality between the OGFs for the binomial and multichoose coefficients:

- $(1 + x)^n$ is the OGF for $\left\{\binom{n}{k}\right\}_{k\geq 0}$.
- $(1 - x)^{-n}$ is the OGF for $\left\{\left(\!\binom{n}{k}\!\right)\right\}_{k\geq 0}$.

Question 115 *What is the coefficient of x^8 in $\dfrac{x}{(1-x)^7}$?*

Several examples

We now know several OGFs in both explicit and concise form. Here, n is a fixed positive integer and c is a fixed real number:

sequence	abbreviation	OGF (explicit)	OGF (concise)
$1, 1, 1, 1, \ldots$	$\{1\}_{k\geq 0}$	$\sum_{k\geq 0} x^k$	$\frac{1}{1-x}$
$1, -1, 1, -1, \ldots$	$\{(-1)^k\}_{k\geq 0}$	$\sum_{k\geq 0}(-1)^k x^k$	$\frac{1}{1+x}$
$1, c, c^2, c^3, \ldots$	$\{c^k\}_{k\geq 0}$	$\sum_{k\geq 0} c^k x^k$	$\frac{1}{1-cx}$
$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \ldots$	$\left\{\binom{n}{k}\right\}_{k\geq 0}$	$\sum_{k\geq 0}\binom{n}{k}x^k$	$(1+x)^n$
$\left(\!\binom{n}{0}\!\right), \left(\!\binom{n}{1}\!\right), \left(\!\binom{n}{2}\!\right), \left(\!\binom{n}{3}\!\right), \ldots$	$\left\{\left(\!\binom{n}{k}\!\right)\right\}_{k\geq 0}$	$\sum_{k\geq 0}\left(\!\binom{n}{k}\!\right)x^k$	$\frac{1}{(1-x)^n}$

Of course, the first two lines of the table are special cases of the third.

Question 116 *What is the coefficient of x^k in $\dfrac{1}{(1-5x)^9}$?*

The following examples illustrate how to use these facts in solving combinatorial problems.

Example: a distribution problem

In how many ways can we distribute 15 identical objects to 6 distinct recipients if each recipient receives at least one object?

Think of this as counting the solutions to $z_1 + z_2 + \cdots + z_6 = 15$ where each $z_i \in \{1, 2, 3, \ldots\}$. This means that to get the OGF we multiply six copies of $x + x^2 + x^3 + \ldots$ together,

$$(x + x^2 + x^3 + \cdots)^6,$$

and the answer is the coefficient of x^{15}.

This OGF is not one we recognize until we factor out an x:

$$x + x^2 + x^3 + \cdots = x(1 + x + x^2 + \cdots) = x \cdot \frac{1}{1-x}.$$

So the concise OGF is $\frac{x^6}{(1-x)^6}$. To get the coefficient of x^{15} in this, it stands to reason that we just need to find the coefficient of $x^{15-6} = x^9$ in $\frac{1}{(1-x)^6}$. Because we recognize this as the OGF for $\left\{\left(\!\binom{6}{k}\!\right)\right\}_{k \geqslant 0}$, the answer is $\left(\!\binom{6}{9}\!\right) = 2002$.

It is worth mentioning how the factor x^6 comes into play. It changes the coefficient that we seek from the one on x^{15} to the one on x^9. Combinatorially this corresponds to distributing one object to each of the 6 recipients (there is one way to do that), and then distributing the remaining $15 - 6 = 9$ objects with no restrictions.

Question 117 *Use an OGF to answer the same question but where each recipient receives at least two objects.*

Example: another distribution problem

In how many ways can we distribute k identical objects to 4 distinct recipients if recipient 1 receives at most two objects?

This is equivalent to counting the solutions to $z_1 + z_2 + z_3 + z_4 = k$ in nonnegative integers z_i where $z_1 \leqslant 2$. The generating function is

$$(1 + x + x^2)(1 + x + x^2 + x^3 + \cdots)^3 = \frac{1 + x + x^2}{(1-x)^3}.$$

Expanded this is

$$\frac{1}{(1-x)^3} + \frac{x}{(1-x)^3} + \frac{x^2}{(1-x)^3}.$$

To find the coefficient of x^k in the above expression, we just find the coefficient of x^k in each of the three terms and add them. The answer is

$$\left(\!\binom{3}{k}\!\right) + \left(\!\binom{3}{k-1}\!\right) + \left(\!\binom{3}{k-2}\!\right).$$

This is because, for example, the coefficient of x^k in $1/(1-x)^3$ is $\left(\!\binom{3}{k}\!\right)$, so the coefficient of x^k in $x/(1-x)^3$ is $\left(\!\binom{3}{k-1}\!\right)$.

Question 118 *Explain this answer combinatorially. How could you have derived it without generating functions?*

Example: die-rolling and an important identity

In how many ways can we get a sum of 18 when five dice are rolled?

Letting z_i be the value showing on the i-th die, we want the solutions to $z_1 + z_2 + z_3 + z_4 + z_5 = 18$ where each $z_i \in \{1, 2, 3, 4, 5, 6\}$. Thus we want the coefficient of x^{18} in

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^5.$$

How can we find this coefficient without the aid of a computer and without multiplying it all out by hand? First notice that

$$(x + x^2 + x^3 + x^4 + x^5 + x^6)^5 = x^5(1 + x + x^2 + x^3 + x^4 + x^5)^5.$$

Now we use the identity $1+x+x^2+x^3+x^4+x^5 = \dfrac{1-x^6}{1-x}$ of Theorem 3.2.2. Substitute in to get the OGF

$$x^5 \left(\frac{1-x^6}{1-x}\right)^5 = x^5 \cdot (1-x^6)^5 \cdot \frac{1}{(1-x)^5}.$$

We want the coefficient of x^{18} in this OGF. It equals the coefficient of $x^{18-5} = x^{13}$ in

$$(1-x^6)^5 \cdot \frac{1}{(1-x)^5}.$$

To get that, it is best to look at the expanded form of both terms in this product. The expansion of $(1-x^6)^5$ can be done with the binomial theorem:

$$(1-x^6)^5 = \binom{5}{0} - \binom{5}{1}x^6 + \binom{5}{2}x^{12} - \binom{5}{3}x^{18} + \binom{5}{4}x^{24} - \binom{5}{5}x^{30}.$$

The expansion of $1/(1-x)^5$ is by now familiar:

$$\frac{1}{(1-x)^5} = \left(\!\!\binom{5}{0}\!\!\right) + \left(\!\!\binom{5}{1}\!\!\right)x + \left(\!\!\binom{5}{2}\!\!\right)x^2 + \left(\!\!\binom{5}{3}\!\!\right)x^3 + \cdots.$$

The OGF is the product of these two expressions, so to find the coefficient of x^{13} in that product we need to determine how the x^{13} term arises when we do the multiplication. Only three terms contribute:

- The $\binom{5}{0}$ term in $(1-x^6)^5$ times the $\left(\!\!\binom{5}{13}\!\!\right)x^{13}$ term in $1/(1-x)^5$.
- The $-\binom{5}{1}x^6$ term in $(1-x^6)^5$ times the $\left(\!\!\binom{5}{7}\!\!\right)x^7$ term in $1/(1-x)^5$.
- The $\binom{5}{2}x^{12}$ term in $(1-x^6)^5$ times the $\left(\!\!\binom{5}{1}\!\!\right)x$ term in $1/(1-x)^5$.

The answer is

$$\binom{5}{0}\left(\!\!\binom{5}{13}\!\!\right) - \binom{5}{1}\left(\!\!\binom{5}{7}\!\!\right) + \binom{5}{2}\left(\!\!\binom{5}{1}\!\!\right) = 780.$$

Summary

A generating function is a power series that stores a number sequence. The ordinary generating function (OGF) for the sequence $a_0, a_1, a_2, \ldots$ is $\sum_{k\geqslant 0} a_k x^k$. Typical combinatorial applications of generating functions involve computations like those of the product principle: we determine a generating function for each way to specify the objects being counted and then multiply them. The algebraic act of multiplying and combining like terms does the counting for us.

Generating functions are especially good at answering questions like: How many n-lists $(z_1, z_2, \ldots, z_n)$ of nonnegative integers satisfy $z_1 + z_2 + \cdots + z_n = k$ and possibly some additional restrictions? We gave several examples of these.

Exercises

1. In football, a team scores points in the following ways: two points (safety), three points (field goal), six points (touchdown only), seven points (touchdown plus extra point), and eight points (touchdown plus two-point conversion). Find a concise OGF of $\{a_k\}_{k\geqslant 0}$ where a_k is the number of ways a team can score a total of k points.
2. In each case, find a concise OGF for answering the question and also identify what coefficient you need.
   (a) How many ways are there to distribute 14 forks to 10 people so that each person receives one or two forks?
   (b) You can buy soda either by the can, or in 6-, 12-, 24-, or 30-packs. How many ways are there to buy exactly k cans of soda?
   (c) How many ways are there to put a total postage of 75 cents on an envelope, using 3-, 5-, 10-, and 12-cent stamps?
   (d) At the movies you select 24 pieces of candy from among five different types. How many ways can you do this if you want at least two pieces of each type?
   (e) How many solutions to $z_1 + z_2 + z_3 = 15$ are there, where the z_i are integers satisfying $0 \leqslant z_i \leqslant 8$?
   (f) How many ways are there to make change for a dollar using only pennies, nickels, dimes, and quarters?
3. Find the coefficient of...
   (a) x^{60} in $\dfrac{1}{(1-x)^{23}}$.
   (b) x^k in $\dfrac{1+x+x^4}{(1-x)^5}$.
   (c) x^3 in $\dfrac{x}{(1-x)^8}$.
   (d) x^{50} in $(x^9 + x^{10} + x^{11} + \cdots)^3$.
   (e) x^{k-1} in $\dfrac{1+x}{(1-2x)^5}$.
4. A professor grades an exam that has 20 questions worth five points each. The professor awards zero, two, four, or five points on each problem. Find a concise OGF that can be used to determine the number of ways to obtain an exam score of k points.

5. A restaurant offers chicken wings at the following sizes and prices.

number of wings	7	10	15	25	60	120
price	\$5.49	\$7.49	\$10.49	\$15.99	\$35.99	\$69.99

   (a) Determine a concise OGF so that the coefficient of x^k equals the number of ways to order exactly k wings.
   (b) Determine a concise OGF so that the coefficient of x^k equals the number of ways to spend exactly k dollars. (Can you keep the units in dollars or do you need to make an adjustment?)

6. Find the number of ways to distribute 15 identical pieces of candy to eight people so that five of the people (being adults) receive at most one piece while the other three (being children) can receive any number.
7. Find the number of solutions to $z_1 + z_2 + z_3 + z_4 = 10$ where the z_i are nonnegative integers such that $z_1 \leqslant 4$, z_2 is odd, z_3 is prime, and $z_4 \in \{1, 2, 3, 6, 8\}$.
8. Find the number of solutions to $6z_1 + 9z_2 + 20z_3 = 150$ where the z_i are nonnegative integers.
9. Use partial fraction decomposition to find the coefficient of x^k in each OGF.
   (a) $\dfrac{1}{(1-x)(1-2x)}$
   (b) $\dfrac{1}{(1-x)(1-x^2)}$

3.4 Using generating functions, part II

In this second section on generating functions we practice the algebraic manipulations needed to extract coefficients and therefore solve counting problems. We also derive some combinatorial identities and encounter an amazing proof of Euler regarding integer partitions. Finally, we introduce the exponential generating function.

Notation for coefficient extraction

Because answering a combinatorial question often amounts to finding a coefficient in a certain generating function, it helps to have notation to streamline the process. If $f(x)$ is a generating function, then we define

$$\Big[\!\Big[f(x) \Big]\!\Big]_{x^k} = \text{the coefficient of } x^k \text{ in } f(x).$$

So if $f(x) = \sum_{k \geqslant 0} a_k x^k$, then $\Big[\!\Big[f(x) \Big]\!\Big]_{x^k} = a_k$.

Here are some properties of this notation. An explanation or proof of each follows.

1. $\Big[\!\Big[c \cdot f(x) \Big]\!\Big]_{x^k} = c \cdot \Big[\!\Big[f(x) \Big]\!\Big]_{x^k}$
2. $\Big[\!\Big[f(x) + g(x) \Big]\!\Big]_{x^k} = \Big[\!\Big[f(x) \Big]\!\Big]_{x^k} + \Big[\!\Big[g(x) \Big]\!\Big]_{x^k}$
3. $\Big[\!\Big[x^j \cdot f(x) \Big]\!\Big]_{x^k} = \Big[\!\Big[f(x) \Big]\!\Big]_{x^{k-j}}$

4. $\left[\!\left[\frac{1}{1-cx}\right]\!\right]_{x^k} = c^k$
5. $\left[\!\left[(1+x)^n\right]\!\right]_{x^k} = \binom{n}{k}$
6. $\left[\!\left[\frac{1}{(1-x)^n}\right]\!\right]_{x^k} = \left(\!\binom{n}{k}\!\right)$

Properties #1-3 have intuitive appeal, and in fact we already used them in our examples in the last section. In particular, Property #1 says that scaling an OGF by a constant c simply scales each coefficient by c. Property #2 says that we may find the coefficient of x^k in the sum of two OGFs by finding the coefficient of x^k in each OGF and adding them. Property #3 says that multiplying an OGF by x^j shifts the location of each coefficient to the right by j places.

Question 119 *Assuming $f(x) = \sum_{k\geqslant 0} a_k x^k$ and $g(x) = \sum_{k\geqslant 0} b_k x^k$ are arbitrary OGFs, prove properties #1 and #3.*

Each of properties #4-6 represents a different way to write a fact you learned in the last section. For example, property #5 just says that $(1+x)^n$ is the OGF of the binomial coefficients $\binom{n}{k}$.

If you recall the die-rolling example of the last section—In how many ways can we get a sum of 18 when five dice are rolled?—the answer was the coefficient of x^{15} in $x^6/(1-x)^6$. Using our new notation, we would find this coefficient as follows:

$$\left[\!\left[\frac{x^6}{(1-x)^6}\right]\!\right]_{x^{15}} = \left[\!\left[\frac{1}{(1-x)^6}\right]\!\right]_{x^9} = \left(\!\binom{6}{9}\!\right).$$

Question 120 *Find $\left[\!\left[(x+x^2)^{10}\right]\!\right]_{x^{14}}$. Begin by factoring out a power of x.*

Another example from the previous section—In how many ways can we distribute k identical objects to 4 distinct recipients if recipient 1 must receive at most two objects?—required finding the coefficient of x^k in $(1+x+x^2)/(1-x)^3$. In new notation,

$$\begin{aligned}
\left[\!\left[\frac{1+x+x^2}{(1-x)^3}\right]\!\right]_{x^k} &= \left[\!\left[\frac{1}{(1-x)^3} + \frac{x}{(1-x)^3} + \frac{x^2}{(1-x)^3}\right]\!\right]_{x^k} \\
&= \left[\!\left[\frac{1}{(1-x)^3}\right]\!\right]_{x^k} + \left[\!\left[\frac{x}{(1-x)^3}\right]\!\right]_{x^k} + \left[\!\left[\frac{x^2}{(1-x)^3}\right]\!\right]_{x^k} \\
&= \left[\!\left[\frac{1}{(1-x)^3}\right]\!\right]_{x^k} + \left[\!\left[\frac{1}{(1-x)^3}\right]\!\right]_{x^{k-1}} + \left[\!\left[\frac{1}{(1-x)^3}\right]\!\right]_{x^{k-2}} \\
&= \left(\!\binom{3}{k}\!\right) + \left(\!\binom{3}{k-1}\!\right) + \left(\!\binom{3}{k-2}\!\right).
\end{aligned}$$

Question 121 *What is the coefficient of x^8 in $\frac{(1+x)^2}{1-3x}$?*

The convolution formula for OGFs

Because most problems that we have solved using generating functions involve multiplying them, we need an understanding of how this happens. In other words, if $f(x)$ and $g(x)$ are the OGFs of two sequences, then what is the sequence for which $f(x)\cdot g(x)$ is the OGF?

Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots$. Try multiplying these out using the distributive law of algebra:

$$(a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots)(b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots).$$

When you do, you get

$$\begin{aligned} &a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 \\ &\quad + (a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0)x^3 + \cdots \end{aligned}$$

In general, the coefficient of x^k is

$$a_0b_k + a_1b_{k-1} + a_2b_{k-2} + \cdots + a_{k-2}b_2 + a_{k-1}b_1 + a_kb_0$$

or $\sum_{j=0}^{k} a_jb_{k-j}$. This is known as the convolution formula for OGFs.

Theorem 3.4.1 (convolution of OGFs) *If* $f(x) = \sum_{j\geqslant 0} a_jx^j$ *and* $g(x) = \sum_{j\geqslant 0} b_jx^j$, *then for any* $k \geqslant 0$,

$$\Big[\!\Big[f(x)\cdot g(x) \Big]\!\Big]_{x^k} = \sum_{j=0}^{k} a_jb_{k-j}.$$

In the context of formal power series, this is simply how multiplication of series is *defined*—it's not a true theorem. With addition of power series defined in the natural way and multiplication defined according to the convolution formula, these operations have the necessary properties (commutativity, associativity, etc.) that allow the theory of algebraic structures to justify our generating function calculations. See the exercises if you're interested in investigating some of this.

Using the convolution formula

The convolution formula allows for effortless derivation of some combinatorial identities. These derivations feel like combinatorial proofs in that we ask a question and answer it in two ways. The question we ask is not, "How many?" but rather, "What is the coefficient?" In combinatorial proofs, the creativity comes in asking the right question. In these algebraic proofs, the creativity comes in producing the correct algebraic expression.

Vandermonde's formula, rediscovered

Of course $(1 + x)^{10} = (1 + x)^6 \cdot (1 + x)^4$ is true by the laws of algebra. From an OGF point of view, this means that *the coefficient of* x^k *in* $(1 + x)^{10}$ *equals the coefficient of* x^k *in* $(1 + x)^6 \cdot (1 + x)^4$. In other words,

$$\Big[\!\Big[(1+x)^{10} \Big]\!\Big]_{x^k} = \Big[\!\Big[(1+x)^4\cdot(1+x)^6 \Big]\!\Big]_{x^k}. \tag{3.13}$$

Try calculating each coefficient. The coefficient on the left is familiar:

$$\Big[\!\Big[(1+x)^{10} \Big]\!\Big]_{x^k} = \binom{10}{k}.$$

Now attack the coefficient on the right with convolution. Since

$$(1+x)^6 \cdot (1+x)^4 = \left(\sum_{k\geqslant 0}\binom{6}{k}x^k\right)\left(\sum_{k\geqslant 0}\binom{4}{k}x^k\right),$$

apply the convolution formula to get

$$\left[\!\left[(1+x)^6 \cdot (1+x)^4\right]\!\right]_{x^k} = \sum_{j=0}^{k}\binom{6}{j}\binom{4}{k-j}.$$

Since these coefficients are equal—by equation (3.13) above—we just proved that

$$\sum_{j=0}^{k}\binom{6}{j}\binom{4}{k-j} = \binom{10}{k}.$$

There is a combinatorial way to prove this. Begin by asking the question: how many k-committees can be formed from a group of six men and four women?

Question 122 *Finish the combinatorial proof of this identity.*

When applied in general, this idea results in the identity known as Vandermonde's formula. We gave a combinatorial proof in Section 2.2.

Theorem 3.4.2 (Vandermonde's formula) *For integers $m, n, k \geqslant 0$,*

$$\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j} = \binom{m+n}{k}.$$

Proof: Let $m, n, k \geqslant 0$. Observe that

$$(1+x)^{m+n} = (1+x)^m \cdot (1+x)^n. \tag{3.14}$$

What is the coefficient of x^k in each of these expressions?

We know the coefficient on the left-hand side is

$$\left[\!\left[(1+x)^{m+n}\right]\!\right]_{x^k} = \binom{m+n}{k}.$$

For the right-hand side, since

$$(1+x)^m \cdot (1+x)^n = \left(\sum_{j\geqslant 0}\binom{m}{k}x^j\right)\left(\sum_{j\geqslant 0}\binom{n}{k}x^j\right),$$

the convolution formula then implies that the coefficient on the right-hand side is

$$\left[\!\left[(1+x)^m \cdot (1+x)^n\right]\!\right]_{x^k} = \sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}.$$

These coefficients are equal by equation (3.14), and the formula follows. ■

A multichoose-coefficient identity

From the equation

$$\frac{1}{(1-x)^n} = \frac{1}{(1-x)^{n-1}} \cdot \frac{1}{1-x}$$

what identity can we derive?

As in the previous example, begin by equating the coefficient of x^k on the left-hand and right-hand sides. On the left,

$$\left[\!\left[\frac{1}{(1-x)^n} \right]\!\right]_{x^k} = \left(\!\binom{n}{k}\!\right).$$

On the right we know that

$$\frac{1}{(1-x)^{n-1}} \cdot \frac{1}{1-x} = \left(\sum_{j \geqslant 0} \left(\!\binom{n-1}{j}\!\right) x^j \right) \left(\sum_{j \geqslant 0} x^j \right),$$

so by the convolution formula

$$\left[\!\left[\frac{1}{(1-x)^{n-1}} \cdot \frac{1}{1-x} \right]\!\right]_{x^k} = \sum_{j=0}^{k} \left(\!\binom{n-1}{j}\!\right) \cdot 1 = \sum_{j=0}^{k} \left(\!\binom{n-1}{j}\!\right).$$

(Notice that the coefficient of x^k in $\frac{1}{1-x}$ is always 1.) This proves the identity

$$\left(\!\binom{n}{k}\!\right) = \sum_{j=0}^{k} \left(\!\binom{n-1}{j}\!\right).$$

Question 123 *What familiar identity results from* $(1+x)^n = (1+x)^{n-1} \cdot (1+x)$*? Prove your answer.*

Counting certain distributions

In how many ways can you distribute 20 identical objects to 10 distinct recipients such that each recipient receives at most five objects?

OGFs and the convolution formula make this problem automatic. This problem is equivalent to counting the solutions to

$$\begin{aligned} z_1 + z_2 + \cdots + z_{10} &= 20 \\ \text{each } z_i &\in \{0, 1, 2, 3, 4, 5\} \end{aligned}$$

and so the answer is the coefficient of x^{20} in

$$(1 + x + x^2 + x^3 + x^4 + x^5)^{10}.$$

Replace $1 + x + x^2 + \cdots + x^5$ by $\frac{1-x^6}{1-x}$ and extract the coefficient of x^{20} in the resulting

expression:

$$\begin{aligned}\left[\!\!\left[\left(\frac{1-x^6}{1-x}\right)^{10}\right]\!\!\right]_{x^{20}} &= \left[\!\!\left[(1-x^6)^{10}\cdot\frac{1}{(1-x)^{10}}\right]\!\!\right]_{x^{20}}\\ &= \left[\!\!\left[\left(\sum_{j\geqslant 0}\binom{10}{j}(-x^6)^j\right)\left(\sum_{j\geqslant 0}\left(\!\!\binom{10}{j}\!\!\right)x^j\right)\right]\!\!\right]_{x^{20}}\\ &= \left[\!\!\left[\left(\sum_{j\geqslant 0}\binom{10}{j}(-1)^j x^{6j}\right)\left(\sum_{j\geqslant 0}\left(\!\!\binom{10}{j}\!\!\right)x^j\right)\right]\!\!\right]_{x^{20}}.\end{aligned}$$

Rather than blindly applying the convolution formula, it is perhaps best to write out the first few terms of the sum on the left: we want the coefficient of x^{20} in

$$= \left(\binom{10}{0} - \binom{10}{1}x^6 + \binom{10}{2}x^{12} - \binom{10}{3}x^{18} + \cdots\right)\left(\sum_{k\geqslant 0}\left(\!\!\binom{10}{k}\!\!\right)x^k\right).$$

What terms in each sum contribute to the x^{20} term when carrying out the multiplication? There are four pairs that do:

term in first sum	term in second sum	resulting term in product
$\binom{10}{0}$	$\left(\!\!\binom{10}{20}\!\!\right)x^{20}$	$\binom{10}{0}\left(\!\!\binom{10}{20}\!\!\right)x^{20}$
$-\binom{10}{1}x^6$	$\left(\!\!\binom{10}{14}\!\!\right)x^{14}$	$-\binom{10}{1}\left(\!\!\binom{10}{14}\!\!\right)x^{20}$
$\binom{10}{2}x^{12}$	$\left(\!\!\binom{10}{8}\!\!\right)x^{8}$	$\binom{10}{2}\left(\!\!\binom{10}{8}\!\!\right)x^{20}$
$-\binom{10}{3}x^{18}$	$\left(\!\!\binom{10}{2}\!\!\right)x^{2}$	$-\binom{10}{3}\left(\!\!\binom{10}{2}\!\!\right)x^{20}$

So the coefficient of x^{20} is

$$\binom{10}{0}\left(\!\!\binom{10}{20}\!\!\right) - \binom{10}{1}\left(\!\!\binom{10}{14}\!\!\right) + \binom{10}{2}\left(\!\!\binom{10}{8}\!\!\right) - \binom{10}{3}\left(\!\!\binom{10}{2}\!\!\right)$$

which equals 2,930,455.

Perhaps you recognize this answer as one that might result from applying inclusion-exclusion. (The alternating signs give it away.) If you did Exercise 8 in Section 3.1, then you obtained this very same answer but with inclusion-exclusion. Use whichever method you prefer. It is worth marveling, however, at how the factor $(1-x^6)^{10}$ produces the correct binomial coefficients with the correct signs!

Question 124 *What is the coefficient of x^7 in $\left(\dfrac{1-x^3}{1-x}\right)^5$?*

Partitions, OGFs, and Euler

The OGF of the partition numbers

We know and have used the OGFs for the binomial and multichoose coefficients. We will find the OGF of the Stirling numbers of the second kind in Section 4.3. How about the OGF of the integer partition numbers $P(n)$?

In an example from Section 3.3 we found that the number of partitions of 12 into parts of size at most 5 equals the coefficient of x^{12} in the OGF

$$\frac{1}{(1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)}.$$

In fact, this is the OGF for the number of partitions of n into parts of size at most 5:

$$\left[\!\left[\frac{1}{(1-x)(1-x^2)\cdots(1-x^5)}\right]\!\right]_{x^n} = \text{partitions of } n \text{ into parts of size at most 5.}$$

Question 125 *Find an OGF so that the coefficient of x^k equals the number of partitions of k into parts of size 3, 5, 7, or 9.*

The same reasoning shows that if we simply extend the product in the denominator to include all factors $1-x^j$ for $j \geqslant 1$, then we get the OGF for the partition numbers.

Theorem 3.4.3 *The OGF of the integer partition numbers $\{P(n)\}_{n\geqslant 0}$ is*

$$\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} = \prod_{j\geqslant 1}\frac{1}{1-x^j}.$$

Euler's amazing discovery

It is Leonhard Euler whom mathematicians credit with the first use of the generating function. Perhaps Euler's most famous result involving generating functions is his proof that the number of partitions of n into odd parts equals the number of partitions of n into distinct parts. It is beautiful, clever, and short. Here it is.

Let o_n equal the number of partitions of n into odd parts and let d_n equal the number of partitions of n into distinct parts. Let $O(x) := \sum_{n\geqslant 0} o_n x^n$ and $D(x) := \sum_{n\geqslant 0} d_n x^n$ be their OGFs. Euler proved the result by showing that $O(x) = D(x)$.

To construct $O(x)$ we can start with the OGF of Theorem 3.4.3 and remove the terms corresponding to parts of even size:

$$O(x) = \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots}.$$

To construct $D(x)$ we just observe that each part can be included 0 or 1 times, so

$$D(x) = (1+x)(1+x^2)(1+x^3)(1+x^4)\cdots.$$

Now here's the most important part of the whole proof. Notice that for $j \geqslant 1$,

$$(1-x^j)(1+x^j) = 1-x^{2j}$$

which means that

$$1+x^j = \frac{1-x^{2j}}{1-x^j}.$$

Do this to each term of $D(x)$ and then cancel all that you can, which amounts to *every* term in the numerator and *every other* term in the denominator:

$$\begin{aligned} D(x) &= (1+x)(1+x^2)(1+x^3)(1+x^4)\cdots \\ &= \frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\cdot\frac{1-x^8}{1-x^4}\cdot\cdots \\ &= \frac{1}{(1-x)(1-x^3)(1-x^5)\cdots} \\ &= O(x). \end{aligned}$$

That's it!

Theorem 3.4.4 (Euler) *The number of partitions of n into distinct parts equals the number of partitions of n into odd parts.*

Exponential generating functions

The next most useful type of generating function in combinatorics is the exponential generating function. Let's take a brief look at it. The reason for its use will become clear in subsequent material.

The most important power series from calculus is that for e^x, namely

$$e^x = \sum_{k\geq 0} \frac{x^k}{k!} \qquad \text{for } |x| < \infty.$$

In combinatorics, one way of interpreting this is that e^x is the OGF of the sequence $\{\frac{1}{k!}\}_{k\geq 0}$ because the coefficient of x^k is $\frac{1}{k!}$.

But that is not the most useful interpretation. We also consider e^x to be the *exponential generating function* of the sequence $1, 1, 1, 1, \ldots$ because the coefficient of $\frac{x^k}{k!}$ is always 1. In an exponential generating function, the placeholder for a_k is $\frac{x^k}{k!}$ rather than x^k.

Definition 3.4.5 (EGF) *The **exponential generating function (EGF)** of the number sequence $\{a_k\}_{k\geq 0}$ is defined as* $\displaystyle\sum_{k\geq 0} a_k \frac{x^k}{k!}$.

You must first strive to understand the somewhat subtle difference between OGFs and EGFs. It helps to start with the familiar functions

$$\frac{1}{1-x}, \qquad e^x, \qquad \text{and} \qquad (1+x)^n,$$

and ask the question, "For what sequence is each of these the EGF?"

Notice that (use the old multiply-by-1 trick, where 1 looks like $\frac{k!}{k!}$ in this case)

$$\frac{1}{1-x} = \sum_{k\geq 0} x^k = \sum_{k\geq 0} k! \frac{x^k}{k!},$$

so although $\frac{1}{1-x}$ is the *ordinary* generating function of the sequence $\{1\}_{k\geq 0}$, it is simultaneously the *exponential* generating function of the sequence $\{k!\}_{k\geq 0}$. Put another way,

$$\left[\!\left[\frac{1}{1-x} \right]\!\right]_{x^k} = 1$$

while, using the obvious extension of our coefficient-extraction notation,

$$\left[\!\left[\frac{1}{1-x} \right]\!\right]_{x^k/k!} = k!.$$

So what then is the EGF of the all-1s sequence $\{1\}_{k\geq 0}$? It is e^x because

$$\left[\!\left[e^x \right]\!\right]_{x^k/k!} = \left[\!\left[\sum_{k\geq 0} \frac{x^k}{k!} \right]\!\right]_{x^k/k!} = 1.$$

In fact, for any real number c,

$$e^{cx} = \sum_{k\geq 0} \frac{(cx)^k}{k!} = \sum_{k\geq 0} c^k \frac{x^k}{k!},$$

and so e^{cx} is the EGF of the sequence $\{c^k\}_{k\geq 0}$.

For $(1+x)^n$ we can use $\binom{n}{k} = \frac{(n)_k}{k!}$ to write

$$\begin{aligned}\left[\!\left[(1+x)^n\right]\!\right]_{x^k/k!} &= \left[\!\left[\sum_{k\geq 0}\binom{n}{k}x^k\right]\!\right]_{x^k/k!} \\ &= \left[\!\left[\sum_{k\geq 0}(n)_k\frac{x^k}{k!}\right]\!\right]_{x^k/k!} \\ &= (n)_k.\end{aligned}$$

This means that $(1+x)^n$ is the EGF of $\{(n)_k\}_{k\geq 0}$. Combinatorially, $(1+x)^n$ is the OGF for the k-subsets of an n-set while it is the EGF for the k-permutations of an n-set.

Question 126 *What is the coefficient of $\frac{x^5}{5!}$ in $(1+x)^9$? What is the coefficient of x^5 in $(1+x)^9$?*

The following table summarizes our work on EGFs.

sequence	abbreviation	EGF (explicit)	EGF (concise)
$1, 1, 1, 1, \ldots$	$\{1\}_{k\geq 0}$	$\sum_{k\geq 0}\frac{x^k}{k!}$	e^x
$1, -1, 1, -1, \ldots$	$\{(-1)^k\}_{k\geq 0}$	$\sum_{k\geq 0}(-1)^k\frac{x^k}{k!}$	e^{-x}
$1, c, c^2, c^3, \ldots$	$\{c^k\}_{k\geq 0}$	$\sum_{k\geq 0}c^k\frac{x^k}{k!}$	e^{cx}
$(n)_0, (n)_1, (n)_2, (n)_3, \ldots$	$\{(n)_k\}_{k\geq 0}$	$\sum_{k\geq 0}(n)_k\frac{x^k}{k!}$	$(1+x)^n$
$0!, 1!, 2!, 3!, \ldots$	$\{k!\}_{k\geq 0}$	$\sum_{k\geq 0}k!\frac{x^k}{k!}$	$\frac{1}{1-x}$

The convolution formula for EGFs

As for OGFs, there is a convolution formula for EGFs. The question is: if $f(x)$ and $g(x)$ are the EGFs of the sequences $\{a_k\}_{k\geq 0}$ and $\{b_k\}_{k\geq 0}$, then what is the sequence that has $f(x)\cdot g(x)$ as its EGF?

This can be accomplished using the convolution formula for OGFs and a quick observation. The quick observation is the link between doing coefficient extraction on OGFs and on EGFs, namely

$$\left[\!\left[f(x)\right]\!\right]_{x^k/k!} = k!\cdot\left[\!\left[f(x)\right]\!\right]_{x^k}.$$

We will use the convolution formula in the next section to solve recurrence relations.

Theorem 3.4.6 (convolution of EGFs) *If $f(x) = \sum_{j\geq 0} a_j\frac{x^j}{j!}$ and $g(x) = \sum_{j\geq 0} b_j\frac{x^j}{j!}$, then for any $k \geq 0$,*

$$\left[\!\left[f(x)\cdot g(x)\right]\!\right]_{x^k/k!} = \sum_{j=0}^{k}\binom{k}{j}a_j b_{k-j}.$$

Proof: Let $f(x)$ and $g(x)$ be the EGFs of the hypothesis. Then

$$\left[\!\left[f(x)\cdot g(x)\right]\!\right]_{x^k/k!} = k!\cdot\left[\!\left[f(x)\cdot g(x)\right]\!\right]_{x^k}.$$

Now find the coefficient using the convolution formula for OGFs and simplify:

$$\begin{aligned} k!\cdot\left[\!\left[f(x)\cdot g(x)\right]\!\right]_{x^k} &= k!\cdot\left[\!\left[\left(\sum_{j\geq 0}\frac{a_j}{j!}x^j\right)\left(\sum_{j\geq 0}\frac{b_j}{j!}x^j\right)\right]\!\right]_{x^k} \\ &= k!\sum_{j=0}^{k}\frac{a_j}{j!}\frac{b_{k-j}}{(k-j)!} \\ &= \sum_{j=0}^{k}\frac{k!}{j!(k-j)!}a_j b_{k-j} \\ &= \sum_{j=0}^{k}\binom{k}{j}a_j b_{k-j}. \end{aligned}$$

■

A quick example

Suppose that the EGF of the sequence $\{a_k\}_{k\geq 0}$ is $\dfrac{e^{2x}}{1-x}$. What is a_k?

Since e^{2x} is the EGF of $\{2^j\}_{j\geq 0}$ and $1/(1-x)$ is the EGF of $\{j!\}_{j\geq 0}$, apply the convolution formula for EGFs with $a_j = 2^j$ and $b_j = j!$ to get

$$\begin{aligned} a_k &= \left[\!\left[e^{2x}\cdot\frac{1}{1-x}\right]\!\right]_{x^k/k!} \\ &= \sum_{j=0}^{k}\binom{k}{j}2^j(k-j)! \\ &= k!\sum_{j=0}^{k}\frac{2^j}{j!}. \end{aligned}$$

Question 127 *Find a formula for the k-th term of the sequence having EGF* $\dfrac{(1+x)^8}{e^x}$.

Summary

The convolution formula for OGFs is a fundamental tool because it allows for analysis of a sequence whose OGF is expressed as a product. As such, many combinatorial identities can be easily derived from convolution simply by comparing coefficients on both sides of an algebraic identity.

The exponential generating function (EGF) is similar to the OGF except that the "placeholder" for the k-th term of the sequence is $x^k/k!$ rather than just x^k. As for OGFs, the convolution formula for EGFs is useful. The sections and chapters to follow should give you insight into how to make the choice between using an OGF or EGF.

Exercises

1. Determine the number of ways to place an order for a dozen donuts where there are six different varieties available and you order between one and four (inclusive) of each variety.
2. Derive a combinatorial identity via the equation
$$\frac{1}{(1-x)^{m+n}} = \frac{1}{(1-x)^m} \cdot \frac{1}{(1-x)^n}.$$
3. Use the convolution formula to find the coefficient of x^k in $\dfrac{(1+x)^n}{(1-x)^m}$.
4. Give an example of a distribution-counting question whose answer is the coefficient of x^k in the OGF given in Exercise 3.
5. Let a, b, and c be nonzero real numbers. Find the coefficient of x^k in $\dfrac{a}{b+cx}$.
6. Let j and n be fixed positive integers. Find the coefficient of x^k in $\dfrac{1}{(1-x^j)^n}$.
7. Prove that if $c \neq 0$, then $\Big[\!\Big[f(x) \Big]\!\Big]_{cx^k} = \dfrac{1}{c} \cdot \Big[\!\Big[f(x) \Big]\!\Big]_{x^k}$.
8. Let a_n equal the number of n-letter passwords where each letter is A, B, or C. Explain why e^{3x} is the EGF for $\{a_n\}_{n \geqslant 0}$.
9. Suppose the EGF of $\{c_n\}_{n \geqslant 0}$ is $(e^x - 1)^2$. Find a formula for c_n.
10. Repeat the previous exercise for $(e^x - 1)^3$.
11. Here is how Euler proved that the binary representation of any nonnegative integer is unique. For $n \geqslant 0$, let b_n denote the number of ways to write n as a sum of powers of 2. Let $B(x)$ be the OGF of $\{b_n\}_{n \geqslant 0}$.
    (a) Explain why $B(x) = (1+x)(1+x^2)(1+x^4)(1+x^8)(1+x^{16})\cdots$.
    (b) Explain why $B(x) = (1+x)B(x^2)$.
    (c) Use part (b) to prove that $b_n = 1$ for all $n \geqslant 0$.
12. (abstract algebra) Let $\mathcal{P}$ be the set of all infinite sequences $[a_0, a_1, a_2, \ldots]$ where the a_i are complex numbers. For $f, g \in \mathcal{P}$, where
$$f = [a_0, a_1, a_2, \ldots] \qquad \text{and} \qquad g = [b_0, b_1, b_2, \ldots],$$
define addition $f + g := [a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots]$ and multiplication
$$f * g := [a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \ldots]$$
where in general the k-th element is $\sum_{i=0}^{k} a_i b_{k-i}$. Obviously $\mathcal{P}$ is closed under these operations.
    Prove that $(\mathcal{P}, +, *)$ is a commutative ring. (The associative property of $*$ requires care.)
13. (abstract algebra) This continues the previous exercise.
    (a) What are the additive and multiplicative identity elements in $\mathcal{P}$?
    (b) Show that $\mathcal{P}$ has no divisors of zero, and hence is an integral domain.

(c) The multiplicative inverse of $f \in \mathcal{P}$ is that $g \in \mathcal{P}$ for which $f * g = [1, 0, 0, 0, \ldots]$. Use f^{-1} to denote the multiplicative inverse of f.
Suppose $f = [a_0, a_1, a_2, \ldots]$. Prove that f^{-1} exists if and only if $a_0 \neq 0$.

Travel Notes

The use of generating functions by combinatorialists was in full force when Niven (1969) wrote a paper that made clear the reason, as mentioned in Section 3.3, when and why one can ignore the issue of convergence. He opens the paper by writing

> *Our purpose is to develop a systematic theory of formal power series. Such theory is known, or at least presumed, by many writers on mathematics, who use it to avoid questions of convergence in infinite series. What is done here is to formulate the theory on a proper logical basis and thus to reveal the absence of the convergence question. Thus "hard" analysis can be replaced by "soft" analysis in many applications.*

It can be argued that his paper was an important step in the establishment of combinatorics as a field in its own right. The exercises in this section labeled "abstract algebra" concern some basic results.

3.5 Techniques for solving recurrence relations

Recurrence relations are convenient ways to describe number sequences. We introduced them in Section 3.2. A most famous one is that which defines the sequence of Fibonacci numbers:

$$\begin{aligned} F_0 &= 1 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \qquad \text{for } n \geq 2. \end{aligned}$$

In this appears sufficient information to calculate the entire sequence, namely the *initial conditions* $F_0 = 1$, $F_1 = 1$; the *recurrence* $F_n = F_{n-1} + F_{n-2}$; and the *index set* $n \geq 2$ over which the recurrence is valid. We can start with the initial conditions and iteratively compute successive values:

$$\begin{aligned} F_0 &= 1 \\ F_1 &= 1 \\ F_2 &= F_1 + F_0 = 1 + 1 = 2 \\ F_3 &= F_2 + F_1 = 2 + 1 = 3 \\ F_4 &= F_3 + F_2 = 3 + 2 = 5 \\ F_5 &= F_4 + F_3 = 5 + 3 = 8 \\ &\vdots \end{aligned}$$

But we cannot, it appears, jump right to the 100th Fibonacci number F_{100} without computing all preceding values.

The goal of this section and the next is to determine formulas for the n-th term of a sequence defined by a recurrence relation. In a sense that is what it means to "solve" a recurrence relation: to have a non-recursive formula for the n-th term.

We have already met several recurrence relations. We can think of the familiar Pascal identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ as a dual recurrence in both n and k. In Theorem 2.3.3 on page 71 we proved the recurrence

$$B(n) = \sum_{j=0}^{n-1} \binom{n-1}{j} B(j)$$

for the Bell numbers. In Section 4.3 we show how to apply the techniques that we learn in this section to obtain a beautiful formula for the Bell number $B(n)$.

The approach to solving recurrence relations uses the recurrence and initial conditions to determine the generating function (either ordinary or exponential, depending) of the sequence and then extracts a formula for the n-th term by finding the coefficient of x^n or $\frac{x^n}{n!}$. This section highlights the techniques on particular examples.

An easy example with OGFs

We begin with a simple example that illustrates the method. Our goal is to find a formula for the n-th term of the sequence $\{a_n\}_{n\geqslant 0}$ defined by the recurrence relation

$$\begin{aligned} a_0 &= 1 \\ a_n &= 3a_{n-1} \qquad \text{for } n \geqslant 1. \end{aligned}$$

Though a formula for a_n is not hard to guess, it is best to start simple.

Question 128 *What appears to be a formula for a_n?*

The method works as follows. First define $f(x) := \sum_{n\geqslant 0} a_n x^n$ as the OGF of the sequence $\{a_n\}_{n\geqslant 0}$. Then use the recurrence to find a concise form for this generating function. Once found, extract the coefficient of x^n to get the formula for a_n.

Take the recurrence $a_n = 3a_{n-1}$ and multiply through by x^n to get

$$a_n x^n = 3a_{n-1}x^n.$$

Then, sum *over the values of the index n for which the recurrence is defined.* In this case, that's over $n \geqslant 1$, so we get

$$\sum_{n\geqslant 1} a_n x^n = \sum_{n\geqslant 1} 3a_{n-1}x^n. \tag{3.15}$$

Our goal now is to write this in terms of the OGF $f(x)$ which requires a little algebraic manipulation of each piece. The first sum equals $f(x)$ less its 0-th term a_0, which in turn equals 1 by the initial condition:

$$\sum_{n\geqslant 1} a_n x^n = \left(\sum_{n\geqslant 0} a_n x^n\right) - a_0 = f(x) - 1.$$

The sum on the right-hand side of equation (3.15) equals $3x \cdot f(x)$:

$$\sum_{n\geqslant 1} 3a_{n-1}x^n = 3x \sum_{n\geqslant 1} a_{n-1}x^{n-1} = 3x \cdot f(x).$$

Factoring out x accomplishes the necessary task of making the index on a_{n-1} agree with the power of x^{n-1}. (You'll be doing that a lot in what follows.)

Now substitute these pieces into the equation (3.15) to get

$$f(x) - 1 = 3x \cdot f(x).$$

Now we just solve for the unknown generating function $f(x)$:

$$f(x) - 1 = 3x \cdot f(x) \iff (1 - 3x) \cdot f(x) = 1 \iff f(x) = \frac{1}{1 - 3x}.$$

So $\frac{1}{1-3x}$ is the OGF of the sequence $\{a_n\}_{n\geqslant 0}$. The formula for a_n follows immediately by extracting the coefficient of x^n:

$$a_n = \left[\!\!\left[\frac{1}{1 - 3x} \right]\!\!\right]_{x^n} = 3^n,$$

so $a_n = 3^n$ for all $n \geqslant 0$.

An easy example with EGFs

Next let's look at the recurrence relation

$$\begin{aligned} b_0 &= 2 \\ b_n &= n b_{n-1} \qquad \text{for } n \geqslant 1. \end{aligned}$$

It is instructive to look at the first few terms.

Question 129 *What are the values of $b_1, b_2, \ldots, b_5$? Can you guess a formula for b_n? What if the initial condition were changed to $b_0 = 1$?*

This sequence yields easily to an EGF but not an OGF. Follow carefully to see if you can spot the reason.

Define $g(x) := \sum_{n\geqslant 0} b_n \frac{x^n}{n!}$ as the EGF of the sequence. Take the recurrence $b_n = n b_{n-1}$ and multiply it by $\frac{x^n}{n!}$ to get

$$b_n \frac{x^n}{n!} = n b_{n-1} \frac{x^n}{n!}$$

and then sum over $n \geqslant 2$ which are the values of n for which the recurrence is defined:

$$\sum_{n\geqslant 1} b_n \frac{x^n}{n!} = \sum_{n\geqslant 1} n b_{n-1} \frac{x^n}{n!}. \tag{3.16}$$

Now do the accounting trick to write this equation in terms of $g(x)$. The sum on the left is $g(x)$ less its 0-th term $b_0 = 2$:

$$\sum_{n\geqslant 1} b_n \frac{x^n}{n!} = \left(\sum_{n\geqslant 0} b_n \frac{x^n}{n!} \right) - b_0 = g(x) - 2.$$

The sum on the right-hand side of equation (3.16) needs b_{n-1} matched with $\frac{x^{n-1}}{(n-1)!}$ in order to relate to $g(x)$. Accomplish this by canceling the n and factoring out an x:

$$\sum_{n\geqslant 1} n b_{n-1} \frac{x^n}{n!} = \sum_{n\geqslant 1} b_{n-1} \frac{x^n}{(n-1)!} = x \sum_{n\geqslant 1} b_{n-1} \frac{x^{n-1}}{(n-1)!} = x \cdot g(x).$$

(See how nicely the EGF's denominator of $n!$ takes care of the n in the numerator?) The equation (3.16) is now equivalent to $g(x)-2 = x\cdot g(x)$. Solve for $g(x)$ to get $g(x) = \frac{2}{1-x}$. Now find b_n by extracting the the coefficient of $\frac{x^n}{n!}$ in $\frac{2}{1-x}$:

$$b_n = \left[\!\!\left[\frac{2}{1-x} \right]\!\!\right]_{x^n/n!} = 2 \cdot \left[\!\!\left[\frac{1}{1-x} \right]\!\!\right]_{x^n/n!} = 2 \cdot n!.$$

Therefore $b_n = 2 \cdot n!$ for all $n \geqslant 0$. (Remember that $\frac{1}{1-x}$ is the EGF of $\{n!\}_{n\geqslant 0}$.)

Another example with OGFs

Now let's do an OGF example that requires a little more work. We will find a formula for the n-th term of the sequence $\{c_n\}_{n\geqslant 0}$ defined by

$$\begin{aligned} c_0 &= 1 \\ c_n &= 4c_{n-1} + 1 \qquad \text{for } n \geqslant 1. \end{aligned}$$

Guessing a formula for c_n based on a few values is a little harder than in the previous examples.

Question 130 *What are the values $c_1, c_2, \ldots, c_5$? Can you guess a formula for c_n?*

Define $h(x) := \sum_{n=0}^{\infty} c_n x^n$ as the OGF for the sequence $\{c_n\}_{n=0}^{\infty}$. Begin with the recurrence and multiply the whole thing by x^n:

$$c_n x^n = 4c_{n-1}x^n + x^n.$$

Next, sum over $n \geqslant 1$ to get

$$\sum_{n\geqslant 1} c_n x^n = \sum_{n\geqslant 1} 4c_{n-1}x^n + \sum_{n\geqslant 1} x^n. \tag{3.17}$$

You should recognize the sum on the left-hand side as the OGF $h(x)$ minus its 0-th term:

$$\sum_{n\geqslant 1} c_n x^n = \left(\sum_{n\geqslant 0} c_n x^n\right) - c_0 = h(x) - 1.$$

From the second sum in equation (3.17), factor out $4x$ to remove the constant and to make the indices on c_{n-1} and x^n agree. Then the remaining sum is just $h(x)$:

$$4x \sum_{n\geqslant 1} c_{n-1}x^{n-1} = 4x \cdot h(x).$$

The right-most sum in equation (3.17) is almost $\frac{1}{1-x}$:

$$\sum_{n\geqslant 1} x^n = \left(\sum_{n\geqslant 0} x^n\right) - 1 = \frac{1}{1-x} - 1.$$

Now we have transformed equation (3.17) into

$$h(x) - 1 = 4x \cdot h(x) + \frac{1}{1-x} - 1. \tag{3.18}$$

Use algebra to solve for the unknown OGF $h(x)$:

$$h(x) = 4x \cdot h(x) + \frac{1}{1-x} \iff h(x) = \frac{1}{(1-4x)(1-x)}.$$

At this point there are two ways to proceed. Either works just fine, but by doing both we gain a couple of interesting things.

Method 1: use the convolution formula

In $h(x) = \frac{1}{1-4x} \cdot \frac{1}{1-x}$, the first term is the OGF for $\{4^n\}_{n\geqslant 0}$ and the second is the OGF for $\{1\}_{n\geqslant 0}$. By the convolution formula for OGFs,

$$c_n = \sum_{j=0}^{n} 4^j \cdot 1 = \sum_{j=0}^{n} 4^j.$$

Our desired formula is $c_n = \sum_{j=0}^{n} 4^j$, for $n \geqslant 0$.

Question 131 *Do the values that this formula produces match those that you computed from the recurrence in Question 130?*

Method 2: use partial fraction decomposition

First, find the partial fraction decomposition of $h(x)$:

$$h(x) = \frac{1}{(1-4x)(1-x)} = \frac{A}{1-4x} + \frac{B}{1-x}.$$

The solution is $A = 4/3$ and $B = -1/3$. (This is the same technique used in calculus to find the antiderivative of rational functions.)

Question 132 *Show the details that give $A = 4/3$ and $B = -1/3$.*

This means

$$h(x) = \frac{4/3}{1-4x} - \frac{1/3}{1-x}.$$

So then

$$\begin{aligned} c_n &= \left[\!\left[\frac{4/3}{1-4x} - \frac{1/3}{1-x} \right]\!\right]_{x^n} \\ &= \frac{4}{3} \cdot \left[\!\left[\frac{1}{1-4x} \right]\!\right]_{x^n} - \frac{1}{3} \left[\!\left[\frac{1}{1-x} \right]\!\right]_{x^n} \\ &= \frac{4}{3} \cdot 4^n - \frac{1}{3} \cdot 1 \\ &= \frac{4^{n+1} - 1}{3}. \end{aligned}$$

for $n \geqslant 0$.

Methods 1 and 2 are both correct, so we get the formula $\sum_{j=0}^{n} 4^j = \frac{4^{n+1}-1}{3}$ as a by-product.

Another example with EGFs

Next let's find a formula for the n-th term of the sequence $\{d_n\}_{n\geqslant 0}$ defined by

$$\begin{aligned} d_0 &= 1 \\ d_n &= n\,d_{n-1} + 1 \qquad \text{for } n \geqslant 1, \end{aligned}$$

which is identical to the previous recurrence relation except for the non-constant n in place of 4. Since an EGF worked so well on the similar recurrence $b_n = n\,b_{n-1}$, let's try it again.

Question 133 *What are the values $d_1, d_2, \ldots, d_5$?*

Define $E(x) := \sum_{n\geqslant 0} d_n \frac{x^n}{n!}$ as the EGF of this sequence. Again, our goal is to find the coefficient of $\frac{x^n}{n!}$ in $E(x)$.

Multiply the recurrence by $\frac{x^n}{n!}$ to get

$$d_n \frac{x^n}{n!} = n\, d_{n-1} \frac{x^n}{n!} + \frac{x^n}{n!}$$

and then sum over the values of n for which the recurrence is defined:

$$\sum_{n\geqslant 1} d_n \frac{x^n}{n!} = \sum_{n\geqslant 1} n\, d_{n-1} \frac{x^n}{n!} + \sum_{n\geqslant 1} \frac{x^n}{n!}. \tag{3.19}$$

Now analyze each term as usual. The first sum equals $E(x)$ minus its first term:

$$\sum_{n\geqslant 1} d_n \frac{x^n}{n!} = \left(\sum_{n\geqslant 0} d_n \frac{x^n}{n!}\right) - d_0 = E(x) - 1.$$

In the second sum we should simplify then factor out x:

$$\sum_{n\geqslant 1} n\, d_{n-1} \frac{x^n}{n!} = \sum_{n\geqslant 1} d_{n-1} \frac{x^n}{(n-1)!} = x \sum_{n\geqslant 1} d_{n-1} \frac{x^{n-1}}{(n-1)!} = x \cdot E(x).$$

And the third is another old friend:

$$\sum_{n\geqslant 1} \frac{x^n}{n!} = \left(\sum_{n\geqslant 0} \frac{x^n}{n!}\right) - 1 = e^x - 1.$$

Now equation (3.19) reads $E(x) - 1 = x \cdot E(x) + e^x - 1$ from which you should get

$$E(x) = \frac{e^x}{1-x}$$

as the EGF of $\{d_n\}_{n\geqslant 0}$.

Now we can use the convolution formula for EGFs to extract the coefficient of $\frac{x^n}{n!}$ in $E(x)$. Since e^x is the EGF of $\{1\}_{n\geqslant 0}$ and $\frac{1}{1-x}$ is the EGF of $\{n!\}_{n\geqslant 0}$, convolution gives

$$d_n = \left[\!\!\left[e^x \cdot \frac{1}{1-x} \right]\!\!\right]_{x^n/n!} = \sum_{j=0}^{n} \binom{n}{j} 1 \cdot (n-j)! = \sum_{j=0}^{n} \binom{n}{j} (n-j)!.$$

A little simplification produces

$$d_n = \sum_{j=0}^{n} \binom{n}{j} (n-j)! = \sum_{j=0}^{n} \frac{n!}{j!(n-j)!} \cdot (n-j)! = n! \sum_{j=0}^{n} \frac{1}{j!}.$$

We have found our formula:

$$d_n = n! \left(\frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} \right) \qquad \text{for } n \geqslant 0.$$

The formula could also be written $d_n = \sum_{j=0}^{n} (n)_j$.

Question 134 *Explain why.*

Combinatorially, $(n)_0 + (n)_1 + (n)_2 + \cdots + (n)_n$ counts the total number of permutations of $[n]$ of *any* size. Therefore if we define d_n to be the number of permutations of $[n]$ of any size, then d_n must satisfy the recurrence relation $d_0 = 1$ and $d_n = n\, d_{n-1} + 1$ for $n \geqslant 1$. (See Exercise 15 of Section 2.1 for a combinatorial proof.)

Should I use an OGF or an EGF?

You may be wondering why we chose an OGF in the first and third examples and an EGF in the second and fourth. It is instructive to swap the choices and see what happens.

In the third example, define $H(x) := \sum_{n\geqslant 0} a_n \frac{x^n}{n!}$ as the EGF of $\{a_n\}_{n\geqslant 0}$. Take the recurrence $a_n = 4a_{n-1} + 1$, multiply through by $\frac{x^{n-1}}{(n-1)!}$, and sum over $n \geqslant 1$:

$$\sum_{n\geqslant 1} a_n \frac{x^{n-1}}{(n-1)!} = \sum_{n\geqslant 1} 4a_{n-1} \frac{x^{n-1}}{(n-1)!} + \sum_{n\geqslant 1} \frac{x^{n-1}}{(n-1)!}. \tag{3.20}$$

The two sums on the right equal $4H(x)$ and e^x, respectively. The piece on the left is interesting because it is the *derivative* of $H(x)$:

$$\begin{aligned}\sum_{n\geqslant 1} a_n \frac{x^{n-1}}{(n-1)!} &= a_1 + a_2 x + a_3 \frac{x^2}{2!} + a_4 \frac{x^3}{3!} + \cdots \\ &= \frac{d}{dx}\left[a_0 + a_1 x + a_2 \frac{x^2}{2!} + a_3 \frac{x^3}{3!} + \cdots\right] \\ &= H'(x).\end{aligned}$$

Equation (3.20) now simplifies to

$$H'(x) = 4H(x) + e^x$$

which is a first-order linear ordinary differential equation with constant coefficients. Standard techniques from introductory differential equations will find $H(x)$ and then you can extract the coefficient of $\frac{x^n}{n!}$ to get a formula for a_n. While this is a great illustration of the intersection of continuous and discrete mathematics, it does require more work than using the OGF.

In the fourth example, define $B(x) := \sum_{n\geqslant 0} b_n x^n$ as the OGF of $\{b_n\}_{n\geqslant 0}$. Take the recurrence $b_n = nb_{n-1} + 1$, multiply through by x^{n-1}, and sum over $n \geqslant 1$.

Question 135 *If you attempt this, where do you run into trouble?*

As a general rule of thumb, try an OGF on a recurrence relation with constant coefficients, and an EGF on one that doesn't have constant coefficients.

Summary

This section provided examples of a method for solving recurrence relations via generating functions. "Solving" a recurrence relation means finding a closed-form (non-recursive) formula for the n-th term. The method is as follows.

- Given a sequence $\{a_n\}_{n\geqslant 0}$ defined by a recurrence relation, define $g(x)$ as either the OGF or the EGF of the sequence.
- Multiply the recurrence by either x^n or $\frac{x^n}{n!}$ and then sum over all values of n for which the recurrence is defined.
- Manipulate the equation in the previous step to get it in terms of the unknown generating function $g(x)$. Be sure to use the initial conditions.
- Solve for $g(x)$ to find the generating function.
- Extract the coefficient of x^n or $\frac{x^n}{n!}$ to obtain a formula for a_n.

Exercises

1. Solve the following recurrence relations using the generating function technique.
   (a) $a_0 = 0$ and $a_n = 2a_{n-1} + 1$ for $n \geqslant 1$.
   (b) $b_0 = \frac{1}{2}$ and $b_n = 3b_{n-1} - \frac{1}{2}$ for $n \geqslant 1$.
   (c) $c_0 = 1$ and $c_n = 3a_{n-1} + 3^n$ for $n \geqslant 1$.
   (d) $d_0 = 1$, $d_1 = 4$, and $d_n = 4d_{n-1} - 4d_{n-2}$ for $n \geqslant 2$.
   (e) $e_0 = e_1 = 1$, $e_2 = 2$, and $e_n = 3e_{n-1} - 3e_{n-2} + e_{n-3}$.
2. Use an EGF to solve the recurrence relation $a_0 = 2$ and $a_n = na_{n-1} - n!$ for $n \geqslant 1$.
3. Let D_n be the number of derangements of an n-set. (See Section 3.1.) Define $D_0 = 1$ and note $D_1 = 0$.
   (a) Give a combinatorial proof: $D_n = (n-1)(D_{n-1} + D_{n-2})$ for $n \geqslant 2$.
   (b) Find the EGF of $\{D_n\}_{n\geqslant 0}$.
   (c) Use part (b) to find a formula for D_n.
4. Find a formula for the n-th term of the sequence defined by the recurrence relation $E_n = nE_{n-1} + (-1)^n$ for $n \geqslant 1$, where $E_0 = 1$. Also, what is the relationship between E_n and the D_n of the previous exercise?
5. Let g_n equal the number of lists of any length taken from $\{1, 2, 4\}$ having elements that sum to n. For example, $g_3 = 3$ because the lists are $(1, 2)$, $(2, 1)$, and $(1, 1, 1)$. Also, $g_4 = 6$ because the lists are (4), $(1, 1, 2)$, $(2, 2)$, $(1, 1, 1, 1)$, $(1, 2, 1)$, and $(2, 1, 1)$. Define $g_0 = 1$.
   (a) Find each of g_1, g_2, and g_5 by complete enumeration.
   (b) Prove that $g_n = g_{n-1} + g_{n-2} + g_{n-4}$ for $n \geqslant 4$.
   (c) Let $G(x)$ be the OGF for $\{g_n\}_{n\geqslant 0}$. Show that $G(x) = \dfrac{1}{1 - x - x^2 - x^4}$.
6. Consider the recurrence relation defined by $b_0 = 1$ and $b_n = \sum_{i=1}^{n} \frac{b_{n-i}}{i!}$ for $n \geqslant 1$. Let $B(x)$ be the OGF of $\{b_n\}_{n\geqslant 0}$. Show that $B(x) = \frac{1}{2 - e^x}$.

Travel Notes

The reader who is familiar with finding power series solutions to differential equations will find many similarities with the methods of this section. Indeed, the method we presented for solving $a_0 = 1$, $a_n = 3a_{n-1}$ for $n \geqslant 1$ has much in common with the following derivation of the solution to $y' = 3y$, $y(0) = 1$. Begin by writing the unknown function y as the power series

$$y = \sum_{n\geqslant 0} a_n \frac{x^n}{n!} = a_0 + a_1 x + a_2 \frac{x^2}{2!} + a_3 \frac{x^3}{3!} + a_4 \frac{x^4}{4!} + \cdots$$

whence

$$y' = a_1 + a_2 x + a_3 \frac{x^2}{2!} + a_4 \frac{x^3}{3!} + a_5 \frac{x^4}{4!} + \cdots$$

and

$$3y = 3a_0 + 3a_1 x + 3a_2 \frac{x^2}{2!} + 3a_3 \frac{x^3}{3!} + 3a_4 \frac{x^4}{4!} + \cdots .$$

Equating coefficients gives $a_1 = 3a_0$, $a_2 = 3a_1$, $a_3 = 3a_2$, and in general $a_n = 3a_{n-1}$. The initial condition $y(0) = 1$ means $a_0 = 1$ and so we are faced with solving $a_0 = 1$, $a_n = 3a_{n-1}$. The solution is $a_n = 3^n$ for $n \geqslant 0$ and so the solution to the differential equation is

$$y = \sum_{n \geqslant 0} 3^n \frac{x^n}{n!} = \sum_{n \geqslant 0} \frac{(3x)^n}{n!} = e^{3x}, \qquad |x| < \infty.$$

3.6 Solving linear recurrence relations

In this section we derive solutions for two types of recurrence relations that arise often enough to earn a once-and-for-all treatment. The reader wishing to omit the derivations can just read Theorems 3.6.1 and 3.6.2 in preparation for their later application.

The first type of recurrence relation we solve is one like

$$\begin{aligned} c_0 &= 1 \\ c_n &= 4c_{n-1} + 1 \qquad \text{for } n \geqslant 1. \end{aligned}$$

It is a ***first-order linear recurrence relation with constant coefficients***. In general, such recurrence relations are of the form

$$\begin{aligned} &a_0 \text{ given} \\ &a_n = \alpha a_{n-1} + \beta \qquad \text{for } n \geqslant 1 \end{aligned}$$

where a_0, α, β are real numbers with $\alpha \neq 0$. It is ***first-order*** because the recurrence for a_n only involves the previous term a_{n-1}. (Similarly, a first-order differential equation only involves an unknown function y and its first derivative y'.) It is ***linear*** because a_n can be written as a linear function of lower-ordered terms.[1] It has ***constant coefficients*** because α and β are constants that do not depend on the index n. The recurrence $d_n = nd_{n-1} + 1$ from the last section is linear but does not have constant coefficients.

An example of the second type of recurrence relation that we solve in this section is the one for the Fibonacci numbers, namely

$$\begin{aligned} F_0 &= 1 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \qquad \text{for } n \geqslant 2. \end{aligned}$$

This is a ***second-order linear recurrence relation with constant coefficients***. In general, such recurrence relations are of the form

$$\begin{aligned} &a_0 \text{ given} \\ &a_1 \text{ given} \\ &a_n = \alpha a_{n-1} + \beta a_{n-2} + \gamma \qquad \text{for } n \geqslant 2, \end{aligned}$$

where $a_0, a_1, \alpha, \beta, \gamma$ are real numbers with $\alpha \neq 0$. In addition if the recurrence has $\gamma = 0$ (as Fibonacci does) it is called ***homogeneous***.

[1] A recurrence such as $c_n = 4c_{n-1}c_{n-2} + 1$ is not linear.

First-order linear recurrence relations

Our first goal is to solve the recurrence relation

$$\begin{aligned} &a_0 \text{ given} \\ &a_n = \alpha a_{n-1} + \beta \qquad \text{for } n \geqslant 1, \end{aligned}$$

where a_0, α, β are real numbers with $\alpha \neq 0$.

Let $f(x)$ be the OGF of $\{a_n\}_{n\geqslant 0}$. As usual, begin by multiplying the recurrence through by x^n and summing over $n \geqslant 1$. This results in

$$\sum_{n\geqslant 1} a_n x^n = \sum_{n\geqslant 1} \alpha a_{n-1} x^n + \sum_{n\geqslant 1} \beta x^n$$

or

$$\sum_{n\geqslant 1} a_n x^n = \alpha x \sum_{n\geqslant 1} a_{n-1} x^{n-1} + \beta \sum_{n\geqslant 1} x^n.$$

Now write this in terms of the OGF $f(x)$ and other known quantities:

$$\begin{aligned} f(x) - a_0 &= \alpha x f(x) + \beta \left(\frac{1}{1-x} - 1 \right) \\ &= \alpha x f(x) + \frac{\beta x}{1-x}. \end{aligned}$$

Solve $f(x) - a_0 = \alpha x f(x) + \beta x/(1-x)$ for $f(x)$ to get

$$f(x) = \frac{a_0(1-x) + \beta x}{(1-\alpha x)(1-x)} = \frac{a_0}{1-\alpha x} + \frac{\beta x}{(1-\alpha x)(1-x)}. \tag{3.21}$$

To find a formula for a_n, just extract the coefficient of x^n:

$$\begin{aligned} a_n &= \left[\!\!\left[\frac{a_0}{1-\alpha x} + \frac{\beta x}{(1-\alpha x)(1-x)} \right]\!\!\right]_{x^n} \\ &= a_0 \cdot \left[\!\!\left[\frac{1}{1-\alpha x} \right]\!\!\right]_{x^n} + \beta \cdot \left[\!\!\left[\frac{1}{(1-\alpha x)(1-x)} \right]\!\!\right]_{x^{n-1}} \\ &= a_0 \alpha^n + \beta \sum_{j=0}^{n-1} \alpha^j \cdot 1 \\ &= a_0 \alpha^n + \beta \sum_{j=0}^{n-1} \alpha^j. \end{aligned}$$

We used the convolution formula for OGFs in the third equality.

This formula for a_n can be cleaned up a little more using the identity

$$\sum_{j=0}^{k} x^j = \frac{1-x^{k+1}}{1-x}. \tag{3.22}$$

Since the formula works for any real number x with $x \neq 1$, there are two cases to consider.

Case 1: $\alpha \neq 1$

If $\alpha \neq 1$, then apply equation (3.22) with $x = \alpha$ and $k = n-1$ to get $\sum_{j=0}^{n-1} \alpha^j = \frac{1-\alpha^n}{1-\alpha}$. In this case, the formula for a_n is

$$a_n = a_0\alpha^n + \beta\left(\frac{1-\alpha^n}{1-\alpha}\right).$$

Case 2: $\alpha = 1$

If $\alpha = 1$, then $\sum_{j=0}^{n-1} \alpha^j = \sum_{j=0}^{n-1} 1 = n$. In this case, the formula for a_n is then

$$a_n = a_0\alpha^n + \beta n.$$

We've now given a complete answer to the question of how to solve a first-order linear recurrence relation with constant coefficients.

Theorem 3.6.1 *Consider the recurrence relation*

$$\begin{aligned} &a_0 \text{ given} \\ &a_n = \alpha a_{n-1} + \beta \qquad \text{for } n \geqslant 1, \end{aligned}$$

where a_0, α, β are real numbers with $\alpha \neq 0$. The OGF of the sequence $\{a_n\}_{n\geqslant 0}$ is

$$\frac{a_0}{1-\alpha x} + \frac{\beta x}{(1-x)(1-\alpha x)}.$$

It follows from the OGF that

$$a_n = \begin{cases} a_0\alpha^n + \beta\left(\dfrac{1-\alpha^n}{1-\alpha}\right) & \text{if } \alpha \neq 1 \\ a_0\alpha^n + \beta n & \text{if } \alpha = 1 \end{cases}$$

is a formula for the n-th term of the sequence.

Applying the theorem

For example, to find the 20th term of

$$\begin{aligned} a_0 &= -1 \\ a_n &= \frac{a_{n-1}}{2} + 3 \qquad \text{for } n \geqslant 1, \end{aligned}$$

just note that $\alpha = 1/2$ and $\beta = 3$. Observing that $\alpha \neq 1$, we apply the formula to get

$$\begin{aligned} a_{20} &= (-1)(1/2)^{20} + 3\left(\frac{1-(1/2)^{20}}{1-1/2}\right) \\ &= -\frac{1}{2^{20}} + 6\left(1 - \frac{1}{2^{20}}\right) \\ &= 6 - \frac{7}{2^{20}} = 6 - \frac{7}{1048576} = \frac{6291449}{1048576}. \end{aligned}$$

In general, the n-th term is $a_n = 6 - \dfrac{7}{2^n}$.

Question 136 *Find the n-th term of the recurrence relation $a_0 = 105$, $a_n = a_{n-1} - \frac{1}{3}$ for $n \geqslant 1$. Also, confirm the formula for the n-th term of $c_0 = 1$, $c_n = 4c_{n-1} + 1$ for $n \geqslant 1$, which we derived in Section 3.5.*

Second-order linear homogeneous recurrence relations

As we mentioned earlier, the recurrence relation that defines the Fibonacci sequence is an example of a second-order linear homogeneous recurrence relation. In general such a recurrence relation looks like

$$\begin{aligned} &a_0 \text{ given} \\ &a_1 \text{ given} \\ &a_n = \alpha a_{n-1} + \beta a_{n-2} \qquad \text{for } n \geqslant 2. \end{aligned}$$

We assume that $\alpha_0, \alpha_1, \alpha, \beta$ are real numbers with $\beta \neq 0$. Exercise 7 asks you to extend the work we are about to do to the non-homogeneous case.

Define $f(x) := \sum_{n\geqslant 0} a_n x^n$ as the OGF of $\{a_n\}_{n\geqslant 0}$. Multiply through by x^n and sum over $n \geqslant 2$, and then make the usual adjustments to the right-hand side:

$$\begin{aligned} \sum_{n\geqslant 2} a_n x^n &= \sum_{n\geqslant 2} \alpha a_{n-1} x^n + \sum_{n\geqslant 2} \beta a_{n-2} x^n \\ &= \alpha x \sum_{n\geqslant 2} a_{n-1} x^{n-1} + \beta x^2 \sum_{n\geqslant 2} a_{n-2} x^{n-2}. \end{aligned}$$

This equation is equivalent to $f(x) - a_0 - a_1 x = \alpha x\big(f(x) - a_0\big) + \beta x^2 f(x)$, and solving for $f(x)$ shows that

$$f(x) = \frac{a_0 + (a_1 - \alpha a_0)x}{1 - \alpha x - \beta x^2}. \tag{3.23}$$

At this point we need to factor the quadratic in the denominator to determine the nature of its roots. In the case of distinct roots, we'll use partial fraction decomposition to extract the coefficients.

Case 1: distinct roots

If the roots are distinct, then it is possible to factor the denominator into the form (remember $\beta \neq 0$)

$$1 - \alpha x - \beta x^2 = (1 - r_1 x)(1 - r_2 x)$$

where $r_1 \neq r_2$. We seek, then, the partial fraction decomposition of

$$\frac{a_0 + (a_1 - \alpha a_0)x}{1 - \alpha x - \beta x^2} = \frac{A}{1 - r_1 x} + \frac{B}{1 - r_2 x}.$$

Multiplying through by $(1 - r_1 x)(1 - r_2 x)$ shows that

$$\begin{aligned} a_0 + (a_1 - \alpha a_0)x &= A(1 - r_2 x) + B(1 - r_1 x) \\ &= (A + B) + \big(-r_2 A - r_1 B\big)x \end{aligned}$$

This leads to the system

$$\begin{aligned} A + \quad B &= a_0 \\ -r_2 A - r_1 B &= a_1 - \alpha a_0. \end{aligned}$$

Its solution is

$$A = \frac{(r_1 - \alpha)a_0 + a_1}{r_1 - r_2} \qquad \text{and} \qquad B = a_0 - A = \cdots = \frac{(\alpha - r_2)a_0 - a_1}{r_1 - r_2}$$

Question 137 *Solve the system by hand to verify the given values of A and B. At what point in the calculation does the need to assume $r_1 \neq r_2$ enter?*

Now, go back to the equation (3.23). We just showed that

$$f(x) = \frac{A}{1 - r_1 x} + \frac{B}{1 - r_2 x}$$

where A and B are as we determined earlier. This means that the coefficient of x^n in $f(x)$ is $Ar_1^n + Br_2^n$. Before organizing this information into a theorem, though, we need to treat the case of repeated roots.

Case 2: repeated roots

In this case, we can factor the denominator into the form

$$1 - \alpha x - \beta x^2 = (1 - r_1 x)^2.$$

Partial fraction decomposition is not necessary. Since

$$\frac{a_0 + (a_1 - \alpha a_0)x}{1 - \alpha x - \beta x^2} = \frac{a_0 + (a_1 - \alpha a_0)x}{(1 - r_1 x)^2},$$

we can begin by finding the coefficient of x^n in $1/(1 - r_1 x)^2$. Use the multichoose OGF as a starting point, namely

$$\frac{1}{(1 - x)^m} = \sum_{n \geqslant 0} \left(\!\!\binom{m}{n}\!\!\right) x^n,$$

but substitute $m = 2$ and replace x by $r_1 x$ to get

$$\frac{1}{(1 - r_1 x)^2} = \sum_{n \geqslant 0} \left(\!\!\binom{2}{n}\!\!\right) (r_1 x)^n = \sum_{n \geqslant 0} (n + 1) r_1^n x^n.$$

Therefore the coefficient of x^n in $1/(1 - r_1 x)^2$ is $(n + 1)r_1^n$. So now, since the OGF of $\{a_n\}_{n \geqslant 0}$ is

$$\frac{a_0 + (a_1 - \alpha a_0)x}{(1 - r_1 x)^2} = \frac{a_0}{(1 - r_1 x)^2} + \frac{(a_1 - \alpha a_0)x}{(1 - r_1 x)^2},$$

the formula for a_n is

$$\begin{aligned}
a_n &= \left[\!\!\left[\frac{a_0}{(1 - r_1 x)^2} + \frac{(a_1 - \alpha a_0)x}{(1 - r_1 x)^2} \right]\!\!\right]_{x^n} \\
&= \left[\!\!\left[\frac{a_0}{(1 - r_1 x)^2} \right]\!\!\right]_{x^n} + \left[\!\!\left[\frac{(a_1 - \alpha a_0)x}{(1 - r_1 x)^2} \right]\!\!\right]_{x^n} \\
&= a_0 \cdot \left[\!\!\left[\frac{1}{(1 - r_1 x)^2} \right]\!\!\right]_{x^n} + (a_1 - \alpha a_0) \cdot \left[\!\!\left[\frac{1}{(1 - r_1 x)^2} \right]\!\!\right]_{x^{n-1}} \\
&= a_0 (n + 1) r_1^n + (a_1 - \alpha a_0) n r_1^{n-1}.
\end{aligned}$$

The whole story

Here's the theorem that summarizes our work.

Theorem 3.6.2 *Consider the recurrence relation*

$$\begin{aligned} &a_0 \text{ given} \\ &a_1 \text{ given} \\ &a_n = \alpha a_{n-1} + \beta a_{n-2} \qquad \text{for } n \geqslant 2, \end{aligned}$$

where a_0, a_1, α, β are real numbers with $\beta \neq 0$. The OGF of the sequence $\{a_n\}_{n\geqslant 0}$ is

$$\frac{a_0 + (a_1 - \alpha a_0)x}{1 - \alpha x - \beta x^2}.$$

To determine a formula for a_n, do the following:

- *Factor the quadratic $1 - \alpha x - \beta x^2$ into the form $(1 - r_1 x)(1 - r_2 x)$, for (possibly complex) numbers r_1 and r_2.*
- *If $r_1 \neq r_2$, then define $A = \dfrac{(r_1 - \alpha)a_0 + a_1}{r_1 - r_2}$ and $B = \dfrac{(\alpha - r_2)a_0 - a_1}{r_1 - r_2}$. The formula is $a_n = Ar_1^n + Br_2^n$ for $n \geqslant 0$.*
- *If $r_1 = r_2$, then the formula is $a_n = a_0(n+1)r_1^n + (a_1 - \alpha a_0)n r_1^{n-1}$ for $n \geqslant 0$.*

Exercise 3 asks you to derive the following formula for the roots of the quadratic $1 - \alpha x - \beta x^2$ needed in the first step of the theorem:

$$r_1, r_2 = \frac{\alpha \pm \sqrt{\alpha^2 + 4\beta}}{2}. \tag{3.24}$$

Applying the theorem

In Section 4.2, we apply Theorem 3.6.2 to find closed-form formulas for both the Fibonacci and the Lucas numbers. Until then, however, we show how to apply the formula to a slight modification to the Fibonacci recurrence:

$$\begin{aligned} &a_0 = 1 \\ &a_1 = 1 \\ &a_n = a_{n-1} - a_{n-2} \qquad \text{for } n \geqslant 2. \end{aligned}$$

The sequence it defines appears pretty innocent. In fact it begins $1, 1, 0, -1, -1, 0$ and then starts over.

The recurrence relation has $a_0 = a_1 = \alpha = 1$ and $\beta = -1$. Using equation (3.24), the roots turn out to be distinct but complex:

$$r_1, r_2 = \frac{1 \pm \sqrt{1^2 + 4(-1)}}{2} = \frac{1 \pm i\sqrt{3}}{2}.$$

Next note that $r_1 - r_2 = i\sqrt{3}$ and so

$$A = \frac{(r_1 - \alpha)a_0 + a_1}{r_1 - r_2} = \frac{(\frac{1+i\sqrt{3}}{2} - 1)(1) + 1}{i\sqrt{3}} = \frac{1}{2}\left(1 - \frac{i}{\sqrt{3}}\right)$$

and

$$B = \frac{(\alpha - r_2)a_0 - a_1}{r_1 - r_2} = \frac{(1 - \frac{1-i\sqrt{3}}{2})(1) - 1}{i\sqrt{3}} = \frac{1}{2}\left(1 + \frac{i}{\sqrt{3}}\right).$$

Therefore

$$a_n = \frac{1}{2}\left(1 - \frac{i}{\sqrt{3}}\right)\left(\frac{1 + i\sqrt{3}}{2}\right)^n + \frac{1}{2}\left(1 + \frac{i}{\sqrt{3}}\right)\left(\frac{1 - i\sqrt{3}}{2}\right)^n$$

for $n \geqslant 0$.

Summary

In this section we applied the recurrence-relation-solving techniques of the previous section to derive general formulas for certain first- and second-order recurrence relations. This means that a closed form formula is readily available for any combinatorial problem whose solution can be described by such a recurrence relation.

Exercises

1. Find a_{30} for the recurrence relation $a_0 = -1$ and $a_n = 1 - 3a_{n-1}$.
2. Solve the following recurrence relations.
   (a) $a_0 = 3$, $a_1 = 7$, and $a_n = 3a_{n-1} - 2a_{n-2}$ for $n \geqslant 2$.
   (b) $b_0 = 1$, $b_1 = 3$, and $b_n = 4(a_{n-1} - a_{n-2})$ for $n \geqslant 2$.
   (c) $c_0 = 2$, $c_1 = 0$, and $c_n = 2c_{n-1} - 2c_{n-2}$ for $n \geqslant 2$.
   (d) $d_0 = 10$ and $d_n = 11d_{n-1} - 10$ for $n \geqslant 1$.
3. Prove that if $1 - \alpha x - \beta x^2 = (1 - r_1 x)(1 - r_2 x)$, then r_1 and r_2 are as given in the formulas in equation (3.24) on page 138.
4. Find a formula for the n-th term of the sequence defined by the recurrence relation $a_n = 2a_{n-1} + 3a_{n-2}$ for $n \geqslant 2$, where $a_0 = 1$ and $a_1 = 2$.
5. Answer the previous exercise but for the initial conditions $a_0 = -1$ and $a_1 = 0$. Re-use as much as possible your work from the previous exercise.
6. Let t_n denote the number of ways to build a tower n units high using blocks of the following types: red 1-unit blocks, red 2-unit blocks, blue 1-unit blocks, and blue 2-unit blocks. For example, $t_1 = 2$ and $t_2 = 6$. Define $t_0 = 1$.

   Derive a recurrence relation for t_n and then use it to find a formula for t_n.
7. Extend Theorem 3.6.2 to recurrence relations of the form $a_n = \alpha a_{n-1} + \beta a_{n-2} + \gamma$, where γ is a given real number and all other parameters are as before.
8. Find $\lim_{\alpha \longrightarrow 1} \frac{1 - \alpha^n}{1 - \alpha}$. Then, explain why this clarifies the relationship between the formulas for a_n shown in Theorem 3.6.1.

CHAPTER 4

Famous Number Families

In this chapter we apply our tools from the previous chapters to study several well-known number families: binomial and multinomial coefficients, Fibonacci and Lucas numbers, Stirling numbers of the first and second kinds, and integer partition numbers. Fibonacci numbers in particular are so compelling that an entire journal, *The Fibonacci Quarterly*, is devoted to their study.

Combinatorial proofs and generating functions are the main tools we'll use. For each family, the main goal is to obtain a "nice" formula. The criteria for what constitutes a nice formula are subjective, but there are some formulas that everyone would agree are nice. For example, we have seen that the Fibonacci numbers are defined by $F_0 = 1$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geqslant 2$. The formula is

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \qquad \text{for } n \geqslant 0.$$

It is easily evaluated for any n and involves only basic arithmetic operations. On the other hand a formula for $P(n)$, the total number of partitions of the integer n does indeed exist but requires a great deal of number theory and complex analysis to understand. Somewhere in between is one possible formula for the Bell numbers, namely

$$B(n) = \frac{1}{e}\sum_{j\geqslant 0}\frac{j^n}{j!}.$$

Although it involves an infinite series, it converges rapidly and thus has use as a computational formula.

4.1 Binomial and multinomial coefficients

We begin with the multinomial coefficients which are generalizations of the binomial coefficients. These will help us answer counting questions involving set partitions where the blocks have specified sizes. We'll then solve the problem of counting the ways to triangulate a regular polygon which requires the so-called extended binomial theorem.

Multinomial coefficients

Think of the binomial coefficient $\binom{10}{4}$ as counting the ways to distribute 10 distinct objects to two distinct recipients such that recipient A receives four objects and recipient B receives

the remaining six objects. Writing $\binom{10}{4,6}$ instead of just $\binom{10}{4}$ makes explicit the number of objects each recipient receives.

The multinomial coefficient $\binom{10}{3,4,3}$ counts the ways to distribute 10 distinct objects to three distinct recipients such that recipient A receives three objects, B receives four, and C receives three. The numbers on the bottom should sum to the number at the top, else the value is 0. For example, $\binom{10}{2,3,4} = 0$ because $2 + 3 + 4 \neq 10$.

In general, the ***multinomial coefficient*** $\binom{n}{t_1, t_2, \ldots, t_k}$ equals the number of distributions of n distinct objects to k distinct recipients such that recipient i receives t_i objects, for $i \in [k]$. We observe that $\binom{n}{t_1,t_2,\ldots,t_k} = 0$ unless $\sum t_i = n$. We define $\binom{0}{0,0,\ldots,0} := 1$.

Question 138 *A gym teacher hands out eight yellow, eight red, and nine blue jerseys to her 25 students to put them on three different teams. How many ways can this be done?*

Formula for the multinomial coefficients

Our first job is to derive a formula for the multinomial coefficients. As an example, how many distributions of 10 distinct objects to four distinct recipients are possible such that recipient 1 receives $t_1 = 3$ objects, recipient 2 receives $t_2 = 0$ objects, recipient 3 receives $t_3 = 5$ objects, and recipient 4 receives $t_4 = 2$ objects?

Consider one of the 10! permutations of [10], say (7, 10, 3, 2, 1, 6, 4, 9, 8, 5). Assign the first $t_1 = 3$ objects in this list to recipient 1, the next $t_2 = 0$ objects to 2, and so on:

$$(\underbrace{7, 10, 3}_{\to 1}, \underbrace{2, 1, 6, 4, 9}_{\to 3}, \underbrace{8, 5}_{\to 4})$$

But there are many permutations that produce the same distribution because sublists of size 3, 5, and 2 (really 3, 0, 5, and 2) can be permuted in any way. There are 3!0!5!2! permutations equivalent to the distribution

$$\begin{aligned} \{3, 7, 10\} &\to \text{recipient } 1 \\ \emptyset &\to \text{recipient } 2 \\ \{1, 2, 4, 6, 9\} &\to \text{recipient } 3 \\ \{5, 8\} &\to \text{recipient } 4 \end{aligned}$$

and so by the equivalence principle there are $\frac{10!}{3!0!5!2!}$ such distributions.

Question 139 *Explain why* $\binom{10}{3}\binom{7}{0}\binom{7}{5}\binom{2}{2}$ *is also a correct answer.*

The argument using the equivalence principle generalizes immediately.

Theorem 4.1.1 *For any* $n \geq 0$ *and* $t_1, t_2, \ldots, t_k \geq 0$ *with* $\sum t_i = n$,

$$\binom{n}{t_1, t_2, \ldots, t_k} = \frac{n!}{t_1!t_2!\cdots t_k!}.$$

See Exercise 7 for the proof.

Question 140 *How many ways can you distribute 12 different books to three children so that each child gets four books?*

A combinatorial proof

When we proved Pascal's identity $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, we counted the number of k-person committees that can be formed from a group of n people. The corresponding idea for multinomial coefficients involving three recipients is

$$\binom{n}{t_1, t_2, t_3} = \binom{n-1}{t_1 - 1, t_2, t_3} + \binom{n-1}{t_1, t_2 - 1, t_3} + \binom{n-1}{t_1, t_2, t_3 - 1}$$

as long as each $t_i > 0$. For example

$$\binom{10}{3, 5, 2} = \binom{9}{2, 5, 2} + \binom{9}{3, 4, 2} + \binom{9}{3, 5, 1}.$$

A combinatorial proof also uses the proof of Pascal's identity as inspiration: condition on which of the three recipients receives object 10. If a certain recipient receives zero objects, then we do not include that recipient in the conditioning.[1] For example,

$$\binom{10}{7, 0, 3} = \binom{9}{6, 0, 3} + \binom{9}{7, 0, 2}.$$

This is because if recipient 2 is to receive zero objects, then the object labeled 10 must be assigned to either recipient 1 or 3.

Theorem 4.1.2 *For any $n \geqslant 0$ and $t_1, t_2, \ldots, t_k \geqslant 0$ with $\sum t_i = n$,*

$$\binom{n}{t_1, t_2, \ldots, t_k} = \sum \binom{n-1}{t_1, \ldots, t_{i-1}, t_i - 1, t_{i+1}, \ldots, t_k}$$

where the sum is over all $i \in [k]$ for which $t_i > 0$.

Combinatorial proof: Assume that $n \geqslant 0$ and that $t_1, t_2, \ldots, t_k \geqslant 0$ satisfy $\sum t_i = n$. How many distributions of n distinct objects to k distinct recipients are possible such that recipient 1 receives t_1 objects, recipient 2 receives t_2 objects, and so on?

Answer 1: There are $\binom{n}{t_1, t_2, \ldots, t_k}$ distributions.

Answer 2: Condition on the recipient that receives object n. If this recipient is i (as long as $t_i > 0$), then there are $\binom{n-1}{t_1, \ldots, t_i - 1, t_{i+1}, \ldots, t_k}$ such distributions. By the sum principle there are $\sum \binom{n-1}{t_1, \ldots, t_i - 1, t_{i+1}, \ldots, t_k}$ total distributions, where the sum is over all i for which $t_i > 0$. ∎

The multinomial coefficients count the possible functions $[n] \longrightarrow [k]$ with prescribed sizes for the pre-image of each element in the codomain. The following theorem results from considering all possible prescribed sizes and adding the results.

Theorem 4.1.3 *For any $n > 0$ and $k > 0$,*

$$k^n = \sum \binom{n}{t_1, t_2, \ldots, t_k}$$

where the sum is over all k-lists $(t_1, t_2, \ldots, t_k)$ of nonnegative integers that sum to n.

[1] Equivalently, one could define $\binom{n}{t_1, t_2, \ldots, t_k} := 0$ if any $t_i < 0$.

Question 141 *How many terms are there in the sum?*

As an illustration, the number of functions $[3] \longrightarrow [3]$ equals

$$\binom{3}{3,0,0} + \binom{3}{0,3,0} + \binom{3}{0,0,3} + \binom{3}{2,1,0} + \binom{3}{2,0,1}$$
$$+ \binom{3}{0,2,1} + \binom{3}{1,2,0} + \binom{3}{1,0,2} + \binom{3}{0,1,2} + \binom{3}{1,1,1}$$
$$= 1 + 1 + 1 + 3 + 3 + 3 + 3 + 3 + 3 + 6 = 27.$$

And of course $3^3 = 27$ as well.

The multinomial theorem

The multinomial coefficients produce a "multinomial theorem" just as the binomial coefficients produce the binomial theorem. A simple modification to the approach that proved the binomial theorem in Section 2.2 works here.

Theorem 4.1.4 (multinomial) *For any $n \geq 0$,*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum \binom{n}{t_1, t_2, \ldots, t_k} x_1^{t_1} x_2^{t_2} \cdots x_k^{t_k}$$

where the sum is over all k-lists $(t_1, t_2, \ldots, t_k)$ of nonnegative integers that sum to n.

Question 142 *Provide a combinatorial proof of the multinomial theorem, assuming that the x_j are positive integers.*

Counting partitions with certain specifications

How many partitions of [20] have three blocks of size 1, three blocks of size 4, and one block of size 5?

It would seem that the multinomial coefficient

$$\binom{20}{1,1,1,4,4,4,5} = \frac{20!}{(1!)^3(4!)^3(5!)^1} \tag{4.1}$$

would have something to do with the answer, since it counts the distributions of 20 distinct objects to seven distinct recipients such that recipients 1-3 each receive one object, recipients 4-6 each receive four objects, and recipient 7 receives five objects. One example distribution is

$$\{17\} \to \text{recipient 1}$$
$$\{3\} \to \text{recipient 2}$$
$$\{11\} \to \text{recipient 3}$$
$$\{2, 5, 6, 10\} \to \text{recipient 4}$$
$$\{1, 7, 19, 20\} \to \text{recipient 5}$$
$$\{9, 15, 16, 18\} \to \text{recipient 6}$$
$$\{4, 8, 12, 13, 14\} \to \text{recipient 7}$$

But the *set partition* derived from this distribution has the blocks

$$\{17\}, \{3\}, \{11\}, \{2, 5, 6, 10\}, \{1, 7, 19, 20\}, \{9, 15, 16, 18\}, \{4, 8, 12, 13, 14\}$$

and so the answer shown in (4.1) above is too large because the recipients are distinct instead of identical. The equivalence principle comes to the rescue: we may rearrange the assignment of the blocks of size 1 to the first three recipients in any of 3! ways, the assignment of the blocks of size 4 to the next three recipients in any of 3! ways, and the assignment of the blocks of size 5 to the last recipient in any of 1! ways (included to make the pattern obvious) and end up with an equivalent partition. There are

$$\binom{20}{1, 1, 1, 4, 4, 4, 5} \Big/ 3!3!1! = \frac{20!}{(1!)^3 (4!)^3 (5!)^1 3!3!1!} = 40{,}738{,}698{,}000$$

partitions of [20] with the blocks as specified, around 40.7 billion.

In general, if a partition of $[n]$ has p_j blocks of size j, where $j \in [n]$, then there are

$$\frac{n!}{(1!)^{p_1} (2!)^{p_2} \cdots (n!)^{p_n}} = n! \Big/ \prod_{j=1}^{n} (j!)^{p_j} \tag{4.2}$$

different partitions in which the blocks of the partition are "labeled" as in the example just discussed. The size of each equivalence class is $p_1! p_2! \cdots p_n!$, and so the total number of partitions of $[n]$ into blocks with the specified sizes equals the number shown in (4.2) above divided by the product of the $p_j!$.

Theorem 4.1.5 *For $n > 0$, the number of partitions of an n-set such that there are p_j blocks of size j, for $j \in [n]$, equals*

$$n! \Big/ \prod_{j=1}^{n} (j!)^{p_j} \, p_j!.$$

Question 143 *In the theorem, what does $\sum_{j=1}^{n} j \cdot p_j$ always equal?*

Example: bridge hands

How many ways are there to arrange a 52-card deck into four piles of 13 cards each? How many ways are there to deal a 52-card deck to four players so that each player receives 13 cards?

The difference between the two questions lies in whether the recipients are identical (first question) or distinct (second question). The first question asks for the number of ways to partition a 52-set into four blocks each of size 13. By Theorem 4.1.5, there are

$$\frac{52!}{(13!)^4 \, 4!} = 2{,}235{,}197{,}406{,}895{,}366{,}368{,}301{,}560{,}000$$

ways. Many bridge hands have been played in the history of the world but it is certainly not the case that every possible partitioning of the deck has been realized.

The second question asks for the number of ways to deal 13 cards to each player. There are $\binom{52}{13, 13, 13, 13} = 53{,}644{,}737{,}765{,}488{,}792{,}839{,}237{,}440{,}000$ ways.

Connection with Stirling and Bell numbers

A link between partitions with specified block sizes and the Stirling numbers of the second kind or the Bell numbers is possible but somewhat cumbersome. For example, we know that the number of partitions of [4] into two blocks is $S(4,2)$. Such a partition must have either one 1-block and one 3-block, or else two 2-blocks. Applying the theorem with $n = 4$ and $(p_1, p_2, p_3, p_4) = (1, 0, 1, 0)$ gives

$$\frac{4!}{(1!)^1(2!)^0(3!)^1(4!)^0 1!0!1!0!} = 4.$$

Applying it with $n = 4$ and $(p_1, p_2, p_3, p_4) = (0, 2, 0, 0)$ gives

$$\frac{4!}{(1!)^0(2!)^2(3!)^0(4!)^0 0!2!0!0!} = 3.$$

This shows that $S(4,2) = 4 + 3 = 7$.

Question 144 *What does the formula give if there is one block of size n? What if there are n blocks of size 1?*

Two more binomial coefficient identities

For the rest of this section we return to the binomial coefficients and first to combinatorial proofs. The skill in giving a combinatorial proof of an identity lies in asking the right question. Here are two proofs for which the questions aren't as obvious as the examples in Section 2.2 were. In both proofs we use the committee-counting interpretation of $\binom{n}{k}$.

The following identity holds for any choices of nonnegative integers n, m, and k, but the restrictions given in the theorem help in the combinatorial interpretation.

Theorem 4.1.6 *For any integers n, m, k satisfying $n, m \geqslant 1$ and $0 \leqslant k \leqslant m$,*

$$\sum_{j \geqslant 0} \binom{n}{j}\binom{m}{k+j} = \binom{n+m}{n+k}.$$

Combinatorial proof: From a group of n women and m men, how many committees of size $n + k$ are possible?

Answer 1: $\binom{n+m}{n+k}$

Answer 2: Notice that at least k men must be on any such committee. Condition on the number j of men on the committee beyond this minimum number k. There are $\binom{m}{k+j}$ ways to select the men. The rest of the committee consists of $n - j$ women, and for each way to select the men there are $\binom{n}{j}$ ways to select j women to *exclude* from the committee, thereby selecting $n - j$ women to include. There are $\binom{n}{j}\binom{m}{k+j}$ possible committees for this value of j. Summing over all j gives the left-hand side of the identity. ■

Question 145 *If $k = 0$, then to what does the identity reduce?*

We give two proofs of the following identity, one combinatorial and one using the binomial theorem and the derivative. Pick your favorite.

Theorem 4.1.7 *For all $n \geqslant 1$,* $\displaystyle\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$.

Combinatorial proof: Let $n \geqslant 1$. Given n people, in how many ways can we select a nonempty committee of any size and also designate one person as the chair?

Answer 1: Pick the chair first in one of n ways. Then, pick any subset of the remaining $n-1$ people to form the rest of the committee. There are 2^{n-1} such subsets, so there are $n2^{n-1}$ total selections.

Answer 2: Condition on the size k of the committee, where $1 \leqslant k \leqslant n$. There are $\binom{n}{k}$ possible committees of size k. For each such committee, there are k ways to select its chair. In total there are $\sum_{k=1}^{n} k\binom{n}{k}$ ways. ■

Proof using the binomial theorem: Since $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$, take the derivative to get

$$n(1+x)^{n-1} = \sum_{k=1}^{n} k \binom{n}{k} x^{k-1}.$$

Let $x = 1$ and the identity follows. ■

The extended binomial theorem

The extended binomial theorem, sometimes known as the binomial series theorem, generalizes the binomial theorem to the case when the n in $(1+x)^n$ is not a nonnegative integer. It is a result in analysis and we state it without proof.

Theorem 4.1.8 (extended binomial theorem) *For any real number α,*

$$(1+x)^{\alpha} = \sum_{k \geqslant 0} \binom{\alpha}{k} x^k, \qquad \text{for } |x| < 1.$$

The presence of an infinite sum requires specifying an interval of convergence, in this case $|x| < 1$. As usual, when we consider $(1+x)^{\alpha}$ as a concise form of the OGF for $\left\{\binom{\alpha}{k}\right\}_{k \geqslant 0}$, the theory of formal power series allows us to finesse this issue.

The only question is: what does $\binom{\alpha}{k}$ mean when α is not a nonnegative integer? Although there is perhaps no combinatorial significance to associate with it, the same algebraic formula still stands:

$$\binom{\alpha}{k} := \frac{(\alpha)_k}{k!} \qquad \text{where } (\alpha)_k := \alpha(\alpha-1)\cdots(\alpha-k+1).$$

In other words, just use the formula $\binom{n}{k} = \frac{(n)_k}{k!}$ as if n were a nonnegative integer.

Question 146 *What is* $\binom{-1/2}{4}$*?*

Extracting coefficients

What is the coefficient of x^k in $1/\sqrt{1-4x}$?

Rewrite and apply the extended binomial theorem:

$$(1-4x)^{-1/2} = \sum_{k \geqslant 0} \binom{-1/2}{k} (-4x)^k.$$

The coefficient is $\binom{-1/2}{k}(-4)^k$. It is well worth attempting a simplification, for two reasons. One, the final answer is clean and pretty. Two, the manipulations involved are good to practice. Start by paring it down:

$$\begin{aligned}\binom{-1/2}{k}(-4)^k &= \frac{(-\frac{1}{2})(-\frac{3}{2})(-\frac{5}{2})\cdots(-\frac{2k-1}{2})(-4)^k}{k!}\\ &= \frac{(1)(3)(5)\cdots(2k-1)(-1)^k(-4)^k}{2^k k!}\\ &= \frac{(1)(3)(5)\cdots(2k-1)2^k}{k!}.\end{aligned}$$

Now comes an algebraic stunt: multiply the last expression by $\frac{k!}{k!}$. Notice that

$$2^k k! = 2^k(1)(2)(3)\cdots(k) = (2)(4)(6)\cdots(2k),$$

and so the numerator of the expression becomes $(2k)!$, i.e.,

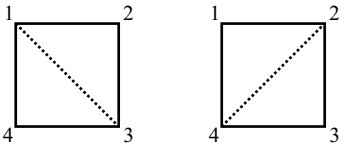
$$\frac{(1)(3)(5)\cdots(2k-1)2^k}{k!}\cdot\frac{k!}{k!} = \frac{(2k)!}{k!k!} = \binom{2k}{k}.$$

Therefore $(1-4x)^{-1/2}$ is the OGF of the sequence $\left\{\binom{2k}{k}\right\}_{k\geq 0}$.

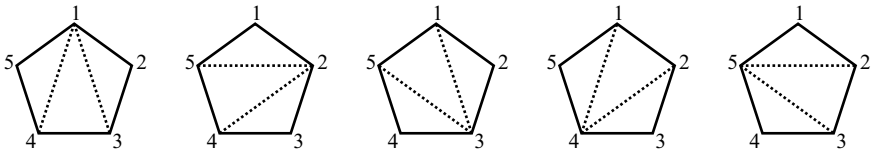
Triangulating a regular polygon with *n* sides

In how many different ways may we triangulate a regular polygon with n sides (an "n-gon") with labeled vertices? (A ***triangulation*** divides the polygon into triangular regions via the addition of non-intersecting diagonals.)

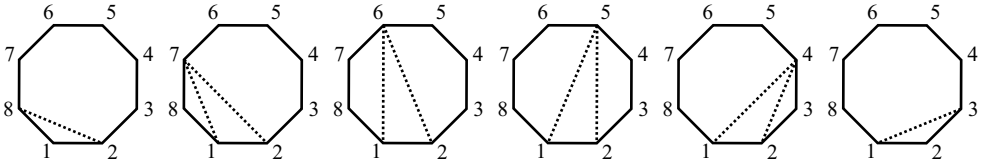
Call this number T_n. The triangle has $T_3 = 1$ triangulation and the square has $T_4 = 2$ triangulations:



Also, the pentagon has $T_5 = 5$ triangulations:



Focus on any one side of the n-gon, say joining vertices 1 and 2. In any triangulation, that side will form one side of a triangle. Consider cases depending on the location of the third vertex of that triangle. There are six cases for an octagon:



If the third corner is labeled 8, then triangulate the remaining 7-sided figure (with corners at 2-3-4-5-6-7-8) in T_7 ways. If the third corner is labeled 7, then triangulate 1-7-8 in T_3 ways and 2-3-4-5-6-7 in T_6 ways, for a total of T_3T_6 triangulations. If the third corner is labeled 6, then triangulate 1-6-7-8 in T_4 ways and 2-3-4-5-6 in T_5 ways, for a total of T_4T_5 triangulations. Continuing this produces

$$T_8 = T_7 + T_3T_6 + T_4T_5 + T_5T_4 + T_6T_3 + T_7.$$

In general, the same idea gives

$$T_n = T_{n-1} + T_3T_{n-2} + T_4T_{n-3} + \cdots + T_{n-2}T_3 + T_{n-1}.$$

for $n \geqslant 4$. By defining $T_2 := 1$ we can write instead

$$T_n = \sum_{k=2}^{n-1} T_k T_{n-k+1} \qquad \text{for } n \geqslant 3, \text{ where } T_2 := 1. \tag{4.3}$$

This is a *nonlinear* recurrence relation, but the techniques of Section 3.5 still work.

Let $f(x) = \sum_{n\geqslant 2} T_n x^{n-2}$ be the OGF of $\{T_n\}_{n\geqslant 2}$. That is, T_n is the coefficient of x^{n-2} in $f(x)$. (The discrepancy between the index n and the power $n-2$ makes the algebra come out somewhat cleaner.)

Multiply equation (4.3) by x^{n-2} and sum over $n \geqslant 3$:

$$\sum_{n\geqslant 3} T_n x^{n-2} = \sum_{n\geqslant 3} \left(\sum_{k=2}^{n-1} T_k T_{n-k+1} \right) x^{n-2}. \tag{4.4}$$

The left-hand side is $f(x) - T_2 = f(x) - 1$. The right-hand side is a convolution that appears to be something close to $[f(x)]^2$. Write out a few terms and see:

$$\begin{aligned} &T_2T_2x + (T_2T_3 + T_3T_2)x^2 + (T_2T_4 + T_3T_3 + T_4T_2)x^3 + \cdots \\ &\quad = x\Big(T_2T_2 + (T_2T_3 + T_3T_2)x + (T_2T_4 + T_3T_3 + T_4T_2)x^2 + \cdots\Big) \\ &\quad = x\big[f(x)\big]^2. \end{aligned}$$

And so equation (4.4) becomes $f(x) - 1 = x\big[f(x)\big]^2$ or

$$x\big[f(x)\big]^2 - f(x) + 1 = 0.$$

Now (more magic with generating functions!) solve this equation for the unknown function f using the quadratic formula:

$$f(x) = \frac{-(-1) \pm \sqrt{(-1)^2 - 4(x)(1)}}{2x} = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Apply the extended binomial theorem to $\sqrt{1-4x}$ to get

$$(1-4x)^{1/2} = \sum_{n\geqslant 0} \binom{1/2}{n} (-4)^n x^n.$$

But the sum for $f(x)$ is over $n \geq 2$, so

$$f(x) = \frac{1}{2x} \pm \frac{1}{2x}\sqrt{1-4x} = \frac{1}{2x} \pm \frac{1}{2x}\sum_{n\geq 2}\binom{1/2}{n}(-4)^n x^n$$
$$= \frac{1}{2x} \pm \sum_{n\geq 2}\frac{1}{2}\binom{1/2}{n}(-4)^n x^{n-1}.$$

Depending on which solution we take,

$$T_n = \pm\frac{1}{2}\binom{1/2}{n-1}(-4)^{n-1} \tag{4.5}$$

since (remember!) T_n is the coefficient of x^{n-2} in $f(x)$. Exercise 14 asks you to show that the negative solution is the one we want, and also that it simplifies to

$$T_n = \frac{1}{n-2}\binom{2n-4}{n-1} \qquad \text{for } n \geq 3. \tag{4.6}$$

Summary

This section covered extensions of the binomial coefficients and the binomial theorem. Both the multinomial coefficients and the multinomial theorem extend the binomial coefficients and binomial theorem, respectively, in a natural, combinatorial way. The extended binomial theorem represents an analytic extension of the binomial theorem. We used it to solve a nonlinear recurrence relation.

Exercises

1. The pro football season lasts 16 games. The list WWLTWWWWLWWWLLTW is the record of a team that won its first two games, lost its third, tied its fourth, etc., and finished with a record of 10-4-2 (10 wins, four losses, two ties).
   (a) How many ways are there for a team to finish 10-4-2?
   (b) How many ways in part (a) do not have consecutive losses?
   (c) How many ways in part (a) have a longest winning streak of six games?
2. Consider the letters in the word DIVISIBILITY.
   (a) How many different 12-lists can be formed by rearranging the letters?
   (b) How many 12-lists in part (a) do not contain adjacent Is?
3. A university has 120 incoming freshman that still have to be assigned to on-campus housing. The only remaining dorm holds 105 students and contains 42 doubles (rooms housing two students) and seven triples (three students). In how many ways can the university select 105 students to house in this dorm and then arrange those students into roommate pairs and triples, without yet assigning them to rooms?
4. In the previous exercise, suppose the university gets approval to house temporarily the remaining 15 students among the dorm's three lounges. Each lounge will house five students. How many ways are there for the university to assign all 120 students to rooms?

5. A mouse that lives in a hotel wants to travel from the ground floor entrance at location $(0, 0, 0)$ to its nest on the 10th floor at location $(12, 9, 10)$. Each move the mouse makes is either one room north, one room east, or one floor up. For example, from $(0, 0, 0)$ the mouse moves either to $(1, 0, 0)$ or $(0, 1, 0)$ or $(0, 0, 1)$, respectively. How many ways are there for the mouse to travel?
6. Suppose $|A| = 42$. How many equivalence relations on A are there that have distinct equivalence classes of sizes 4, 7, 7, 8, 8, and 8?
7. Use the equivalence principle to prove the formula for the multinomial coefficients given in Theorem 4.1.1.
8. Give a combinatorial proof: $\displaystyle\sum_{k=m}^{n} \binom{n}{k}\binom{k}{m} = \binom{n}{m}2^{n-m}$.
9. Give a combinatorial proof: $\displaystyle\binom{kn}{2} = k\binom{n}{2} + n^2\binom{k}{2}$.
10. Give two proofs of the following, one combinatorial and one non-combinatorial: For $n \geqslant 2, n(n-1)2^{n-2} = \displaystyle\sum_{k\geqslant 2} k(k-1)\binom{n}{k}$.
11. Compute $\displaystyle\sum_{k=0}^{n} \binom{2n-2k}{n-k}\binom{2k}{k}$ for $n = 0, 1, 2, 3$. Make a conjecture and then prove it combinatorially.
12. Given a positive integer n, a ***composition of*** n is a list of positive integers that sum to n. For example, $(3, 1, 1)$ and $(1, 3, 1)$ and $(1, 4)$ and (5) are each a composition of 5. In general, how many compositions of n are possible?
13. Find the coefficient of x^n in $\sqrt{1-8x}$.
14. Finish the demonstration of formula (4.6). Be sure to justify why the negative solution in equation (4.5) is the correct one.
15. The associative property of multiplication says that $x(yz) = (xy)z$. In other words, to compute the product xyz you could either find yz first then multiply that by x, or you could find xy first and then multiply that by z. Thus there are two ways to compute a product of three numbers via pairwise products and without changing the order of the numbers.

    There are five ways to do this with a product of four numbers:

    $$w(x(yz)) \quad w((xy)z) \quad (wx)(yz) \quad (w(xy))z \quad ((wx)y)z$$

    Let a_n equal the number of ways to do this with a product of n numbers. We just found that $a_3 = 2$ and $a_4 = 5$.

    Derive a recurrence relation for a_n and then solve it to find a formula for a_n.
16. Define $\left\{ {n \atop k} \right\}$ as the number of $(n + k)$-lists of the form $(a_1, a_2, \ldots, a_{n+k})$ where n of the elements are 1s and k of the elements are -1s and where for all i, the sum of the first i entries is nonnegative:

    $$a_1 + a_2 + \cdots + a_i \geqslant 0 \qquad \text{for all } i \in [n + k].$$

(a) Find $\left\{ {3 \atop 2} \right\}$ and $\left\{ {4 \atop 4} \right\}$ by complete enumeration. Also, explain why $\left\{ {n \atop k} \right\} = 0$ when $k > n$.

(b) Find $\left\{ {n \atop 0} \right\}$ for $n \geqslant 0$ and $\left\{ {n \atop 1} \right\}$ for $n \geqslant 1$.

(c) Give a combinatorial proof: $\left\{ {n \atop k} \right\} = \left\{ {n \atop k-1} \right\} + \left\{ {n-1 \atop k} \right\}$. Also, for what values of n and k is this identity valid?

(d) Prove that $\left\{ {n \atop n} \right\} = \left\{ {n \atop n-1} \right\}$ for $n \geqslant 1$.

(e) Compute a table of the values $\left\{ {n \atop k} \right\}$ for k and n satisfying $0 \leqslant k \leqslant n \leqslant 8$.

Travel Notes

The paper Pólya (1956), entitled "On picture-writing," is a classic exposition by the master problem-solver George Pólya. In it he explains how generating functions can be easily derived from symbolic series (as we did at the beginning of Section 3.3) and also solves the problem of counting triangulations of the regular n-gon that we covered in this section.

Exercise 16 is from "Counting arrangements of 1's and −1's" by D. F. Bailey which appeared in *Mathematics Magazine* **69**, April 1996, 128-131. His purpose was to provide a new derivation of the formula $\frac{1}{n+1}\binom{2n}{n}$ for the n-th Catalan number.

4.2 Fibonacci and Lucas numbers

The following recurrence relation defines the well-known Fibonacci numbers:

$$\begin{aligned} F_0 &= 1 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2} \qquad \text{for } n \geqslant 2. \end{aligned}$$

The first few Fibonacci numbers are shown below.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
F_n	1	1	2	3	5	8	13	21	34	55	89	144	233	377

The same recurrence but with one change in the initial conditions defines the Lucas numbers:

$$\begin{aligned} L_0 &= 2 \\ L_1 &= 1 \\ L_n &= L_{n-1} + L_{n-2} \qquad \text{for } n \geqslant 2. \end{aligned}$$

And the first few Lucas numbers are shown below.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
L_n	2	1	3	4	7	11	18	29	47	76	123	199	322	521

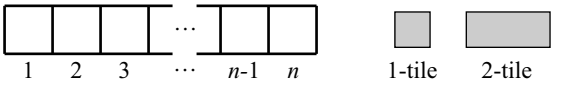
Both the Fibonacci and Lucas numbers (though the Fibonacci more so) are quite celebrated in mathematics and elsewhere. This section mainly concentrates on the Fibonacci numbers but look to the exercises for results about the Lucas numbers.

Combinatorial interpretations of the Fibonacci numbers

Tiling the n-board

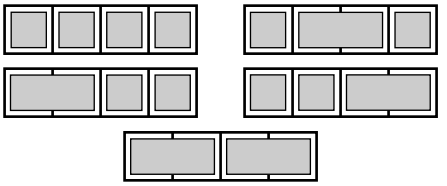
One way to make combinatorial sense of the Fibonacci numbers is to think of them as answers to certain questions of tiling. This interpretation is particularly concrete and convenient.

Consider a $1 \times n$ checkerboard (or "n-board"), with its squares labeled 1 through n, and an unlimited number of two types of tiles: 1×1 squares ("1-tiles") and 1×2 rectangles ("2-tiles").

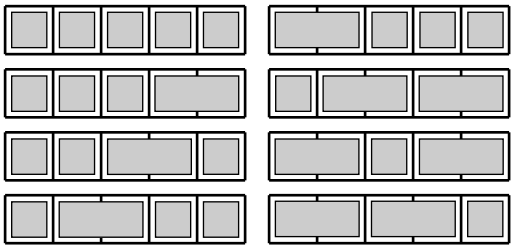


In how many ways may we tile the n-board using these two types of tiles?

For example, there are five ways to tile the 4-board:



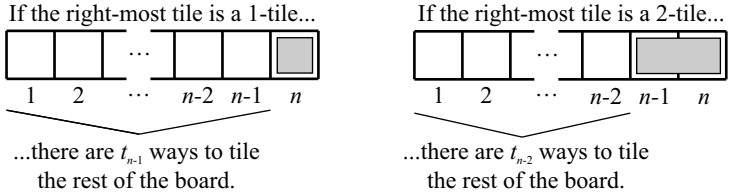
There are eight ways to tile the 5-board:



There is only one way to tile the 1-board, and we will say that there is one way to tile the 0-board (using the "empty tiling"). Although we think of the squares of the board as labeled in increasing order from left to right, the pictures of tilings do not include those labels unless needed for clarity.

Question 147 *Write out all of the tilings of the 3-board and of the 6-board.*

That the Fibonacci numbers count such tilings follows naturally. Let t_n denote the number of tilings of the n-board. We don't know yet that $t_n = F_n$ so we had better use different notation.[2] We already know that $t_0 = t_1 = 1$. For the n-board with $n \geqslant 2$, condition on the right-most tile. If it is a 1-tile, then there are t_{n-1} ways to tile the $(n-1)$-board to its left. If it is a 2-tile, then there are t_{n-2} ways to tile the $(n-2)$-board to its left. An illustration follows.



[2] This is not just a matter of style but rather important!

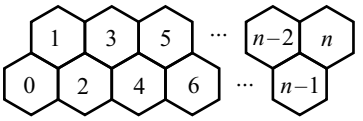
The sum principle then implies that $t_n = t_{n-1} + t_{n-2}$.

Since the sequence $\{t_n\}_{n\geqslant 0}$ satisfies the same initial conditions and the same recurrence as the Fibonacci sequence $\{F_n\}_{n\geqslant 0}$, those two sequences must be equal and so we can dispense with the t_n notation.

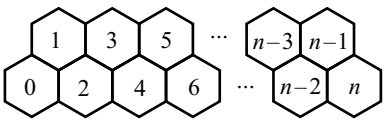
Theorem 4.2.1 *For $n \geqslant 0$, the n-th Fibonacci number F_n equals the number of ways to tile a $1 \times n$ checkerboard using only 1×1 and 1×2 tiles.*

Walking in the n-honeycomb

You are at the cell labeled 0 in the *n-honeycomb* shown below:



Your goal is to walk to the cell labeled n and you can only make one of two moves: from cell k to cell $k+1$, or from cell k to cell $k+2$. Let w_n be the number of ways that you can walk to cell n using moves of this type. The above diagram of the n-honeycomb assumes that n is odd. If n is even then it looks as follows:



In either case, since you begin at cell 0 there is one way to get there: do nothing. So $w_0 = 1$. Also, there is one way to get from cell 0 to cell 1, so $w_1 = 1$.

Question 148 *How many ways are there to walk from cell 0 to cell 5? Write them all out.*

When $n \geqslant 2$, any path from cell 0 to cell n must either end with a move from cell $n-1$ to cell n, or a move from cell $n-2$ to cell n. In the first case, there are w_{n-1} ways to walk from 0 to $n-1$. In the second case, there are w_{n-2} ways to walk from 0 to $n-2$. By the sum principle, $w_n = w_{n-1} + w_{n-2}$.

Again, the numbers w_n satisfy the same initial conditions and recurrence as the Fibonacci numbers, so they must be equal.

Theorem 4.2.2 *For $n \geqslant 0$, the n-th Fibonacci number F_n equals the number of paths from 0 to n in the n-honeycomb, where each move is $k \to k+1$ or $k \to k+2$.*

Combinatorial proofs

Let's now survey some of the identities that result from the two combinatorial interpretations (tiling and walking in the honeycomb) of the Fibonacci numbers.

Conditioning on the number of 1-tiles

Any tiling of the n-board must end with a certain number of 1-tiles, between 0 and n. Conditioning on this number allows us to derive a basic identity.

For example, any tiling of the 8-board must fall into one of the eight categories shown in Figure 4.1. The first category includes all tilings that end with no 1-tiles, the second includes all tilings that end with exactly one 1-tile, and so on. Notice that no tiling can end with exactly seven 1-tiles, and so the last category contains the one tiling that ends with

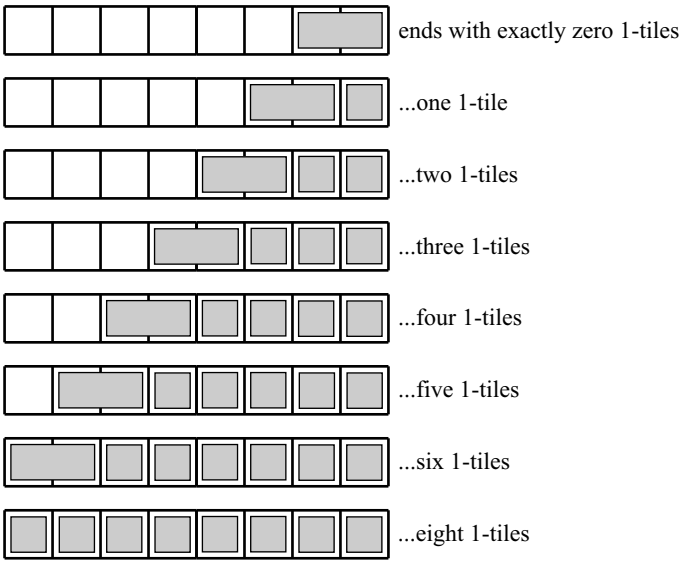


Figure 4.1. Tilings of the 8-board.

exactly eight 1-tiles—the all-1-tile tiling. There are F_6 ways to complete the tilings in the first category, F_5 ways in the second, and so on. This proves that

$$F_8 = 1 + F_0 + F_1 + F_2 + \cdots + F_6.$$

For the general case, any tiling of the n-board must either contain all 1-tiles, or else end with exactly i of the 1-tiles, where $0 \leqslant i \leqslant n-2$. There is one tiling in the first case and there are $\sum_{i=0}^{n-2} F_i$ in the second. We have our first Fibonacci identity.

Theorem 4.2.3 *For any $n \geqslant 2$, the identity $F_n = 1 + \sum_{i=0}^{n-2} F_i$ holds.*

Alternatively, the identity could be written $F_n - 1 = \sum_{i=0}^{n-2} F_i$ and proved combinatorially by asking the question: how many tilings of the n-board use at least one 2-tile? Exercise 2 asks you to prove its sister identity by conditioning on the number of 2-tiles at the end of the tiling.

A link with binomial coefficients

A list taken from [2] provides a concise way to represent a tiling of the n-board. For example, the list representations of the eight tilings of the 5-board shown appear in Figure 4.2. This produces a natural one-to-one correspondence between the tilings of the 5-board using 1- and 2-tiles, and the lists (of any length) taken from [2] that have the sum of their elements equal to 5.

In general, a one-to-one correspondence exists between the tilings of the n-board using 1- and 2-tiles, and the lists taken from [2] that have the sum of their elements equal to n. To prove it, condition on the number of 2-tiles used in the tiling. This number, call it i, ranges from 0 to $\lfloor n/2 \rfloor$.

Question 149 *Why do we need to round down?*

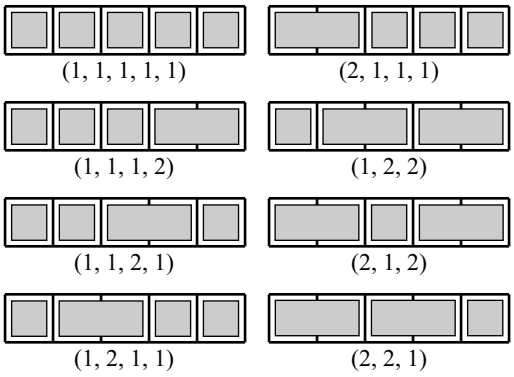


Figure 4.2. Tilings as lists taken from [2].

If the tiling contains i of the 2-tiles, then these tiles occupy $2i$ of the n squares on the board. The remaining $n-2i$ squares must be covered by 1-tiles, which puts the total number of tiles in the tiling at $i+(n-2i)=n-i$. That means that the tiling can be represented as an $(n-i)$-list taken from [2], and where the number of 2s in the list is i. There are $\binom{n-i}{i}$ such lists. Summing over the possible values of i finishes the proof of the following identity.

Theorem 4.2.4 *For any $n \geqslant 0$, the identity* $F_n = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}$ *holds.*

It is perhaps more elegant to write the identity as

$$F_n = \sum_{i \geqslant 0} \binom{n-i}{i}$$

because $\binom{n-i}{i} = 0$ for $i > \lfloor n/2 \rfloor$. For example,

$$\begin{aligned} \sum_{i \geqslant 0} \binom{5-i}{i} &= \binom{5}{0} + \binom{4}{1} + \binom{3}{2} + \binom{2}{3} + \binom{1}{4} + \cdots \\ &= 1 + 4 + 3 + 0 + 0 + \cdots \\ &= 8 \end{aligned}$$

and indeed $F_5 = 8$.

Breaking a tiling

Let $n \geqslant 2$ and consider any tiling of the n-board. Consider what happens between squares k and $k+1$, where $1 \leqslant k < n$. Either a single 2-tile covers both of these squares or it doesn't. See Figure 4.3 for an illustration.

If a single 2-tile does not cover squares k and $k+1$, then we can "break" the tiling at that point and count such tilings as follows. There are F_k ways to tile the k-board to the left of the break, and for each way to do so there are F_{n-k} ways to tile the $(n-k)$-board to the right. The product principle gives $F_k F_{n-k}$ total tilings in this case.

If a single 2-tile covers squares k and $k+1$, then we may break the tiling before square k and after square $k+1$. There are F_{k-1} tilings of the left-hand board that remains, and

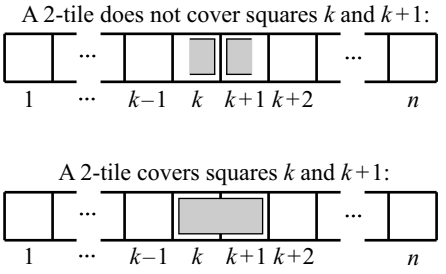


Figure 4.3. Breaking a tiling near square k.

for each such tiling there are F_{n-k-1} tilings of the right-hand board. Again the product principle gives $F_{k-1}F_{n-k-1}$ total tilings in this case.

Add the results of the two cases and you get the following theorem.

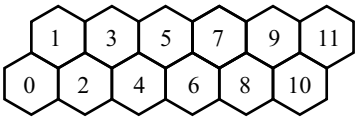
Theorem 4.2.5 *For any n and k satisfying $n \geqslant 2$ and $1 \leqslant k < n$, the identity*

$$F_n = F_k F_{n-k} + F_{k-1} F_{n-k-1}$$

holds.

Parity and the honeycomb

Consider the paths from 0 to 11 in the 11-honeycomb:



One of the cells labeled 0, 2, 4, 6, 8, and 10 must be the *last* even-numbered cell visited. Arrange all the possible paths into disjoint piles according to the last even cell visited.

Say 6 is the last even cell visited. There are F_6 ways to get to 6, but then only one way to complete the path to 11: it must go $6 \to 7 \to 9 \to 11$ because such a path must not visit any more even cells. Likewise if 8 is the last even cell visited, there are F_8 ways to get to 8 but then only one way to complete the path to 11: $8 \to 9 \to 11$.

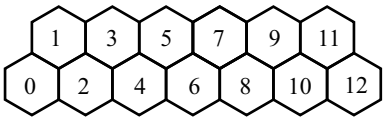
So if j is the last even cell visited ($j = 0, 2, 4, 6, 8$), then there are F_j possible paths. Since our cases are disjoint and exhaustive, the sum principle implies that

$$F_{11} = F_0 + F_2 + F_4 + F_6 + F_8 + F_{10}.$$

This essentially gives a proof of the following theorem.

Theorem 4.2.6 *For all $n \geqslant 0$, the identity $F_{2n+1} = \sum_{i=0}^{n} F_{2i}$ holds.*

We should not go on before trying to swap "even" with "odd." Look instead at the 12-honeycomb:



By considering cases based on the last odd cell visited, you might think that the analogous identity is

$$F_{12} = F_1 + F_3 + F_5 + F_7 + F_9 + F_{11}.$$

But this isn't quite right.

Question 150 *Why not? What adjustment must you make and why?*

You should now have an idea about how to prove the following theorem.

Theorem 4.2.7 *For all $n \geqslant 1$, the identity $F_{2n} = 1 + \sum_{i=1}^{n} F_{2i-1}$ holds.*

Algebraic proofs

Suppose you suspect a certain identity about Fibonacci numbers is true but can't find a combinatorial proof? You could try an algebraic proof, say by induction. Two examples follow.

A Fibonacci identity

Although a combinatorial proof is possible of the following theorem, we give a proof by strong induction for variety's sake.

Theorem 4.2.8 *For $n \geqslant 2$, the identity $2F_n = F_{n+1} + F_{n-2}$ holds.*

Proof: Our proof is by strong induction on n. When $n = 2, 2F_2 = 2(2) = 4$ and $F_3 + F_0 = 3 + 1 = 4$. When $n = 3, 2F_3 = 2(3) = 6$ and $F_4 + F_1 = 5 + 1 = 6$. The equation is true both when $n = 2$ and $n = 3$.

Now let $k \geqslant 3$ and assume that the identity is true when $n = j$ for all integers j satisfying $2 \leqslant j \leqslant k$. In particular, this means that

$$\begin{aligned} 2F_k &= F_{k+1} + F_{k-2} \\ 2F_{k-1} &= F_k + F_{k-3}. \end{aligned}$$

We must show that the equation is true for $n = k + 1$, namely $2F_{k+1} = F_{k+2} + F_{k-1}$. Starting with $2F_{k+1}$, use the Fibonacci recurrence to write

$$2F_{k+1} = 2\big(F_k + F_{k-1}\big) = 2F_k + 2F_{k-1}.$$

Now, apply the inductive hypothesis to each term and then apply the Fibonacci recurrence to show

$$\begin{aligned} 2F_k + 2F_{k-1} &= \big(F_{k+1} + F_{k-2}\big) + \big(F_k + F_{k-3}\big) \\ &= \big(F_{k+1} + F_k\big) + \big(F_{k-2} + F_{k-3}\big) \\ &= F_{k+2} + F_{k-1}. \end{aligned}$$

Therefore the equation is true for all $n \geqslant 2$. ■

Question 151 *What is the need for checking two base cases, $n = 2$ and $n = 3$? Why wouldn't a single base case suffice?*

The link between Fibonacci and Lucas numbers

The Fibonacci and Lucas numbers obey the same recurrence, so one might think that a close relationship exists between the two. The following theorem confirms this.

Theorem 4.2.9 *For all $n \geqslant 2$, $L_n = F_{n-2} + F_n$.*

Proof: Our proof is by strong induction on n. When $n = 2$, the equation reads $L_2 = F_0 + F_2$. Since $L_1 = 3$ and $F_0 + F_2 = 1 + 2 = 3$ it is true for $n = 2$. When $n = 3$, the equation reads $L_3 = F_1 + F_3$. This also is true because $L_3 = 4$ and $F_1 + F_3 = 1 + 3 = 4$.

Now assume that k is an integer, $k \geqslant 3$, and that the equation is true for $n = j$ where $2 \leqslant j \leqslant k$. In particular, this means that

$$\begin{aligned} L_k &= F_{k-2} + F_k \\ L_{k-1} &= F_{k-3} + F_{k-1}. \end{aligned}$$

We must show that the equation is true for $n = k + 1$, namely $L_{k+1} = F_{k-1} + F_{k+1}$. Starting with L_{k+1} and then applying the Lucas recurrence, inductive hypothesis, and Fibonacci recurrence shows that

$$\begin{aligned} L_{k+1} &= L_k + L_{k-1} \\ &= (F_{k-2} + F_k) + (F_{k-3} + F_{k-1}) \\ &= (F_{k-2} + F_{k-3}) + (F_k + F_{k-1}) \\ &= F_{k-1} + F_{k+1}. \end{aligned}$$

Therefore the equation is true for all $n \geqslant 2$. ■

Exercise 11 asks for a combinatorial proof.

Formulas

For the Fibonacci numbers

Is it possible to "jump" right to the n-th Fibonacci number without computing all the previous numbers using the recurrence relation, or without computing a sum of binomial coefficients using Theorem 4.2.4? Theorem 3.6.2 on page 138 tells us that the answer is yes. To apply the theorem, we set $\alpha = \beta = a_0 = a_1 = 1$.

Question 152 *According to that theorem, what is the OGF of $\{F_n\}_{n \geqslant 0}$?*

To find a formula for F_n we must find r_1 and r_2 so that

$$1 - x - x^2 = (1 - r_1 x)(1 - r_2 x).$$

Since $(1 - r_1 x)(1 - r_2 x) = 1 - (r_1 + r_2)x + r_1 r_2 x$, it must be the case that $r_1 + r_2 = 1$ and $r_1 r_2 = -1$. A solution to these two equations in two unknowns is

$$r_1 = \frac{1 + \sqrt{5}}{2} \qquad \text{and} \qquad r_2 = \frac{1 - \sqrt{5}}{2}.$$

Question 153 *What would the values of r_1 and r_2 be if the quadratic were $1 - 2x - 3x^2$ instead of $1 - x - x^2$?*

We are in the case of distinct roots ($r_1 \neq r_2$), so we need to compute A and B as in the theorem. You should get

$$A = \frac{1+\sqrt{5}}{2\sqrt{5}} \qquad \text{and} \qquad B = \frac{-1+\sqrt{5}}{2\sqrt{5}}.$$

That means that

$$\begin{aligned} F_n &= Ar_1^n + Br_2^n \\ &= \left(\frac{1+\sqrt{5}}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{-1+\sqrt{5}}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n. \end{aligned}$$

A little algebraic adjustment (factor out $1/\sqrt{5}$ and then absorb what's left into the powers of r_1 and r_2) produces the formula of the following theorem.

Theorem 4.2.10 (Fibonacci numbers) *The Fibonacci numbers $\{F_n\}_{n\geqslant 0}$, which are defined by $F_0 = F_1 = 1$ and $F_n = F_{n-1}+F_{n-2}$ for $n \geqslant 2$, have OGF equal to $1/(1-x-x^2)$. From this,*

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$$

for all $n \geqslant 0$.

This formula is beautiful and miraculous, perhaps because it describes an *integer* sequence using a sum of powers of *irrational* numbers.

From a computational point of view, it is not necessary to calculate the second term in the formula. This is because it is always less than $\frac{1}{2}$ in absolute value.

Question 154 *Explain why* $\left|\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right| < \frac{1}{2}$, *for all $n \geqslant 0$.*

As such, F_n is always the closest integer to the first term of the formula.

Corollary 4.2.11 *The n-th Fibonacci number is the closest integer to* $\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}$.

For the Lucas numbers

To obtain a formula for the Lucas numbers, we take the same approach but use $L_0 = 2$ instead of $F_0 = 1$.

Theorem 4.2.12 (Lucas numbers) *The Lucas numbers $\{L_n\}_{n\geqslant 0}$, which are defined by $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for $n \geqslant 2$, have OGF equal to $(2-x)/(1-x-x^2)$. From this,*

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$$

for all $n \geqslant 0$.

Question 155 *Prove this theorem.*

Question 156 *Determine whether a result similar to Corollary 4.2.11 holds for the Lucas numbers.*

Summary

This section barely scratched the surface of the many, many known results concerning the Fibonacci and Lucas numbers. Several combinatorial interpretations of each number family exist. The benefit of having many different interpretations is that they each inspire different identities. To complement the combinatorial methods, the algebraic techniques of induction and generating functions provided other identities as well as closed-form formulas for both the Fibonacci and Lucas numbers.

Exercises

1. Express the answer to each question in terms of the Fibonacci numbers.

   (a) How many subsets of $[n]$ do not contain consecutive integers?

   (b) How many n-digit binary numbers do not contain adjacent 0s?

   (c) How many ways are there to climb a flight of n stairs where each step takes you from stair i to either stair $i + 1$ or stair $i + 2$.

   (Hint: Derive a recurrence in each case.)

2. Derive and prove an identity similar to that of Theorem 4.2.3 by conditioning on the number of 2-tiles at the end of the tiling.

3. Suppose you make a mistake in computing the Fibonacci sequence by hand using the recurrence. You compute the numbers $F_0, F_1, \ldots, F_{m-1}$ correctly, but your value of F_m actually equals $1 + F_m$. Assuming that this is the only mistake you make, how far off is each subsequent number that you compute? Specifically, for any $k > 0$, how large is the error between your value of F_{m+k} and the true value of F_{m+k}?

4. Prove: $\gcd(F_n, F_{n-1}) = 1$ for all $n \geqslant 1$. In other words, adjacent Fibonacci numbers are relatively prime.

5. Prove Theorem 4.2.4 by strong induction.

6. Prove by strong induction.

   (a) $3F_n = F_{n+2} + F_{n-2}$ for $n \geqslant 2$.

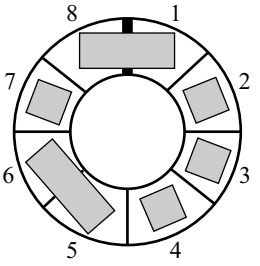
   (b) $4F_n = F_{n+2} + F_n + F_{n-2}$ for $n \geqslant 2$.

7. Prove by strong induction: for any $n \geqslant 0$, $\sum_{k=0}^{n} F_k^2 = F_n F_{n+1}$.

8. Prove: for $n \geqslant 1$, $F_n^2 - F_{n+1} F_{n-1} = (-1)^n$.

9. Given nonnegative integers G_0 and G_1, the *generalized Fibonacci numbers* are then defined by the recurrence $G_n = G_{n-1} + G_{n-2}$ for $n \geqslant 2$. State and prove a theorem, analogous to Theorems 4.2.10 and 4.2.12, for the generalized Fibonacci numbers.

10. The Lucas numbers count tilings of the *circular n-board* or *n-bracelet* with 1- and 2-tiles. A tiling of the 8-bracelet appears below.



The "clasp" at the top is the line dividing squares 8 and 1. In general, if a single 2-tile covers both squares n and 1, we consider the tiling to correspond to a *closed* bracelet. Otherwise the tiling corresponds to an *open* bracelet.[3] The tiling above is closed.

(a) Write out all of the tilings of the 3-, 4-, and 5-bracelets. Which tilings are open and which are closed?

(b) Let β_n equal the number of tilings of the n-bracelet. Prove that $\beta_n = L_n$ for all $n \geqslant 0$. How are you defining the initial conditions and how do they make sense combinatorially?

(c) Explain combinatorially why $L_n \geqslant F_n$ for all $n \geqslant 0$.

11. Give a combinatorial (tiling) proof of Theorem 4.2.9.

12. Conjecture and prove formulas for each of the following sums of Fibonacci numbers.

(a) $\displaystyle\sum_{i=0}^{n} F_{3i}$

(b) $\displaystyle\sum_{i=0}^{n} F_{4i}$

Travel Notes

Some authors define the Fibonacci numbers as $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geqslant 2$. You should be aware of which convention is in force before reading.

There are many combinatorial problems whose answer involves the Fibonacci numbers (see Exercise 1 for some), so there are many ways to interpret these numbers. The tiling interpretation of Fibonacci and Lucas numbers originally appeared in Brigham, Caron, Chinn & Grimaldi (1996). The book by Benjamin & Quinn (2003) offers an excellent and extensive presentation of combinatorial proofs for Fibonacci and Lucas identities using the tiling interpretation. The honeycomb interpretation is due to Danrun Huang and Kyung H. Sun at St. Cloud State University but has not yet been published.

4.3 Stirling numbers

In this section we determine generating functions for the Stirling and Bell numbers and then derive a formula for the Bell numbers. Also, we introduce the Stirling numbers of the first kind and then provide both their algebraic and combinatorial interpretations.

[3] Some authors use "in phase" to mean "open" and "out of phase" to mean "closed."

From our work in Sections 2.3 and 3.1, we already know the following facts about Stirling numbers of the second kind and Bell numbers.

- The Stirling number of the second kind $S(n,k)$ counts the partitions of an n-set into k blocks. Equivalently, it counts the distributions of n distinct objects to k identical recipients such that each recipient receives at least one object. The numbers $S(n,k)$ satisfy the recurrence

$$S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k) \qquad \text{for } n > 0 \text{ and } k > 0,$$

  where $S(0,0) := 1$ and $S(n,0) = S(0,k) = 0$ for $n > 0$ and $k > 0$. We derived this by conditioning on whether element n is in a block by itself. (This is Theorem 2.3.1 on page 70.)

- We used inclusion-exclusion to find a formula for $S(n,k)$. For $n \geqslant 0$ and $k \geqslant 0$,

$$S(n,k) = \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} (-1)^i (k-i)^n.$$

  (This is Theorem 3.1.4 on page 90.)

- The Bell number $B(n)$ counts the total number of partitions of an n-set. As such, $B(n) = \sum_{k=1}^{n} S(n,k)$ and $B(0) := 1$. The numbers $B(n)$ satisfy the recurrence

$$B(n) = \sum_{j=0}^{n-1} \binom{n-1}{j} B(j) \qquad \text{for } n > 0.$$

  (This is Theorem 2.3.3 on page 71.)

Generating functions

Stirling numbers of the second kind

Our first order of business is to determine generating functions for the Stirling and Bell numbers. For the Stirling numbers, which depend on two parameters n and k, we will fix k and compute the OGF of the sequence $\{S(n,k)\}_{n \geqslant 0}$.

So, fix any $k \geqslant 0$ and define

$$f_k(x) := \sum_{n \geqslant 0} S(n,k) x^n$$

to be the OGF we want. The $k = 0$ case is easy and also provides a basis for the $k > 0$ case:

$$\begin{aligned} f_0(x) &= \sum_{n \geqslant 0} S(n,0) x^n \\ &= S(0,0) + S(1,0)x + S(2,0)x^2 + \cdots \\ &= S(0,0) \\ &= 1. \end{aligned}$$

When $k > 0$ we start with the recurrence given at the beginning of this section, multiply by x^n, and sum over $n \geqslant 1$ to get

$$\sum_{n \geqslant 1} S(n,k) x^n = \sum_{n \geqslant 1} S(n-1,k-1) x^n + \sum_{n \geqslant 1} k \cdot S(n-1,k) x^n. \tag{4.7}$$

Let's analyze each term. The left-hand term equals $f_k(x)$ because $S(0,k) = 0$ for $k > 0$:

$$\begin{aligned}\sum_{n\geqslant 1} S(n,k)x^n &= S(1,k)x + S(2,k)x^2 + S(3,k)x^3 + \cdots \\ &= S(0,k) + S(1,k)x + S(2,k)x^2 + S(3,k)x^3 + \cdots \\ &= f_k(x).\end{aligned}$$

The middle term equals $xf_{k-1}(x)$:

$$\sum_{n\geqslant 1} S(n-1,k-1)x^n = x\sum_{n\geqslant 1} S(n-1,k-1)x^{n-1} = xf_{k-1}(x).$$

And the last term equals $kxf_k(x)$:

$$\sum_{n\geqslant 1} k\cdot S(n-1,k)x^n = kx\sum_{n\geqslant 1} S(n-1,k)x^{n-1} = kxf_k(x).$$

This shows that equation (4.7) can be rewritten as

$$f_k(x) = xf_{k-1}(x) + kxf_k(x) \qquad \text{for } k > 0.$$

There is a problem here that we haven't encountered before: *two* unknown OGFs appear, namely $f_k(x)$ and $f_{k-1}(x)$.

One remedy involves solving for $f_k(x)$ and noticing that it provides a recurrence:

$$f_k(x) = \frac{x}{1-kx} f_{k-1}(x) \qquad \text{for } k > 0. \tag{4.8}$$

This tells how to determine, by repeated multiplication, the OGF $f_k(x)$ for any $k > 0$. We already know that $f_0(x) = 1$. Then

$$\begin{aligned}f_1(x) &= \frac{x}{1-x} f_0(x) = \frac{x}{1-x} \\ f_2(x) &= \frac{x}{1-2x} f_1(x) = \frac{x^2}{(1-x)(1-2x)} \\ f_3(x) &= \frac{x}{1-3x} f_2(x) = \frac{x^3}{(1-x)(1-2x)(1-3x)}\end{aligned}$$

and so forth. We have proved the following theorem.

Theorem 4.3.1 *For any $k \geqslant 0$, the OGF of the sequence $\{S(n,k)\}_{n\geqslant 0}$ is 1 if $k = 0$ and is*

$$\frac{x^k}{(1-x)(1-2x)\cdots(1-kx)} = \prod_{j=1}^{k} \frac{x}{1-jx}$$

if $k > 0$.

Question 157 *Using the generating function, what is a formula for $S(n,2)$? That is, what is the coefficient of x^n in $x^2/(1-x)(1-2x)$? Make sure your answer matches the formula for $S(n,2)$ that we found in Section 2.3.*

Bell numbers

The Bell numbers have a well-known and beautiful EGF. To find it in concise form we'll end up solving a simple differential equation.

Define

$$g(x) := \sum_{n\geqslant 0} B(n)\frac{x^n}{n!}$$

as the EGF for the Bell numbers. As usual start with a recurrence, in this case the one that appears at the beginning of this section. For reasons that will become clear in a moment, multiply by $\frac{x^{n-1}}{(n-1)!}$ (rather than the usual $\frac{x^n}{n!}$) and then sum over $n \geqslant 1$ to get

$$\sum_{n\geqslant 1} B(n)\frac{x^{n-1}}{(n-1)!} = \sum_{n\geqslant 1}\left(\sum_{j=0}^{n-1}\binom{n-1}{j}B(j)\right)\frac{x^{n-1}}{(n-1)!}. \tag{4.9}$$

A few alarm bells should go off. First, the left-hand side equals the *derivative* of $g(x)$. Second, the right-hand side looks like a product of EGFs. In fact, by letting $m := n-1$ the right-hand side becomes

$$\sum_{n\geqslant 1}\left(\sum_{j=0}^{n-1}\binom{n-1}{j}B(j)\right)\frac{x^{n-1}}{(n-1)!} = \sum_{m\geqslant 0}\left(\sum_{k=0}^{m}\binom{m}{k}B(k)\right)\frac{x^m}{m!}.$$

The convolution formula for EGFs then implies it is the product of the EGFs for the sequences $\{B(n)\}_{n\geqslant 0}$ and $\{1\}_{n\geqslant 0}$:

$$\begin{aligned}\sum_{m\geqslant 0}\left(\sum_{k=0}^{m}\binom{m}{k}B(k)\right)\frac{x^m}{m!} &= \underbrace{\left(\sum_{n\geqslant 0}B(n)\frac{x^n}{n!}\right)}_{\text{Bell numbers}}\underbrace{\left(\sum_{n\geqslant 0}\frac{x^n}{n!}\right)}_{\text{all-1s}}\\ &= g(x)\cdot e^x.\end{aligned}$$

In other words, equation (4.9) reduces to $g'(x) = e^x g(x)$. This is a simple differential equation to solve: what function g has its derivative equal to e^x times g itself? The general solution is $g(x) = e^{e^x+C}$ for some constant C. To determine C, notice that $g(0) = B(0) = 1$. Therefore $1 = e^{e^0+C} = e^{1+C}$ and so $C = -1$.

Theorem 4.3.2 *The exponential generating function for the Bell numbers* $\{B(n)\}_{n\geqslant 0}$ *is* e^{e^x-1}.

A formula for the Bell numbers

As we recalled at the beginning of this section we do know a formula for the Stirling numbers of the second kind. It is

$$S(n,k) = \frac{1}{k!}\sum_{i=0}^{k}\binom{k}{i}(-1)^i(k-i)^n,$$

which could also be written

$$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}j^n. \tag{4.10}$$

Question 158 *Verify this.*

It is natural to ask whether a similar formula exists for the Bell numbers. It does.

We know that $B(n) = \sum_{k\geqslant 0} S(n,k)$. This is OK written as an infinite sum because $S(n,k) = 0$ for $k > n$. Using the formula shown in equation (4.10) above,

$$B(n) = \sum_{k\geqslant 0} S(n,k) = \sum_{k\geqslant 0}\left(\frac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}j^n\right).$$

Writing $\binom{k}{j} = \frac{k!}{j!(k-j)!}$ and canceling the $k!$ terms shows

$$\sum_{k\geqslant 0}\left(\frac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}j^n\right) = \sum_{k\geqslant 0}\sum_{j=0}^{k}\frac{(-1)^{k-j}}{(k-j)!}\frac{j^n}{j!}.$$

Switching the order of the summation produces

$$\sum_{k\geqslant 0}\sum_{j=0}^{k}\frac{(-1)^{k-j}}{(k-j)!}\frac{j^n}{j!} = \sum_{j\geqslant 0}\sum_{k\geqslant j}\frac{(-1)^{k-j}}{(k-j)!}\frac{j^n}{j!} = \sum_{j\geqslant 0}\left(\frac{j^n}{j!}\sum_{k\geqslant j}\frac{(-1)^{k-j}}{(k-j)!}\right).$$

Question 159 *Verify that the order of summation was correctly switched.*

Now for fixed $j \geqslant 0$, the inner sum is a familiar Maclaurin series:

$$\sum_{k\geqslant j}\frac{(-1)^{k-j}}{(k-j)!} = \sum_{i\geqslant 0}\frac{(-1)^i}{i!} = e^{-1}.$$

So now

$$\sum_{j\geqslant 0}\frac{j^n}{j!}\sum_{k\geqslant j}\frac{(-1)^{k-j}}{(k-j)!} = \sum_{j\geqslant 0}\frac{j^n}{j!}e^{-1} = e^{-1}\sum_{j\geqslant 0}\frac{j^n}{j!}.$$

We have derived a beautiful formula for the n-th Bell number.

Theorem 4.3.3 *For any $n > 0$, $B(n) = \dfrac{1}{e}\displaystyle\sum_{j\geqslant 0}\frac{j^n}{j!}$.*

It is perhaps miraculous that the formula of the theorem always produces an integer. For example, $B(5) = 52$ and so

$$\begin{aligned}\frac{1}{e}\sum_{j\geqslant 0}\frac{j^5}{j!} &= \frac{1}{e}\left(\frac{0^5}{0!}+\frac{1^5}{1!}+\frac{2^5}{2!}+\frac{3^5}{3!}+\frac{4^5}{4!}+\frac{5^5}{5!}+\cdots\right)\\ &= \frac{1}{e}\left(\frac{0}{1}+\frac{1}{1}+\frac{32}{2}+\frac{243}{6}+\frac{1024}{24}+\frac{3125}{120}+\cdots\right)\end{aligned}$$

equals 52, exactly. The infinite series provides a reasonable method for computing the Bell numbers because of its rapid convergence. Here are the first 15 Bell numbers:

n	1	2	3	4	5	6	7	8	9	10
$B(n)$	1	2	5	15	52	203	877	4140	21,147	115,975

n	11	12	13	14	15
$B(n)$	678,570	4,213,597	27,644,437	190,899,322	1,382,958,545

Question 160 *Use a computer to calculate some partial sums of $\frac{1}{e}\sum_{j\geqslant 0}\frac{j^{10}}{j!}$. How many terms do you need to find the value of $B(10)$?*

Polynomials and change of basis

Stirling numbers and coefficients of polynomials

To further understand the link between the algebraic and the combinatorial, the rest of this section offers some insight into how the Stirling numbers relate to the coefficients of certain polynomials.

Let's begin by finding a hard answer to an easy question. How many functions $[n] \longrightarrow [k]$ are there? One answer is k^n. To get another answer, condition on the size of the function's range. If its range is of size j, where $1 \leqslant j \leqslant n$, then there are $\binom{k}{j}$ ways to select j elements of $[k]$ to comprise the range of the function. Once accomplished, there are $S(n, j) \cdot j!$ ways to map all of $[n]$ to these j elements in an *onto* fashion. This gives a combinatorial proof of

$$k^n = \sum_{j=1}^{n} \binom{k}{j} S(n, j) \cdot j!.$$

Question 161 *In conditioning on the size j of the range, we stated that $1 \leqslant j \leqslant n$. A more natural choice might be $1 \leqslant j \leqslant k$, but why is the original choice justified?*

Now do some adjusting. Since $\binom{k}{j} \cdot j! = (k)_j$, rewrite the just-derived identity as

$$k^n = \sum_{j=1}^{n} S(n, j)(k)_j.$$

This polynomial equation in k is true for infinitely many positive integers k. Uniqueness of polynomials then allows for replacement of k by an indeterminate x to get the following theorem.

Theorem 4.3.4 *For any $n \geqslant 0$, $x^n = \sum_{j=0}^{n} S(n, j)(x)_j$.*

Proof: The proof for $n > 0$ appears before the theorem. When $n = 0$, recall that $(x)_0 := 1$. In that case, the theorem's formula is also correct: $\sum_{j=0}^{0} S(0, j)(x)_j = S(0, 0)(x)_0 = 1 \cdot 1 = x^0$. ■

The theorem is interesting because although we derived it in a combinatorial fashion, it is an algebraic fact about the polynomials $(x)_j$. Specifically, it says that the Stirling numbers of the second kind describe how to write the polynomial x^n as a linear combination of the polynomials $(x)_j$ for $0 \leqslant j \leqslant n$. For those versed in linear algebra, the numbers $S(n, j)$ are the coordinates of the polynomial x^n relative to the basis $\{(x)_0, (x)_1, (x)_2, \ldots, (x)_n\}$ for the vector space of polynomials of degree at most n. For example, the theorem guarantees that

$$x^3 = S(3, 0)(x)_0 + S(3, 1)(x)_1 + S(3, 2)(x)_2 + S(3, 3)(x)_3.$$

Check it:

$$\begin{aligned} &S(3, 0)(x)_0 + S(3, 1)(x)_1 + S(3, 2)(x)_2 + S(3, 3)(x)_3 \\ &\quad = 0(1) + 1(x) + 3x(x - 1) + 1(x)(x - 1)(x - 2) \\ &\quad = x + 3x^2 - 3x + x^3 - 3x^2 + 2x \\ &\quad = x^3. \end{aligned}$$

Question 162 *Write x^4 as a linear combination of the polynomials $(x)_0$, $(x)_1$, $(x)_2$, $(x)_3$, and $(x)_4$. Do the same for $5x^4 - 10x^3$.*

Stirling numbers of the first kind

Perhaps it is more interesting to go in the other direction: when you expand, say,

$$(x)_5 = x(x-1)(x-2)(x-3)(x-4) = x^5 - 10x^4 + 35x^3 - 50x^2 + 24x,$$

where do the coefficients $1, -10, 35, -50, 24$ come from? Do they have a combinatorial meaning?

Since $(x)_n = x(x-1)(x-2)\cdots(x-n+1)$ is a polynomial of degree n, there are numbers $s(n,k)$ for $0 \leqslant k \leqslant n$ for which

$$(x)_n = \sum_{k=0}^{n} s(n,k)x^k.$$

This is the definition of the ***Stirling numbers of the first kind***.

Question 163 *Based on the $(x)_5$ example of the previous paragraph, what is $s(5,k)$ for $0 \leqslant k \leqslant 5$?*

A recurrence for computing $s(n,k)$ follows from writing $(x)_n = (x)_{n-1}(x-n+1)$ or $(x)_n = x(x)_{n-1} - (n-1)(x)_{n-1}$. Now use the definition of the numbers $s(n,k)$ to rewrite this equation as

$$\underbrace{\sum_{k=0}^{n} s(n,k)x^k}_{(x)_n} = x\underbrace{\sum_{k=0}^{n-1} s(n-1,k)x^k}_{(x)_{n-1}} - (n-1)\underbrace{\sum_{k=0}^{n-1} s(n-1,k)x^k}_{(x)_{n-1}}. \tag{4.11}$$

Finally, just match the coefficients on x^k on each side of the equation to derive the following recurrence.

Theorem 4.3.5 *For $n > 0$ and $k > 0$, the Stirling numbers of the first kind satisfy the identity*

$$s(n,k) = s(n-1,k-1) - (n-1)\cdot s(n-1,k). \tag{4.12}$$

Question 164 *Why is $s(n-1,k-1)$ the coefficient of x^k in the middle term of equation (4.11)?*

Like the Stirling numbers of the second kind, the Stirling numbers of the first kind satisfy similar boundary conditions: $s(0,0) = 1$, $s(n,0) = 0$ for $n > 0$, and $s(0,k) = 0$ for $k > 0$.

Question 165 *What is the reason for each of the boundary conditions? Explain in terms of the definition of the Stirling numbers of the first kind. (Remember $(x)_0 := 1$.)*

The recurrence allows computation of ***Stirling's triangle of the first kind***:

$n\downarrow\ k\rightarrow$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	−1	1	0	0	0	0	0
3	0	2	−3	1	0	0	0	0
4	0	−6	11	−6	1	0	0	0
5	0	24	−50	35	−10	1	0	0
6	0	−120	274	−225	85	−15	1	0
7	0	720	−1764	1624	−735	175	−21	1

(4.13)

As usual, the entry in row n and column k is $s(n,k)$.

Counting permutations of $[n]$ with k cycles

The Stirling numbers of the second kind have a combinatorial interpretation. Do the Stirling numbers of the first kind have one as well? Yes, sort of.

Cycle notation

Recall that a ***permutation of*** $[n]$ is a bijection $[n] \longrightarrow [n]$. Equivalently, it is an n-list taken from $[n]$ such that each element appears exactly once. For example, the permutation $(7, 4, 3, 2, 6, 1, 5)$ of $[7]$ is a convenient notation for the bijection $f : [7] \longrightarrow [7]$ that has $f(1) = 7$, $f(2) = 4$, $f(3) = 3$, and so on.

To write this f as a ***product of disjoint cycles***, do the following. Start with element 1 and then repeatedly apply f to it until you reach 1 again:

$$1 \implies f(1) = 7 \implies f(7) = 5 \implies f(5) = 6 \implies f(6) = 1.$$

Record this piece of the permutation as the ***cycle*** (1 7 5 6). In it, the image of any element appears immediately to the right of that element. At the end it wraps around, so that the image of 6 is 1.

Next, start with the smallest element not appearing in the above cycle and repeatedly apply f again:

$$2 \implies f(2) = 4 \implies f(4) = 2.$$

Record this as the cycle (2 4). Now do it again, starting this time with 3. It has $f(3) = 3$, so the corresponding cycle is (3). This exhausts all the elements of [7], so

$$f = (1\ 7\ 5\ 6)(2\ 4)(3)$$

is now written as a product of disjoint cycles.

The above procedure, when made formal, will always result in a correct representation of f as a product of disjoint cycles. (See Exercise 3.) Such a representation is not unique, however, as $f = (5\ 6\ 1\ 7)(3)(2\ 4)$ is also a correct representation of f.

To make sure you understand cycle notation, let's find the "ordinary" (i.e., 7-list) way to describe the permutation (1 2 4)(3 7)(5)(6). It has

$$\begin{array}{lll} f(1) = 2 & f(3) = 7 & f(5) = 5 \\ f(2) = 4 & f(4) = 1 & f(6) = 6 \end{array} \qquad f(7) = 3$$

so as a 7-list, $f = (2, 4, 7, 1, 5, 6, 3)$.

Question 166 *Write the permutation* $(10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$ *as a product of disjoint cycles. Write the permutation* (1 9 8 7)(2)(3 6 5 4) *as a 9-list.*

Permutations and Stirling numbers of the first kind

Let $c(10, 4)$ denote the number of permutations of [10] that contain exactly four cycles. Such a permutation either has the element 10 in a cycle by itself, such as in (1 7 2)(3 9 8 6)(4 5)(10); or else has the element 10 in a cycle with at least one other element, such as in (1 9 5 3)(2)(4)(6 10 8 9).

There are $c(9, 3)$ permutations of the first type since deleting the cycle containing 10 alone leaves a permutation of [9] containing exactly three cycles. There are $9 \cdot c(9, 4)$

permutations of the second type, for we may create such a permutation by first selecting a permutation of [9] into four cycles and then choosing the location of the element 10 in any of nine ways: *before* any of the nine elements already appearing. For example, the second permutation given in the previous paragraph was created by selecting the following permutation of [9] into four blocks:

$$(1\,9\,5\,3)(2)(4)(6\,8\,9)$$

and then choosing to put element 10 before element 8. The requirement of only placing 10 before any of the given nine elements is important. If we also allowed placement after the last element of a cycle, then we would over-count because, for example, the cycle (1 9 5 3 10) is the same as the cycle (10 1 9 5 3).

Definition 4.3.6 *For any $n \geq 0$ and $k \geq 0$, the expression $c(n,k)$ equals the number of permutations of $[n]$ having exactly k cycles. We define $c(0,0) := 1$.*

Notice that, like the Stirling numbers of the first kind, $c(n,0) = c(0,k) = 0$ for positive values of n and k. The discussion prior to the definition provides the idea behind the proof of the following identity.

Theorem 4.3.7 *For $n > 0$ and $k > 0$, the numbers $c(n,k)$ satisfy the identity*

$$c(n,k) = c(n-1,k-1) + (n-1)\cdot c(n-1,k).$$

Question 167 *Give a combinatorial proof of the theorem.*

The triangle of the numbers $c(n,k)$ should look familiar:

$n\downarrow\ k\rightarrow$	0	1	2	3	4	5	6	7
0	1	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0
3	0	2	3	1	0	0	0	0
4	0	6	11	6	1	0	0	0
5	0	24	50	35	10	1	0	0
6	0	120	274	225	85	15	1	0
7	0	720	1764	1624	735	175	21	1

Namely, the numbers $c(n,k)$ appear to be the absolute values of the numbers $s(n,k)$. That $c(n,k)$ has a combinatorial interpretation while $s(n,k)$ has an algebraic interpretation adds to the intrigue.

While a comparison of the two tables of values may convince you that $c(n,k) = \left|s(n,k)\right|$, one way to provide a rigorous proof is to use a double induction on n and k. In fact we can prove something more specific: $s(n,k) = (-1)^{n+k}c(n,k)$.

The base cases occur on the left and top edges of the tables that we constructed for $s(n,k)$ and $c(n,k)$. That is, for values of n and k where at least one is zero. Since $s(0,0) = 1 = c(0,0)$ and $s(n,0) = 0 = c(n,0)$ and $s(0,k) = 0 = c(0,k)$ for all $n > 0$ and $k > 0$, it follows that $s(n,k) = (-1)^{n+k}c(n,k)$ for these values of n and k.

Now let $n > 0$ and $k > 0$ be fixed, and assume that the statement is true for all nonnegative integers m and i for which $m \leqslant n$ and $i \leqslant k$ but where equality does not hold

in both cases. Begin by writing the recursion for $s(n,k)$, then use the inductive hypothesis to replace the lesser terms, and then do a little algebra:

$$\begin{aligned} s(n,k) &= s(n-1,k-1) - (n-1)\cdot s(n-1,k) \\ &= (-1)^{n-1+k-1} c(n-1,k-1) - (n-1)\cdot(-1)^{n-1+k} c(n-1,k) \\ &= (-1)^{n+k} c(n-1,k-1) + (n-1)\cdot(-1)^{n+k} c(n-1,k) \\ &= (-1)^{n+k}\big[c(n-1,k-1) + (n-1)\cdot c(n-1,k)\big] \\ &= (-1)^{n+k} c(n,k). \end{aligned}$$

Question 168 *Justify the third equality above. What has happened to the powers of* -1 *and why?*

Therefore the statement is true for all nonnegative integers n and k.

Theorem 4.3.8 *For all* $n \geq 0$ *and* $k \geq 0$, $s(n,k) = (-1)^{n+k} c(n,k)$. *In particular, the absolute value of the Stirling number of the first kind* $s(n,k)$ *equals the number of permutations of* $[n]$ *with exactly* k *cycles.*

The difference operator

Our last adventure in this section reveals another algebraic bridge to the Stirling numbers.

Let $f(n)$ be a function defined for integers $n \geq 0$. Define the ***difference operator*** Δ by

$$\Delta f(n) := f(n+1) - f(n).$$

The difference operator can be iterated as follows: $\Delta^k f(n) := \Delta\big(\Delta^{k-1} f(n)\big)$. For example,

$$\begin{aligned} \Delta^2 f(n) = \Delta\big(\Delta f(n)\big) &= \Delta\big(f(n+1) - f(n)\big) \\ &= f(n+2) - f(n+1) - \big(f(n+1) - f(n)\big) \\ &= f(n+2) - 2f(n+1) + f(n). \end{aligned}$$

Since $\Delta^3 f(n) = \Delta\big(\Delta^2 f(n)\big)$, it follows that

$$\begin{aligned} \Delta^3 f(n) &= \Delta\big(f(n+2) - 2f(n+1) + f(n)\big) \\ &= f(n+3) - 2f(n+2) + f(n+1) \\ &\quad - \big(f(n+2) - 2f(n+1) + f(n)\big) \\ &= f(n+3) - 3f(n+2) + 3f(n+1) - f(n). \end{aligned}$$

Indeed the pattern becomes obvious for $\Delta^4 f(n)$:

$$\Delta^4 f(n) = f(n+4) - 4f(n+3) + 6f(n+2) - 4f(n+1) + f(n).$$

Question 169 *Verify this formula by calculating* $\Delta\big(\Delta^3 f(n)\big)$.

The following theorem, which Exercise 14 asks you to prove by induction, shows how the binomial coefficients appear in the computation of $\Delta^m f(n)$.

Theorem 4.3.9 *If* $f(n)$ *is a function defined for all integers* $n \geq 0$, *then*

$$\Delta^m f(n) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} f(n+m-k)$$

for all $m \geq 1$.

In what we are about to derive, our main concern is when $n = 0$. In that case the formula of the theorem says

$$\Delta^m f(0) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} f(m-k),$$

which can be rewritten (let $j := m - k$ so that $k = m - j$)

$$\Delta^m f(0) = \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} f(j). \tag{4.14}$$

This gives a formula for the m-th difference of f at 0 in terms of $f(0), f(1), \ldots, f(m)$.

The question is, can we invert this formula? That is, is it possible to get a formula for $f(n)$ in terms of the differences $\Delta^k f(0)$? The answer is yes. Exercise 10 asks for a proof of the following result.

Theorem 4.3.10 *If $f(n)$ is a function defined for all integers $n \geqslant 0$, then*

$$f(n) = \sum_{k=0}^{n} \binom{n}{k} \Delta^k f(0).$$

The theorem says that if we know the differences of the function at 0, then we can reconstruct the function itself.

Example: a difference table

Given a function $f(n)$ defined on nonnegative integers n, the ***difference table*** for f at $n = 0$ is

$$\begin{array}{ccccccccccc}
f(0) & & f(1) & & f(2) & & f(3) & & f(4) & \cdots \\
& \Delta f(0) & & \Delta f(1) & & \Delta f(2) & & \Delta f(3) & \cdots & \\
& & \Delta^2 f(0) & & \Delta^2 f(1) & & \Delta^2 f(2) & & \Delta^2 f(3) & \cdots \\
& & & \Delta^3 f(0) & & \Delta^3 f(1) & & \Delta^3 f(2) & \cdots & \\
& & & & \Delta^4 f(0) & & \Delta^4 f(1) & & \Delta^4 f(2) & \cdots \\
& & & & & \ddots & & \ddots & & \ddots
\end{array}$$

The numbers $f(0), f(1), f(2), \ldots$ go in the first row. To get the second row, we know $\Delta f(0) = f(1) - f(0)$ so put that number directly below the space between $f(0)$ and $f(1)$. In this way you can compute the rest of the row by taking the entry to the northeast and subtracting the entry to the northwest. Because of the definition of the difference operator, subsequent rows are computed in exactly the same way.

As an example, construct the ***difference table*** for $f(n) = n^3$.

$$\begin{array}{ccccccccccc}
\mathbf{0} & & 1 & & 8 & & 27 & & 64 & & 125 & \cdots \\
& \mathbf{1} & & 7 & & 19 & & 37 & & 61 & \cdots & \\
& & \mathbf{6} & & 12 & & 18 & & 24 & \cdots & & \\
& & & \mathbf{6} & & 6 & & 6 & \cdots & & & \\
& & & & \mathbf{0} & & 0 & \cdots & & & &
\end{array}$$

This shows that $f(0) = 0$, $\Delta f(0) = 1$, $\Delta^2 f(0) = \Delta^3 f(0) = 6$, and $\Delta^m f(0) = 0$ for $m > 3$. These entries are printed in boldface in the difference table because they are the

ones appearing in Theorem 4.3.10. That theorem shows (those same entries are in boldface below)

$$\begin{aligned} n^3 &= \sum_{k=0}^{n} \binom{n}{k} \Delta^k f(0) \\ &= \mathbf{0}\binom{n}{0} + \mathbf{1}\binom{n}{1} + \mathbf{6}\binom{n}{2} + \mathbf{6}\binom{n}{3} + \mathbf{0}\binom{n}{4} + \cdots + \mathbf{0}\binom{n}{n} \\ &= \binom{n}{1} + 6\binom{n}{2} + 6\binom{n}{3}. \end{aligned}$$

Since this is true for infinitely many values of the nonnegative integer n, it is true as a polynomial equation when we replace n by an indeterminate x and use $\binom{x}{k} = \frac{(x)_k}{k!}$. As such,

$$x^3 = \binom{x}{1} + 6\binom{x}{2} + 6\binom{x}{3} = (x)_1 + \frac{6}{2!}(x)_2 + \frac{6}{3!}(x)_3.$$

In general, with $f(x) = x^n$,

$$x^n = \sum_{k=0}^{n} \binom{x}{k} \Delta^k f(0) = \sum_{k=0}^{n} \frac{\Delta^k f(0)}{k!} (x)_k.$$

But we also know that $x^n = \sum_{k=0}^{n} S(n,k)(x)_k$ and so $S(n,k) = \dfrac{\Delta^k f(0)}{k!}$ or $\Delta^k f(0) = S(n,k) \cdot k!$.

All of this shows that if $f(x) = x^n$, then $\Delta^k f(0)$ has a combinatorial interpretation: it equals the number of onto functions $[n] \longrightarrow [k]$.

Summary

For fixed $k \geqslant 0$, the OGF of the numbers $S(n,k)$ is $x^k/(1-x)(1-2x)\cdots(1-kx)$. The EGF of the numbers $B(n)$ is e^{e^x-1} and a beautiful formula for the n-th Bell number is

$$B(n) = \frac{1}{e} \sum_{j \geqslant 0} \frac{j^n}{j!}.$$

Algebraically, the Stirling numbers of the first and second kinds are the coefficients in certain polynomial expansions:

$$(x)_n = \sum_{k=0}^{n} s(n,k) x^k \qquad \text{and} \qquad x^n = \sum_{k=0}^{n} S(n,k)(x)_k.$$

Although the Stirling numbers of the first kind alternate in sign, their absolute values have a combinatorial interpretation: $\left|s(n,k)\right|$ equals the number of permutations of $[n]$ with exactly k cycles. The difference operator provides another link between polynomials and Stirling numbers of the second kind.

Exercises

1. Write the polynomial $3x^4 - x^3 + 4x + 10$ as a linear combination of the polynomials $(x)_0, (x)_1, (x)_2, (x)_3, (x)_4$.
2. Write $3(x)_4 - 12(x)_3 + 4(x)_1 - 17$ as a linear combination of the polynomials $1, x, x^2, x^3, x^4$.
3. Describe an algorithm that takes as its input a permutation of $[n]$, written as an n-list, and outputs the permutation written in cycle notation. The cycle notation should have the following properties: (1) the first cycle should begin with element 1; (2) each successive cycle should begin with the smallest element not belonging to any of the previous cycles.
4. (a) Give a combinatorial proof: for $n \geq 1$, $c(n, n-1) = \binom{n}{2}$.
   (b) Give a combinatorial proof: for $n \geq 1$, $c(n, 1) = (n-1)!$.
   (c) Give an algebraic proof: for $n \geq 1$, $s(n, n-1) = -\binom{n}{2}$.
   (d) Give an algebraic proof: for $n \geq 1$, $s(n, 1) = (-1)^{n-1}(n-1)!$.
5. Let f be a continuous function. Prove that the general solution to the differential equation $y' = f(x)y$ is $y = e^{F(x)+C}$ where F is an antiderivative of f and C is a constant.
6. Prove: for any $n \geq 0$, $(-x)_n = (-1)^n (x)^{(n)}$. (The notation $(x)^{(n)}$ is "rising factorial" notation. See Exercise 16 of Section 2.1.)
7. Prove: for any $n \geq 0$, $(x)^{(n)} = \sum_{k \geq 0} c(n, k) x^k$. (See previous exercise.)
8. Write the expansion of $(1+x)^n$ as a linear combination of the polynomials $(x)_k$. That is, determine the coefficients a_k so that $(1+x)^n = \sum_{k=0}^{n} a_k (x)_k$.
9. Let $k \geq 0$. In this section we derived the OGF of the sequence $\{S(n,k)\}_{n \geq 0}$. Show that the EGF of the same sequence is $\frac{1}{k!}(e^x - 1)^k$.
10. Prove Theorem 4.3.10.
11. Find and prove a formula for the number of partitions of $[n]$ in which consecutive integers never appear in the same block.
12. Following the example for x^3 in this section, construct the difference table for $f(n) = n^4$ and then write x^4 as a linear combination of the polynomials $\binom{x}{j}$ for $0 \leq j \leq 4$.
13. Prove that, like the derivative, the difference operator Δ satisfies $\Delta\big(f(n) + g(n)\big) = \Delta f(n) + \Delta g(n)$ and for any number c, $\Delta\big(cf(n)\big) = c\Delta f(n)$.
14. Prove Theorem 4.3.9 by induction on m.

Travel Notes

When $f(x) = x^n$ the appearance of the equation

$$f(x) = \sum_{k=0}^{n} \frac{\Delta^k f(0)}{k!} (x)_k$$

may remind you of the Maclaurin series of an infinitely differentiable function, namely

$$g(x) = \sum_{k \geq 0} \frac{g^{(k)}(0)}{k!} x^k.$$

Both equations describe how to express a function ($f(x)$ or $g(x)$, respectively) as a linear combination of other functions (falling factorials $(x)_k$ or power functions x^k) where the coefficients of that linear combination involve measurements of change at $x = 0$ (the k-th difference or the k-th derivative, respectively). Indeed there is a *calculus of finite differences* that is the discrete version of ordinary, continuous calculus.

4.4 Integer partition numbers

In Sections 2.4 and 3.4, we learned some facts about partitions of integers. Recall that $P(n,k)$ equals the number of partitions of the integer n into k parts, and $P(n)$ equals the total number of partitions of the integer n. Among other things, the partition numbers satisfy the identity

$$P(n,k) = \sum_{j=1}^{k} P(n-k, j).$$

(This is Theorem 2.4.2 on page 79.) Simply put, this says that the number of partitions of n into k parts equals the number of partitions of $n-k$ into at most k parts. It is perhaps less cumbersome to write it like

$$P(n,k) = P(n-k, \text{at most } k \text{ parts}). \tag{4.15}$$

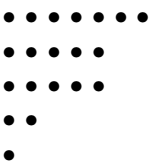
We also learned that the OGF of $\{P(n)\}_{n \geq 0}$ is

$$\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots} = \prod_{j \geq 1} \frac{1}{1-x^j}.$$

(This is Theorem 3.4.3 on page 120.) In this section we will prove two more combinatorial theorems about partition numbers, find the OGF of $P(n,k)$ for fixed k, and investigate the prospect of formulas for partition numbers.

Ferrers diagrams

A ***Ferrers diagram*** is a useful tool not only for visualizing a partition but also for proving theorems about partitions. The Ferrers diagram for the partition $7+5+5+2+1$ of 20 is



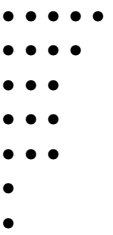
There is one row for each part of the partition and as many dots in each row as the size of its corresponding part. A Ferrers diagram also lists the parts in non-increasing order, from top to bottom.

Operations on Ferrers diagrams

One operation that we can perform on a Ferrers diagram is to delete its first column. This corresponds to subtracting 1 from each part. In fact, this is exactly what we did when we gave the bijective proof that $P(n,k) = P(n-k, \text{at most } k \text{ parts})$ in Theorem 2.4.2 on page 79.

Question 170 *What operation on Ferrers diagrams leads to an immediate bijective proof of the identity* $P(n, \text{largest part } k) = P(n-k, \text{largest part at most } k)$*?*

Another and perhaps more subtle operation is to take the conjugate. To obtain the ***conjugate of a Ferrers diagram***, simply swap the role of rows and columns.[4] For example, the conjugate of the Ferrers diagram of the partition shown earlier is



This Ferrers diagram corresponds to the partition $5+4+3+3+3+1+1$ of 20. We can in this way speak of the ***conjugate*** of a partition without referring to Ferrers diagrams. Ferrers diagrams offer a convenient way to carry out the conjugation. See, though, Exercise 2.

Question 171 *What is the conjugate of the partition* $19+1$*?*

Here are some basic facts about conjugation.

- Fact 1: The conjugate of a partition of n is also a partition of n.
- Fact 2: The conjugate operation, applied twice, returns the original partition.
- Fact 3: If a partition has largest part k, then its conjugate has k parts. Likewise, if a partition has k parts, then its conjugate has largest part k.
- Fact 4: If a partition has at most k parts, then its conjugate has largest part at most k. Likewise, if a partition has largest part at most k, then its conjugate has at most k parts.
- Fact 5: Conjugation is always a one-to-one operation.

Question 172 *Why is Fact 5 true? Give a quick proof.*

Proofs using Ferrers diagrams

Identities based on Facts 3 and 4

Consider the partitions of n into k parts (call this set A) and the partitions of n with largest part k (call it B). The conjugate operation is a function from A to B by Fact 3. It is a one-to-one function by Fact 5. It is onto by Facts 2 and 3: given a partition in B, take its conjugate to get a partition in A; then the conjugate of this partition is the original partition from B. We have just given a bijective proof of the following theorem.

Theorem 4.4.1 *For any positive integers n and k,* $P(n,k) = P(n, \text{largest part } k)$.

[4] Perhaps "transpose" is a better term (like the transpose of a matrix), but the term "conjugate" has stuck.

Fact 4 above also leads to a similar combinatorial theorem of which we will make good use when we derive some algebraic results.

Theorem 4.4.2 *For any $n, k \geq 1$,*

$$P(n, \textit{at most } k \textit{ parts}) = P(n, \textit{largest part at most } k).$$

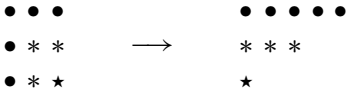
Question 173 *Provide a proof of this theorem using conjugation.*

Self-conjugate partitions

A partition is ***self-conjugate*** provided that its conjugate equals itself. Examples of self-conjugate partitions are $3+3+3$ and $7+4+2+2+1+1+1$ and 1. Our next result says that the self-conjugate partitions of n are in one-to-one correspondence with the partitions of n into distinct odd parts.

Ferrers diagrams help us understand why. Take the partition $3+3+3$ of 9:

Now "unpeel" one layer of this Ferrers diagram by removing the dots in its first row and column, of which there are five. What is left is the self-conjugate partition $2+2$, from which we can similarly unpeel the dots (three of them) in its first row and column. Then only the self-conjugate partition 1 is left, and that is easy to unpeel. In this way we create the partition $5+3+1$ which has distinct odd parts. The following diagram, using different symbols for each unpeeled layer, shows the correspondence:

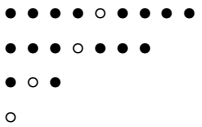


Question 174 *Via the unpeeling operation, to what partition does the self-conjugate partition $7+4+2+2+1+1+1$ correspond? Does it have distinct odd parts?*

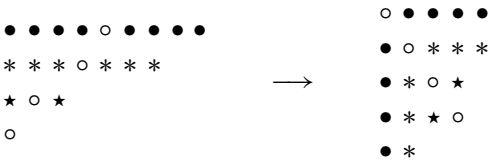
This operation always transforms a self-conjugate partition into one with distinct odd parts.

Question 175 *Explain why this happens in general.*

The reverse operation does indeed transform a partition into distinct odd parts into a self-conjugate partition. To illustrate the reverse operation, begin with the Ferrers diagram of a partition into distinct odd parts and locate the center dot in each row. For example, the centers of the partition $9+7+3+1$ are marked with $\circ$ in the following:



Now, bend each row around its center and nest each resulting L-shape so that a self-conjugate partition results:



Question 176 *In general, why must there always be a center dot in each row of such a partition? Why is the resulting partition always self-conjugate?*

These ideas prove the theorem.

Theorem 4.4.3 *For $n \geqslant 1$, $P(n, \text{self-conjugate}) = P(n, \text{distinct odd parts})$.*

Generating functions

The OGF for the partition numbers $P(n)$ is given at the beginning of this section. By stopping its infinite product at a fixed positive integer k, we get the OGF for the number of partitions of n with largest part at most k. But, by Theorem 4.4.2, this means we have also found the OGF for the number of partitions of n with at most k parts. In other words,

$$\sum_{n\geqslant 0} P(n, \text{at most } k \text{ parts})x^n = \prod_{j=1}^{k} \frac{1}{1-x^j}.$$

Now, to get the OGF for $P(n,k)$, we can just use the self-evident identity

$$P(n,k) = P(n, \text{at most } k \text{ parts}) - P(n, \text{at most } k-1 \text{ parts})$$

and subtract the corresponding OGFs. We have

$$\begin{aligned}
&\frac{1}{(1-x)\cdots(1-x^{k-1})(1-x^k)} - \frac{1}{(1-x)\cdots(1-x^{k-1})} \\
&= \frac{1}{(1-x)\cdots(1-x^{k-1})(1-x^k)} - \frac{1-x^k}{(1-x)\cdots(1-x^{k-1})(1-x^k)} \\
&= \frac{1-(1-x^k)}{(1-x)\cdots(1-x^{k-1})(1-x^k)} \\
&= \frac{x^k}{(1-x)\cdots(1-x^{k-1})(1-x^k)}.
\end{aligned}$$

Theorem 4.4.4 *For any $k \geqslant 1$, the OGF of the sequence $\{P(n,k)\}_{n\geqslant 0}$ equals*

$$\frac{x^k}{(1-x)(1-x^2)\cdots(1-x^k)} = \prod_{j=1}^{k} \frac{x}{1-x^j}.$$

Compare this with Theorem 4.3.1 on page 164. The similarity is striking!

Formulas for partition numbers

We have reasonable, closed-form formulas for all of the counting functions that we introduced in Chapter 2 except for the integer partition numbers. Are formulas for $P(n)$ and $P(n,k)$ possible? Yes and no.

A formula for $P(n)$ is possible but completely beyond the scope of this text. Formulas for $P(n,1)$, $P(n,2)$, $P(n,3)$, and so forth are possible but the difficulty appears to increase as the number of parts increases.

We already know that $P(n,1) = 1$ and that $P(n,2) = \lfloor \frac{n}{2} \rfloor$.

Question 177 *Justify the formula for $P(n,2)$.*

The following theorem, which we devote the rest of this subsection to proving, provides a formula for $P(n,3)$. The notation $\{x\}$ denotes the closest integer to x.

Theorem 4.4.5 *For any $n \geqslant 0$, $P(n,3)$ equals the closest integer to $\frac{n^2}{12}$. That is, $P(n,3) = \left\{\frac{n^2}{12}\right\}$.*

Our proof strategy is first to obtain a formula for $P(n, \text{at most 3 parts})$ and then apply equation (4.15), namely

$$P(n,3) = P(n-3, \text{at most 3 parts}).$$

It is an interesting journey.

We begin by using Theorem 4.4.2 to write

$$P(m, \text{at most 3 parts}) = P(m, \text{largest part at most 3}).$$

Therefore the OGF for the partitions of m with at most 3 parts is

$$\sum_{m \geqslant 0} P(m, \text{at most 3 parts}) x^m = \frac{1}{(1-x)(1-x^2)(1-x^3)}. \tag{4.16}$$

To find the coefficient of x^m in the expression on the right-hand side, we factor the denominator in preparation for finding its partial fraction decomposition (PFD):

$$\begin{aligned} 1 - x^2 &= (1-x)(1+x) \\ 1 - x^3 &= (1-x)(1+x+x^2). \end{aligned}$$

The quadratic $1+x+x^2$ is irreducible over the real numbers—it cannot be factored further. There are at least two options.

Option one is to go full steam ahead with the normal PFD; Exercise 5 asks you to take this route. Option two comes out cleaner but at first glance appears to require some luck. Change the PFD's form a bit and instead use

$$\frac{1}{(1-x)(1-x^2)(1-x^3)} = \frac{A}{(1-x)^3} + \frac{B}{(1-x)^2} + \frac{C}{1-x^3} + \frac{D}{1-x^2}. \tag{4.17}$$

Since the decomposition on the right doesn't include all terms required of a PFD, we should expect no guarantee that values A, B, C, D exist that make the equation true. But if they do then it will be very easy to extract the coefficient of x^m, and herein would lie the advantage.

The usual clearing-of-denominators procedure in equation (4.17) produces

$$\begin{aligned} 1 = {} & A(1+x)(1+x+x^2) + B(1+x)(1-x^3) \\ & + C(1-x)(1-x^2) + D(1-x)(1-x^3), \end{aligned}$$

and the solution is $A = 1/6$, $B = D = 1/4$, and $C = 1/3$.

Question 178 *Carry out the algebra that shows that this is the solution.*

We have found the decomposition

$$\frac{1}{(1-x)(1-x^2)(1-x^3)} = \frac{1/6}{(1-x)^3} + \frac{1/4}{(1-x)^2} + \frac{1/3}{1-x^3} + \frac{1/4}{1-x^2}.$$

Replacing each term on the right-hand side with its infinite series representation shows that we seek the coefficient of x^m in

$$\frac{1}{6}\sum_{m\geqslant 0}\left(\!\!\binom{3}{m}\!\!\right)x^m+\frac{1}{4}\sum_{m\geqslant 0}\left(\!\!\binom{2}{m}\!\!\right)x^m+\frac{1}{3}\sum_{m\geqslant 0}x^{3m}+\frac{1}{4}\sum_{m\geqslant 0}x^{2m}.$$

That coefficient, and therefore a formula for $P(m,\text{ at most 3 parts})$, is

$$\frac{1}{6}\left(\!\!\binom{3}{m}\!\!\right)+\frac{1}{4}\left(\!\!\binom{2}{m}\!\!\right)+\big[\text{either } 1/3 \text{ or } 0\big]+\big[\text{either } 1/4 \text{ or } 0\big].$$

This is only marginally acceptable as a formula because of the sloppiness of the last two terms. But it turns out that a bit more algebra justifies it. Begin by simplifying the first two terms:

$$\frac{1}{6}\left(\!\!\binom{3}{m}\!\!\right)+\frac{1}{4}\left(\!\!\binom{2}{m}\!\!\right)=\cdots=\frac{(m+3)^2}{12}-\frac{1}{3}.$$

Question 179 *Verify this.*

So now the coefficient of x^m in the OGF is

$$\frac{(m+3)^2}{12}-\frac{1}{3}+\big[\text{either } 1/3 \text{ or } 0\big]+\big[\text{either } 1/4 \text{ or } 0\big].$$

By enumerating the four possibilites, we learn that the sum of the terms other than the first one only takes on one of four possible values:

$$\begin{aligned}-\tfrac{1}{3}+0+0&=-\tfrac{1}{3}\\ -\tfrac{1}{3}+0+\tfrac{1}{4}&=-\tfrac{1}{12}\\ -\tfrac{1}{3}+\tfrac{1}{3}+0&=0\\ -\tfrac{1}{3}+\tfrac{1}{3}+\tfrac{1}{4}&=\tfrac{1}{4}\end{aligned}$$

But each of these numbers is, in absolute value, less than $\frac{1}{2}$. Therefore, we can conclude that $P(m,\text{ at most 3 parts})$ equals the closest integer to $\frac{(m+3)^2}{12}$. That is,

$$P(m,\text{ at most 3 parts})=\left\{\frac{(m+3)^2}{12}\right\}.$$

To get our result, apply this formula with $m=n-3$:

$$P(n,3)=P(n-3,\text{ at most 3 parts})=\left\{\frac{\big((n-3)+3\big)^2}{12}\right\}=\left\{\frac{n^2}{12}\right\}.$$

This completes the proof of Theorem 4.4.5.

An asymptotic approximation for $P(n,k)$

Essentially the same approach works to discover formulas for $P(n,4)$ and higher, but the contortions involved grow more complicated at each step. This suggests that an all-encompassing exact formula for $P(n,k)$ will not be, well, simple.

Let's lower our standards a bit and instead search for an approximation to $P(n,k)$ for fixed k. The type of approximation that we will seek is an important one in mathematics: an asymptotic approximation. Asymptotic approximations are often just as useful, and in some instances more useful, than exact formulas.

Given two functions $f(n)$ and $g(n)$, we say that f ***is asymptotically equivalent to*** g provided that

$$\lim_{n\longrightarrow\infty}\frac{f(n)}{g(n)}=1.$$

The notation $f(n)\sim g(n)$ indicates asymptotic equivalence. This is an equivalence relation; see Exercise 7(a).

Question 180 *Show that* $f(n)=4n^3-100n+12$ *and* $g(n)=19+20n-21n^2+4n^3$ *are asymptotically equivalent.*

So, we seek a familiar function (e.g., a polynomial or exponential function) that is asymptotically equivalent to $P(n,k)$. Our strategy for obtaining this involves first squeezing $P(n,k)$ between the following lower and upper bounds.

$$\frac{\left(\!\!\binom{k}{n-k}\!\!\right)}{k!}\leqslant P(n,k)\leqslant\frac{\left(\!\!\binom{k}{n+\binom{k}{2}-k}\!\!\right)}{k!}.$$

We can prove these bounds combinatorially. Then, we will show that the lower and upper bound are each asymptotically equivalent to $\frac{n^k}{k!(k-1)!}$. This then forces $P(n,k)$ to be asymptotically equivalent to this function as well.

The combinatorial proofs of the upper and lower bounds rely on thinking of a partition as a solution to a certain system. Another way to think of a partition of n into k parts is as a k-list $(z_1,z_2,\ldots,z_k)$ that satisfies

$$\begin{aligned}z_1+z_2+\cdots+z_k&=n\\ z_1\geqslant z_2\geqslant\cdots\geqslant z_k&\geqslant 1.\end{aligned}\tag{4.18}$$

The second condition forces the parts into non-increasing order. This makes sure that we don't consider, say, $4+2+1$ and $2+4+1$, or rather $(4,2,1)$ and $(2,4,1)$, to be different partitions.

But if we drop that second condition and instead consider the k-lists $(z_1,z_2,\ldots,z_k)$ that satisfy

$$\begin{aligned}z_1+z_2+\cdots+z_k&=n\\ \text{all } z_i&\geqslant 1,\end{aligned}\tag{4.19}$$

then there are $\left(\!\!\binom{k}{n-k}\!\!\right)$ lists. We discussed this in Section 2.2.

Question 181 *How many solutions do equations (4.18) and (4.19) have when* $n=8$ *and* $k=4$*?*

A lower bound for $P(n,k)$

Let's attempt a count of the solutions to the "bigger" system (4.19) by first starting with the solutions to the "smaller" system (4.18). Bigger and smaller refer to the fact that every solution to (4.18) is a solution to (4.19), but not the other way around.

Consider the $n=7$ and $k=3$ case for a moment. There are $\left(\!\!\binom{3}{7-3}\!\!\right)$ solutions to the bigger system and $P(7,3)$ to the smaller. Take any partition of 7 into three parts, say

$4+2+1$ or $(4,2,1)$. We may permute this 3-list in 3! ways to create different solutions to the bigger system (4.19), namely

$$(4,2,1) \quad (4,1,2) \quad (2,4,1) \quad (2,1,4) \quad (1,4,2) \quad (1,2,4).$$

But if we started with a partition that did not have distinct parts then we would create fewer than 3! solutions. If we chose $(3,2,2)$ then it would lead to only three different solutions:

$$(3,3,2) \quad (3,2,3) \quad (2,3,3).$$

But no matter: $3! \cdot P(7,3)$ is then an *over-estimate* of the $\left(\!\binom{3}{7-3}\!\right)$ solutions to the bigger system. This shows that $3! \cdot P(7,3) \geqslant \left(\!\binom{3}{7-3}\!\right)$ or

$$P(7,3) \geqslant \frac{\left(\!\binom{3}{7-3}\!\right)}{3!}.$$

Once generalized, this proves our lower bound on $P(n,k)$.

Theorem 4.4.6 *For any $n,k \geqslant 1$, $P(n,k) \geqslant \dfrac{\left(\!\binom{k}{n-k}\!\right)}{k!}$.*

Question 182 *Use the theorem to find lower bounds on $P(n,2)$ and $P(n,3)$ as a function of n.*

An upper bound for $P(n,k)$

Now let's attempt to use the solutions to the smaller system (4.18) in a different way. Again consider the $n=7$ and $k=3$ case. Here are the $P(7,3)=4$ partitions of 7 into three parts, written as solutions to the smaller system:

$$(5,1,1) \quad (4,2,1) \quad (3,3,1) \quad (3,2,2).$$

Our strategy in getting the lower bound worked because we over-counted the solutions to the bigger system (4.19). An under-count should lead to an upper bound.

Transform the four solutions above so that they all have distinct parts by adding 2 to the first part, 1 to the second part, and 0 to the third:

$$(7,2,1) \quad (6,3,1) \quad (5,4,1) \quad (5,3,1).$$

Now each is a partition of $7+(2+1+0)=10$ into three distinct parts. Then permute each in one of 3! ways as before. This time, we do create $P(7,3)\cdot 3! = 24$ distinct solutions to

$$\begin{aligned} z_1+z_2+z_3 &= 10 \\ \text{all } z_i &\geqslant 1. \end{aligned}$$

But there are more solutions than just the 24 that we constructed, namely those like $(4,4,2)$ which have at least one repeated element. So we have under-estimated the solutions to this system and found that $P(7,3)\cdot 3! \leqslant \left(\!\binom{3}{10-3}\!\right)$ or

$$P(7,3) \leqslant \frac{\left(\!\binom{3}{10-3}\!\right)}{3!}.$$

In general, take a partition of n into k parts, say $(z_1, z_2, \ldots, z_k)$ and transform it into the partition

$$\big(z_1+(k-1), z_2+(k-2), \ldots, z_{k-1}+1, z_k+0\big) \tag{4.20}$$

that has *distinct* parts.

Question 183 *Explain why this partition must have distinct parts, even though the original one* $(z_1, z_2, \ldots, z_k)$ *may not have.*

By doing the transformation shown in (4.20) just above, we have added a total of

$$1 + 2 + \cdots + (k-2) + (k-1) = \frac{k(k-1)}{2} = \binom{k}{2}$$

to the original partition of n, so this is now a partition of $n + \binom{k}{2}$ into k distinct parts. If we now permute the elements of this partition in one of $k!$ ways, we have created $P(n,k) \cdot k!$ distinct solutions to

$$z_1 + z_2 + \cdots + z_k = n + \binom{k}{2}$$
$$\text{all } z_i \geqslant 1.$$

But there are potentially more solutions since the ones we created do not include those with repeated elements. Therefore $P(n,k) \cdot k!$ is a lower bound on the total number of solutions:

$$P(n,k) \cdot k! \leqslant \left(\!\!\binom{k}{n + \binom{k}{2} - k}\!\!\right).$$

We now have our upper bound on $P(n,k)$.

Theorem 4.4.7 *For any* $n, k \geqslant 1$, $P(n,k) \leqslant \dfrac{\left(\!\!\binom{k}{n+\binom{k}{2}-k}\!\!\right)}{k!}$.

Question 184 *Use the theorem to find upper bounds on* $P(n,2)$ *and* $P(n,3)$ *as a function of* n.

The squeeze

We know that $\left(\!\!\binom{k}{n-k}\!\!\right) = \binom{n-1}{k-1}$ and $\left(\!\!\binom{k}{n+\binom{k}{2}-k}\!\!\right) = \binom{n+\binom{k}{2}-1}{k-1}$.

Question 185 *Verify these.*

Our bound now looks like

$$\frac{\binom{n-1}{k-1}}{k!} \leqslant P(n,k) \leqslant \frac{\binom{n+\binom{k}{2}-1}{k-1}}{k!}.$$

Let's first show that the lower and upper bounds are asymptotically equivalent. It can be seen more easily in the context of an example. Since we are holding k fixed, let's pick a particular value of k, say $k = 4$. Now the lower bound as a function of n is

$$\frac{\binom{n-1}{4-1}}{4!} = \frac{\binom{n-1}{3}}{4!} = \frac{(n-1)_3}{4!3!}$$

and the upper bound is

$$\frac{\binom{n+\binom{4}{2}-1}{4-1}}{4!} = \frac{\binom{n+5}{3}}{4!} = \frac{(n+5)_3}{4!3!}.$$

Now take their ratio:

$$\frac{(n-1)_3}{4!3!} \Big/ \frac{(n+5)_3}{4!3!} = \frac{(n-1)_3}{(n+5)_3} = \frac{(n-1)(n-2)(n-3)}{(n+5)(n+4)(n+3)}.$$

As $n \longrightarrow \infty$ this approaches 1 because of a favorite calculus trick: both numerator and denominator are cubic polynomials of the form n^3 + [lower order terms] and so the limit as $n \longrightarrow \infty$ equals the ratio of their leading coefficients, which is 1.

So in this case ($k = 4$) the upper and lower bounds are asymptotically equivalent, but to what function? We claim that they are asymptotically equivalent to $n^3/4!3!$. This is because

$$\frac{\binom{n-1}{4-1}}{4!} \Big/ \frac{n^3}{4!3!} = \frac{(n-1)_3}{4!3!} \Big/ \frac{n^3}{4!3!} = \frac{(n-1)_3}{n^3} = \frac{(n-1)(n-2)(n-3)}{n^3}$$

which again goes to 1 as $n \longrightarrow \infty$. Now, since both the upper and lower bound are asymptotically equivalent to $\frac{n^3}{4!3!} = \frac{n^3}{144}$, and since $P(n,4)$ is squeezed between them for all n, it follows that

$$P(n,4) \sim \frac{n^3}{144}.$$

That last step requires proof even though it sounds intuitive. See Exercise 7(b).

The computations for general k are much the same. The goal is to show that both the lower and upper bound are asymptotically equivalent to $\frac{n^{k-1}}{k!(k-1)!}$. The exercises ask you to fill in the details.

Theorem 4.4.8 *If $k > 0$ is fixed, then $P(n,k)$ is asymptotically equivalent to*

$$\frac{n^{k-1}}{k!(k-1)!}$$

as a function of n.

It is worth remarking that for fixed k, $P(n,k)$ grows as a polynomial function of n.

Question 186 *How close is the asymptotic approximation to the exact formulas for $P(n,1)$, $P(n,2)$, and $P(n,3)$?*

Summary

Ferrers diagrams provide an inspiration for bijective proofs of partition identities. In terms of formulas for $P(n,k)$, we know that

$$P(n,1) = 1 \qquad P(n,2) = \left\lfloor \frac{n}{2} \right\rfloor \qquad P(n,3) = \left\{ \frac{n^2}{12} \right\}$$

where $\{\cdot\}$ denotes the closest-integer-to operator. Other formulas for $P(n,k)$ and for $P(n)$ are possible but require advanced methods. For fixed k, an asymptotic approximation for $P(n,k)$ is

$$P(n,k) \sim \frac{n^{k-1}}{k!(k-1)!}.$$

Exercises

1. What is the conjugate of the partition $(n-k)+k$ of n, where $n \geqslant 2$ and $1 \leqslant k \leqslant \lfloor n/2 \rfloor$?
2. Let $z_1 + z_2 + \cdots + z_k$ be a partition of n into k parts, where as usual $z_1 \geqslant z_2 \geqslant \cdots \geqslant z_k \geqslant 1$. Show how to compute the conjugate of this partition using only the z_i's and without referring to Ferrers diagrams.

3. Suppose that $P(n)$, the total number of partitions of the given integer n, is odd. Prove or disprove: at least one of those partitions is self-conjugate.
4. Find a formula for $P(n, 2)$ using the technique we used for $P(n, 3)$. Start by finding the partial fraction decomposition of the OGF for $P(n$, at most 2 parts):
$$\frac{1}{(1-x)(1-x^2)} = \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{1+x}.$$
Your final answer will look different than the formula $P(n, 2) = \lfloor \frac{n}{2} \rfloor$ that we already know.
5. This outlines an alternate way to obtain the formula for $P(n, 3)$.
   (a) Find r_1 and r_2 so that $1 + x + x^2 = (1 - r_1 x)(1 - r_2 x)$.
   (b) Find A through F that determines the partial fraction decomposition of the OGF for $P(m$, at most 3 parts):
$$\frac{1}{(1-x)(1-x^2)(1-x^3)} = \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{(1-x)^3} + \frac{D}{1+x} + \frac{E}{1-r_1 x} + \frac{F}{1-r_2 x}.$$
   (c) Find the coefficient of x^m and prove $P(m$, at most 3 parts$) = \left\{ \frac{(m+3)^2}{12} \right\}$.
6. Fix an integer $t \geqslant 0$. Prove: as $n \longrightarrow \infty$, the value of $P(n, n-t)$ becomes constant. What is the value of that constant, and at what value of n does this occur?
7. We used the following properties of asymptotic equivalence in this section. Assume for convenience that all functions are positive-valued.
   (a) Prove that the "is asymptotically equivalent to" relation is an equivalence relation. (This is a nice review of the properties of limits.)
   (b) Prove: if $f(n) \leqslant g(n) \leqslant h(n)$ for all n and if $f \sim h$, then $f \sim g$.
8. Give a combinatorial proof: for any $n > 0$, $nP(n) = \sum_{j=1}^{n} P(n-j)\sigma(j)$. Here $\sigma(j)$ is defined to be the sum of the divisors of j.
9. This exercise concerns an upper bound on $P(n)$. Recall we define $P(0) := 1$.
   (a) Prove that $P(n) \leqslant P(n-1) + P(n-2)$ for $n \geqslant 2$.
   (b) Use part (a) to prove that $P(n) \leqslant F_n$ for $n \geqslant 0$, where F_n is the n-th Fibonacci number.

Travel Notes

The book by Andrews & Eriksson (2004) is an excellent introduction to the current state-of-the art regarding integer partitions. Among other things it discusses formulas for $P(n, 4)$ and $P(n, 5)$. It also gives many examples of proofs of partition identities using bijections and Ferrer's diagrams.

The study of integer partitions is one of the areas where combinatorics intersects most significantly with number theory. The formula for $P(n)$ that started with the 1918 work of Hardy & Ramanujan and culminated with the 1937 work of Rademacher is a result in analytic number theory and complex analysis.

CHAPTER 5

Counting Under Equivalence

You have probably seen ball-and-stick models of the molecular structure of chemical compounds. Each ball represents a different atom and each stick represents a chemical bond. In the 1930s, the Hungarian mathematician George Pólya considered the problem of enumerating the isomers of a chemical compound. He solved it, and the main result of his efforts was a powerful, all-purpose tool that has since been applied to solve numerous other counting problems: Pólya's enumeration theorem.

Pólya's problem involved counting under equivalence. In such a problem, the goal is to count the equivalence classes of an equivalence relation. The equivalence principle of Section 1.4 applies when all equivalence classes have the same size. Creating a more general principle to handle situations in which not all equivalence classes have the same size requires some abstract algebra (specifically, group theory) to make the necessary modifications. This results in a formula, known as the Cauchy-Frobenius-Burnside theorem, which looks a bit like the formula of the equivalence principle. To that result Pólya added generating functions to arrive at his theorem.

The reader familiar with basic group theory, orbits, and the symmetric, dihedral, and cyclic groups can skim Sections 5.2 and 5.3 until the statement of the Cauchy-Frobenius-Burnside theorem in Section 5.3. Section 5.1 is essential, however, as it contains two examples to which we refer throughout this chapter.

5.1 Two examples

In this short section we present two examples that we use to illustrate most of the concepts in this chapter. The first example is used by many authors and the reason is a good one: it exposes enough depth of the more general problems we wish to study while remaining of manageable size.

Square-coloring

In how many different ways can we construct a square using four indistinguishable sticks and four styrofoam balls, where each ball is either black or white?

These constructions are known as ***colorings*** of the corners of the square. If we regard the square as a fixed object (suppose it's mounted on a wall) then any coloring is a function $f : [4] \longrightarrow \{\text{black}, \text{white}\}$ from the set of corners (which we can number 1–4) to the

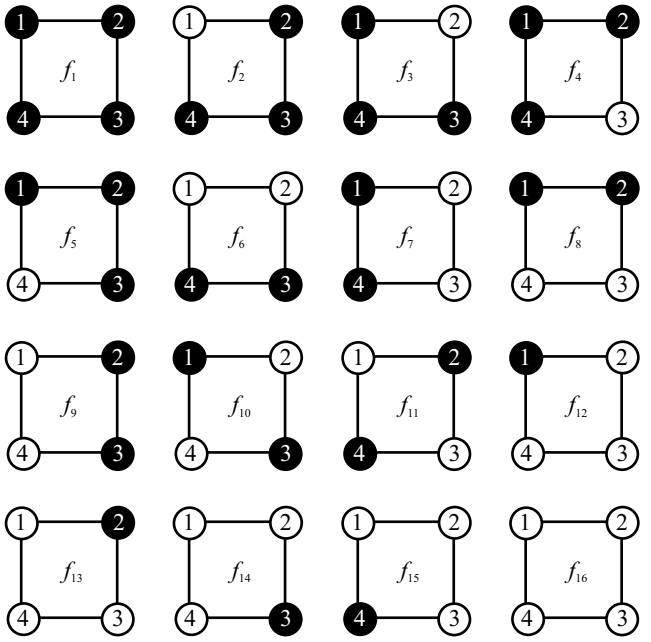
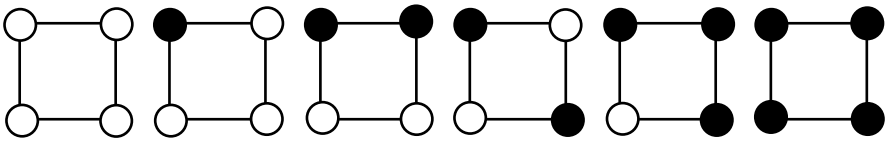


Figure 5.1. The 16 black-white colorings of the labeled corners of a square.

set of possible colors. There are $2^4 = 16$ possible colorings. Figure 5.1 displays these 16 functions as colorings, labeled $f_1, f_2, \ldots, f_{16}$.

But if we regard the square as freely movable in space (suppose it's a toy you can toss around), then many of those 16 colorings are equivalent. Under this notion of equivalence there are only six different colorings:



Notice that the labels no longer appear on the corners. The underlying equivalence relation must account for the fact that rotating or flipping a square does not change its coloring. Such operations rely on the square itself, not the colorings, and are known as the ***symmetries of the square***.

Each of the six colorings listed above is a representative from a different equivalence class. It is important to notice that not all equivalence classes have the same size. For example, $\{f_2, f_3, f_4, f_5\}$ is the equivalence class containing f_2, while $\{f_{10}, f_{11}\}$ is the equivalence class containing f_{10}.

Question 187 *What are the sizes of the other four equivalence classes?*

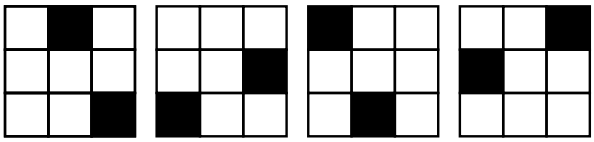
This problem opens the door to many natural generalizations. Instead of a square, we might ask the same question of a regular pentagon, hexagon, or n-gon. We might also ask how many colorings use a specified number of colors of each type. For example, there is one 2-coloring of the square that uses one white and three black. The theory will allow us to answer all of these questions.

This problem also offers a glimpse of Pólya's original motivation for developing his theory. When the colors are really molecules and the sticks are really chemical bonds, then the answer gives the number of chemical compounds of a certain type. Counting chemical compounds requires significant knowledge of chemistry, so we do not treat this application in this book.

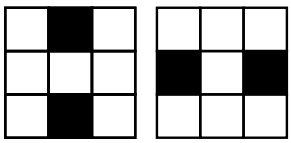
Grid-coloring

In how many ways can we color the squares of a 3×3 grid such that each square is either black or white?

If the squares of the grid are numbered or otherwise distinguished, then there are 2^9 colorings, corresponding to the possible functions $f : [9] \longrightarrow \{\text{black}, \text{white}\}$. But if the grid is allowed to rotate in the plane (suppose it's drawn on a piece of paper, like a tic-tac-toe board) then there are fewer colorings. For example, the following colorings are all equivalent:



Like the problem of coloring the square, each equivalence class does not have the same size. The above grids form an equivalence class of size four, while the grids



form an equivalence class of size two.

Again, we might also be interested in colorings with certain properties. The question, "How many different grids have five squares black and four squares white?" is the same question as, "How many different tic-tac-toe boards have five Xs and four Os?"

5.2 Permutation groups

Our first task is to introduce those parts of group theory that are applicable to the counting methods we wish to develop. We begin with permutations for we use them to describe how an object like the square can move in space or how the 3×3 grid can move in the plane.

In this chapter we typically write permutations in one of two ways. The first way, known as ***two-line form***, is self explanatory. For example, the permutation $f = (7, 4, 3, 2, 6, 1, 5)$ of $[7]$ is written in two-line form as

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 2 & 6 & 1 & 5 \end{pmatrix}.$$

To find $f(i)$, simply look directly below element i.

The other way is to write f as a product of disjoint cycles, and we explained how to do this in Section 4.3. (See the subsection entitled "Cycle notation" for the idea.) In this case, f can be written as a product of disjoint cycles as $f = (1\ 7\ 5\ 6)(2\ 4)(3)$.

Question 188 *Write the permutation* $(1\ 7\ 3)(2)(4\ 9\ 5\ 6\ 8)$ *in two-line form.*

Groups

The set of all permutations of $[n]$, together with the operation $\circ$ of function composition, forms what is known as ***the symmetric group on n elements*** and is denoted $(S_n, \circ)$ or just S_n. For our purposes in this chapter, it is the most important example of a group. Other common examples of groups include the sets $\mathbb{Z}$ or $\mathbb{R}$ or $\mathbb{C}$ each with the operation of addition, or the set of nonzero real numbers with the operation of multiplication. From linear algebra, the set of invertible $n \times n$ matrices forms a group under the operation of matrix multiplication. We discuss some of these after giving the definition of group.

Definition 5.2.1 (group) *A **group** is a pair $(G, *)$ where G is a set and $*$ is a binary operation[1] on G that satisfies the following four properties.*

- ***Closure:** For each $a, b \in G$, we have $a * b \in G$.*
- ***Associativity:** For each $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.*
- ***Existence of an identity:** There is an element $e \in G$ such that for each $a \in G$, we have $a * e = a$ and $e * a = a$.*
- ***Existence of inverses:** For each $a \in G$, there exists $x \in G$ such that $a * x = e$ and $x * a = e$.*

For example, the set of integers with the operation of addition, namely $(\mathbb{Z}, +)$, is a group for the following reasons. It satisfies the closure property because $a + b$ is an integer whenever a and b are integers. We know addition to be an associative operation: $a + (b + c) = (a + b) + c$ holds for all integers a, b, and c. The integer 0 serves as an identity because $a + 0 = 0 + a = a$ for any integer a. Finally, for any integer a, the integer $-a$ is its inverse because $a + (-a) = 0$ and $(-a) + a = 0$.

The group $(\mathbb{Z}, +)$ satisfies an additional property—the commutative property—not mentioned in the definition of group. That is, $a + b = b + a$ for all integers a and b. A group needn't satisfy commutativity, and indeed some of the groups we use in this text (most notably the symmetric group) are not commutative. A group whose binary operation is commutative is a ***commutative group*** or an ***Abelian group***.

Question 189 *(linear algebra) For the group of invertible 2×2 matrices, what is the identity element? What is the inverse of $\begin{bmatrix} 4 & 1 \\ -2 & 2 \end{bmatrix}$? Is this a commutative group?*

The following list contains some facts about groups. The cancellation laws are particularly useful.

- **Left- and right-cancellation:** Whenever $a * b = a * c$, it follows that $b = c$, and this is the left-cancellation law. Similarly, whenever $b * a = c * a$, it follows that $b = c$, and this is the right-cancellation law.
- **Uniqueness of identity:** A group has one and only one identity element. This means that we can speak of *the* identity, which we denote either as e or I.
- **Uniqueness of inverses:** Any group element has one and only one inverse. Thus the notation a^{-1} denotes without ambiguity *the* inverse of the element a.

Exercise 5 asks you to prove these properties.

[1] A binary operation is a function that operates on two objects at a time, like addition, subtraction, etc. Formally, a binary operation on G is a function $G \times G \longrightarrow G$.

The symmetric group

We now prove that the set S_n together with function composition deserves the name "group." Most of the proof uses results that we proved in Section 1.3 and its Exercises.

Theorem 5.2.2 (symmetric group) *For any integer $n > 0$, $(S_n, \circ)$ is a group. That is, the set of all permutations of $[n]$ is a group under the operation of function composition.*

Proof: Let n be a positive integer.

Closure: Theorem 1.3.5 (page 30) says that the composition of two bijections $[n] \longrightarrow [n]$ is also a bijection $[n] \longrightarrow [n]$, so S_n is closed under function composition.

Associativity: Theorem 1.3.6 (page 30) says that function composition is associative, so S_n has the associative property.

Existence of an identity: Define $e : [n] \longrightarrow [n]$ by $e(j) = j$ for all $j \in [n]$. This is clearly a bijection $[n] \longrightarrow [n]$ so $e \in S_n$. Let $f \in S_n$. Then $f \circ e = f$ and $e \circ f = f$ because $f\big(e(j)\big) = f(j)$ and $e\big(f(j)\big) = f(j)$ for all $j \in [n]$. Therefore S_n has an identity element, namely the "identity permutation."

Existence of inverses: Exercise 8 (page 32) shows that the inverse of a bijection $\pi : [n] \longrightarrow [n]$ is itself a bijection $\pi^{-1} : [n] \longrightarrow [n]$. Moreover $\pi \circ \pi^{-1} = e$ and $\pi^{-1} \circ \pi = e$ where e is the identity permutation defined in the last paragraph. Therefore each element of S_n has an inverse in S_n. ■

A group G is a ***finite group*** provided that G is a finite set. In that case $|G|$ is the ***order of G***. If G is an infinite set, then the group has ***infinite order***.

Question 190 *What is the order of S_n?*

Symmetries of an object

It is the symmetries of an object (like the square or the 3×3 grid of Section 5.1) that we model using groups. The group elements describe all ways that we can physically reorient the object without changing its structure.

Symmetries of the square

In what ways can we pick up the square of Section 5.1, move it around, and then put it back down in the same place? Since we will be coloring the corners of the square, let us number the corners (as in Figure 5.1) so that we can keep track of how each motion affects each corner's location.

There are eight such motions of the square in space: leave it unchanged, rotate the square clockwise by a multiple of 90°, or flip it in three dimensions about one of its four axes of symmetry. The identity motion I leaves the square unmoved. Label the rotation motions as R_1, R_2, and R_3, corresponding to the multiple of 90° that the square rotates—either 90° or 180° or 270°.

The square has two axes of symmetry that pass through opposing corners (1 and 3, and 2 and 4). Call the motions that flip the square about these axes of symmetry F_1 and F_2, respectively. The square also has two axes of symmetry that pass through the midpoints of opposing sides (either sides 1-2 and 3-4, or sides 2-3 and 1-4). Label the first motion $F_{1,2}$ and the second $F_{2,3}$. Figure 5.2 shows how these motions act on the corners, and Table 5.1 shows each of these motions written as a permutation in S_4.

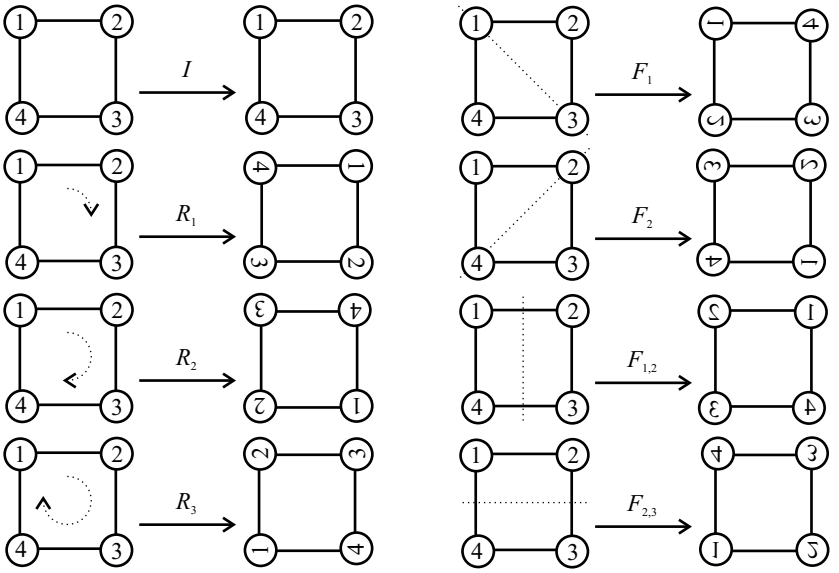


Figure 5.2. Symmetries of the square as they act on its corners.

motion	two-line form	product of disjoint cycles
I	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$	(1)(2)(3)(4)
R_1	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$	(1 2 3 4)
R_2	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$	(1 3)(2 4)
R_3	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$	(1 4 3 2)
F_1	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$	(1)(2 4)(3)
F_2	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$	(1 3)(2)(4)
$F_{1,2}$	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$	(1 2)(3 4)
$F_{2,3}$	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$	(1 4)(2 3)

Table 5.1. Symmetries of the square as permutations in S_4.

For example, the $F_{1,2}$ motion that "flips" (or rotates in three dimensions) the square about the axis passing through the midpoints of sides 1-2 and 3-4 has the net effect of switching the places of corners 1 and 2, and switching the places of corners 3 and 4. We can record its action on the corners as the permutation

$$F_{1,2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\ 2)(3\ 4)$$

in S_4. Similarly, the R_3 motion that rotates the square clockwise in the plane by 270° moves corner 1 to corner 4's original location, corner 2 to corner 1's original location, corner 3 or corner 2's original location, and corner 4 to corner 3's original location. We can record its action on the corners as the permutation

$$R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1\,4\,3\,2)$$

in S_4.

Symmetries of the 3 × 3 grid

For the 3 × 3 grid of Section 5.1, there are only four motions: do nothing (the identity I), rotate 90 degrees clockwise (R_1), rotate 180 degrees clockwise (R_2), and rotate 270 degrees clockwise (R_3). Though this problem and the previous one both involve squares, the grid in this problem is not allowed to move in three dimensions: think of it as drawn on a piece of paper, which can only be reoriented with two-dimensional motions.

Figure 5.3 shows how these motions act on the numbered squares, and Table 5.2 shows each of these motions written as a permutation in S_9. Explanations similar to those used for the square also apply here, using the original numbering of the nine squares as the reference point. Notice that all four motions leave square 5 fixed.

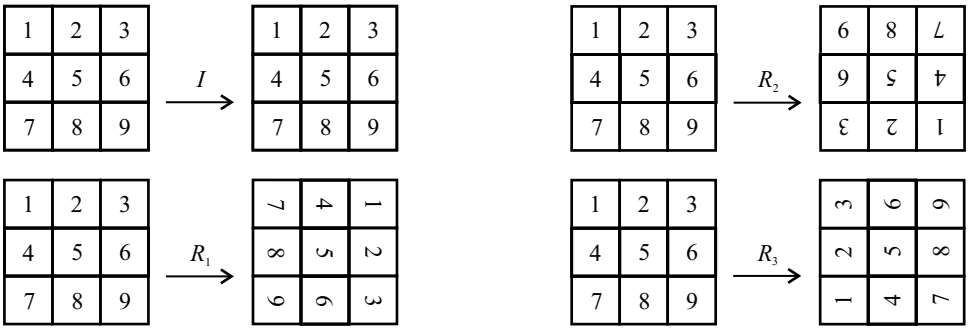


Figure 5.3. Symmetries of the 3 × 3 grid as they act on its squares.

motion	two-line form	product of disjoint cycles
I	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$	(1)(2)(3)(4)(5)(6)(7)(8)(9)
R_1	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 9 & 2 & 5 & 8 & 1 & 4 & 7 \end{pmatrix}$	(1 3 9 7)(2 6 8 4)(5)
R_2	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$	(1 9)(2 8)(3 7)(4 6)(5)
R_3	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 4 & 1 & 8 & 5 & 2 & 9 & 6 & 3 \end{pmatrix}$	(1 7 9 3)(2 4 8 6)(5)

Table 5.2. Symmetries of the 3 × 3 grid as permutations in S_9.

Subgroups

The eight symmetries of the square $\{I, R_1, R_2, R_3, F_1, F_2, F_{1,2}, F_{2,3}\}$ form a proper subset of the $4! = 24$ permutations in S_4. Most permutations in S_4, then, do not correspond to rearrangements of the corners of the square that we can realize by picking it up, rotating and/or flipping it, and putting it back down. For example, the permutation (1)(2)(3 4) does not correspond to action on the corners by one of these motions: we cannot, through a motion that doesn't involve the disassembly of the stick-styrofoam ball construction, switch the locations of corners 3 and 4 and at the same time leave corners 1 and 2 in their original locations. For this reason, the eight motions we use are sometimes called the ***rigid motions*** of the square.

Likewise, the four symmetries of the 3×3 grid $\{I, R_1, R_2, R_3\}$ form a small subset of the $9! = 362{,}880$ permutations in S_9.

But the results of group theory still apply to the 8- and 4-subsets given above, even though they are only small subsets of the known groups S_4 and S_9. This is because each is a subgroup—a group living inside another group.

Definition 5.2.3 (subgroup) *Let $(G, *)$ be a group. A **subgroup of** G is a pair $(H, *)$ such that $H \subseteq G$ and $(H, *)$ is a group. We write $H \leqslant G$ to indicate that H is a subgroup of G.*

We use the symbol $\leqslant$ to distinguish it from $\subseteq$, because as we will see not every subset of a group is a subgroup. The context in which the subgroup symbol appears should distinguish it from ordinary less-than-or-equal-to. It is always true that $\{e\} \leqslant G$ for any group G. This is the ***trivial subgroup***.

The subgroup test

Practically, the test for whether a particular subset of a *finite* group is a subgroup is straightforward: just check that the subset is closed under the group operation. In the proof of the following theorem, and elsewhere, the notation a^n refers to repeated application of the group operation. For example, $a^2 = a * a$ and $a^3 = a * a * a$. Also, $a^1 = a$ and $a^0 = e$.

Theorem 5.2.4 *Let $(G, *)$ be a finite group, and let H be a nonempty subset of G. Then $H \leqslant G$ if and only if H is closed under $*$.*

Proof: Assume that $(G, *)$ is a finite group and that H is a nonempty subset of G.

($\Longrightarrow$) Assume that $H \leqslant G$. Then $(H, *)$ is a group, so it is closed under $*$.

($\Longleftarrow$) Assume that H is closed under $*$. We must prove that $(H, *)$ has the three remaining group properties.

Associativity: Let $a, b, c \in H$. Then $a, b, c \in G$ since $H \subseteq G$. Since G is a group and therefore associative, it follows that $a * (b * c) = (a * b) * c$. Therefore H has the associative property.

Existence of an identity: Suppose $|H| = m$ for some positive integer m. If $m = 1$ then $H = \{a\}$ for some $a \in G$. Since H is closed, it follows that $a * a = a$. Now, working this equation in the group G, left-cancellation of $a*a = a*e$ implies that $a = e$. Therefore $H = \{e\}$ and so H is the trivial subgroup of G.

Now assume that $m > 1$. Let $a \in H$. Since H is closed under $*$, the $m + 1$ elements

$$a, a^2, a^3, \ldots, a^{m+1} \tag{5.1}$$

all belong to H. But because $|H| = m$ this list must repeat: $a^i = a^j$ for some integers i and j satisfying $1 \leqslant i < j \leqslant m+1$. Rewrite $a^j = a^i * a^{j-i}$ and note that $0 < j-i < m$. This means

$$a^i * e = a^i * a^{j-i}.$$

Working in the group G, left-cancellation implies $e = a^{j-i}$ where e is the identity element of G. But since $a^{j-i} \in H$, we have shown that $e \in H$ and hence that H contains an identity.

Existence of inverses: Let $a \in H$. Definition 5.2.1 requires us to find some $b \in H$ satisfying $a * b = e$ and $b * a = e$. Form the same list (5.1) from which we learned that $a^{j-i} = e$. This means that if we choose $b := a^{j-i-1} \in H$ (where $a^0 := e$) then

$$a * b = a * a^{j-i-1} = a^{j-i} = e,$$

and similarly $b * a = e$. Therefore every element of H contains an inverse that belongs to H. This completes the proof that $H \leqslant G$. ■

In the case of an *infinite* group, the subgroup test requires more than just checking closure. See Exercise 11.

The symmetries of a square

Now that we have the subgroup test, a systematic way to check that

$$\{I, R_1, R_2, R_3, F_1, F_2, F_{1,2}, F_{2,3}\} \leqslant S_4$$

is to use a ***group table***, which shows the result of composing any two permutations that correspond to the actions of the eight motions on the corners. Table 5.3 gives this group table. The entry in any row and column is the net motion that results from applying first the column's motion followed by the row's motion.

For example, what is the motion $F_{2,3} \circ R_1$ that results from first rotating the square clockwise by 90 degrees and then flipping it about its horizontal axis? Since

$$\begin{aligned} F_{2,3}\big(R_1(1)\big) &= F_{2,3}(2) = 3 \\ F_{2,3}\big(R_1(2)\big) &= F_{2,3}(3) = 2 \\ F_{2,3}\big(R_1(3)\big) &= F_{2,3}(4) = 1 \\ F_{2,3}\big(R_1(4)\big) &= F_{2,3}(1) = 4, \end{aligned}$$

$\circ$	I	R_1	R_2	R_3	F_1	F_2	$F_{1,2}$	$F_{2,3}$
I	I	R_1	R_2	R_3	F_1	F_2	$F_{1,2}$	$F_{2,3}$
R_1	R_1	R_2	R_3	I	$F_{1,2}$	$F_{2,3}$	F_2	F_1
R_2	R_2	R_3	I	R_1	F_2	F_1	$F_{2,3}$	$F_{1,2}$
R_3	R_3	I	R_1	R_2	$F_{2,3}$	$F_{1,2}$	F_1	F_2
F_1	F_1	$F_{2,3}$	F_2	$F_{1,2}$	I	R_2	R_3	R_1
F_2	F_2	$F_{1,2}$	F_1	$F_{2,3}$	R_2	I	R_1	R_3
$F_{1,2}$	$F_{1,2}$	F_1	$F_{2,3}$	F_2	R_1	R_3	I	R_2
$F_{2,3}$	$F_{2,3}$	F_2	$F_{1,2}$	F_1	R_3	R_1	R_2	I

Table 5.3. The group table for the symmetries of the square.

it follows that

$$F_{2,3} \circ R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = F_2.$$

Therefore the entry in $F_{2,3}$'s row and R_1's column is F_2. Likewise,

$$\begin{aligned} R_1\big(F_{2,3}(1)\big) &= R_1(4) = 1 \\ R_1\big(F_{2,3}(2)\big) &= R_1(3) = 4 \\ R_1\big(F_{2,3}(3)\big) &= R_1(2) = 3 \\ R_1\big(F_{2,3}(4)\big) &= R_1(1) = 2, \end{aligned}$$

so $R_1 \circ F_{2,3} = F_1$. One thing to notice is that the order in which we apply the motions matters! This group is not commutative.

It is straightforward but tedious to verify the remaining 62 entries of the group table. Because the net result of applying any two motions in succession equals one of the eight original motions, we have a subgroup of S_4 by Theorem 5.2.4.

Question 191 *Is $\{I, R_1, R_2, R_3, F_{1,2}\}$ a subgroup of S_4? Explain why or why not.*

The symmetries of the 3 × 3 grid

The group table for the grid problem is smaller and it appears in Table 5.4. Although this group table just equals the upper left corner of the group table for the symmetries of the square, remember that these four motions are permutations in S_9 and not in S_4.

Question 192 *Is the subgroup shown in Table 5.4 commutative?*

$\circ$	I	R_1	R_2	R_3
I	I	R_1	R_2	R_3
R_1	R_1	R_2	R_3	I
R_2	R_2	R_3	I	R_1
R_3	R_3	I	R_1	R_2

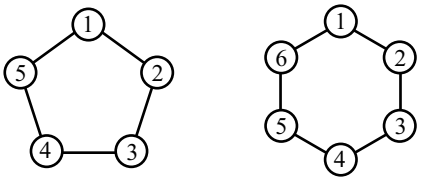
Table 5.4. The group table for the symmetries of the 3×3 grid.

The dihedral and cyclic groups

The dihedral group

Instead of coloring the corners of a square, consider coloring the corners of a regular pentagon, hexagon, or (in general) regular n-gon, where $n \geq 3$. If we allow any rigid, three-dimensional motion to determine a reorientation of that figure, then what is the size of the symmetry group?

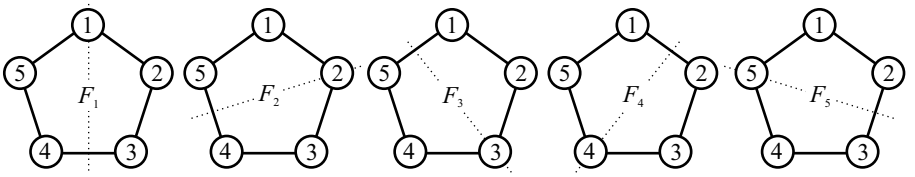
Label the vertices of a regular n-gon using the set $[n]$ and then orient it so that vertex 1 sits at the top. For $n = 5$ and $n = 6$ the labelings are:



Like the square (a regular 4-gon), we can perform two-dimensional rotations. Including the identity element I (the 0° rotation) there are five possible rotations for the pentagon and six for the hexagon. Label these I, R_1, R_2, R_3, R_4 in the case of the pentagon and $I, R_1, R_2, R_3, R_4, R_5$ in the case of the hexagon. The rotation R_j is a rotation by $360j/n$ degrees.

Question 193 *What are the permutations in S_5 (for the pentagon) and S_6 (for the hexagon) that correspond to these rotation motions?*

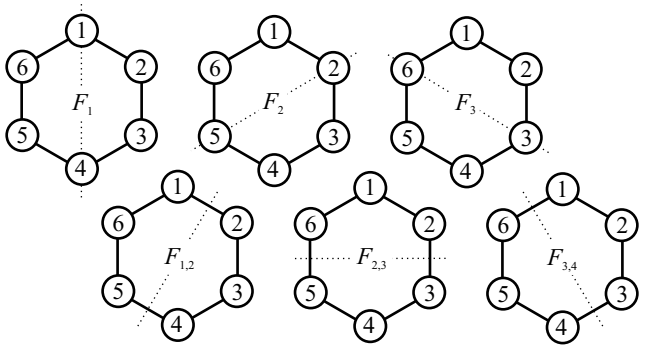
Now there are the three-dimensional flip motions. The pentagon has five axes of symmetry. Each such axis passes through a vertex and the midpoint of the side directly opposite that vertex. As such, a vertex uniquely identifies an axis of symmetry. Label the corresponding flip motions F_1, F_2, F_3, F_4, F_5 as shown below:



(The above diagram shows the "before" positions of the pentagon as well as the axes of symmetry, unlike Figure 5.2 which shows both the before and after positions for the square.)

Question 194 *What are the permutations in S_5 that correspond to these five flip motions?*

The hexagon has six axes of symmetry. Three of them pass through pairs of opposing vertices: 1 and 4, 2 and 5, 3 and 6. Label the corresponding flip motions as F_1, F_2, F_3. The other three pass through pairs of opposing sides: 1-2 and 4-5; 2-3 and 5-6; and 3-4 and 6-1. Label the corresponding flip motions $F_{1,2}, F_{2,3}, F_{3,4}$ as shown below:



Question 195 *What are the permutations in S_6 that correspond to these six flip motions?*

The parity of n, the number of corners, accounts for the difference in the nature of the axes of symmetry in the pentagon and the hexagon.

As you might expect, the symmetry group of the regular n-gon, where $n \geq 3$, has n rotation motions (including the identity) and n flip motions. As such it has order $2n$ and is known as the ***dihedral group of the regular n-gon***, notated D_n. It is composed of the n rotations $I, R_1, R_2, \ldots, R_{n-1}$ and n flip motions as follows. If n is odd, they are

$$F_1, F_2, \ldots, F_n$$

where the flip F_i is about the axis of symmetry passing through vertex i and the midpoint of the side directly opposite. If n is even, they are

$$F_1, F_2, \ldots, F_{\frac{n}{2}}, F_{1,2}, F_{2,3}, \ldots, F_{\frac{n}{2},\frac{n}{2}+1}$$

where the flip F_i is about the axis passing through vertex i and the vertex directly opposite, and the flip $F_{i,i+1}$ is about the axis passing through the midpoint of the side joining vertices i and $i+1$, and the side directly opposite.

The symmetry group of the square that we gave earlier is the dihedral group D_4 of order 8. In general, the action of the symmetries of the regular n-gon on its corners, when thought of as permutations in S_n, indeed forms a subgroup of S_n of order $2n$. That is, $D_n \leqslant S_n$ and $|D_n| = 2n$.

The cyclic group

One way to define the ***cyclic group of order*** n, denoted by C_n, is as the subgroup of D_n that consists of the identity together with the $n-1$ rotation operations on the regular n-gon. As such, it is essentially the same group as $(\mathbb{Z}_n, \oplus)$ where $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ is the set of residues modulo n and $\oplus$ is addition modulo n.

For example, the group table for C_4 is shown in Table 5.4. The group table for $(\mathbb{Z}_4, \oplus)$ is

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Except for the names of the group elements, the two groups behave in exactly the same manner. This illustrates the concept of *group isomorphism* which, while very important in group theory, we won't cover.

Summary

For the purposes of counting, and especially counting when there are symmetries of a physical object to consider, the most important groups are

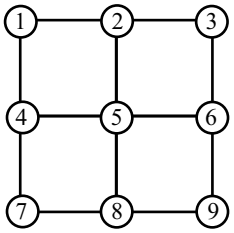
- the symmetric group, denoted by S_n, which is the set of all permutations of $[n]$, or equivalently bijections $[n] \longrightarrow [n]$, under the operation of function composition;
- the dihedral group, denoted by D_n, which is the set of symmetries of the regular n-gon; and
- the cyclic group, denoted by C_n, which is the set of rotational symmetries of the regular n-gon, or equivalently the set of integers modulo n with addition.

The groups D_n and C_n are each subgroups of S_n.

Exercises

1. How many cycles does the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 3 & 2 & 8 & 7 & 1 & 5 & 4 \end{pmatrix}$ have?
2. How may different permutations in S_5 have exactly two cycles? Exactly three cycles?

3. Let $\pi := (1\ 3\ 5)(2)(4\ 6)$ and $\tau := (1\ 6\ 5\ 4\ 3\ 2)$ be permutations in S_6. Find
   (a) π^{-1} and τ^{-1},
   (b) $\pi \circ \tau$ and $\tau \circ \pi$,
   (c) $\pi^{-1} \circ (\tau \circ \pi^2)$, and
   (d) π^{-2} and τ^{-3}
4. Explain why $(\mathbb{R}, \cdot)$ is not a group, where $\mathbb{R}$ is the set of real numbers and $\cdot$ is multiplication. Then, make a small change to the set $\mathbb{R}$ so that it is a group under multiplication and prove that it is so.
5. Let $(G, *)$ be a group. Prove the left- and right-cancellation laws. Then, use them to prove that a group's identity element is unique, and that the inverse of any $a \in G$ is unique.
6. Let $(G, *)$ be a finite group. Prove that every row of its group table is a permutation of G.
7. Let $(G, *)$ be a finite group of order n, and let $a \in G$. It is true that the list $a, a^2, a^3, \ldots, a^{n+1}$ must contain a repeat. Prove that a is the first repeated element.
8. In addition to numbering the corners of the pentagon, label the sides a, b, c, d, e. Describe how the dihedral group D_5 acts on the sides of the pentagon. Write the result of each motion as a permutation of $\{a, b, c, d, e\}$ and make a table similar to Table 5.1. Then do the same for the hexagon.
9. Find the symmetry group, as a subgroup of S_9, for the following stick-styrofoam ball structure free to move in space. (Corners are numbered for convenience.)



10. Repeat the previous exercise, but for a 4×4 structure.
11. Let $(G, *)$ be a group (not necessarily finite), and let H be a nonempty subset of G. Prove: $H \leqslant G$ if and only if (1) H is closed under $*$, and (2) whenever $a \in H$, it follows that $a^{-1} \in H$.
12. Consider the symmetric group $(S_5, \circ)$ and one of its elements $\pi := (1\ 3\ 4)(2\ 5)$.
   (a) Define $\pi^0 := e$, the identity permutation, and $\pi^1 := \pi$. Compute $\pi^2 := \pi \circ \pi$, $\pi^3 := \pi \circ \pi \circ \pi$, and so on until this list starts to repeat.
   (b) Let the set H consist of the permutations that you found in part (a). Use a group table to show that H is a subgroup of S_5.
13. Let $(G, *)$ be a group, and fix any $\pi \in G$. Prove that the set

$$\langle \pi \rangle := \{\pi^n : n \in \mathbb{Z}\}$$

   is a subgroup of G. (The set $\langle \pi \rangle$ is called the ***cyclic subgroup of G generated by*** π. In the previous exercise you found the cyclic subgroup of S_5 generated by the permutation $(1\ 3\ 4)(2\ 5)$.)

14. Continuing the previous exercise, prove that the cyclic subgroup $\langle \pi \rangle$ is commutative.

15. This exercise outlines a proof of Lagrange's theorem which is an important result in group theory. Let $(G, *)$ be a group.

    (a) Let H be a subgroup of G and let $a \in G$. The ***right coset of H in G containing*** a is the set
    $$Ha := \{h * a : h \in H\}.$$
    Prove: if $a, b \in G$, then the function $f : Ha \longrightarrow Hb$ given by $f(h * a) = h * b$ is a bijection.

    (b) Define a relation $\equiv$ on G by the following: $a \equiv b$ if and only if $a * b^{-1} \in H$. Prove: $\equiv$ is an equivalence relation on G.

    (c) Prove: the equivalence classes of the equivalence relation in part (b) are the right cosets of H in G.

    (d) Combine your results in parts (a)-(c) to prove Lagrange's theorem: If $(G, *)$ is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

    (e) Explain how Lagrange's theorem gives an alternative way to answer Question 191 on page 196.

5.3 Orbits and fixed point sets

This section bridges the gap between group theory and counting. We can think of the symmetry group of the square (i.e., the dihedral group D_4) as it acts on certain features of the square: the corners, the edges, the possible colorings of the corners, the possible colorings of the edges, etc. In fact, we have already done this for the corners and it is shown in Figure 5.2 and Table 5.1. We numbered the corners because those are what we wish to color.

Square-coloring

Recall the square-coloring example of Section 5.1. As it acts on the four numbered corners of the square, the $F_1 = (1)(2\ 4)(3)$ operation leaves corners 1 and 3 fixed but switches the locations of corners 2 and 4. But as it acts on the *16 colorings* of the square's corners pictured in Figure 5.1, it does this:

$$F_1 = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_8 & f_9 & f_{10} & f_{11} & f_{12} & f_{13} & f_{14} & f_{15} & f_{16} \\ f_1 & f_2 & f_5 & f_4 & f_3 & f_9 & f_8 & f_7 & f_6 & f_{10} & f_{11} & f_{12} & f_{15} & f_{14} & f_{13} & f_{16} \end{pmatrix}.$$

For example, flipping the colored square labeled f_5 about the axis joining corners 1 and 3 results in the colored square f_3. This means $F_1(f_5) = f_3$. The $R_1 = (1\ 2\ 3\ 4)$ operation acts on the colorings as follows:

$$R_1 = \begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_8 & f_9 & f_{10} & f_{11} & f_{12} & f_{13} & f_{14} & f_{15} & f_{16} \\ f_1 & f_3 & f_4 & f_5 & f_2 & f_7 & f_8 & f_9 & f_6 & f_{11} & f_{10} & f_{13} & f_{14} & f_{15} & f_{12} & f_{16} \end{pmatrix}.$$

Notice that each is a bijection on the set of colorings.

Grid-coloring

In the grid-coloring example of Section 5.1, the action of the symmetry group on the nine squares comprising the grid is shown in Figure 5.3 and Table 5.2. But it also acts on the $2^9 = 512$ possible colorings of the nine squares. Unlike the square example, explicitly enumerating all possible colorings is too cumbersome.

But, like the square example, each of the four operations I, R_1, R_2, and R_3 produces a bijection on the set of colorings.

Group acting on functions

Group theory provides a useful tool—the Cauchy-Frobenius-Burnside theorem—that solves both the square-coloring and grid-coloring problems with comparable effort, even though there are more initial black-white colorings of the grid than the square (512 vs. 16). The key concept is that of a group acting on a set of functions. In our examples, the functions are colorings and for many problems it suffices to have an intuitive notion for what group action means. Developing the theory, however, requires a precise definition.

Definition 5.3.1 (group acting on functions) *Let A and C be finite sets, and let G be a group of permutations of A. For the set C^A of functions $f : A \longrightarrow C$, the* **action of G on C^A** *is defined by*

$$\big(\pi(f)\big)(a) := f\big(\pi^{-1}(a)\big) \qquad \text{for each } \pi \in G \text{ and } a \in A.$$

In the square example, $A = [4]$ is the set of labeled corners, $C = \{\text{black}, \text{white}\}$ is the set of colors, and G is the dihedral group D_4 as it acts on the set A of corners.

The definition's purpose is to make precise what, say, $R_1(f_2)$ means. After all, R_1 describes how the group acts on the *corners* and not the *colorings*. Intuitively, saying $R_1(f_2) = f_3$ makes sense because rotating the coloring f_2 clockwise by 90° produces the coloring f_3. (Refer back to Figure 5.1.) The definition defines what the function $R_1(f_2)$ is. Since $R_1^{-1} = R_3$, the definition says

$$\begin{aligned}
R_1\big(f_2(1)\big) &= f_2\big(R_1^{-1}(1)\big) = f_2\big(R_3(1)\big) = f_2(4) = \text{black} = f_3(1)\\
R_1\big(f_2(2)\big) &= f_2\big(R_1^{-1}(2)\big) = f_2\big(R_3(2)\big) = f_2(1) = \text{white} = f_3(2)\\
R_1\big(f_2(3)\big) &= f_2\big(R_1^{-1}(3)\big) = f_2\big(R_3(3)\big) = f_2(2) = \text{black} = f_3(3)\\
R_1\big(f_2(4)\big) &= f_2\big(R_1^{-1}(4)\big) = f_2\big(R_3(4)\big) = f_2(3) = \text{black} = f_3(4).
\end{aligned}$$

So indeed $R_1(f_2) = f_3$ because f_3 is the coloring that labels corners 1-4 in the order black-white-black-black.

Question 196 *Use the same method to find $F_2(f_{11})$.*

Two important concepts

Orbit

As our goal is to count inequivalent colorings, we must make our notion of equivalence precise. In the square-coloring example, we consider two colorings equivalent provided that we can "reach" one from the other via group operations.

For example, colorings f_7 and f_8 are equivalent because the 90-degree rotation operation takes one coloring to the other: $R_1(f_7) = f_8$. It is also the case that $F_1(f_7) = f_8$ and

that $R_3(f_8) = f_7$, but the point is that there is at least one way to get from f_7 to f_8 or vice versa.

When a group acts on a set of functions (e.g., colorings) the *orbit* of a function is the set of all functions "reachable" by applying the group operations to the original function.

Definition 5.3.2 (orbit) *Let A and C be finite sets, and let G be a group of permutations of A. For any $f \in C^A$, the **orbit of f under G** is the set*

$$\text{orb}_G(f) := \{\pi(f) : \pi \in G\}.$$

For example, to find the orbit of coloring f_7, we apply each of the eight group operations to f_7 and gather the results:

$$\begin{array}{cccc} I(f_7) = f_7 & R_1(f_7) = f_8 & R_2(f_7) = f_9 & R_3(f_7) = f_6 \\ F_1(f_7) = f_8 & F_2(f_7) = f_6 & F_{2,3}(f_7) = f_7 & F_{1,2}(f_7) = f_9. \end{array}$$

This means the orbit of f_7, namely $\text{orb}_{D_4}(f_7)$, equals $\{f_6, f_7, f_8, f_9\}$. As other examples, $\text{orb}_{D_4}(f_{10}) = \{f_{10}, f_{11}\}$ and $\text{orb}_{D_4}(f_1) = \{f_1\}$.

Question 197 *What is the orbit of f_{15}?*

Notice that each orbit contains colorings of the corners of the square that we do indeed consider equivalent.

Question 198 *In general, explain why any function f is in its own orbit.*

Fixed point set

Given a group operation, its fixed point set is the set of functions that are left unchanged by the operation.

Definition 5.3.3 (fixed point set) *Let A and C be finite sets, and let G be a group of permutations of A. For any $\pi \in G$, the **fixed point set of π in G** is the set*

$$\text{fix}_G(\pi) := \{f \in C^A : \pi(f) = f\}.$$

In the square example, the only colorings unchanged by the R_1 motion are the all-black coloring f_1 and the all-white coloring f_{16}. Therefore

$$\text{fix}_{D_4}(R_1) = \{f_1, f_{16}\}.$$

The colorings unchanged by the $F_{1,2}$ operations are

$$\text{fix}_{D_4}(F_{1,2}) = \{f_1, f_6, f_8, f_{16}\}.$$

Question 199 *In general, what group element π has $\text{fix}_G(\pi) = C^A$, always?*

The goal: count the orbits

We now prove that the orbits partition the set of functions acted upon by the group. Once accomplished, we then re-cast our original goal of counting the inequivalent arrangements as that of counting the orbits.

Let A and C be finite sets and let G be a group of permutations of A. Let $f \in C^A$. Our first observation is that every orbit is nonempty. This follows from your work in Question 198, in which you observed that any function is in its own orbit.

A second observation follows almost immediately. Because f belongs to its own orbit, this means that every element of C^A is in some orbit. Therefore the union of the orbits equals C^A, the set of functions acted upon by the group.

To complete the proof that the orbits partition C^A, we show that the set of orbits contains disjoint sets. We accomplish this by proving that any two orbits that are not disjoint must be equal.

Theorem 5.3.4 *Let A and C be finite sets, and let G be a group of permutations of A. Then the orbits of C^A partition C^A. That is, the set*

$$\mathcal{O} := \{\text{orb}_G(f) : f \in C^A\}$$

is a partition of C^A.

Proof: Let A and C be finite sets, and let G be a group of permutations of A. We have already shown that $\mathcal{O}$ contains nonempty sets whose union is C^A. We now prove that these sets are disjoint.

Assume that $\text{orb}_G(f_1)$ and $\text{orb}_G(f_2)$ are two orbits that are not disjoint, and let g be any function belonging to both orbits. By Definition 5.3.2, this means that $g = \pi_1(f_1)$ and $g = \pi_2(f_2)$ for some $\pi_1, \pi_2 \in G$. We prove that $\text{orb}_G(f_1) = \text{orb}_G(f_2)$ by showing that each is a subset of the other.

Let $h \in \text{orb}_G(f_1)$. This means $h = \pi(f_1)$ for some $\pi \in G$. But because $\pi_1(f_1) = \pi_2(f_2)$, we can write $f_1 = \pi_1^{-1}(\pi_2(f_2))$. Therefore

$$h = \pi(f_1) = \pi\left(\pi_1^{-1}(\pi_2(f_2))\right) = \underbrace{(\pi \circ \pi_1^{-1} \circ \pi_2)}_{=:\sigma}(f_2).$$

By closure of the group G, the operation σ belongs to G. This means that $h = \sigma(f_2)$ where $\sigma \in G$. Therefore $h \in \text{orb}_G(f_2)$, and hence $\text{orb}_G(f_1) \subseteq \text{orb}_G(f_2)$.

The proof that $\text{orb}_G(f_2) \subseteq \text{orb}_G(f_1)$ is similar and left to you in the next question. Therefore $\mathcal{O}$ must contain disjoint sets. This completes the proof that the orbits partition C^A. ■

Question 200 *What are the details that prove $\text{orb}_G(f_2) \subseteq \text{orb}_G(f_1)$?*

In the square-coloring example of Section 5.1, we noted that there are only six inequivalent colorings. This means that there are six orbits.

Question 201 *Write down the six orbits for the square example.*

The Cauchy-Frobenius-Burnside theorem

In the interest of illustrating how to count orbits in an efficient manner, we jump right to the statement of the theorem that allows us to do so. We prove it in Section 5.5.

Theorem 5.3.5 (Cauchy-Frobenius-Burnside) *Let A and C be finite sets, let G be a group of permutations of A, and let $\mathcal{O}$ be the set of orbits of C^A. Then*

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{\pi \in G} \left|\text{fix}_G(\pi)\right|.$$

Applying the Cauchy-Frobenius-Burnside (CFB) theorem, then, amounts to determining the size of each fixed point set. Doing so requires knowing the cycle structure of each group operation. Let's use it to finish our two examples.

Finishing the square-coloring example

In Table 5.1 on page 192, we wrote each of the eight group operations as a product of disjoint cycles. This allows for easy computation of the sizes of the fixed point sets.

Here is the idea. To count the colorings that a certain group operation leaves fixed, it suffices to count the number of ways to assign a color to each *cycle* of the operation. This is because every corner in a given cycle must receive the same color in order for the coloring to remain fixed under the operation.

For example, the R_2 operation can be written (1 3)(2 4), meaning that it swaps corners 1 and 3, and it swaps corners 2 and 4. Therefore, corners 1 and 3 must receive the same color, as must corners 2 and 4. There are two choices of colors (black or white) for each, so $\left|\text{fix}_{D_4}(R_2)\right| = 2^2$. The identity operation I can be written (1)(2)(3)(4). Therefore any corner can receive any color because any coloring remains fixed under the identity operation. This means $\left|\text{fix}_{D_4}(I)\right| = 2^4$.

In general, with two colors available, the number of colorings left fixed by a given operation equals $2^{c(\pi)}$ where $c(\pi)$ is the number of disjoint cycles in the permutation π. The following table summarizes this information.

motion π	product of disjoint cycles	$\left\|\text{fix}_{D_4}(\pi)\right\|$
I	(1)(2)(3)(4)	2^4
R_1	(1 2 3 4)	2^1
R_2	(1 3)(2 4)	2^2
R_3	(1 4 3 2)	2^1
$F_{2,3}$	(1 4)(2 3)	2^2
$F_{1,2}$	(1 2)(3 4)	2^2
F_1	(1)(2 4)(3)	2^3
F_2	(1 3)(2)(4)	2^3

By the CFB theorem the number of orbits, and therefore inequivalent colorings, equals

$$\frac{1}{|G|}\sum_{\pi\in G}\left|\text{fix}_G(\pi)\right| = \frac{1}{8}\left(2^4 + 2^1 + 2^2 + 2^1 + 2^2 + 2^2 + 2^3 + 2^3\right) = 6.$$

Of course, this agrees with our initial answer in Section 5.1.

Question 202 *Find the answer if we had three colors available instead of two.*

Finishing the grid-coloring example

Applying the same ideas to the grid-coloring example of Section 5.1, we arrive at the following table. The relevant group is C_4, the cyclic group of order 4 as it acts on the nine squares of the grid.

motion π	product of disjoint cycles	$\left\lvert \text{fix}_{C_4}(\pi) \right\rvert$
I	(1)(2)(3)(4)(5)(6)(7)(8)(9)	2^9
R_1	(1 3 9 7)(2 6 8 4)(5)	2^3
R_2	(1 9)(2 8)(3 7)(4 6)(5)	2^5
R_3	(1 7 9 3)(2 4 8 6)(5)	2^3

By the CFB theorem, the number of inequivalent colorings equals

$$\frac{1}{4}\left(2^9 + 2^3 + 2^5 + 2^3\right) = 140.$$

Computing the size of a fixed point set

Our technique of computing the sizes of the fixed point sets relies on the following result. In the language of colorings, it says that a group operation fixes a coloring exactly when each cycle of the group operation is monochromatic.

Theorem 5.3.6 *Let A and C be finite sets, and let G be a group of permutations of A. For any $f \in C^A$ and $\pi \in G$, it follows that $\pi(f) = f$ if and only if f is constant on every cycle of π.*

The proof, which Exercise 4 asks you to provide, makes use of Definition 5.3.1.

Summary

Let G be a group acting on a set of functions C^A. So far, we can think of these functions as colorings.

- The orbit of $f \in C^A$ is a subset of C^A. It contains the elements of C^A that are "reachable" from f via the group operations.
- The fixed point set of $\pi \in G$ is a subset of C^A. It contains the elements of C^A that are unchanged by π.

The Cauchy-Frobenius-Burnside theorem allows calculation of the number of orbits in terms of the sizes of the fixed point sets. In the case of our examples, it was possible to calculate the size of each fixed point set by first writing each group element π as a product of disjoint cycles.

Exercises

1. Consider the square example, but where each corner can be colored black, white or red. Let f be the coloring that colors corners 1 and 2 black, corner 3 white, and corner 4 red. Write down all of the colorings in the orbit of f.
2. How many ways are there to construct the figure in Exercise 9 of Section 5.2 if each ball can be one of k colors? Apply the CFB theorem.
3. In how many different ways can we construct a square using four sticks and four indistinguishable styrofoam balls, where each stick is either black or white? (That is, we are coloring edges and not corners.)
   (a) Label the square's edges a, b, c, d. Find the cycle structure of each element in the dihedral group as it acts on the edges and then apply the CFB theorem.

(b) Now change the question to: In how many different ways can we construct a square using four sticks and four styrofoam balls, where each stick is either black or white and each ball is either black or white? Answer this using the CFB theorem. (Hint: The dihedral group now acts on the set $\{1, 2, 3, 4, a, b, c, d\}$ of corners and edges.)

4. Prove Theorem 5.3.6.
5. This exercise shows why the CFB theorem is a generalization of the equivalence principle. Consider counting the number of different ways we can seat five people around a circular table. Initially we assume the seats are numbered or otherwise distinguishable.
   (a) What is the symmetry group that acts on the seatings?
   (b) How many seatings are left fixed by the identity?
   (c) Explain why zero seatings are left fixed by each of the rotation operations.
   (d) Use the CFB theorem to find the number of different seatings when the seats are indistinguishable.
6. How many different stacks of 8 coins can be made, where the coins all have the same size but are either gold or silver? The stack can either be left alone or turned upside-down.
7. Generalize the previous problem to an n-coin stack where k different types of coins are used. (Hint: The parity of n matters.)

Travel Notes

The Cauchy-Frobenius-Burnside theorem is often called Burnside's lemma or occasionally Burnside's theorem. All of these names are apparently wrong. According to research done by Neumann (1979), Cauchy first proved the result for a special case in 1845 and then Frobenius proved it in its current form in 1887. The link with Burnside did not occur until the 1960s when some authors using the result found it in Burnside's 1911 book on group theory and, in the absence of any reference to its origin, attributed it to Burnside. The use of the name "Burnside's lemma" gradually became commonplace.

Rightly or wrongly, many now know the result as Burnside's lemma so we choose to include Burnside's name. Neumann's paper ("A lemma that is not Burnside's") is worth reading. He suggests calling it the Cauchy-Frobenius lemma.

5.4 Using the CFB theorem

Now that we have answered the two counting questions posed in Section 5.1, we devote this section to illustrating how to apply the Cauchy-Frobenius-Burnside theorem from scratch to answer four additional counting questions. We defer the proof of the CFB theorem to the next section.

Example 1: coloring the faces of a triangular prism

A triangular prism has an equilateral triangle for its base and top, and rectangular sides. In how many different ways can we color the five faces of this prism if each face can be painted using one of k colors?

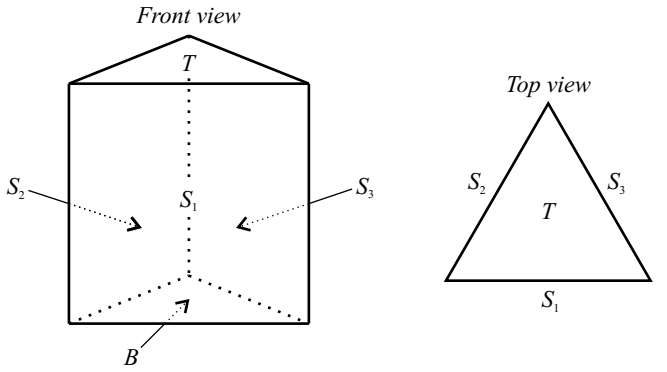


Figure 5.4. A triangular prism.

A picture of the triangular prism appears in Figure 5.4, with top T, bottom B, and sides S_1, S_2, and S_3. First we determine the symmetry group G of the prism. There are three clockwise rotations about the vertical axis that passes through the centers of the top and bottom faces: the identity I, the 120° rotation R_1, and the 240° rotation R_2. We can also pass an axis through the center of each side (perpendicular to that side) and rotate the prism by 180° about that axis; we call these operations F_1, F_2, and F_3 corresponding to the axis that passes through the center of side S_1, S_2, and S_3, respectively. The relevant information required to apply the CFB theorem is given in the table below.

motion π	**product of disjoint cycles**	$\lvert\mathbf{fix}_G(\pi)\rvert$
I	$(B)(T)(S_1)(S_2)(S_3)$	k^5
R_1	$(B)(T)(S_1\ S_2\ S_3)$	k^3
R_2	$(B)(T)(S_1\ S_3\ S_2)$	k^3
F_1	$(B\ T)(S_1)(S_2\ S_3)$	k^3
F_2	$(B\ T)(S_1\ S_3)(S_2)$	k^3
F_3	$(B\ T)(S_1\ S_2)(S_3)$	k^3

For example, the F_2 operation exchanges the bottom and top face; it leaves face 2 fixed but exchanges faces 1 and 3. Thus $F_2 = (B\ T)(S_1\ S_3)(S_2)$. We can assign one of k colors to each of the three cycles, so $\left|\mathrm{fix}_G(F_2)\right| = k^3$. The entries for the other five operations follow similarly.

By the CFB theorem, the number of inequivalent colorings is

$$\frac{1}{6}\left(k^5 + k^3 + k^3 + k^3 + k^3 + k^3\right) = \frac{1}{6}\left(k^5 + 5k^3\right).$$

(On a side note, this also shows that $k^5 + 5k^3$ is divisible by 6 for $k \geq 1$.)

Example 2: counting necklaces

How many different six-bead necklaces are possible where each bead can be one of three colors? How many different seven-bead necklaces are possible where each bead can be one of three colors?

motion π	product of disjoint cycles	$\lvert\text{fix}_{D_6}(\pi)\rvert$
I	(1)(2)(3)(4)(5)(6)	3^6
R_1	(1 2 3 4 5 6)	3^1
R_2	(1 3 5)(2 4 6)	3^2
R_3	(1 4)(2 5)(3 6)	3^3
R_4	(1 5 3)(2 6 4)	3^2
R_5	(1 6 5 4 3 2)	3^1
F_1	(1)(2 6)(3 5)(4)	3^4
F_2	(1 3)(2)(4 6)(5)	3^4
F_3	(1 5)(2 4)(3)(6)	3^4
$F_{1,2}$	(1 2)(3 6)(4 5)	3^3
$F_{2,3}$	(1 4)(2 3)(5 6)	3^3
$F_{3,4}$	(1 6)(2 5)(3 4)	3^3

Table 5.5. Cycle structure for the six-bead necklace.

The symmetry group of each necklace is the same as that of the regular 6-gon or 7-gon, respectively. As such, we work with the dihedral groups D_6 and D_7.

For the six-bead necklace arrange the necklace in a circle with the beads equally spaced, and numbered as follows:

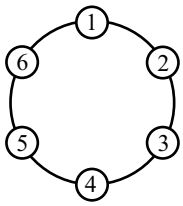
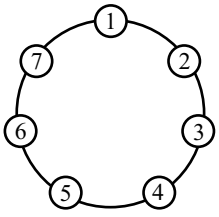


Table 5.5 shows the cycle structure and the number of necklaces fixed by each operation. By the CFB theorem, the number of different necklaces equals

$$\frac{1}{12}\left(3^6 + 3\cdot 3^4 + 4\cdot 3^3 + 2\cdot 3^2 + 2\cdot 3^1\right) = 92.$$

That is, out of the $3^6 = 729$ initial necklaces (i.e., those with the beads numbered and the necklace unmovable) there are only 92 truly distinct possibilities.

For the seven-bead necklace, arrange it as shown:



motion π	product of disjoint cycles	$\left\lvert \mathrm{fix}_{D_7}(\pi) \right\rvert$
I	(1)(2)(3)(4)(5)(6)(7)	3^7
R_1	(1 2 3 4 5 6 7)	3^1
R_2	(1 3 5 7 2 4 6)	3^1
R_3	(1 4 7 3 6 2 5)	3^1
R_4	(1 5 2 6 3 7 4)	3^1
R_5	(1 6 4 2 7 5 3)	3^1
R_6	(1 7 6 5 4 3 2)	3^1
F_1	(1)(2 7)(3 6)(4 5)	3^4
F_2	(1 3)(2)(4 7)(5 6)	3^4
F_3	(1 5)(2 4)(3)(6 7)	3^4
F_4	(1 7)(2 6)(3 5)(4)	3^4
F_5	(1 2)(3 7)(4 6)(5)	3^4
F_6	(1 4)(2 3)(5 7)(6)	3^4
F_7	(1 6)(2 5)(3 4)(7)	3^4

Table 5.6. Cycle structure for the seven-bead necklace.

Table 5.6 lists the relevant information, and the CFB theorem tells us that there are

$$\frac{1}{14}\left(3^7 + 7 \cdot 3^4 + 6 \cdot 3^1\right) = 198$$

different seven-bead necklaces using three colors of beads.

Question 203 *What is the answer to each necklace-counting question if k colors are available instead of three?*

The n-bead necklace

After working out the six-bead and seven-bead cases, and perhaps the nine-bead case on your own, you will begin to get some intuition about what is required for the n-bead necklace. It is clear that the number-theoretic properties of n play a central role. See Exercises 15 and 16.

Example 3: a non-geometric example

Consider the following operations on a binary number. The first is the SHIFT operation which shifts each digit one place to the left, with wrap-around at the end. For example, SHIFT(00010) = 00100 and SHIFT(01011) = 10110. The other is the FLIP operation which changes each 0 to a 1 and each 1 to a 0. For example, FLIP(00010) = 11101 and FLIP(01011) = 10100.

How many different 5-digit binary numbers are there if two such numbers are considered equivalent if one can be obtained from the other by any combination of SHIFT and FLIP operations?

For example, the following numbers are all equivalent:

$$01001 \xrightarrow[\text{SHIFT}]{} 10010 \xrightarrow[\text{SHIFT}]{} 00101 \xrightarrow[\text{FLIP}]{} 11010 \xrightarrow[\text{SHIFT}]{} 10101.$$

In preparation for constructing the symmetry group, let's represent a 5-digit binary number as $d_1d_2d_3d_4d_5$. We need the identity operation, operations that SHIFT either one, two, three, or four times, and the flip operation. Here is the relevant information. (We use d_i' to indicate that digit d_i's value has "flipped.")

motion π	Result	product of disjoint cycles
I	$d_1d_2d_3d_4d_5$	$(d_1)(d_2)(d_3)(d_4)(d_5)$
S_1	$d_2d_3d_4d_5d_1$	$(d_1\ d_5\ d_4\ d_3\ d_2)$
S_2	$d_3d_4d_5d_1d_2$	$(d_1\ d_4\ d_2\ d_5\ d_3)$
S_3	$d_4d_5d_1d_2d_3$	$(d_1\ d_3\ d_5\ d_2\ d_4)$
S_4	$d_5d_1d_2d_3d_4$	$(d_1\ d_2\ d_3\ d_4\ d_5)$
F	$d_1'd_2'd_3'd_4'd_5'$	? ? ?

But what about the FLIP operation, F? We cannot compute its cycle structure as we did for the SHIFT operations because FLIP changes each digit's *value* and not its location. This means that, unlike all previous examples, we are not dealing with a permutation group. In addition, the symmetry group cannot consist just of the operations in $H := \{I, S_1, S_2, S_3, S_4, F\}$ because this set is not closed under composition and thus is not a group. For example, if we apply S_2 first and then F, we get

$$\begin{aligned} FS_2(d_1d_2d_3d_4d_5) &= F\Big(S_2(d_1d_2d_3d_4d_5)\Big) \\ &= F(d_3d_4d_5d_1d_2) \\ &= d_3'd_4'd_5'd_1'd_2'. \end{aligned}$$

(The notation FS_2 is an abbreviation for $F \circ S_2$, the composition of F with S_2.) There is no way to get from $d_1d_2d_3d_4d_5$ to $d_3'd_4'd_5'd_1'd_2'$ with a single operation in the set H defined just above. Thus, H is not closed so it is not a group.

We can make it a group by adding four more operations—those of the form FS_i for $i = 1, 2, 3, 4$. One can then check that

$$G := \{I, S_1, S_2, S_3, S_4, F, FS_1, FS_2, FS_3, FS_4\}$$

is indeed a group. It is not necessary to construct the 10×10 group table as an intuitive check should suffice.

Question 204 *What group operation is the net result of applying S_3 followed by S_4? F followed by S_3? FS_2 followed by S_4? S_4 followed by FS_2? Is this group commutative?*

Now in order to apply the CFB theorem we need the sizes of the fixed point sets:

motion π	$\lvert\text{fix}_G(\pi)\rvert$	motion π	$\lvert\text{fix}_G(\pi)\rvert$
I	2^5	F	0
S_1	2^1	FS_1	0
S_2	2^1	FS_2	0
S_3	2^1	FS_3	0
S_4	2^1	FS_4	0

The cycle structure that we computed in the previous table helps compute the sizes of the fixed point sets for the first five operations. None of the remaining five operations leaves any 5-digit binary number fixed.

Question 205 *Explain why.*

Finally, using the CFB theorem, there are

$$\frac{1}{10}\left(2^5 + 2^1 + 2^1 + 2^1 + 2^1 + 0 + 0 + 0 + 0 + 0\right) = 4$$

different 5-digit binary numbers under this notion of equivalence.

Question 206 *Give one representative from each of the four equivalence classes.*

Example 4: coloring the 3 × 3 grid in a specific way

How many different black-white colorings of the 3×3 grid have exactly five black squares and four white squares?

In our original grid-coloring question in Section 5.1, the set C^A was the set of $2^9 = 512$ possible 2-colorings. In this case, the set C^A is the set of all possible 2-colorings that use five black and four white squares, of which there are $\binom{9}{5}$. Therefore the symmetry group of the grid stays the same but the set C^A changes. This requires re-computing the size of each fixed point set.

The identity operation I leaves all $\binom{9}{5}$ colorings fixed. To determine how many colorings that the R_1 operation leaves fixed, examine its cycle structure:

$$R_1 = (1\ 3\ 9\ 7)(2\ 6\ 8\ 4)(5).$$

Since each coloring contains exactly five black and four white squares, this operation fixes only two colorings. This is because the squares in the cycle (1 3 9 7) must be all black or all white. Once those squares are colored, the squares in (2 6 8 4) must receive the opposite color. This produces four black and four white squares, so the square numbered 5 must receive black. For the same reason, the R_3 operation also fixes only two colorings.

Though the $R_2 = (1\ 9)(2\ 8)(3\ 7)(4\ 6)(5)$ operation involves more cycles, the approach to counting the colorings it fixes remains the same. There are six in total.

Question 207 *Provide the details (consider cases) that show that the R_2 operation fixes six colorings.*

The following table summarizes the results:

motion π	product of disjoint cycles	$\lvert \text{fix}_{C_4}(\pi) \rvert$
I	(1)(2)(3)(4)(5)(6)(7)(8)(9)	$\binom{9}{5}$
R_1	(1 3 9 7)(2 6 8 4)(5)	2
R_2	(1 9)(2 8)(3 7)(4 6)(5)	6
R_3	(1 7 9 3)(2 4 8 6)(5)	2

By the CFB theorem, the number of inequivalent colorings equals

$$\frac{1}{4}\left(\binom{9}{5} + 2 + 6 + 2\right) = 34. \tag{5.2}$$

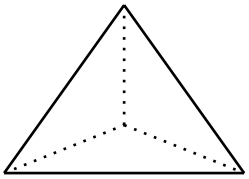
It is worth noting that once we make the type of coloring more specific (here, five black and four white squares, instead of any number of each type) the size of each fixed point set might be less straightforward to determine. Pólya's enumeration theorem, the subject of Section 5.6, uses generating functions to rectify this difficulty.

Summary

Applying the Cauchy-Frobenius-Burnside theorem amounts to understanding the symmetry group of the object in question and then analyzing its cycle structure. In many problems, we can make use of known symmetry groups such as the dihedral group D_n or the cyclic group C_n. Other problems might require starting from scratch.

Exercises

1. Answer the triangular prism question but in the case that the base and top of the prism are a (non-equilateral) isosceles triangle.
2. Consider instead coloring the six *corners* of the triangular prism in the first example. Determine how the symmetry group operates on the corners, and then count the number of inequivalent colorings such that each corner receives one of k colors.
3. How many different seven-bead necklaces are possible, where each bead can be either red or blue? How many have exactly three red and four blue beads?
4. In how many different ways can we color the four corners of the regular tetrahedron if each corner can receive one of k colors? (Hint: The symmetry group of the regular tetrahedron has size 12, and each face is an equilateral triangle.)

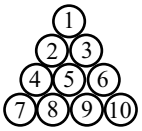


The regular tetrahedron

5. In how many different ways can we color the six faces of a cube if each face can receive one of three different colors? Of those colorings, how many have at least one face of each color? (Hint: The symmetry group of the cube has size 24.)

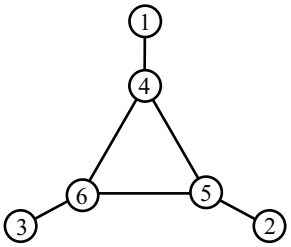
6. Repeat the previous exercise but for coloring the eight corners of the cube.

7. How many different ways are there to construct a design of the following shape using red, green, and white poker chips? The design is put on a table that can be viewed from any angle. (Chip locations are numbered for convenience.)



8. Now repeat the previous question but instead assume the design is a styrofoam-ball structure that is free to rotate in space.

9. How many different structures of the following design are possible, where each of the styrofoam balls can be one of four colors and each of the sticks can be one of three colors?



10. How many different black-white colorings of the 3×3 grid have exactly three black squares and six white squares? How many have exactly two black squares and seven white squares?

11. Repeat the problem of counting the black-white colorings of the 3×3 grid, but do so for the 4×4 and the 5×5 grids.

12. Generalize the previous problem to count the k-colorings of the $n \times n$ grid.

13. Write down the four orbits in Example 3 of this section. That is, show how the set of 5-digit binary numbers is partitioned into equivalence classes.

14. How many different 6-digit binary numbers are there if two such numbers are considered equivalent if one can be obtained from the other by any combination of SHIFT and FLIP operations? (Hint: There is an issue here not present in the example shown in the text.)

15. Consider a p-bead necklace, where p is a prime number greater than 2. Prove that the cycle structure of each planar rotation (other than the zero-degree rotation, or identity) contains exactly one cycle.

16. How many different n-bead necklaces are possible, where each bead can be one of k colors? Make your formula as useful as possible. (Hint: You will need to use number-theoretic properties of the integer n.)

5.5 Proving the CFB theorem

In this short section we prove the Cauchy-Frobenius-Burnside theorem. In addition to orbits and fixed point sets, we use the concept of stabilizer.

Definition 5.5.1 (stabilizer) *Let A and C be finite sets, and let G be a group of permutations of A. For any $f \in C^A$, the **stabilizer of** f **under** G is the set*

$$\text{stab}_G(f) := \{\pi \in G : \pi(f) = f\}.$$

Thus, the stabilizer of a function is the set of all group operations that leave that function unchanged.

We break the proof of the CFB theorem into three steps of which the first is the most technical.

Step 1: linking orbits and stabilizers

To understand the link between orbits and stabilizers, we again use the square-coloring problem of Section 5.1 to illustrate. Table 5.7 lists the orbit and stabilizer for each of the 16 colorings. (Refer back to Figure 5.1.) For each coloring, the size of its orbit times the size of its stabilizer equals 8, the size of the symmetry group.

Take any coloring, say f_2. Its orbit is $\{f_2, f_3, f_4, f_5\}$. For each coloring in this orbit, identify a group operation that takes f_2 to that coloring. Rewrite the orbit thus:

$$\text{orb}_{D_4}(f_2) = \{\underbrace{I(f_2)}_{=f_2}, \underbrace{R_1(f_2)}_{=f_3}, \underbrace{F_2(f_2)}_{=f_4}, \underbrace{F_{2,3}(f_2)}_{=f_5}\}.$$

Other rewritings may be possible. For instance, we could have rewritten f_4 as $R_2(f_2)$.

Since the size of the group equals the product of the sizes of f_2's orbit and its stabilizer, the product principle suggests that we should be able to construct a meaningful one-to-one correspondence between the eight group elements and the pairs (O, S) where O is from the orbit of f_2 and S from the stabilizer of f_2.

Take any group element, say R_2. To which pair (O, S) should we map R_2? A natural choice for the element O of the orbit is $R_2(f_2)$, which equals f_4. Now, the key idea in the later proof comes in the choice of the stabilizer element S. We know, from the way we write the orbit above, that $f_4 = F_2(f_2)$, so that the rotation motion R_2 has the same action on the coloring f_2 as does the flip motion F_2. To build an element in the stabilizer, then, just choose

$$S := F_2^{-1} \circ R_2.$$

This is guaranteed to be in the stabilizer because the F_2 and R_2 operations have the same effect on f_2:

$$(F_2^{-1} \circ R_2)(f_2) = F_2^{-1}(R_2(f_2)) = F_2^{-1}(F_2(f_2)) = f_2.$$

Therefore R_2 should map to $(f_4, F_2^{-1} \circ R_2)$.

Question 208 *Using the group table for the symmetries of the square (Table 5.3, page 195), what group element equals $F_2^{-1} \circ R_2$?*

To tackle the general case, suppose the orbit of the function f has size n, say

$$\text{orb}_G(f) = \{\sigma_1(f), \sigma_2(f), \ldots, \sigma_n(f)\}. \tag{5.3}$$

f	$\mathrm{orb}_{D_4}(f)$	$\mathrm{stab}_{D_4}(f)$	$\lvert\mathrm{orb}_{D_4}(f)\rvert \cdot \lvert\mathrm{stab}_{D_4}(f)\rvert$
f_1	$\{f_1\}$	D_4	$1 \cdot 8 = 8$
f_2	$\{f_2, f_3, f_4, f_5\}$	$\{I, F_1\}$	$4 \cdot 2 = 8$
f_3	$\{f_2, f_3, f_4, f_5\}$	$\{I, F_2\}$	$4 \cdot 2 = 8$
f_4	$\{f_2, f_3, f_4, f_5\}$	$\{I, F_1\}$	$4 \cdot 2 = 8$
f_5	$\{f_2, f_3, f_4, f_5\}$	$\{I, F_2\}$	$4 \cdot 2 = 8$
f_6	$\{f_6, f_7, f_8, f_9\}$	$\{I, F_{1,2}\}$	$4 \cdot 2 = 8$
f_7	$\{f_6, f_7, f_8, f_9\}$	$\{I, F_{2,3}\}$	$4 \cdot 2 = 8$
f_8	$\{f_6, f_7, f_8, f_9\}$	$\{I, F_{1,2}\}$	$4 \cdot 2 = 8$
f_9	$\{f_6, f_7, f_8, f_9\}$	$\{I, F_{2,3}\}$	$4 \cdot 2 = 8$
f_{10}	$\{f_{10}, f_{11}\}$	$\{I, R_2, F_1, F_2\}$	$2 \cdot 4 = 8$
f_{11}	$\{f_{10}, f_{11}\}$	$\{I, R_2, F_1, F_2\}$	$2 \cdot 4 = 8$
f_{12}	$\{f_{12}, f_{13}, f_{14}, f_{15}\}$	$\{I, F_1\}$	$4 \cdot 2 = 8$
f_{13}	$\{f_{12}, f_{13}, f_{14}, f_{15}\}$	$\{I, F_2\}$	$4 \cdot 2 = 8$
f_{14}	$\{f_{12}, f_{13}, f_{14}, f_{15}\}$	$\{I, F_1\}$	$4 \cdot 2 = 8$
f_{15}	$\{f_{12}, f_{13}, f_{14}, f_{15}\}$	$\{I, F_2\}$	$4 \cdot 2 = 8$
f_{16}	$\{f_{16}\}$	D_4	$1 \cdot 8 = 8$

Table 5.7. Orbits and stabilizers in the square example.

Here $\sigma_1, \sigma_2, \ldots, \sigma_n$ are distinct elements of G. We map $\pi \in G$ to the pair

$$\big(\pi(f),\ \sigma_j^{-1} \circ \pi\big)$$

where σ_j is that group element listed in the orbit (5.3) that produces the same action on f as does π. The second element of the pair indeed belongs to the stabilizer because

$$\big(\sigma_j^{-1} \circ \pi\big)(f) = \sigma_j^{-1}\big(\pi(f)\big) = \sigma_j^{-1}\big(\sigma_j(f)\big) = f.$$

Therefore this function is well-defined. To complete the proof, we show that it is bijective.

Lemma 5.5.2 *Let A and C be finite sets, and let G be a group of permutations of A. Then for any $f \in C^A$, we have*

$$\big|\mathrm{orb}_G(f)\big| \cdot \big|\mathrm{stab}_G(f)\big| = |G|.$$

Proof: Let A and C be finite sets, and let G be a group of permutations of A. Let $f \in C^A$ and suppose its orbit has n distinct elements as listed in (5.3) above. Define the function $\mathcal{F} : G \longrightarrow \mathrm{orb}_G(f) \times \mathrm{stab}_G(f)$ by

$$\mathcal{F}(\pi) = \big(\pi(f),\ \sigma_j^{-1} \circ \pi\big) \qquad \text{where } \sigma_j \text{ satisfies } \pi(f) = \sigma_j(f),$$

which we already showed is well-defined. We now show that $\mathcal{F}$ is bijective.

$\mathcal{F}$ **is one-to-one:** Let $\pi, \tau \in G$ and assume that $\mathcal{F}(\pi) = \mathcal{F}(\tau)$. This means that for some j and k,

$$\underbrace{\big(\pi(f),\ \sigma_j^{-1} \circ \pi\big)}_{=\mathcal{F}(\pi)} = \underbrace{\big(\tau(f),\ \sigma_k^{-1} \circ \tau\big)}_{=\mathcal{F}(\tau)}$$

where $\pi(f) = \sigma_j(f)$ and $\tau(f) = \sigma_k(f)$ for some j and k. But $\pi(f) = \tau(f)$ since the first components of the pairs are equal, so it follows that $\sigma_j = \sigma_k$. Since the second components of the pairs are equal, we use $\sigma_j = \sigma_k$ and left-cancellation to show

$$\sigma_j^{-1} \circ \pi = \sigma_k^{-1} \circ \tau \quad \Longrightarrow \quad \sigma_j^{-1} \circ \pi = \sigma_j^{-1} \circ \tau \quad \Longrightarrow \quad \pi = \tau.$$

Therefore $\mathcal{F}$ is one-to-one.

$\mathcal{F}$ **is onto:** Let $\big(\sigma_j(f),\ \tau\big)$ be in the codomain. We must find some $\pi \in G$ that maps to this pair. Define $\pi := \sigma_j \circ \tau$. Then, since τ belongs to the stabilizer,

$$\pi(f) = \big(\sigma_j \circ \tau\big)(f) = \sigma_j\big(\tau(f)\big) = \sigma_j(f),$$

and so the first element of $\mathcal{F}(\pi)$ equals $\sigma_j(f)$. The second element is

$$\sigma_j^{-1} \circ \pi = \sigma_j^{-1} \circ (\sigma_j \circ \tau) = \tau,$$

so indeed $\mathcal{F}(\pi) = \big(\sigma_j(f),\ \tau\big)$ and therefore $\mathcal{F}$ is onto. ■

Question 209 *Suppose that $|G|$ is prime. What can you say about the size of any orbit or stabilizer?*

Step 2: a formula for the number of orbits

Next we derive a formula for the number of orbits.

Lemma 5.5.3 *Let A and C be finite sets, let G be a group of permutations of A, and let $\mathcal{O}$ be the set of orbits of C^A. Then we have*

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{f \in C^A} \big|\mathrm{stab}_G(f)\big|.$$

Proof: Let A and C be finite sets, and let G be a group of permutations of A. By Lemma 5.5.2, we know that for any $f \in C^A$,

$$\frac{1}{\big|\mathrm{orb}_G(f)\big|} = \frac{1}{|G|} \cdot \big|\mathrm{stab}_G(f)\big|.$$

Sum both sides over all functions $f \in C^A$ to get

$$\sum_{f \in C^A} \frac{1}{\big|\mathrm{orb}_G(f)\big|} = \frac{1}{|G|} \sum_{f \in C^A} \big|\mathrm{stab}_G(f)\big|.$$

The sum on the left equals $|\mathcal{O}|$, the total number of orbits. ■

Question 210 *Justify the last line of the proof.*

Step 3: adjusting the formula to get the CFB theorem

The following lemma shows how to replace the sum in Lemma 5.5.3 by one whose number of terms equals the size of the group G and not the size of the colorings (i.e., functions) C^A. This adjustment prevents the workload from increasing as the number of colors increases.

Lemma 5.5.4 *Let A and C be finite sets, and let G be a group of permutations of A. Then we have*

$$\sum_{f \in C^A} \left|\text{stab}_G(f)\right| = \sum_{\pi \in G} \left|\text{fix}_G(\pi)\right|.$$

Combinatorial proof: How many pairs $(\pi, f) \in G \times C^A$ are there, where $\pi(f) = f$?

Answer 1: Condition on the function f. By Definition 5.5.1, there are $\left|\text{stab}_G(f)\right|$ elements of G that satisfy $\pi(f) = f$. Summing over all functions in C^A gives a total of $\sum_{f \in C^A} \left|\text{stab}_G(f)\right|$ possible pairs.

Answer 2: Condition instead on the group element π. By Definition 5.3.3, there are $\left|\text{fix}_G(\pi)\right|$ elements of C^A that satisfy $\pi(f) = f$. Summing over all elements in G gives a total of $\sum_{\pi \in G} \left|\text{fix}_G(\pi)\right|$ possible pairs. ■

The CFB theorem (Theorem 5.3.5, page 203) now follows immediately by combining the results of Lemmas 5.5.3 and 5.5.4.

5.6 The cycle index and Pólya's theorem

The Cauchy-Frobenius-Burnside theorem provides for easy computation in problems where we seek the number of inequivalent "colorings" with no further restrictions. But if we add a restriction, like having exactly five black and four white squares in the grid example, our set of colorings changes and we may have to re-compute the sizes of the fixed point sets. Pólya's enumeration theorem uses a generating function to inventory the colorings according to specific properties. It is flexible enough to answer many counting questions at once.

We state Pólya's enumeration theorem (Theorem 5.6.2) without proof and instead focus on its applications. Good references for the reader interested in the proof are the books by Erickson (1996), Bogart (1990), or Roberts & Tesman (2004).

The cycle index of a group

In preparation for understanding Pólya's theorem, we first introduce the cycle index of a group. The cycle index is a multinomial that encodes the cycle structure of the group elements.

Here is how it works for the square-coloring example of Section 5.1. The flip motion $F_1 = (1)(2\ 4)(3)$ has two 1-cycles and one 2-cycle, so we use the multinomial term $z_1^2 z_2$ to represent this. The identity motion I has four 1-cycles, so we use the term z_1^4. The R_1 motion has one 4-cycle, so its term is z_4. The complete list of terms appears in the table below.

motion π	product of disjoint cycles	term in cycle index
I	(1)(2)(3)(4)	z_1^4
R_1	(1 2 3 4)	z_4
R_2	(1 3)(2 4)	z_2^2
R_3	(1 4 3 2)	z_4
$F_{2,3}$	(1 4)(2 3)	z_2^2
$F_{1,2}$	(1 2)(3 4)	z_2^2
F_1	(1)(2 4)(3)	$z_1^2 z_2$
F_2	(1 3)(2)(4)	$z_1^2 z_2$

The cycle index Z is then defined to be the sum of these terms, divided by the size of the group:

$$\begin{aligned} Z(z_1, z_2, z_3, z_4) &:= \frac{1}{8}\Big(z_1^4 + z_4 + z_2^2 + z_4 + z_2^2 + z_2^2 + z_1^2 z_2 + z_1^2 z_2\Big) \\ &= \frac{1}{8}\Big(z_1^4 + 2z_1^2 z_2 + 3z_2^2 + 2z_4\Big). \end{aligned} \tag{5.4}$$

Question 211 *What is the cycle index for the group of symmetries for the grid problem?*

In general, suppose that a given group element has c_1 cycles of length 1, c_2 cycles of length 2, and so on. In the cycle index, this group element will contribute the multinomial term

$$z_1^{c_1} z_2^{c_2} \cdots z_m^{c_m}$$

where m is the length of the largest cycle appearing. The cycle index averages the above multinomial terms. Notice its similarity in appearance to the formula of the CFB theorem (Theorem 5.3.5).

Definition 5.6.1 (cycle index) *Let G be a finite group, and suppose that each element is written as a product of disjoint cycles. If the overall length of the longest such cycle is m, then we define the* ***cycle index of*** *G as the multinomial*

$$Z(z_1, z_2, \ldots, z_m) := \frac{1}{|G|} \sum_{\pi \in G} z_1^{c_1(\pi)} z_2^{c_2(\pi)} \cdots z_m^{c_m(\pi)}$$

where $c_j(\pi)$ denotes the number of j-cycles in π.

Notice that the cycle index depends only on the group—the definition makes no mention of a group acting on a set.

The cycle index for certain groups

Because the cycle index depends only on the symmetry group and not on the functions or colorings themselves, it is possible to compute the cycle index for the standard and useful groups S_n, D_n, and C_n. See the Exercises.

The pattern inventory

Next, we tell the cycle index to keep an inventory of the number of inequivalent colorings with certain properties. In the square-coloring example, each 1-cycle contributes one black corner or one white corner to the coloring. In the spirit of generating functions, this suggests replacing each occurrence of z_1 by the symbolic series $b + w$ to indicate the "black or white" choice.

Likewise, each 2-cycle contributes either two black corners or two white corners to the coloring. Replace each z_2 by $b^2 + w^2$ to indicate this choice. Overall, making the replacements

$$\begin{aligned} z_1 &\longleftarrow b + w \\ z_2 &\longleftarrow b^2 + w^2 \\ z_3 &\longleftarrow b^3 + w^3 \\ z_4 &\longleftarrow b^4 + w^4 \end{aligned}$$

in the cycle index Z shown in equation (5.4) creates an inventory of inequivalent colorings organized by the number of black and white corners used in each:

$$\begin{aligned} &Z(b + w, b^2 + w^2, b^3 + w^3, b^4 + w^4) \\ &\quad = \frac{1}{8}\Big((b + w)^4 + 2(b + w)^2(b^2 + w^2) + 3(b^2 + w^2)^2 + 2(b^4 + w^4)\Big) \\ &\quad = \cdots \\ &\quad = b^4 + b^3w + 2b^2w^2 + bw^3 + w^4. \end{aligned}$$

The "$\cdots$" hides algebraic simplification that is perhaps best left to a computer algebra system like Maple or Mathematica.

The end result is a generating function where the coefficient of $b^i w^j$ equals the number of inequivalent colorings with i black and j white corners. The number of inequivalent colorings with two black and two white corners is two, because of the $2b^2w^2$ term. The rest of the terms have coefficient equal to 1, so there is only one inequivalent coloring with each other combination of black and white corners shown. This generating function is known as the *pattern inventory*.

We can do the same for the grid-coloring example of Section 5.1. Table 5.2 on page 193 contains the relevant information for computing the cycle index, which is

$$Z(z_1, z_2, z_3, z_4) = \frac{1}{4}\Big(z_1^9 + 2z_1z_4^2 + z_1z_2^4\Big).$$

The pattern inventory is then

$$\begin{aligned} &Z(b + w, b^2 + w^2, b^3 + w^3, b^4 + w^4) \\ &\quad = \frac{1}{4}\Big((b + w)^9 + 2(b + w)(b^4 + w^4)^2 + (b + w)(b^2 + w^2)^4\Big) \\ &\quad = \cdots \\ &\quad = b^9 + 3b^8w + 10b^7w^2 + 22b^6w^3 + 34b^5w^4 \\ &\qquad + 34b^4w^5 + 22b^3w^6 + 10b^2w^7 + 3bw^8 + w^9. \end{aligned}$$

In particular, there are 34 inequivalent colorings with five black squares and four white squares because of the coefficient on b^5w^4. Of course, this agrees with the answer we computed at the end of Section 5.4.

Question 212 *Explain why the coefficients in the pattern inventory are symmetric. That is, why is the coefficient of $b^j w^{9-j}$ always equal to that of $b^{9-j} w^j$?*

It is worth seeing, however, the miraculous way the pattern inventory generating function carries out those computations for us. The first term in parentheses in the pattern inventory is $(b+w)^9$, and so the coefficient of b^5w^4 is $\binom{9}{5}$ by the binomial theorem. The second term is

$$2(b+w)(b^4+w^4)^2 = 2(b+w)(b^8+2b^4w^4+w^8)$$

so 4 is the coefficient of b^5w^4. The third term is

$$(b+w)(b^2+w^2)^4 = (b+w)(b^8+4b^6w^2+6b^4w^4+4b^2w^6+w^8)$$

so 6 is the coefficient of b^5w^4. That means the coefficient we seek is

$$\frac{1}{4}\left(\binom{9}{5}+4+6\right) = 34.$$

Compare this with our previous work in equation (5.2) on page 212.

Pólya's enumeration theorem

What we call Pólya's enumeration theorem is not the most general version of his result. It is possible to modify our version so that "weights" may be assigned to the colors. This results in additional flexibility. See the example at the close of this section for a preview.

Theorem 5.6.2 (Pólya) *Let A and C be finite sets, let G be a group of permutations of A, and suppose that the cycle index of G is $Z(z_1, z_2, \ldots, z_m)$. If $C = \{c_1, c_2, \ldots, c_t\}$, then the pattern inventory can be obtained from the cycle index by making the substitution*

$$z_k \longleftarrow c_1^k + c_2^k + \cdots + c_t^k \qquad \text{for all } k \in [m]$$

in the cycle index.

The ***pattern inventory*** is the generating function in which the coefficient of $c_1^{i_1}c_2^{i_2}\cdots c_t^{i_t}$ equals the number of inequivalent colorings in which color c_1 appears i_1 times, color c_2 appears i_2 times, and so forth.

Example: coloring the faces of a triangular prism

In how many different ways can we color the five faces of the triangular prism (see Example 1 of Section 5.4) such that each face receives either black, white, or red and exactly one red face appears?

Let's borrow the table we used in Section 5.4 to find the cycle index.

motion π	product of disjoint cycles	term in cycle index
I	$(B)(T)(S_1)(S_2)(S_3)$	z_1^5
R_1	$(B)(T)(S_1\ S_2\ S_3)$	$z_1^2 z_3$
R_2	$(B)(T)(S_1\ S_3\ S_2)$	$z_1^2 z_3$
F_1	$(B\ T)(S_1)(S_2\ S_3)$	$z_1 z_2^2$
F_2	$(B\ T)(S_1\ S_3)(S_2)$	$z_1 z_2^2$
F_3	$(B\ T)(S_1\ S_2)(S_3)$	$z_1 z_2^2$

The cycle index is then

$$Z(z_1, z_2, z_3) = \frac{1}{6}\Big(z_1^5 + 2z_1^2 z_3 + 3z_1 z_2^2\Big).$$

To get the pattern inventory, replace each z_k by $b^k + w^k + r^k$:

$$\frac{1}{6}\Big((b+w+r)^5 + 2(b+w+r)^2(b^3+w^3+r^3) + 3(b+w+r)(b^2+w^2+r^2)^2\Big).$$

Now expand it:

$$\begin{aligned} &b^5 + w^5 + r^5 + 2b^4w + 3b^3w^2 + 3b^2w^3 + 2bw^4 + 4b^3wr + 6b^2w^2r \\ &\quad + 6b^2wr^2 + 4bw^3r + 6bw^2r^2 + 4bwr^3 + 2b^4r + 3b^3r^2 \\ &\quad + 3b^2r^3 + 2br^4 + 2w^4r + 3w^3r^2 + 3w^2r^3 + 2wr^4. \end{aligned}$$

We seek the sum of the coefficients on the terms that look like $b^i w^j r$. Those terms are

$$4b^3wr + 6b^2w^2r + 4bw^3r + 2b^4r + 2w^4r,$$

and so the answer is $4 + 6 + 4 + 2 + 2 = 18$.

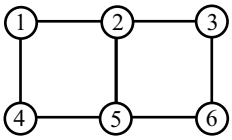
Question 213 *How many colorings are there in which at most one red face appears?*

Question 214 *The pattern inventory tells us that there are four colorings that have one black, three white, and one red face. Draw these colorings.*

The flexibility of Pólya's theorem

To close this chapter, we present an example that illustrates how to use the cycle index to answer specific counting questions. As we mentioned before stating Pólya's theorem, these methods can be made rigorous by assigning a "weight" to each color. We will avoid formality and let the examples suffice.

Let's count the different ways to construct the following structure using seven indistinguishable sticks and six styrofoam balls of various colors. (The locations of the balls are numbered in preparation for finding the symmetry group.)



How many different structures are possible under each of the following conditions?

(a) Each ball is either red, blue, or green.

(b) There are two of each color used.

(c) No reds are used.

(d) At least two greens are used.

(e) At least one blue and one green are used.

Our first job is to determine the symmetry group G of this figure. It has four elements: identity (I), rotate 180 degrees (R_{180}), flip along the horizontal axis of symmetry (F_H), and flip along the vertical axis of symmetry (F_V). The information for the cycle index is:

motion π	**product of disjoint cycles**	**term in cycle index**
I	(1)(2)(3)(4)(5)(6)	z_1^6
R_{180}	(1 6)(2 5)(3 4)	z_2^3
F_H	(1 4)(2 5)(3 6)	z_2^3
F_V	(1 3)(2)(4 6)(5)	$z_1^2 z_2^2$

The cycle index is

$$Z(z_1, z_2) = \frac{1}{4}\Big(z_1^6 + 2z_2^3 + z_1^2 z_2^2\Big).$$

If we replace z_1 by $r + b + g$ and z_2 by $r^2 + b^2 + g^2$, we get the pattern inventory:

$$\begin{aligned} &Z(r + b + g, r^2 + b^2 + g^2) \\ &\quad = \frac{1}{4}\Big((r + b + g)^6 + 2(r^2 + b^2 + g^2)^3 + (r + b + g)^2(r^2 + b^2 + g^2)^2\Big). \end{aligned}$$

All of the above questions can be answered by making appropriate substitutions in either the cycle index or the pattern inventory. Here is how.

(a) Here, we'd normally apply the CFB theorem but notice that the principle that we used to count the size of each fixed point set (namely, each cycle must be monochromatic) implies that we can get the answer by letting $z_1 = 3$ and $z_2 = 3$ in the cycle index:

$$Z(3, 3) = \frac{1}{4}\Big(3^6 + 2 \cdot 3^3 + 3^2 \cdot 3^2\Big) = 216.$$

Equivalently we could let $r = 1$, $b = 1$, and $g = 1$ in the pattern inventory.

(b) The answer is the coefficient of $r^2 b^2 g^2$ in the pattern inventory. Using software such as Maple, the answer is 27.

(c) We could add the coefficients of all the terms with no r in the pattern inventory. There is a faster way to do this: evaluate the pattern inventory at $r = 0$, $b = 1$, and $g = 1$. The answer is 24.

(d) We can get an inventory of colorings that use any number of greens from 0 to 6 by evaluating the pattern inventory at $r = 1$ and $b = 1$, and leaving g alone. Using Maple, this results in

$$24 + 52g + 71g^2 + 44g^3 + 20g^4 + 4g^5 + g^6.$$

Therefore, there are $71 + 44 + 20 + 4 + 1 = 140$ structures using at least two greens. Equivalently, we could subtract the number of structures using at most one green from the total: $216 - 24 - 52 = 140$.

(e) We first count the complement by determining the number of structures having either no blues or no greens. The answer is $24 + 24 - 1 = 47$ because there are 24 with no blues (same answer as part (c)), 24 with no greens, and 1 with no blues and no greens. Therefore, the number with at least one blue and at least one green is $216 - 47 = 169$.

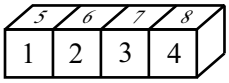
Summary

The cycle index of a permutation group keeps track of the cycle structure of each permutation. The pattern inventory, which is obtained from the cycle index, is a generating function that allows for specific counting questions to be answered at a glance. In our examples involving coloring, the pattern inventory organizes all possible colorings by the number of times each color is used, and is flexible enough to answer very specific counting questions.

Exercises

1. Find the cycle index for the symmetric groups S_3 and S_4.
2. Find the cycle index for the cyclic groups C_4 and C_5.
3. Find the cycle index for the cyclic group C_p, where p is a prime.
4. Find the cycle index for the dihedral group D_n as it acts on the corners of the regular n-gon. You'll need to consider two cases depending on the parity of n.
5. If H is a subgroup of G, then how is the cycle index of H related to the cycle index of G?
6. How many different seven-bead necklaces are possible, assuming each bead is one of four different colors and each necklace contains exactly one bead of one color and exactly two beads of each of the three remaining colors?
7. How many different 20-bead necklaces are possible, assuming each bead is one of three different colors? How many of those necklaces have at least three beads of each color?
8. How many different colorings of the six faces of a cube are possible, assuming that two faces must be white, two must be black, and two must be red? (Hint: Use your work in Exercise 5 of Section 5.4.)
9. Find the answer to Exercise 7 of Section 5.4 assuming that you only have one red chip available.
10. Find the answer to Exercise 8 of Section 5.4 assuming that you only have one red ball available.

11. A 4-inch by 1-inch by 1-inch block has four squares on each of its rectangular faces as shown below. Assume that the squares opposite squares 1–4 are labeled 9–12 and the squares opposite those labeled 5–8 are labeled 13–16.



Each numbered square can be colored red, blue, or green.

(a) Find the cycle index, assuming the block is free to move in space.

(b) How many different colorings of the block are there?

(c) How many different colorings have at least one green square?

(d) How many different colorings have exactly five green squares?

12. Let A and C be finite sets, let G be a group of permutations of A, and let $\mathcal{O}$ be the set of orbits of C^A. Use the CFB theorem to prove that $|\mathcal{O}| = Z_G(c, c, \ldots, c)$ where Z_G is the cycle index of G and $c = |C|$ (i.e., c is the number of "colors").

Travel Notes

Pólya's enumeration theorem is sometimes called the Pólya-Redfield theorem. A number of authors have noted that the paper of Redfield (1927) contained similar ideas of which Pólya was unaware when he did his work. At any rate, no one argues that it was anyone other than Pólya who demonstrated the wide-ranging utility of the theory that now bears his name.

The original paper is Pólya (1937) and is written in German. The book Pólya & Read (1987) contains an English translation of Pólya's 1937 paper in German as well as additional material.

CHAPTER 6

Combinatorics on Graphs

In this chapter we undertake a small survey of combinatorial problems that arise in graph theory. Combinatorics and graph theory are closely intertwined and so graph theory abounds with enumeration, existence, construction, and optimization problems. We concentrate on two enumeration problems (labeled trees and binary search trees in Section 6.2 and proper colorings in Section 6.3) and a certain existence question (Ramsey theory in Section 6.4). Though we don't treat them here, much work is being done today on optimization problems on graphs. This is because graphs serve as excellent models for computers as well as communications and transportation networks.

6.1 Basic graph theory

In this opening section we cover the basic vocabulary and concepts of graph theory that are necessary for the combinatorial problems we will encounter in later sections. The reader familiar with basic graph theory can safely skip most of this section but should read some of the combinatorial results and also try the Exercises.

Graph vocabulary

A graph can be thought of as a set-theoretic object or as a geometric object and each is profitable in different situations. A graph at its heart, though, is set-theoretic.

Definition 6.1.1 *A **graph** is a 2-list (V, E) where V is a nonempty, finite set and E is a set of 2-subsets of V. The set V is the **vertex set** and the set E is the **edge set**. The elements of V are called **vertices** and the elements of E are called **edges**.*

We usually refer to graphs with capital letters G, H, etc. Writing $G = (V, E)$ means that G is a graph with vertex set V and edge set E. The edge set E is allowed to be empty. Sometimes we write $V(G)$ and $E(G)$ instead of just V and E to emphasize the name of the graph G.

For example,

$$G_1 = \Big(\underbrace{\{1,2,3,4,5,6\}}_{\text{vertex set } V}, \underbrace{\big\{\{1,2\},\{1,4\},\{2,4\},\{2,5\},\{2,6\},\{4,5\},\{5,6\}\big\}}_{\text{edge set } E} \Big)$$

is a graph. The picture shown at the left in Figure 6.1 gives a visual representation of this graph. Each of the six vertices is represented by a circle with its label next to it, and each

edge is represented by a line connecting the two vertices in the edge.

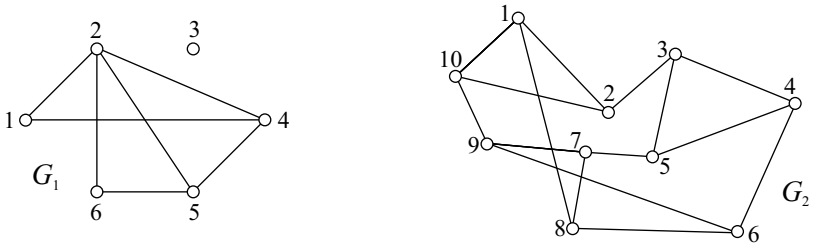


Figure 6.1. Two graphs G_1 and G_2.

Question 215 *Write the vertex and edge sets of the graph G_2 shown at the right in Figure 6.1.*

A vertex and an edge are ***incident*** provided that the vertex belongs to the edge (in the set-theoretic interpretation) or provided that the vertex "touches" the edge (in the geometric interpretation). The ***degree of a vertex*** is the number of edges that are incident to that vertex. The notation $d_G(v)$ indicates the degree of the vertex v in the graph G. If the graph G is understood, we might simply write $d(v)$.

Two vertices are ***adjacent*** provided that they are both contained in a single edge (set-theoretic) or provided that there is an edge connecting them (geometric). The notation $u \sim v$ indicates that vertices u and v are adjacent. For any edge $\{u, v\}$, the vertices u and v are the ***endpoints*** of the edge.

Question 216 *Is $5 \sim 6$ in G_1? Is $5 \sim 6$ in G_2?*

If we consider is-adjacent-to (or $\sim$) as a relation of the set of vertices of a graph, we see that $\sim$ is *irreflexive* (no vertex is adjacent to itself) and *symmetric* (if $v \sim w$ then $w \sim v$). Thus a graph is from this point of view a certain kind of relation. See the discussion at the beginning of Section 1.3.

For the graph G_1 of Figure 6.1, vertex 2 is incident to the edge $\{2, 6\}$ while it is not incident to $\{4, 5\}$. Similarly $2 \sim 6$ while vertices 1 and 5 are not adjacent ($1 \not\sim 5$). That same graph has

$$d(1) = 2,\ \ d(2) = 4,\ \ d(3) = 0,\ \ d(4) = 3,\ \ d(5) = 3,\ \ d(6) = 2.$$

The vertex 3, which has degree 0, is called an ***isolated vertex***.

Question 217 *Is it possible to draw a graph with vertex set $[5]$ and having $d(1) = d(2) = d(3) = d(5) = 3$ and $d(4) = 2$? Support your answer in either case.*

A graph is ***k-regular*** provided $d(v) = k$ for every vertex v. The graph G_2 in Figure 6.1 is 3-regular while the graph G_1 is not k-regular for any value of k. A graph that is k-regular for some value of k is called a ***regular graph***.

Graph parameters

For any graph $G = (V, E)$ we define the following:

$$n(G) = \text{the number of vertices of } G$$
$$e(G) = \text{the number of edges of } G$$
$$\delta(G) = \text{the minimum degree in } G$$
$$\Delta(G) = \text{the maximum degree in } G.$$

That is, $n(G) = |V(G)|$ and $e(G) = |E(G)|$. The letter n is used almost universally to denote the number of vertices of a graph. The letter m is sometimes used to denote the number of edges.

In the graphs of Figure 6.1 we have

$$\begin{array}{ll} n(G_1) = 6 & n(G_2) = 10 \\ e(G_1) = 7 & e(G_2) = 15 \\ \delta(G_1) = 0 & \delta(G_2) = 3 \\ \Delta(G_1) = 4 & \Delta(G_2) = 3 \end{array}$$

In general, G is k-regular if and only if $\delta(G) = \Delta(G) = k$.

Question 218 *Draw an example of a seven-vertex graph with $\delta = 3$ and $\Delta = 4$.*

Two counting questions

The handshaking lemma

Our first combinatorial property of graphs concerns what happens when we sum all of the degrees in the graph. Doing so counts each edge twice: a generic edge $\{v, w\}$ counts 1 toward the value of $d(v)$ and 1 toward the value of $d(w)$. Therefore, if we add all of the degrees, then we wind up with twice the number of edges. This proves the following theorem known as the "handshaking lemma."

Lemma 6.1.2 (handshaking) *If $G = (V, E)$ is a graph, then* $\displaystyle\sum_{v \in V(G)} d(v) = 2e(G).$

The graph G_1 of Figure 6.1 has seven edges, so the sum of the degrees should be 14:

$$\begin{aligned} \sum_{v \in V(G_1)} d(v) &= d(1) + d(2) + d(3) + d(4) + d(5) + d(6) \\ &= 2 + 4 + 0 + 3 + 3 + 2 = 14. \end{aligned}$$

Question 219 *If G is a 4-regular graph on n vertices, then how many edges does G have?*

We next use the handshaking lemma to prove a result about the parity of the degrees in a graph.

Theorem 6.1.3 *If G is a graph, then there are an even number of vertices of odd degree.*

Proof: Assume that $G = (V, E)$ is a graph. Split the sum in the handshaking lemma into those with even degree and those with odd degree:

$$2e(G) = \left(\sum_{v : d(v) \text{ even}} d(v) \right) + \left(\sum_{v : d(v) \text{ odd}} d(v) \right).$$

Since both $2e(G)$ and the first sum are even numbers, the second sum must also be an even number. Since the latter sum is a sum of odd numbers, there must be an even number of them. ■

Question 220 *Is it possible to draw a 3-regular graph on 11 vertices?*

How many graphs?

Any graph on n vertices has at most $\binom{n}{2}$ edges, since there are that many possible 2-subsets of an n-set. Such a graph could have no edges as well (every vertex is isolated), so for any graph G,

$$0 \leqslant e(G) \leqslant \binom{n}{2}.$$

The number of possible graphs on n vertices is then $2^{\binom{n}{2}}$ because each of the $\binom{n}{2}$ possible edges can either be "in" or "out" of the graph. For example, there are $2^{\binom{3}{2}} = 8$ possible graphs having vertex set [3]. These are shown in Figure 6.2.

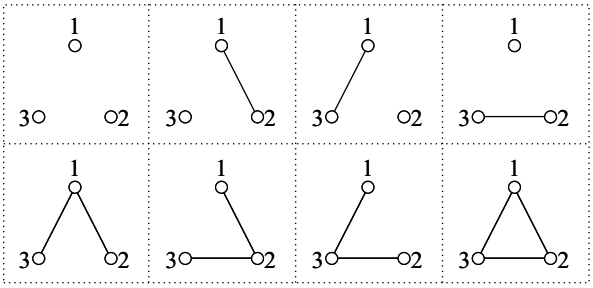
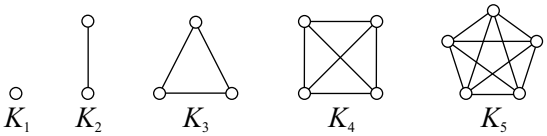


Figure 6.2. The eight labeled graphs on three vertices.

Special kinds of graphs

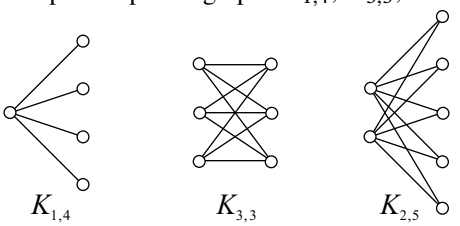
Complete graphs, cycles, and paths

For $n \geqslant 1$ the ***complete graph on n vertices***, denoted K_n, has every pair of vertices joined by an edge. Here are pictures of the complete graphs K_n for $n = 1, 2, 3, 4, 5$:



The complete graph K_n has $\binom{n}{2} = \frac{n(n-1)}{2}$ edges.

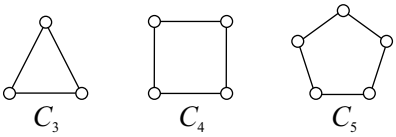
For $r, s \geqslant 1$, the ***complete bipartite graph on r and s vertices***, denoted $K_{r,s}$, is a graph for which the vertex set can be partitioned into two blocks, one of size r and one of size s, such that the edge set contains all possible edges joining two vertices from different blocks. Here are pictures of the complete bipartite graphs $K_{1,4}$, $K_{3,3}$, and $K_{2,5}$:



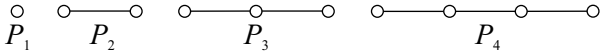
We'll explain more about bipartite graphs later in this section. A complete bipartite graph of the form $K_{1,s}$ is sometimes called a ***star***.

Question 221 *How many edges does $K_{r,s}$ have?*

For $n \geqslant 3$, the ***cycle on n vertices***, denoted C_n, has n vertices and n edges arranged in a cycle. Here are pictures of the cycles C_n for $n = 3, 4, 5$:



For $n \geqslant 1$, the ***path on n vertices***, denoted P_n, has n vertices and $n-1$ edges arranged in a path. Here are pictures of the paths P_n for $n = 1, 2, 3, 4$:



The Petersen and Grötsch graphs

The Petersen graph and the Grötsch graph appear in Figure 6.3. Both are 3-regular graphs and are important because they often serve as counterexamples to or testing grounds for new theories.

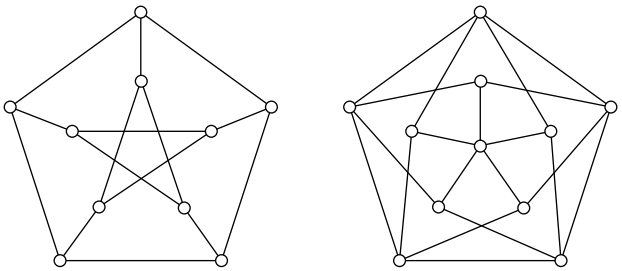
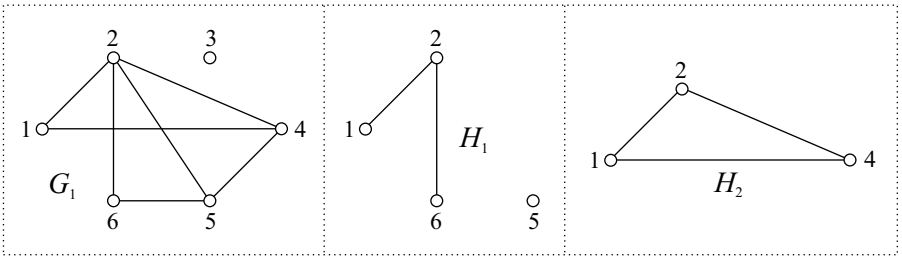


Figure 6.3. The Petersen and Grötsch graphs.

Subgraphs

Given a graph $G = (V, E)$, we say that a graph H is a ***subgraph*** of G, and write $H \subseteq G$, provided $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. Here again is the graph G_1 of Figure 6.1 as well as two different subgraphs H_1 and H_2:



If H is a subgraph of G, then it is sometimes customary to say that G contains H. For example, the subgraph H_2 of G_1 is a 3-cycle so we would say that G_1 contains C_3 as a subgraph or simply that G_1 contains a C_3.

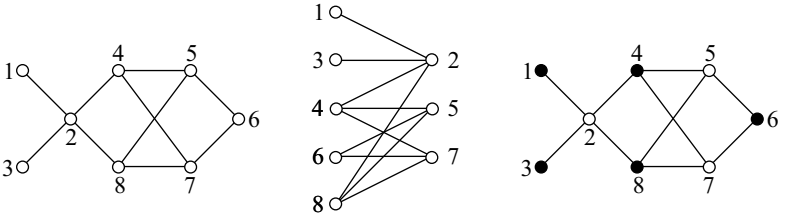
Question 222 *Does G_1 contain a C_4? What is the largest cycle that the graph G_2 of Figure 6.1 contains?*

We can often tell much about the structure of a graph by studying its subgraphs. In particular, it is often useful to identify whether a graph contains certain complete graphs or cycles as subgraphs.

Bipartite graphs

A graph is ***bipartite*** provided that its vertex set can be partitioned into two blocks in such a way that each edge of the graph has one endpoint in each block. The blocks of the partition are the ***partite sets***.

A graph that is bipartite can be drawn in a way that makes its structure obvious. One way to do this is to gather all the vertices in one partite set on one side, gather all those in the other partite set on the other side, and then draw the edges. Visually, every edge should "bridge the gap" between the partite sets. Another way is to color each vertex either black or white so that every edge contains one black and one white endpoint. Here is a graph and two ways to verify that it is bipartite:



If a graph $G = (V, E)$ is bipartite, then it is customary to write $G = (V_1 \cup V_2, E)$ to emphasize the partition of the vertex set into two partite sets. The graph we just showed has $V_1 = \{1, 3, 4, 6, 8\}$ and $V_2 = \{2, 5, 7\}$.

Is the graph G_1 of Figure 6.1 bipartite? If it were, then we can assume without loss of generality that vertex 1 is colored black and vertex 2 white. But then no matter whether vertex 4 is colored black or white, it will result in an edge with either two black or two white endpoints. This graph is not bipartite.

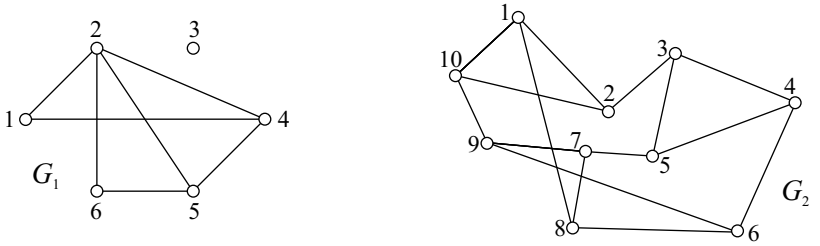
The odd cycle (namely C_3) present in the graph G_1 ensures that the graph is not bipartite. Perhaps surprisingly, odd cycles are the only way to ruin bipartiteness. The proof of the following result is included in most graph theory texts.

Theorem 6.1.4 *A graph is bipartite if and only if it does not contain any odd cycles.*

Question 223 *Is the Petersen graph bipartite? Is the Grötsch graph? For what values of n is K_n bipartite? For what values of n is P_n bipartite?*

Walks, paths, and connectedness

We now mention two ways to traverse a graph. Here again are the graphs G_1 and G_2 of Figure 6.1.



A ***walk*** in a graph is a finite list of vertices such that any two vertices that are adjacent on the list are adjacent in the graph. An example of a walk in G_1 is $(2, 5, 4, 2, 6, 2, 1)$ or just 2542621, and an example of a walk in G_2 is $(8, 6, 8, 6, 8, 6, 9, 10, 1, 8)$. In G_1, the list $(2, 5, 1, 2, 6, 2)$ is not a walk because 5 and 1 are adjacent on the list but $5 \not\sim 1$ in G_1. In general if a walk starts at vertex u and ends at vertex v, then it is a ***u-v walk***.

Although we only need to list the vertices in order to specify the walk, a walk should be thought of as a list that alternates vertex-edge-vertex-edge, and so on. The ***length of a walk*** is the number of edges traversed and so equals one fewer than the length of the list. The length of the walk $(2, 5, 4, 2, 6, 2, 1)$ is 6 and the length of the walk $(8, 6, 8, 6, 8, 6, 9, 10, 1, 8)$ is 9.

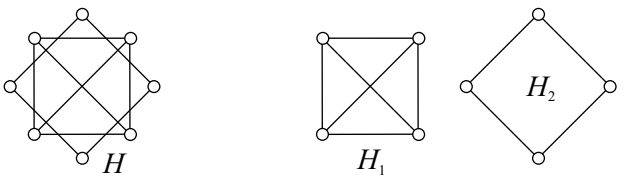
Question 224 *Let v be any vertex of $K_{3,3}$. How many different length-6 walks start and end at v?*

A ***path*** in a graph is a walk that does not contain any repeated vertices. None of the walks of the previous paragraph are paths, but $(2, 6, 5, 4)$ and $(2, 5)$ are paths in G_1.

Question 225 *Find a* 4-3 *path of length 9 in G_2.*

A graph is ***connected*** provided that for every pair of vertices u and v, there exists a u-v path. Otherwise the graph is ***disconnected***. Informally speaking, connected means that it is possible to travel from any one vertex to any other vertex along the edges of the graph. The graph G_1 is disconnected since there is, for example, no 1-3 path. The graph G_2 however is connected because there is a path joining every pair of vertices. Even though there are $\binom{10}{2} = 45$ such pairs, it is not necessary to check for a path between every one. In Question 225, you found a path containing all 10 vertices and that implies G_2 is connected.

A graph may look connected but may in fact be disconnected, as graph H shown below does:



The graph H is in two "pieces" called components. A ***connected component*** or simply ***component*** of a graph is a connected subgraph that can't be made larger by the addition of any vertices or edges. The component H_1 is a complete graph on 4 vertices and the component H_2 is a 4-cycle. We write $H = H_1 \cup H_2$ to indicate that H is disconnected and that its components are H_1 and H_2. The graph G_1 shown earlier also has two components while G_2, being connected, has one component.

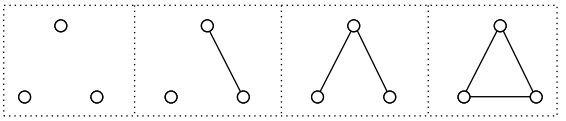
Question 226 *Draw the graph $K_{2,3} \cup P_5 \cup K_4 \cup K_1$.*

Labeled graphs, unlabeled graphs, and isomorphism

In the graphs shown in this section, sometimes we have labeled the vertices and other times we have not. For example, the graphs of Figure 6.1 have labeled vertices but the examples of complete graphs, cycles, and paths that we showed had unlabeled vertices. Vertices can generally be left unlabeled when we care only about the structure of the adjacency relationships in a graph. In drawing K_5, for example, the pertinent structure is that every

pair of vertices is adjacent. It doesn't matter whether we label the vertices with the integers 1-5, the letters a-e, or the names Sue, Ray, Jason, Carrie, and Ellie.

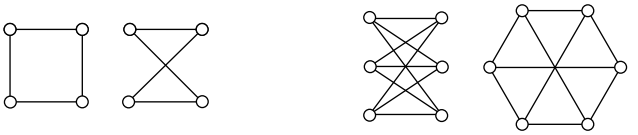
The problem of counting unlabeled graphs is much harder than that of counting labeled graphs. We found that there were $2^{\binom{3}{2}} = 8$ different labeled graphs on three vertices and these were pictured in Figure 6.2. However, there are only four different unlabeled graphs on three vertices:



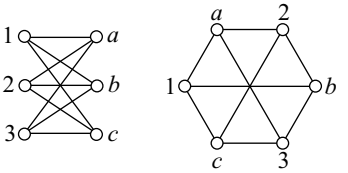
Each unlabeled graph is a representative from a different equivalence class, where we consider two labeled graphs equivalent provided they "look" the same when their vertex labels are deleted.

Question 227 *How many different unlabeled graphs on four vertices have exactly three edges?*

"Look the same" is a nebulous concept. We instead need the concept of *isomorphism*. We motivate it before launching into a general definition. It's not too hard to see that the two graphs on the left represent the same unlabeled graph, in this case the cycle C_4. But what about the two on the right?



One way to make sure they are exactly the same graph is to label the vertices of each with the same set of labels and then check that their edge sets are equal. Here is one such labeling:



Both graphs have the same edge set, namely $\{1a, 1b, 1c, 2a, 2b, 2c, 3a, 3b, 3c\}$. (Here we write $1a$ as an abbreviation for $\{1, a\}$, etc.) They indeed represent the same unlabeled graph.

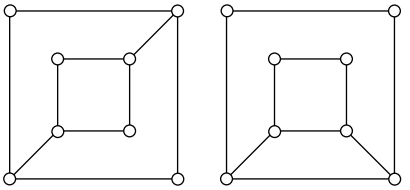
It is not necessary to use the same labels for each vertex set, so long as all adjacency relations are preserved. The following definition makes this precise.

Definition 6.1.5 *Graphs G and H are **isomorphic** provided that there exists a bijection $\phi : V(G) \longrightarrow V(H)$ that satisfies the following property: for each $u, v \in V(G)$, we have $u \sim v$ in G if and only if $\phi(u) \sim \phi(v)$ in H. The function ϕ is called an **isomorphism**. If G and H are isomorphic, we write $G \cong H$.*

If two graphs are isomorphic, then every graph parameter or structural property possessed by one of the graphs is also possessed by the other. This is most often used (in the contrapositive) to prove that two graphs are not isomorphic by exhibiting a property possessed by one graph and not by the other.

Example: determining whether two graphs are isomorphic

Are the following graphs isomorphic?



We *cannot* conclude that they are not isomorphic simply by saying the drawings are "close but don't quite look the same." Since the same unlabeled graph can be drawn in very different-looking ways, we cannot appeal to any characteristic of the drawing. What is needed is a property that G has and H doesn't have, or vice versa.

Notice that both graphs have the same number of vertices and edges. Also, they both have four vertices of degree 2 and four of degree 3. But notice in G that every edge joins a degree-2 vertex with a degree-3 vertex. This is not the case in H, so $G \ncong H$.

Question 228 *Draw two 2-regular graphs on six vertices that are not isomorphic.*

Some combinatorial properties

Vertices of same degree

In any group of n people, there must be two people that have exactly the same number of acquaintances within the group. If we consider the group of people to be the set of vertices and if we draw an edge between two vertices whenever the corresponding people are acquainted, then the statement about people becomes the following existence statement about graphs.

Theorem 6.1.6 *In any graph there must be two vertices of the same degree.*

Proof: Assume $G = (V, E)$ is a graph on n vertices. If G has a vertex of degree $n-1$, then this vertex is adjacent to every other vertex in the graph. That means there are no degree-0 vertices so we have $1 \leqslant d(v) \leqslant n-1$ for all v. Since there are n vertices, the pigeonhole principle implies that there are two vertices of the same degree.

If G has no vertex of degree $n-1$, then we have $0 \leqslant d(v) \leqslant n-2$ for all v. Again since there are n vertices, the pigeonhole principle implies that there are two vertices of the same degree. ■

Regular bipartite graphs

Our next counting theorem shows that if a bipartite graph is regular, then this forces the two vertex sets to have the same size.

Theorem 6.1.7 *If $G = (V_1 \cup V_2, E)$ is a k-regular bipartite graph, where $k > 0$, then $|V_1| = |V_2|$.*

Combinatorial proof: Assume that $G = (V_1 \cup V_2, E)$ is a k-regular bipartite graph, where $k > 0$. How many edges does G have?

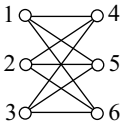
Answer 1: Since G is bipartite, every edge touches exactly one vertex of V_1. Since G is k-regular, it has $k|V_1|$ edges.

Answer 2: Since G is bipartite, every edge touches exactly one vertex of V_2. Since G is k-regular, it has $k|V_2|$ edges.

This proves that $k|V_1| = e(G) = k|V_2|$, and we can then conclude that $|V_1| = |V_2|$ because $k > 0$. ■

Counting walks

Question 224 addressed the question of counting certain length-6 walks in the complete bipartite graph $K_{3,3}$. Label the vertices of this graph as follows:

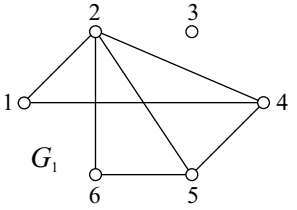


To count, say, the length-6 walks that start at 1 and end at 3, we need to count lists of the form $(1, v_1, v_2, v_3, v_4, v_5, 3)$ where the choices for v_1-v_5 respect the adjacency relationships in the graph. Since $K_{3,3}$ is 3-regular and bipartite, this is easy: there are three choices for each of the five vertices, so there are $3^5 = 243$ walks.

Question 229 *Consider $K_{3,5}$ and let v be any vertex in the partite set of size 3. How many length-10 walks start and end at v? Also, answer the same question but for length-9 walks.*

If a graph is not highly structured then it may not be as straightforward to count walks. Here is a clever way to do so using matrix multiplication. Given a labeled graph $G = (V, E)$ on n vertices, its ***adjacency matrix*** is that $n \times n$ matrix A where $A_{ij} = 1$ when $i \sim j$ and $A_{ij} = 0$ otherwise.

Here is the adjacency matrix B of the graph G_1. The rows and columns of B are labeled with the vertex set $V(G_1)$.



$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array} = B.$$

Notice that this matrix is symmetric ($B_{ij} = B_{ji}$ for all i, j) and has 0s on the diagonal.

Now, if we want to know the number of 1-4 walks of length 5, we simply compute B^5 and look at the entry in row 1 and column 4. Using MATLAB we find

$$B^5 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 24 & 45 & 0 & 38 & 33 & 27 \\ 45 & 64 & 0 & 58 & 58 & 45 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 38 & 58 & 0 & 44 & 52 & 33 \\ 33 & 58 & 0 & 52 & 44 & 38 \\ 27 & 45 & 0 & 33 & 38 & 24 \end{pmatrix} \end{array}$$

so the answer is 38. Moreover, for any vertices i and j the number of i-j walks of length 5 is readily available because it equals the (i, j)-entry of B^5. For example, the number of 6-2 walks of length 5 is 45.

Question 230 *Assume that this walk-counting property is true. Why are the entries in row 3 and column 3 all 0? Also, why is B^5 symmetric? Explain both of your answers in the context of counting walks in G_1.*

Why does this work? You will formally establish it by induction in Exercise 13 but here is the general idea. The result we wish to prove is as follows.

Theorem 6.1.8 *Let G be a graph and let A be its adjacency matrix. For all $k \geqslant 1$, the (i, j)-entry of A^k equals the number of i-j walks of length k in G.*

Let's look at the example of G_1 to illuminate the inductive step. Assume that the matrix B^5 correctly counts walks as stated in the theorem. That is, for all i and j,

$$B^5_{ij} = \text{number of } i\text{-}j \text{ walks of length 5 in } G_1.$$

Based on the truth of this, let's show why $B^6_{1,4}$ equals the number of 1-4 walks of length 6. The key is to write $B^6 = BB^5$ and then use the definition of matrix multiplication and the inductive hypothesis. The definition of matrix multiplication gives

$$\begin{aligned} B^6_{1,4} &= \sum_{k=1}^{6} B_{1,k} B^5_{k,4} \\ &= B_{1,1}B^5_{1,4} + B_{1,2}B^5_{2,4} + B_{1,3}B^5_{3,4} + B_{1,4}B^5_{4,4} \\ &\quad + B_{1,5}B^5_{5,4} + B_{1,6}B^5_{6,4}. \end{aligned}$$

But $B_{1,2} = B_{1,4} = 1$ while the rest of the $B_{k,4} = 0$. Therefore

$$B^6_{1,4} = B^5_{2,4} + B^5_{4,4} = 58 + 44 = 102.$$

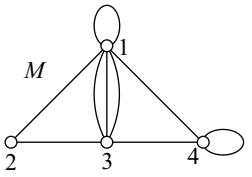
Despite the cumbersome notation this makes perfect sense: to specify a length-6 walk from 1 to 4, the first edge we traverse must take us either to vertex 2 or vertex 4.

- If we start by traversing $\{1, 2\}$, the remainder of the walk is a length-5 walk from 2 to 4. There are $B^5_{2,4} = 58$ of these.
- If we start by traversing $\{1, 4\}$, the remainder of the walk is a length-5 walk from 4 to 4. There are $B^5_{4,4} = 44$ of these.

By the sum principle there are $B^5_{2,4} + B^5_{4,4} = 58 + 44$ walks. This is the basic idea that is used to prove the theorem. (See Exercise 13.)

A note on multigraphs

At the beginning of this section we defined a graph as a pair $G = (V, E)$ where V is a finite set and E is a set of 2-subsets of V. This definition does not allow for two copies of the same edge to appear in the graph (because E is a set instead of a multiset) nor does it allow for an edge to join a vertex to itself (because the edges are 2-subsets, not 2-multisets). If either of these restrictions are relaxed then we get a ***multigraph***. Here is an example:



This multigraph $M = (V, E)$ has

$$V = \{1, 2, 3, 4\}$$
$$E = \big\{\{1, 1\}, \{1, 2\}, \{1, 3\}, \{1, 3\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{3, 4\}, \{4, 4\}\big\}.$$

Notice that each edge is a 2-multiset taken from V and that E itself is a multiset.

The edge $\{1, 1\}$ is a ***loop*** and the edges $\{1, 3\}, \{1, 3\}, \{1, 3\}$ are ***multiple edges***. A loop contributes 2 to the degree of its incident vertex, so in this multigraph

$$d(1) = 7, \quad d(2) = 2, \quad d(3) = 5, \quad d(4) = 4.$$

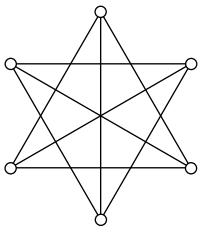
Question 231 *Does the handshaking lemma still hold for multigraphs? Give a proof or counterexample.*

Summary

In this section we provided a large amount of information and terminology about graphs. We also proved some basic enumerative and existence results about graphs.

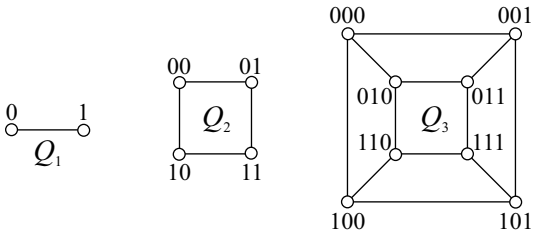
Exercises

1. How many labeled graphs on n vertices have exactly m edges?
2. Let G be the graph whose vertex set is the set of 2-subsets of $[5]$ and where two vertices are adjacent if and only if their corresponding subsets are disjoint.
   (a) Draw G.
   (b) Find, with proof, a graph mentioned in this section that is isomorphic to G.
3. Prove: if G is a connected graph with n vertices and $n - 1$ edges, where $n \geqslant 2$, then G has at least two vertices of degree 1.
4. There are $2^{\binom{4}{2}} = 2^6 = 64$ labeled graphs on 4 vertices. How many unlabeled (i.e., non-isomorphic) graphs on 4 vertices are there?
5. Determine, with proof, whether the following graph is isomorphic to $K_{3,3}$.



6. Let $G = (V, E)$ be a graph. The ***complement of*** G is that graph $\overline{G} = (V, E^c)$ where E^c is the complement of E relative to the edge set of $K_{n(G)}$. In other words, for all $i, j \in V(G)$ we have $\{i, j\} \in E^c$ if and only if $\{i, j\} \notin E$.
   Prove that if $G \cong \overline{G}$, then either $n(G) \equiv 0 \pmod 4$ or $n(G) \equiv 1 \pmod 4$.
7. Prove that if $\delta(G) \geqslant k$, then G contains a path of length at least k.
8. Prove that the number of labeled graphs in which every vertex has even degree is $2^{\binom{n-1}{2}}$.

9. For $k \geqslant 1$, the graph Q_k is called the ***k-dimensional cube***. Its vertex set is the set of k-digit binary numbers, and two vertices are adjacent if and only if their binary numbers differ in exactly one place. Here are Q_1, Q_2, and Q_3:



Notice that $n(Q_k) = 2^k$.

(a) Find $e(Q_k)$.

(b) Prove that Q_k is bipartite, for all $k \geqslant 1$.

10. (based on West (2001)) Use graphs to give combinatorial proofs of the following results.

(a) $\binom{n}{2} = \binom{k}{2} + k(n-k) + \binom{n-k}{2}$.

(b) Suppose $n_1, n_2, \ldots, n_k$ are positive integers. If $\sum_{i=1}^{k} n_i = n$, then

$$\sum_{i=1}^{k} \binom{n_i}{2} \leqslant \binom{n}{2}.$$

When does equality hold?

11. Prove that if G is an n-vertex graph with $\delta(G) \geqslant \lfloor n/2 \rfloor$, then any two vertices are either adjacent or have a common neighbor.

12. (linear algebra) Find the number of...

(a) 5-5 walks of length 8 in the graph G_1 of Figure 6.1.

(b) 000-001 paths of length 8 in the cube graph Q_3. (See Exercise 9.)

(c) u-v walks of length 8 in the cycle C_5, where u and v are any two adjacent vertices.

13. (linear algebra) Prove Theorem 6.1.8 by induction on k.

14. (linear algebra) Let A be the adjacency matrix of $K_{r,r}$. Assume that A is written in the form

$$A = \begin{pmatrix} \mathbf{0} & J \\ J & \mathbf{0} \end{pmatrix}$$

where J is the $r \times r$ matrix of all 1s and $\mathbf{0}$ is the $r \times r$ zero matrix. Find, with proof, a formula for A^k.

15. (linear algebra) Let A be the $n \times n$ matrix that has 0s on the diagonal and 1s everywhere else. Find a formula for A^k by counting walks in a certain graph.

Travel Notes

By most accounts graph theory had its birth in the 1730s when Leonhard Euler solved the now-famous "bridges of Königsberg" problem. The field then mostly lay dormant until the mid-to-late 1800s when mathematicians such as Arthur Cayley and James Joseph Sylvester took an interest and produced some key results. In the 20th century the field quickly exploded into the active research area that it is today thanks to practical applications as well as the rise of the computer.

The term "graph" was coined by Sylvester who in 1877 was installed as the inaugural professor of mathematics at the newly-opened Johns Hopkins University. Some authors use "simple graph" instead of just "graph" to denote a graph without loops or multiple edges. West (2001) and Chartrand & Zhang (2005) are excellent, comprehensive introductions to graph theory.

6.2 Counting trees

The most fundamental and important graphs in many applications, first and foremost computer science, are trees. Figure 6.4 shows three examples. A ***tree*** is a connected, acyclic graph. A ***forest*** is an acyclic graph. Naturally each connected component of a forest is a tree. In this section we mention a few basic properties of trees and then investigate two enumeration questions. The first is simply to count the number of labeled trees on n vertices, and we give two of the several possible proofs of this. We then take up the enumeration of binary search trees. These are a fundamental data structure in computer science.

Question 232 *Give a quick explanation why trees are bipartite.*

Essential properties of trees

Leaves of a tree

A ***leaf*** of a tree is a vertex of degree 1. Each of the trees in Figure 6.4 possesses at least two leaves and this is no accident. Any tree on at least two vertices must have at least two leaves. The proof uses an important technique: maximality.

Theorem 6.2.1 *If T is a tree with at least two vertices, then T has at least two leaves.*

Proof: Assume that T is a tree on n vertices, where $n \geqslant 2$. Let P be a path in T of maximum length. Call the vertices at the ends of the path v_1 and v_2. These must be leaves of T and here is why.

Suppose, for sake of contradiction, that v_1 is not a leaf of T. We already know that some edge, say $\{v_1, w\}$ is on the path P. Our assumption that v_1 is not a leaf of T means

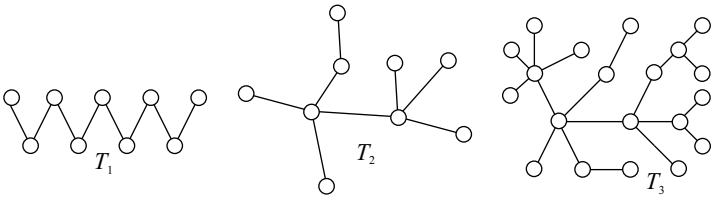


Figure 6.4. Three examples of trees.

that there is some other vertex u adjacent to v_1. This vertex u cannot be on the path P, for then $P + \{v_1, u\}$ would be a subgraph of T containing a cycle—impossible since T is a tree. But neither can u be off the path P, for then $P + \{v_1, u\}$ would be a longer path in T than P—impossible since P is already a path of maximum length.

No such vertex u can exist, so therefore v_1 is a leaf of T. The same argument shows that v_2 is a leaf of T, so therefore T has at least two leaves. ■

Deleting a leaf of a tree

Deleting a leaf from a tree leaves a smaller tree. Many proofs involving trees make good use of this fact, usually within the context of a proof by mathematical induction.

Theorem 6.2.2 *If T is a tree with at least two vertices and if v is a leaf of T, then $T - v$ is also a tree.*

Proof: Assume that T is a tree on at least two vertices and that v is a leaf of T. Consider the graph $T - v$. We must show that $T - v$ is connected and acyclic.

Deletion of the vertex v cannot create a cycle, so $T - v$ remains acyclic. Is it connected? Take any two vertices u and w in $T - v$. These vertices are also in the tree T, so there is a path P_{uw} in T that joins u and w. This path cannot pass through the vertex v in T because it is a leaf, and so deletion of v and its incident edge means that the path P_{uw} remains intact in $T - v$. Since there is a path between any two vertices of $T - v$, it follows that $T - v$ is connected. Therefore $T - v$ is a tree. ■

Counting the edges of a tree

A graph on n vertices may have anywhere from 0 to $\binom{n}{2}$ edges. A tree on n vertices has no choice over the number of edges it contains. Observe that in Figure 6.4, T_1 has nine vertices and eight edges, T_2 also has nine vertices and eight edges, and T_3 has 20 vertices and 19 edges.

Theorem 6.2.3 *Any tree on n vertices contains exactly $n - 1$ edges.*

Proof by induction on *n:* Let $n = 1$. The only tree on one vertex is the graph consisting of a single vertex and no edges. In this case $n - 1 = 1 - 1 = 0$ so the base case is true.

Assume n is an integer, $n \geqslant 1$, and that any tree on n vertices has exactly $n - 1$ edges. Let T be a tree on $n + 1$ vertices. Since $n \geqslant 1$, we know that $n + 1 \geqslant 2$ so Theorem 6.2.1 guarantees that T has a leaf, say v. Now Theorem 6.2.2 guarantees that $T - v$ is a tree on n vertices, and so the inductive hypothesis tells us that $T - v$ has $n - 1$ edges. When we reattach v to $T - v$ to get T, we have added one edge. This means that T has $(n-1)+1 = n$ edges. Since T has $n + 1$ vertices and $(n + 1) - 1 = n$ edges, this completes the proof. ■

Characterizations of a tree

There are many ways to characterize a tree. We omit the proof of the following theorem and leave some of the details to the Exercises.

Theorem 6.2.4 *If T is a graph on n vertices, then the following statements are equivalent.*

1. *T is a tree.*
2. *T is connected and has $n - 1$ edges.*
3. *T is acyclic and has $n - 1$ edges.*
4. *T is connected, but the deletion of any edge disconnects the graph.*

Counting labeled trees

In the last section we easily answered the question of enumerating the labeled graphs on n vertices: there are $2^{\binom{n}{2}}$. Enumerating the labeled *trees* on n vertices is a different story. Cayley (1889) first proved the formula of the following theorem.

Theorem 6.2.5 (Cayley) *For $n \geqslant 2$, there are n^{n-2} labeled trees on n vertices.*

We present two proofs of it. One is a bijective proof and the other uses a recurrence relation and induction. Neither is Cayley's original proof.

Question 233 *Draw the 16 labeled trees on four vertices.*

A bijective proof of Cayley's formula

Prüfer (1918) provided the following proof of Cayley's formula. His method involves a bijection between the labeled trees with vertex set $[n]$ and the $(n-2)$-lists taken from $[n]$. As there are n^{n-2} such lists, this proves Cayley's formula once the bijection is established. The $(n-2)$-list corresponding to a labeled tree is called the ***Prüfer sequence*** of the tree.

> **To construct the Prüfer sequence of a labeled tree:** Let $L = (\,)$, the empty list. Find the leaf with the smallest label. Delete this leaf from the tree and append the label of its neighbor to the end of L. Repeat this until the tree has only two vertices.

Figure 6.5 shows how to construct the 7-list that is the Prüfer sequence of the 9-vertex tree in the top left corner of the figure. The Prüfer sequence of that tree is $(2, 6, 1, 2, 9, 1, 6)$.

Question 234 *What is the Prüfer sequence of the path of length n where the vertices are labeled in increasing order from left to right? What is the Prüfer sequence of the n-vertex path shown below?*

Also, what is the tree that has Prüfer sequence $(3, 3, 3, 3, 3)$*?*

It is clear that the function that maps each n-vertex tree to its Prüfer sequence is well defined, for Prüfer sequences are indeed lists of length $n-2$ taken from the set of vertex labels $[n]$. It is worth writing out the correspondence that this function produces for a small value of n.

Question 235 *Find the Prüfer sequence of each of the 16 labeled trees on 4 vertices and then verify that every possible 2-list taken from* $[4]$ *is represented.*

We next consider the trickier issue of reversing the procedure. That is, given an $(n-2)$-list taken from $[n]$ we need to determine the tree to which it corresponds. In the following procedure, the list U (for "used") keeps track of vertices as they are considered.

> **To undo the Prüfer sequence:** Let L be any $(n-2)$-list taken from $[n]$. Let $U = (\,)$. Repeat the following until L is the empty list.
>
> - Let u be the least vertex that appears on neither L nor U.
> - Let l be the first vertex on L. Add the edge $\{l, u\}$.
> - Delete l from L. Add u to the end of U.
>
> When L is the empty list, add the edge joining the two vertices that don't appear on U.

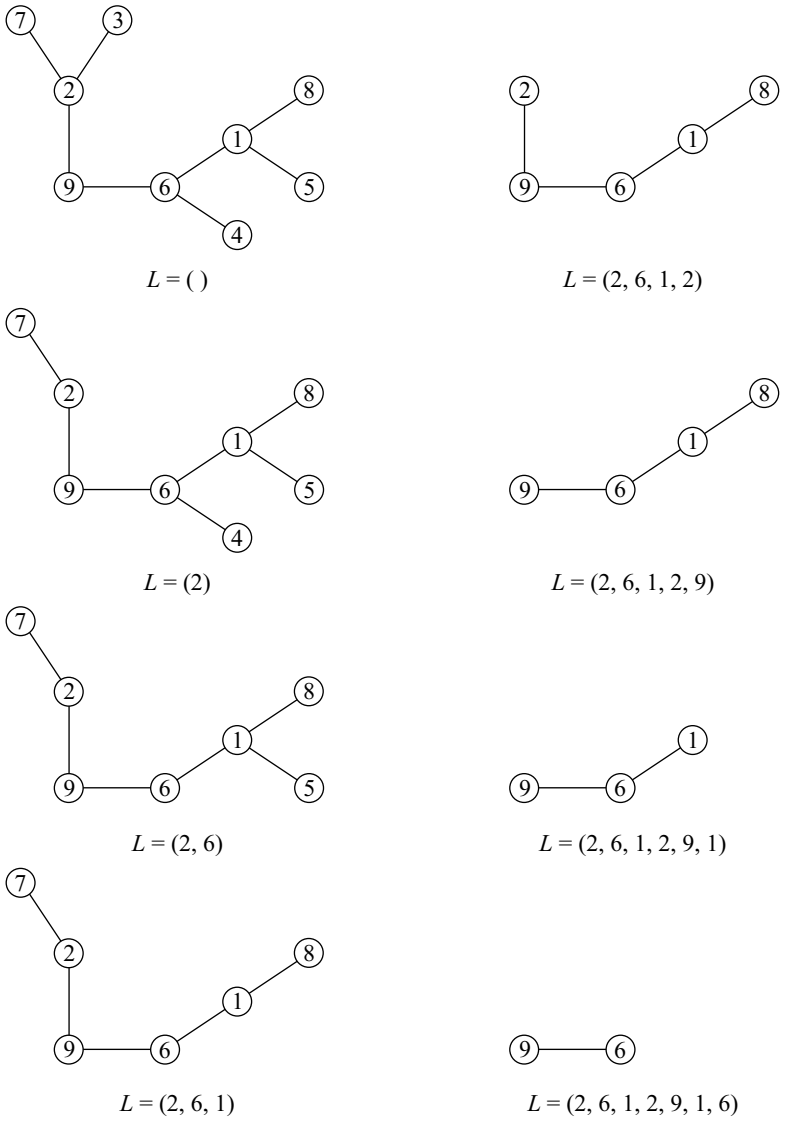


Figure 6.5. Constructing the Prüfer sequence for a nine-vertex tree.

Does this produce a tree? Notice that the procedure produces $n-1$ edges because one edge is added per element of L, of which there are $n-2$, and then one more edge is added at the end. That is a good start.

Consider the example $L = (4, 4, 7, 1, 3, 4)$. This is a 6-list so the tree has vertex set [8]. Figure 6.6 shows what this procedure does with L. The right-hand column of the table keeps track of the order in which the procedure adds the edges.

Question 236 *Apply the procedure to* $L = (2, 6, 1, 2, 9, 1, 6)$ *and verify that it produces the tree of Figure 6.5.*

To see that the collection of edges that the procedure adds produces a tree, consider adding them in the *reverse* order.

List L	List U	Edge added
$(4,4,7,1,3,4)$	$()$	$a = \{4,2\}$
$(4,7,1,3,4)$	(2)	$b = \{4,5\}$
$(7,1,3,4)$	$(2,5)$	$c = \{7,6\}$
$(1,3,4)$	$(2,5,6)$	$d = \{1,7\}$
$(3,4)$	$(2,5,6,7)$	$e = \{3,1\}$
(4)	$(2,5,6,7,1)$	$f = \{4,3\}$
$()$	$(2,5,6,7,1,3)$	$g = \{8,4\}$

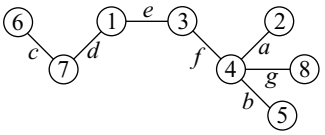


Figure 6.6. Undoing the Prüfer sequence.

Question 237 *Draw the vertices 1-8 and then iteratively add edges g, f, e, d, b, c, a in that order. Notice that the graph being "grown" always stays connected. Do the same for the sequence $L = (2,6,1,2,9,1,6)$ of the previous Question.*

As we add the edges listed in the table, from bottom to top, notice that a new vertex is connected at each step. In fact these new vertices are those of the final U in reverse order. When we add any edge (other than the one at the bottom of the table) of the form $\{l,u\}$ where l was the vertex deleted from the current L, this vertex l must appear at least once among the edges below $\{l,u\}$ on the table. This is because once once all occurrences of l are deleted from L, then l will eventually be a least vertex appearing on neither L nor U. It might never get put on U, but if not then it will be part of the last edge of the table. This proves that once all the edges are added, we have a connected graph on n vertices and $n-1$ edges. This is a tree by Theorem 6.2.4.

It can be observed that the procedure we gave for undoing the Prüfer sequence is the correct inverse function. That is, let $f : \mathcal{T} \longrightarrow \mathcal{L}$ be the function that finds the Prüfer sequence of a tree, where $\mathcal{T}$ is the set of labeled n-vertex trees and $\mathcal{L}$ is the set of $(n-2)$-lists taken from $[n]$. Then the function $g : \mathcal{L} \longrightarrow \mathcal{T}$ that constructs a tree from an $(n-2)$-list indeed satisfies $g(f(T)) = T$ for all labeled trees T. This establishes f as a bijection and proves Cayley's theorem.

Side effects

Theorem 6.2.6 *If T is a tree and L is the Prüfer sequence of T, then any vertex v appears exactly $d(v)-1$ times in L.*

Proof: Assume that $T = (V,E)$ is a tree and L is its Prüfer sequence. In computing L we iteratively "pruned" T until only two vertices and the edge between them were left. Call these vertices i and j.

Now let $v \in V$. If v is neither i nor j, then v was deleted at some point in the computation of L. Prior to its deletion, we had deleted all of its neighbors except for one (since v must be a leaf in order to be deleted) so v was recorded $d(v)-1$ times in L.

If v is one of i and j, then all of its neighbors were deleted except one (either j or i, respectively) so again v appears $d(v) - 1$ times in L. ■

Prüfer's idea tells us that the labeled trees with vertex set $[n]$ are in one-to-one correspondence with the $(n-2)$-lists taken from $[n]$. The previous theorem shows further that the Prüfer sequence records each vertex exactly $d(v) - 1$ times. So, the labeled trees with vertex set $[n]$ are in one-to-one correspondence with the $(n-2)$-lists taken from $[n]$ in which each $i \in [n]$ appears exactly $d(i) - 1$ times. The multinomial coefficients count the latter set. (Recall their definition in Section 4.1.)

Corollary 6.2.7 *For $n \geq 2$, there are*

$$\binom{n-2}{d_1 - 1,\ d_2 - 1,\ \ldots,\ d_n - 1}$$

labeled trees with vertex set $[n]$ such that vertex i has degree d_i, for $i \in [n]$.

Question 238 *In the multinomial coefficient, it should be the case that the sum of the bottom numbers equals the top number. Does it? Give a quick calculation.*

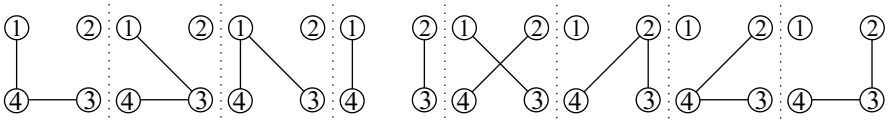
Another proof of Cayley's formula

Here is a recursive proof of Cayley's formula due to Riordan & Renyi. It illustrates a useful problem-solving technique: when faced with a difficult problem, solve a more difficult problem. Their approach is to count *forests* of a particular type and then specialize to trees at the end.[1]

Define $T(n, k)$ to be the number of labeled forests such that

- the vertex set is $[n]$,
- the forest has k trees, and
- each vertex in $[k]$ is in a different tree.

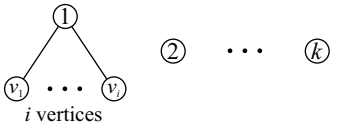
For example, $T(4, 2) = 8$ because here are the labeled forest with vertex set [4] consisting of two trees where the vertices in $[2] = \{1, 2\}$ are in different trees:



Notice that $T(n, 1)$ is just the number of labeled trees on n vertices.

First we derive a recurrence. How many labeled forests are there on vertex set $[n]$, containing k trees, and where each vertex in $[k]$ is in a different tree? One answer is $T(n, k)$.

For another answer we divide into cases according to the degree of vertex 1. Its neighbors must be chosen from the set $\{k+1, k+2, \ldots, n\}$ because vertices $2, 3, \ldots, k$ are not in the same tree as vertex 1. If vertex 1 has i neighbors, where $0 \leq i \leq n-k$, then there are $\binom{n-k}{i}$ ways to choose them. At this point our forest looks like this:



[1] Actually the "more difficult problem" will only appear so because of the additional structure imposed. Additional structure often makes a counting problem *easier*.

Of course, if vertex 1 has $i = 0$ neighbors then no edges are present. Now for each way to choose vertex 1's neighbors, there are $T(n-1, k-1+i)$ ways to complete the labeled forest. This is because, if we ignore vertex 1 and its incident edges for the moment, the remaining graph must be a labeled forest on $n-1$ vertices in which each of vertices $2, \ldots, k$ and $v_1, \ldots, v_i$ are in different trees. There are $k-1+i$ such vertices. By summing over all i, we have shown

$$T(n,k) = \sum_{i=0}^{n-k} \binom{n-k}{i} T(n-1, k-1+i) \qquad \text{where } 1 \leqslant k \leqslant n. \tag{6.1}$$

The boundary conditions are $T(n,0) = 0$ for all $n \geqslant 1$, and $T(0,0) = 1$.

Now that the recurrence is established, the rest of the proof shows that the formula $T(n,k) = k\,n^{n-k-1}$ holds for all n and k. We give a careful proof that serves as a good example of a more complicated induction argument.

Theorem 6.2.8 *The number of labeled forests such that the vertex set is $[n]$, the forest has k trees, and each vertex in $[k]$ is in a different tree is $T(n,k) = k\,n^{n-k-1}$. In particular, the number of labeled trees with n vertices is $T(n,1) = n^{n-2}$.*

Proof: We prove by induction on n that the formula $T(n,k) = k\,n^{n-k-1}$ holds for all k satisfying $1 \leqslant k \leqslant n$. For the base case, let $n = 1$. We must show that

$$T(1,k) = k \cdot 1^{1-k-1} \text{ for all } k \text{ satisfying } 1 \leqslant k \leqslant 1.$$

The only such k is $k = 1$. Since $T(1,1) = 1$ and $1 \cdot 1^{1-1-1} = 1$, the base case is true.

Now assume n is an integer, $n \geqslant 1$, and that the statement is true for n. That is,

$$T(n,k) = k\,n^{n-k-1} \text{ holds for all } k \text{ satisfying } 1 \leqslant k \leqslant n. \tag{6.2}$$

We must prove that $T(n+1,k) = k(n+1)^{n+1-k-1} = k(n+1)^{n-k}$ for all k satisfying $1 \leqslant k \leqslant n+1$.

By the recurrence (6.1) we have

$$T(n+1,k) = \sum_{i=0}^{n+1-k} \binom{n+1-k}{i} T(n, k-1+i).$$

We can apply the inductive hypothesis of equation (6.2) to $T(n, k-1+i)$ as long as $1 \leqslant k-1+i \leqslant n$. This holds for all k satisfying $2 \leqslant k \leqslant n$, so we will have to address the $k = 1$ and $k = n+1$ cases separately.

The $k = n+1$ case is easy. Notice that $T(n+1, n+1) = 1$. Also, when $k = n+1$ in the formula we get

$$(n+1)(n+1)^{n+1-(n+1)-1} = (n+1)(n+1)^{-1} = 1,$$

so $T(n+1,k) = k(n+1)^{n+1-k-1} = k(n+1)^{n-k}$ when $k = n+1$. The $k = 1$ case is left to Question 239 after the proof.

The hard case is when k satisfies $2 \leqslant k \leqslant n$. Use equation (6.2) to write

$$\begin{aligned} T(n+1,k) &= \sum_{i=0}^{n+1-k} \binom{n+1-k}{i} T(n, k-1+i) \\ &= \sum_{i=0}^{n+1-k} \binom{n+1-k}{i} (k-1+i) n^{n-(k-1+i)-1} \\ &= \sum_{i=0}^{n+1-k} \binom{n+1-k}{i} (k-1+i) n^{n-k-i}. \end{aligned}$$

Split the sum in two:

$$= \underbrace{\sum_{i=0}^{n+1-k} \binom{n+1-k}{i} (k-1) n^{n-k-i}}_{\text{Sum I}} + \underbrace{\sum_{i=0}^{n+1-k} \binom{n+1-k}{i} i\, n^{n-k-i}}_{\text{Sum II}}.$$

Let's work on Sum I first. Factor out $\frac{k-1}{n}$ and then use the binomial theorem to obtain

$$\begin{aligned} \text{Sum I} &= \frac{k-1}{n} \sum_{i=0}^{n+1-k} \binom{n+1-k}{i} n^{n+1-k-i} \\ &= \frac{k-1}{n} (n+1)^{n+1-k}. \end{aligned}$$

Now work on Sum II. First factor out $n+1-k$ in preparation for using the property $\binom{m}{r}\frac{r}{m} = \binom{m-1}{r-1}$. After that, re-index the sum and use the binomial theorem:

$$\begin{aligned} \text{Sum II} &= (n+1-k) \sum_{i=0}^{n+1-k} \binom{n+1-k}{i} \frac{i}{n+1-k} n^{n-k-i} \\ &= (n+1-k) \sum_{i=0}^{n+1-k} \binom{n-k}{i-1} n^{n-k-i} \\ &= (n+1-k) \sum_{j=0}^{n-k} \binom{n-k}{j} n^{n-k-j-1} \\ &= \frac{n+1-k}{n} \sum_{j=0}^{n-k} \binom{n-k}{j} n^{n-k-j} \\ &= \frac{n+1-k}{n} (n+1)^{n-k}. \end{aligned}$$

Now we can finish it:

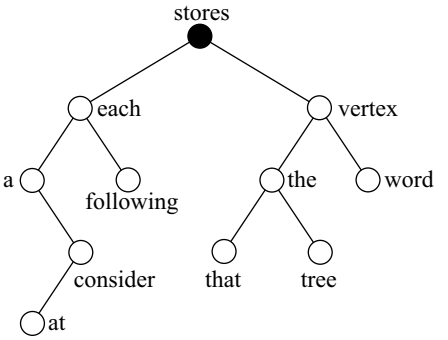
$$\begin{aligned} T(n+1,k) &= \text{Sum I} + \text{Sum II} \\ &= \frac{k-1}{n}(n+1)^{n+1-k} + \frac{n+1-k}{n}(n+1)^{n-k} \\ &= \frac{(n+1)^{n-k}}{n}\Big((k-1)(n+1) + n + 1 - k\Big) \\ &= k(n+1)^{n-k}. \end{aligned}$$

This completes the proof. ■

Question 239 *Prove the $k = 1$ portion of the inductive step. That is, use the inductive hypothesis to prove $T(n+1, 1) = (n+1)^{n-1}$.*

Counting binary trees

Next we turn our attention to the enumeration of a different type of tree. Consider the following tree that stores a word at each vertex.

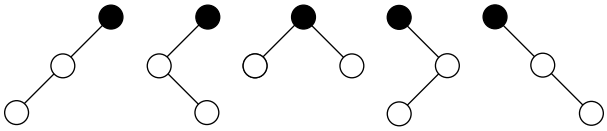


This tree is to be interpreted in a different way than other trees. For one, the way in which it is drawn on the page makes a difference. The black vertex at the top is the ***root***. Each of the vertices below it is a ***child*** of the root. The vertex labeled "each" is the ***left child*** of the root and the vertex labeled "vertex" is the ***right child*** of the root. The vertex labeled "consider" has a left child but no right child. This is an example of a ***rooted binary tree*** or simply ***binary tree***.

Each vertex in a binary tree has a left subtree and a right subtree. The ***left subtree*** of v is the binary tree rooted at the left child of v and containing only the portion of the original tree at or below v. The ***right subtree*** is defined similarly. A subtree can be empty, as the right subtree of the vertex labeled "consider" is. A subtree can also consist of a single vertex, as the left subtree of the vertex labeled "consider" does.

The binary tree shown above is actually being used as a so-called binary search tree. It stores the 11 words in the sentence before the picture of the tree according to the following rule: at every vertex v, the word stored at v comes (1) alphabetically after every word in the left subtree of v, and (2) alphabetically before every word in the right subtree of v. Binary search trees are fundamental and important data structures in computer science. They enable efficient storage, sorting, and searching of data.

Our goal is to determine the number of binary trees on n vertices. Let this number be β_n. Clearly $\beta_1 = 1$ and $\beta_2 = 2$. The binary trees on three vertices are

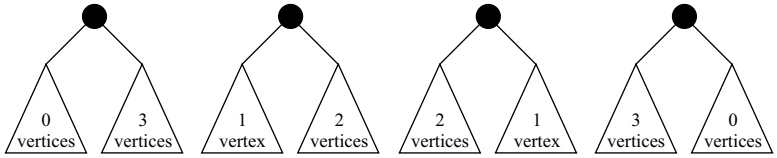


so $\beta_3 = 5$. It will be convenient to define $\beta_0 := 1$. So far we have

n	0	1	2	3	4
β_n	1	1	2	5	?

Question 240 *Determine β_4 by writing out all binary trees on four vertices.*

A binary tree is inherently recursive: the left and right subtrees of the root are themselves binary trees. So, to determine β_n we derive a recurrence relation and then solve it using generating functions. Begin by drawing the root at the top. Now we have two decisions to make: In how many ways can we specify each of the left and right subtrees of the root? For example, to determine β_4 we first place the root and then consider the following four cases depending on how many vertices are in the left subtree of the root:



Notice that if, say, the left subtree has zero vertices then it is empty—there is no left-edge present from the root. The convention $\beta_0 = 1$ takes care of this nicely. By counting each of the four cases and adding their answers we get

$$\begin{aligned}\beta_4 &= \beta_0\beta_3 + \beta_1\beta_2 + \beta_2\beta_1 + \beta_3\beta_0 \\ &= (1)(5) + (1)(2) + (2)(1) + (5)(1) \\ &= 14\end{aligned}$$

so there are 14 binary trees on four vertices.

Question 241 *Determine β_5 using this method.*

In general, the recurrence relation is

$$\begin{aligned}\beta_0 &= 1 \\ \beta_n &= \sum_{i=0}^{n-1} \beta_i \beta_{n-1-i} \qquad \text{for } n \geqslant 1.\end{aligned}$$

This is a nonlinear recurrence relation but we have solved it before. In Section 4.1, we determined the number of ways to triangulate a regular n-gon, where $n \geqslant 3$. This number is

$$T_n = \frac{1}{n-2}\binom{2n-4}{n-1}.$$

The recurrence and the initial conditions for T_n and for β_n are the same but we have to adjust the indices. The correct adjustment is $\beta_n = T_{n+2}$, so we get

$$\beta_n = \frac{1}{(n+2)-2}\binom{2(n+2)-4}{(n+2)-1} = \frac{1}{n}\binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}$$

and therefore we have the following theorem.

Theorem 6.2.9 *For $n \geqslant 1$, he number of binary trees on n vertices is* $\dfrac{1}{n+1}\binom{2n}{n}$.

The number $\frac{1}{n+1}\binom{2n}{n}$ is the famous ***n-th Catalan number***. The Catalan numbers pop up in combinatorial problems about as often as the Fibonacci numbers do.

Question 242 *Based on the work in Section 4.1, show that $\beta_n = T_{n+2}$ is indeed the correct correspondence between the two number sequences $\{T_k\}_{k\geqslant 3}$ and $\{\beta_k\}_{k\geqslant 1}$.*

Summary

A tree is a connected acyclic graph. After deriving some basic properties of trees, we considered two difficult problems concerning their enumeration. In the first, we determined that the number of labeled trees on n vertices is n^{n-2}. This is known as Cayley's formula. In the second, we determined that the number of binary trees on n vertices equals the n-th Catalan number. The techniques we used ranged from bijective proof to recurrence relations and induction to generating functions.

Exercises

1. Prove: a forest with n vertices and k components has $n - k$ edges. Explain how this generalizes Theorem 6.2.3.
2. Improve Theorem 6.2.1 by proving that any tree has at least Δ leaves, where Δ is the maximum degree in the graph.
3. Prove Theorem 6.2.4.
4. Let G be a labeled graph and let e be any edge. A ***spanning tree*** of G is a subgraph of G that is a tree and that contains every vertex of G. Define $\tau(G)$ to be the number of spanning trees of G. Give a combinatorial proof: $\tau(G) = \tau(G - e) + \tau(G \cdot e)$.

   (Here $G \cdot e$, read "G contract e," is the (multi)graph obtained from G by deleting the edge e and then combining the endpoints of e in to one vertex, bringing along all incident edges. See also the description of this operation in Section 6.3.)
5. Use the recurrence of the previous exercise to find the number of spanning trees of the following labeled graphs.

   (a) C_5

   (b) K_4

   (c) $K_n - e$, where e is any edge of K_n
6. (linear algebra) The following result is known as the ***matrix-tree theorem***. Let G be a connected labeled graph with adjacency matrix A. Let $M := D - A$ where D is a diagonal matrix where the degrees of the vertices of G appear on the diagonal. Then the number of spanning trees of G equals the cofactor of any element[2] of M. Use this to find the number of spanning trees of C_5, K_4, K_5, and $K_{3,3}$.
7. Prove that $T(n, n-1) = n - 1$ and $T(n, n-2) = (n-2)n$ by counting the trees involved and not using the formula for $T(n, k)$.
8. Here is another way to prove Cayley's formula. Let $L(n, k)$ denote the number of labeled trees with vertex set $[n]$ and where vertex n has degree k.

   (a) Use properties of multinomial coefficients (see Section 4.1) and Corollary 6.2.7 of this section to prove that $L(n, k) = \binom{n-2}{k-1}(n-1)^{n-k-1}$.

   (b) Derive Cayley's formula by summing $L(n, k)$ over appropriate values of k.

[2]The cofactor of an element in position (i, j) of $\boldsymbol{M}$ is $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting from $\boldsymbol{M}$ the row and column in which the element appears.

9. Let τ_n equal the number of ternary trees on n vertices, for $n \geqslant 0$. A ***ternary tree*** is similar to a binary tree but each vertex can have a left, middle, and right child. Set $\tau_0 := 1$.
   (a) Verify that $\tau_1 = 1$, $\tau_2 = 3$, and $\tau_3 = 12$, by drawing the possible trees.
   (b) Determine τ_4 via a recurrence relation. Then derive a recurrence relation for τ_n.
   (c) Let $T(x)$ be the OGF of $\{\tau_n\}_{n\geqslant 0}$. Prove that $T(x) = x\big(T(x)\big)^3 + 1$. Comment on the prospect of finding a formula for τ_n like that of Theorem 6.2.9.

Travel Notes

Arthur Cayley (1821–1895) is perhaps better known for his work in algebra. Many of the known proofs of Cayley's formula are discussed in Moon (1967) but still more have been discovered since then.

Recursion is a central theme in computer science so it is natural that a recursive structure like a binary tree can be counted using a recurrence relation. The field of data structures —essentially the study of the storage and manipulation of data in a computer—has generated numerous combinatorial problems on graphs. Perhaps the best reference for the mathematics of algorithms and data structures is the book by Cormen, Leiserson & Rivest (1990).

6.3 Coloring and the chromatic polynomial

We now turn to the problem of coloring the vertices of a graph which, at least initially, appears to have nothing to do with counting. Given a graph, the goal of the coloring problem is to determine the fewest number of colors necessary so that each vertex of the graph can be assigned a color in such a way that adjacent vertices receive different colors. The coloring problem is therefore an optimization problem.

Figure 6.7 shows two (unlabeled) graphs that have been colored. The colors are a, b, c in the graph G on the left and the colors are a, b, c, d, e in the graph H on the right. For G, it is not possible to use fewer colors for if only two colors were available then we would be forced to assign the same color to adjacent vertices.

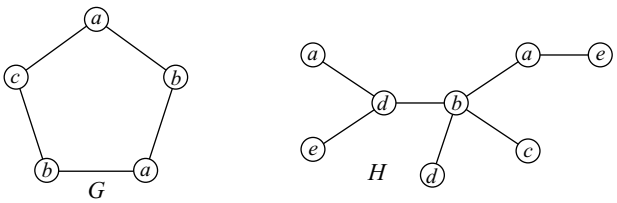


Figure 6.7. Proper colorings of some graphs.

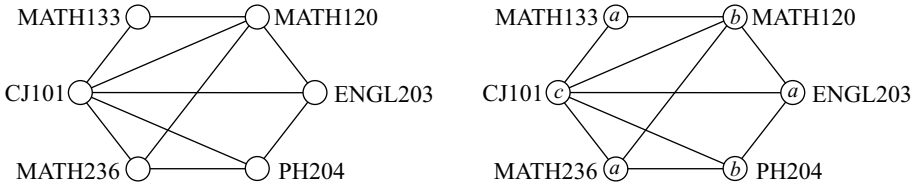
Question 243 *Can the graph H on the right be colored with fewer colors? Find the fewest number required and show how to color it with that many colors.*

Applications of coloring

"Coloring" may sound juvenile but it has many applications. Here are two.

Scheduling

A college must schedule final exams so that no student has two exams scheduled at the same time. On the left in the figure below is a graph representing a small portion of the schedule. Each course gets a vertex, and two courses are joined by an edge whenever there is at least one student enrolled in both courses. (This is an example of what is sometimes called a "conflict graph.")



On the right is a coloring of the vertices (courses) using three colors a, b, c. No two adjacent vertices receive the same color. In the context of the scheduling problem, the colors correspond to time slots. This means that we can schedule, say, the MATH133, ENGL203, and MATH236 finals from 8–10 A.M., the MATH120 and PH204 finals from 10:15 A.M.–12:15 P.M., and the CJ101 final from 1–3 P.M., and no student will have two exams scheduled in the same slot.

Question 244 *Is it possible to schedule the exams using only two time slots? Justify.*

A small problem like the one above is easy enough but it becomes much more difficult when hundreds of courses are involved.

Map coloring

Get a map of the lower 48 states and color each state in such a way that no states sharing a border receive the same color. (States like Arizona and Colorado meet at a corner but do not share a border.) How many colors do you need? The answer is four. In addition it is true that four is the maximum number of colors necessary for any map of countries, states, counties, etc., no matter how convoluted.[3]

This problem—known as the four-color problem—was posed as a mathematical problem in the late 1800s. After several incorrect proofs (including one which was believed to be correct for a 10-year period) it was finally proved in 1976 by Appel & Haken and is now known as the four-color theorem.

Colorings, proper colorings, and chromatic number

We first explain some of the terminology of coloring. A ***coloring*** of a graph is simply an assignment of colors to the vertices of the graph, one color per vertex. In a coloring there is no requirement that adjacent vertices receive different colors. A coloring that uses k different colors is a ***k-coloring***.

A ***proper coloring*** is a coloring in which adjacent vertices receive different colors. Equivalently, a proper coloring is a coloring in which no edge has both endpoints the same color. A ***proper k-coloring*** is a proper coloring that uses k different colors. If a graph has a proper k-coloring then we say the graph is ***k-colorable***. Please note the distinction between

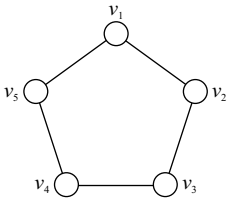
[3] Almost. Any country/state/county must be one contiguous region. Such maps are called "planar maps."

k-coloring and k-colorable. The latter involves a proper coloring while the former does not necessarily.

Both of the colorings shown in Figure 6.7 are proper colorings. The coloring of G is a proper 3-coloring and the coloring of H is a proper 5-coloring. In other words, these colorings show that G is 3-colorable and that H is 5-colorable. Our main interest in this section is in the smallest value of k for which the graph is k-colorable.

Definition 6.3.1 *For any graph G the **chromatic number of** G, denoted by $\chi(G)$, is the smallest positive integer k for which G is k-colorable. That is, $\chi(G)$ is the smallest positive integer k for which it is possible to color the vertices of G using k colors in such a way that no edge has both endpoints the same color.*

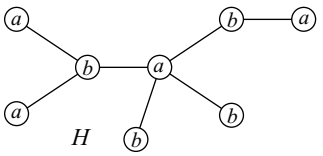
Any proof that $\chi(G) = k$ must involve two things, namely (1) a proper k-coloring of G, and (2) a proof that no proper $(k-1)$-coloring of G is possible. We already argued informally that the 5-cycle has chromatic number 3, after discussing graph G of Figure 6.7. Here is a formal proof that $\chi(C_5) = 3$. First we observe that the coloring of Figure 6.7 is a proper 3-coloring, so C_5 is 3-colorable. Now, assume for sake of contradiction that C_5 were 2-colorable. Then there would exist a proper 2-coloring of C_5. Label the vertices as shown below.



Without loss of generality, assume v_1 is colored blue. Then v_2 must be colored red, then v_3 colored blue, then v_4 colored red, and v_5 colored blue. So this means the adjacent vertices v_1 and v_5 are both colored blue, a contradiction. This proves that no proper 2-coloring of C_5 exists so therefore $\chi(C_5) = 3$.

Question 245 *Find the chromatic number of the (disconnected) graph consisting of a 5-cycle and a 4-cycle. In general, if G is disconnected, then what is the relationship between $\chi(G)$ and the chromatic numbers of its components?*

We next show $\chi(H) = 2$, where H is the tree of Figure 6.7, by the same method. Here is a proper 2-coloring of H:



This shows that H is 2-colorable. Is H 1-colorable? No, because any graph with at least one edge cannot be properly 1-colored. Therefore $\chi(H) = 2$.

Basic properties of chromatic number

Before investigating more complicated examples we now present some properties of $\chi(G)$.

Proposition 6.3.2 *The chromatic number satisfies the following properties. Let G be any graph.*

1. $\chi(G) = 1$ *if and only if* G *has no edges, so that* $\chi(G) \geq 2$ *if and only if* G *has at least one edge.*
2. $\chi(G) = 2$ *if and only if* G *has at least one edge and is bipartite.*
3. $\chi(K_n) = n$.
4. *If* $n \geq 3$, *then* $\chi(C_n) = \begin{cases} 2 & \text{if } n \text{ is even} \\ 3 & \text{if } n \text{ is odd.} \end{cases}$
5. *If* H *is a subgraph of* G, *then* $\chi(G) \geq \chi(H)$.

Most of these properties follow immediately from the definition of chromatic number. Property 2 is true because we can color the vertices in one side of the bipartition red and the vertices on the other side blue. Property 3 is true because every pair of vertices are adjacent in K_n, so it is not possible to have two vertices with the same color. For Property 4, the case when n is even follows from Property 2. The case when n is odd follows by generalizing the argument we used to prove that $\chi(C_5) = 3$ given earlier. Property 5 is perhaps the most useful of those listed.

Question 246 *Prove Property 5.*

Another example

Find the chromatic number of the graph G shown in Figure 6.8.

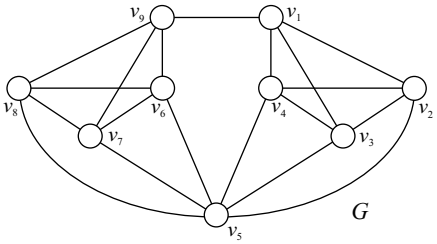


Figure 6.8. What is the chromatic number of this graph?

First we notice that K_4 is a subgraph of G, so $\chi(G) \geq 4$ by Properties 3 and 5. Is this graph 4-colorable? Let's assume a proper 4-coloring exists and try to find it.

- Since v_1, v_2, v_3, v_4 form a K_4 subgraph, they must receive different colors. Without loss of generality, assume that they are colored a, b, c, d respectively.
- v_5 is adjacent to v_2, v_3, v_4, so v_5 must be colored a.
- Neither of v_6, v_7, v_8 can be colored a because they are adjacent to v_5 which is colored a. In addition, these three vertices are mutually adjacent, so they must all receive different colors. This means that among v_6, v_7, v_8 each of the three colors b, c, d is used.
- We only have v_9 left to color, but its neighbors have been colored a, b, c, d. There is no color left for v_9.

Therefore G is not 4-colorable.

However, G is 5-colorable because our proof just given shows that if there is a fifth color available then we can color v_9 with that color and obtain a proper 5-coloring of G. Therefore $\chi(G) = 5$.

The chromatic polynomial

The arguments used to find the chromatic number of the graphs we've considered so far have an *ad hoc* flavor. Can we find a chromatic number by a more systematic procedure? Yes and no. Yes because there are such procedures that can be programmed into a computer, and no because even the computer will have a difficult time with somewhat large graphs.

One approach involves solving a problem larger than just finding the chromatic number, namely counting the proper k-colorings of the graph. Given a graph G, we define

$$p(G,k) = \text{number of proper } k\text{-colorings of } G.$$

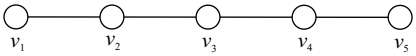
This is the ***chromatic polynomial of*** G**.** It is not at all clear *a priori* that this is indeed a polynomial; perhaps it should be called a "chromatic function." Anyway, we'll prove later that it's a polynomial.

Since $p(G,k)$ counts the proper k-colorings of G, we see that $\chi(G)$ is the smallest value of k for which $p(G,k) \neq 0$. This is because if G is not k-colorable, then $p(G,k) = 0$.

Question 247 *Find $\chi(G)$ for a graph G having $p(G,k) = (k-1)^7 - k + 1$.*

Example: chromatic polynomial of P_5

Consider P_5, the path on five vertices:



To properly k-color P_5, we may color v_1 with any of the k colors. For each way to do so, there are $k-1$ ways to color v_2, since v_2 can receive any color except v_1's. For each way to color v_1 and v_2, there are $k-1$ ways to color v_3, since v_3 can receive any color except v_2's. Similarly there are $k-1$ ways to color each of v_4 and v_5. By the product principle there are $k(k-1)^4$ proper k-colorings of P_5. That is,

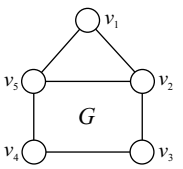
$$p(P_5,k) = k(k-1)^4 \qquad \text{or} \qquad p(P_5,k) = k^5 - 4k^4 + 6k^3 - 4k^2 + k.$$

Either way to write the chromatic polynomial (factored form or expanded form) is fine and each has its advantages. The factored form makes it clear that $\chi(P_5) = 2$ because $p(P_5,1) = 0$ while $p(P_5,2) > 0$. The expanded form exhibits certain information about the graph which we will explain later in this section.

Question 248 *To extend Question 245, find the chromatic polynomial of the (disconnected) graph $P_4 \cup P_5$. In general, if G is disconnected, then what is the relationship between $p(G,k)$ and the chromatic polynomials of its components?*

Example: chromatic polynomial of another graph

Find the chromatic polynomial of the graph G shown below:



First observe that v_1, v_2, v_5 must receive different colors since they form a K_3 subgraph. There are k ways to color v_1, then $k-1$ ways to color v_2, and then $k-2$ ways to color v_5. To determine how many ways we can color v_3 and v_4, we break up the proper colorings into two cases.

- **Case 1:** v_3 and v_5 have the same color. Since v_5's color (and therefore v_3's) is already specified, we need only specify v_4's color. Its neighbors v_3 and v_5 have the same color, so there are $k-1$ ways to color v_4. In this case there are $k(k-1)(k-2)(k-1) = k(k-1)^2(k-2)$ proper k-colorings of G.
- **Case 2:** v_3 and v_5 have different colors. Then there are $k-2$ ways to specify v_3's color since it must be different from both v_2's and v_5's color. There are $k-2$ ways to specify v_4's color (any color except v_3's or v_5's, for a total of $k(k-1)(k-2)(k-2)(k-2) = k(k-1)(k-2)^3$ proper k-colorings in this case.

By the sum principle the chromatic polynomial of G is

$$p(G,k) = k(k-1)^2(k-2) + k(k-1)(k-2)^3.$$

Therefore $\chi(G) = 3$ because $p(G,1) = 0$ and $p(G,2) = 0$ while $p(G,3) = 18$.

Question 249 *Give a complete enumeration of the 18 proper 3-colorings of G.*

Chromatic polynomial of paths and complete graphs

It is easy to find the chromatic polynomial of the path P_n and the complete graph K_n because their structure makes proper k-colorings easy to count. As you might have guessed based on our derivation of $p(P_5,k)$, the chromatic polynomial of P_n is $k(k-1)^{n-1}$.

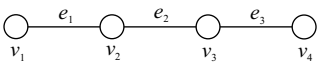
Question 250 *Find $p(K_n,k)$.*

Inclusion-exclusion

Now we explore some ways to find the chromatic polynomial other than the direct counting methods of the last two examples. First we try inclusion-exclusion. This is perhaps a natural choice because finding a proper coloring is naturally a "pattern avoidance" problem: we need to avoid the presence of any edge having both endpoints the same color.

Example: chromatic polynomial via inclusion-exclusion

Consider P_4 with both its vertices and edges labeled:



To use inclusion-exclusion to count the proper k-colorings of P_4, first define the universe $\mathcal{U}$ to be the set of all k-colorings of P_4. Here it is paramount to notice that these are *not necessarily proper colorings*. Define the properties

$$\varepsilon_1 := \text{"edge } e_1 \text{ has both endpoints the same color"}$$
$$\varepsilon_2 := \text{"edge } e_2 \text{ has both endpoints the same color"}$$
$$\varepsilon_3 := \text{"edge } e_3 \text{ has both endpoints the same color."}$$

Then $p(P_4,k) = N_=(\emptyset)$ because the latter equals the number of k-colorings in which no edge has both endpoints the same color—the proper k-colorings of P_4.

Here are the values of the $N_{\geqslant}$ function:

$$\begin{array}{llll} N_{\geqslant}(\emptyset) & = k^4 & N_{\geqslant}(\varepsilon_1\varepsilon_2) & = k^2 \\ N_{\geqslant}(\varepsilon_1) & = k^3 & N_{\geqslant}(\varepsilon_1\varepsilon_3) & = k^2 \\ N_{\geqslant}(\varepsilon_2) & = k^3 & N_{\geqslant}(\varepsilon_2\varepsilon_3) & = k^2 \\ N_{\geqslant}(\varepsilon_3) & = k^3 & N_{\geqslant}(\varepsilon_1\varepsilon_2\varepsilon_3) & = k. \end{array}$$

For example, $N_{\geqslant}(\emptyset) = k^4$ because each of the four vertices can be colored with any of the four colors.

Question 251 *Justify the other values.*

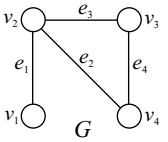
By the inclusion-exclusion formula,

$$\begin{aligned} p(P_4, k) &= k^4 - (k^3 + k^3 + k^3) + (k^2 + k^2 + k^2) - k \\ &= k^4 - 3k^3 + 3k^2 - k. \end{aligned}$$

This can also be written $p(P_4, k) = k(k-1)^3$.

Example: another chromatic polynomial via inclusion-exclusion

Next consider the graph G shown below.



Define the universe $\mathcal{U}$ to be the set of all (not necessarily proper) k-colorings of G. Define the properties

$$\varepsilon_i := \text{“edge } e_i \text{ has both endpoints the same color,”} \qquad \text{for } i = 1, 2, 3, 4.$$

Then $p(G, k) = N_{=}(\emptyset)$ as before. We compute

$$\begin{array}{llll} N_{\geqslant}(\emptyset) & = k^4 & N_{\geqslant}(\varepsilon_1\varepsilon_2) = k^2 & N_{\geqslant}(\varepsilon_1\varepsilon_2\varepsilon_3) & = k \\ N_{\geqslant}(\varepsilon_1) & = k^3 & N_{\geqslant}(\varepsilon_1\varepsilon_3) = k^2 & N_{\geqslant}(\varepsilon_1\varepsilon_2\varepsilon_4) & = k \\ N_{\geqslant}(\varepsilon_2) & = k^3 & N_{\geqslant}(\varepsilon_1\varepsilon_4) = k^2 & N_{\geqslant}(\varepsilon_1\varepsilon_3\varepsilon_4) & = k \\ N_{\geqslant}(\varepsilon_3) & = k^3 & N_{\geqslant}(\varepsilon_2\varepsilon_3) = k^2 & N_{\geqslant}(\varepsilon_2\varepsilon_3\varepsilon_4) & = k^2 \\ N_{\geqslant}(\varepsilon_4) & = k^3 & N_{\geqslant}(\varepsilon_2\varepsilon_4) = k^2 & N_{\geqslant}(\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4) & = k. \\ & & N_{\geqslant}(\varepsilon_3\varepsilon_4) = k^2 & & \end{array}$$

Notice that $N_{\geqslant}(\varepsilon_1\varepsilon_2\varepsilon_3) = k$ because if e_1, e_2, e_3 all have the same color endpoints, then all four vertices in G must be colored the same color. However, $N_{\geqslant}(\varepsilon_2\varepsilon_3\varepsilon_4) = k^2$ because if e_2, e_3, e_4 all have the same color endpoints then vertices v_2, v_3, v_4 must be colored the same color. There are k ways to specify this color, and then k ways to specify v_1's color.

Anyway, by the inclusion-exclusion formula the chromatic polynomial of G is

$$p(G, k) = k^4 - 4k^3 + 6k^2 - 3k - k^2 + k = k^4 - 4k^3 + 5k^2 - 2k.$$

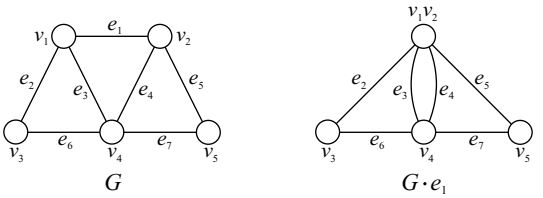
Question 252 *Find $p(C_4, k)$ using this method.*

A recurrence for the chromatic polynomial

The inclusion-exclusion approach requires one property for each edge and therefore the computation of $2^{e(G)}$ values of the $N_{\geqslant}$ function. Even though each value of $N_{\geqslant}$ is easy to compute, this is not a viable approach for a 50-vertex graph, even for a computer, since $2^{50} \approx 1.1$ quadrillion. Our next approach is recursive.

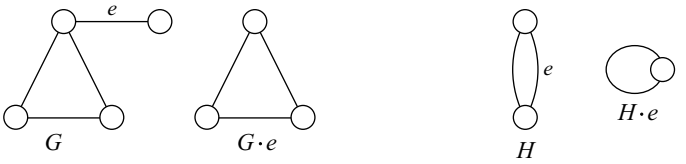
Contracting an edge

The graph operation we need to derive the recurrence relation is that of edge contraction. Here is a picture:



The original graph G is on the left and the graph $G \cdot e_1$, read "G contract e_1," is on the right. To construct $G \cdot e_1$, we delete e_1, combine the two endpoints of e_1 into a single vertex, and bring along any incident edges. Notice that $G \cdot e_1$ is not a simple graph because of the presence of multiple edges.

Here are two other examples, this time involving unlabeled graphs.



Notice that contracting an edge that is part of a set of multiple edges results in a loop.

Question 253 *If e is any edge of C_9, then what is $C_9 \cdot e$? Answer the same question for $K_6 \cdot e$.*

The recurrence

The recurrence for the chromatic polynomial involves the chromatic polynomial of the original graph as well as those of the graph obtained by deleting any one edge and the graph obtained by contracting along that same edge.

Theorem 6.3.3 *If G is a graph and e is any edge of G, then*

$$p(G,k) = p(G-e,k) - p(G \cdot e,k).$$

Proof: Assume G is a graph and e is any edge of G. We instead prove the equivalent identity

$$p(G-e,k) = p(G,k) + p(G \cdot e,k).$$

Let u and v be the endpoints of the edge e in G. How many proper k-colorings does $G-e$ have?

Answer 1: It has $p(G-e,k)$ proper k-colorings.

Answer 2: Divide the proper k-colorings of $G-e$ into two types: those in which u and v receive different colors, and those in which u and v receive the same color.

For any proper k-coloring of $G-e$ in which u and v receive different colors, reinstating the edge e results in a proper k-coloring of G. Conversely, if we take any proper k-coloring of G and delete the edge e, the result is a proper k-coloring of $G-e$ in which u and v receive different colors (since $u \sim v$ in G and therefore u and v received different colors). Therefore the colorings in this case are in one-to-one correspondence with the proper k-colorings of G, of which there are $p(G,k)$.

For any proper k-coloring of $G-e$ in which u and v receive the same color, that same coloring is a proper k-coloring of $G \cdot e$ and conversely. Therefore the colorings in this case are in one-to-one correspondence with the proper k-colorings of $G \cdot e$, of which there are $p(G \cdot e, k)$.

Therefore there are $p(G,k) + p(G \cdot e, k)$ proper k-colorings of $G-e$. ■

When using the recurrence to compute the chromatic polynomial, if at any time we create a graph with the contraction operation that has multiple edges between a pair of vertices, then we may safely delete all but one of those edges (for each such pair of vertices).

Question 254 *Explain why.*

If we delete multiple edges at each stage then the contraction operation will never produce a loop. But if do not delete multiple edges and encounter a loop at some point of the recurrence, then we just set $p(G,k) = 0$ if G is a graph containing a loop. This is because a vertex with a loop is adjacent to itself and so the graph cannot be properly colored with any number of colors.

Example: the chromatic polynomial of C_4

To get the chromatic polynomial of C_4, we select any edge and compute

$$p(C_4,k) = p(C_4 - e, k) - p(C_4 \cdot e, k).$$

Notice that $C_4 - e = P_4$, the path on four vertices, and $C_4 \cdot e = C_3$. We observe that $p(C_3,k) = k(k-1)(k-2)$ and therefore

$$\begin{aligned} p(C_4,k) &= p(P_4,k) - p(C_3,k) \\ &= k(k-1)^3 - k(k-1)(k-2). \end{aligned}$$

Question 255 *Find $p(C_5,k)$ and $p(C_6,k)$ using this method.*

Example: the chromatic polynomial of C_n

The pattern of the last example could be continued to find $p(C_n,k)$ but we now show an alternate derivation using Theorem 6.3.3 and induction. We wish to establish

$$p(C_n,k) = (k-1)^n + (-1)^n(k-1) \qquad \text{for } n \geqslant 3.$$

Consider the base case $n = 3$. We know $p(C_3,k) = k(k-1)(k-2)$. The right-hand side of the identity equals

$$\begin{aligned} (k-1)^3 + (-1)^3(k-1) &= k^3 - 3k^2 + 3k - 1 - k + 1 \\ &= k^3 - 3k^2 + 2k \\ &= k(k-1)(k-2), \end{aligned}$$

so it is true when $n = 3$.

Now assume $n \geqslant 4$ and that the identity is true for C_{n-1}. Use Theorem 6.3.3 to write

$$p(C_n, k) = p(C_n - e, k) - p(C_n \cdot e, k).$$

Since $C_n - e = P_n$ and $C_n \cdot e = C_{n-1}$, we can use the chromatic polynomial of P_n and the inductive hypothesis, respectively, to write

$$\begin{aligned} p(C_n, k) &= k(k-1)^{n-1} - \Big((k-1)^{n-1} + (-1)^{n-1}(k-1)\Big) \\ &= k(k-1)^{n-1} - (k-1)^{n-1} + (-1)^n(k-1) \\ &= (k-1)^n + (-1)^n(k-1). \end{aligned}$$

Therefore the identity is true for C_n.

Theorem 6.3.4 *For $n \geqslant 3$, $p(C_n, k) = (k-1)^n + (-1)^n(k-1)$.*

Properties of the chromatic polynomial

The recurrence we just derived, while cumbersome to use on arbitrary graphs, is good for finding the chromatic polynomial of highly-structured graphs. It is also useful for proving general properties of the chromatic polynomial using mathematical induction.

Theorem 6.3.5 *If G is a graph, then the function $p(G, k)$ satisfies the following properties.*

CP1: $p(G, k)$ is a polynomial of degree $n(G)$ having leading coefficient 1 and constant coefficient 0.

CP2: The coefficient of k^{n-1} in $p(G, k)$ is $-e(G)$.

CP3: The coefficients of $p(G, k)$ are alternately nonnegative and nonpositive.

CP4: If $e(G) \geqslant 1$, then the sum of the coefficients of $p(G, k)$ equals 0.

Proof: Assume G is a graph. We first prove properties CP1-CP3 by induction on $e(G)$, the number of edges of G.

The base case is $e(G) = 0$. A graph with zero edges consists of $n(G)$ isolated vertices. The chromatic polynomial of such a graph is $p(G, k) = k^{n(G)}$. Properties CP1-CP3 are true in this case.

Now let G be a graph having $e(G)$ edges, where $e(G) \geqslant 1$, and assume that Properties CP1-CP3 are true for any graph on $e(G) - 1$ edges. Let e be any edge of G. By Theorem 6.3.3,

$$p(G, k) = p(G - e, k) - p(G \cdot e, k).$$

Since $G - e$ and $G \cdot e$ are each graphs with $e(G) - 1$ edges, we apply the inductive hypothesis to their chromatic polynomials. Let $n := n(G)$ so that $n(G - e) = n$ and that $n(G \cdot e) = n - 1$. Write the chromatic polynomials as

$$p(G - e, k) = k^n - \big(e(G) - 1\big)k^{n-1} + \sum_{i=1}^{n-2} (-1)^{n-i} a_i k^i$$

where $a_i \geqslant 0$ for all $i \in [n-2]$, and

$$p(G \cdot e, k) = k^{n-1} - \big(e(G) - 1\big)k^{n-2} + \sum_{j=1}^{n-3} (-1)^{n-1-j} b_j k^j$$

where $b_j \geqslant 0$ for all $j \in [n-3]$. Then

$$\begin{aligned} p(G,k) &= p(G-e,k) - p(G\cdot e,k) \\ &= k^n - e(G)k^{n-1} + \big(a_{n-2} + e(G) - 1\big)k^{n-2} \\ &\quad + \sum_{i=1}^{n-3} (-1)^{n-i}(a_i + b_i)k^i. \end{aligned}$$

This is a polynomial, it has degree $n = n(G)$, leading coefficient 1, and constant coefficient 0. The coefficient of k^{n-1} is $-e(G)$. Also, the coefficients are alternately nonnegative and nonpositive. The coefficient of k^n is 1 and the coefficient of k^{n-1} is $-e(G) \leqslant 0$. The coefficient of k^{n-2} is $a_{n-2} + e(G) - 1$ and this is nonnegative because $a_{n-2} \geqslant 0$ and $e(G) - 1 \geqslant 0$. The remaining coefficients are of the form $(-1)^{n-i}(a_i + b_i)$, and noting that $a_i + b_i \geqslant 0$ and the presence of the factor of $(-1)^{n-i}$ shows that the remaining coefficients alternate as well. Therefore $p(G,k)$ satisfies Properties CP1–CP3.

To prove Property CP4, assume that G has at least one edge. Then $p(G,1) = 0$ because G is not 1-colorable. Evaluating a polynomial function at 1 gives the sum of the coefficients. Therefore the sum of the coefficients of $p(G,k)$ is 0. ■

Question 256 *Can $k^5 - 6k^4 + 3k^3 - 10k^2 + k - 3$ be the chromatic polynomial of some graph? Can $k^4 - 4k^3 + 3k^2 - k$?*

See Exercise 14 for a stronger version of Property CP3.

Summary

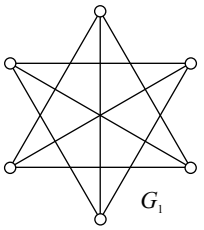
The chromatic number $\chi(G)$ of a graph G equals the minimum number of colors required to properly color the vertices. A proper coloring of the vertices is an assignment of colors to vertices so that adjacent vertices receive different colors. Any proof that $\chi(G) = k$ requires demonstrating a proper k-coloring of G as well as a proof that no proper $(k-1)$-coloring exists.

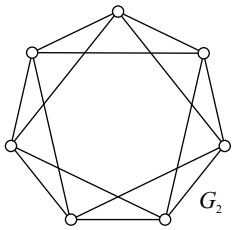
Coloring is an optimization problem. We turned it into a counting problem via the chromatic polynomial. The chromatic number is difficult to compute in general as our efforts in this section show. Both the inclusion-exclusion approach and the recurrence relation approach are intractable for even moderately large graphs unless the graph is highly structured like K_n, C_n, or P_n.

Exercises

1. Print a map of the lower 48 states from a web site and then color it using four colors. Also, include a proof of why four colors are necessary to color this map.
2. If T is a tree, then what is $\chi(T)$?
3. Prove that $\chi(G) \leqslant \Delta(G) + 1$, where $\Delta(G)$ is the maximum degree of G.
4. Determine, with proof, $\chi(W_n)$. Here, the graph W_n is the "wheel" consisting of a cycle C_n as well as one additional vertex that is adjacent to every vertex on the cycle. (So W_n has $n+1$ vertices.)
5. Determine, with proof, the chromatic number of the Petersen graph and of the Grötsch graph, which are shown in Figure 6.3 on page 229.

6. Determine, with proof, the chromatic numbers of the graphs below:





7. Find $\chi(G)$ given that $p(G,k) = k^6 - 9k^5 + 31k^4 - 51k^3 + 40k^2 - 12k$. Also, how many vertices and edges does G have?

8. Define $\omega(G)$, called the ***clique number of*** G, to be the largest integer r such that G contains K_r as a subgraph.

   (a) Find an equation or inequality relating $\omega(G)$ and $\chi(G)$.

   (b) Give an example of a graph G for which $\omega(G) = 2$ and $\chi(G) = 3$.

   (c) Give an example of a graph G for which $\omega(G) = 2$ and $\chi(G) = 4$.

9. Determine the chromatic polynomial of each of the following graphs.

   (a) the star $K_{1,n}$

   (b) $K_{2,n}$

   (c) $C_3 \cup P_4 \cup K_5$

10. Find the chromatic polynomial of the graph that consists of C_5 plus one additional vertex that is adjacent to exactly one of the vertices of C_5.

11. Find $p(K_n - e, k)$ where e is any edge of K_n.

12. How many roots does $p(G,k)$ have, at least? Come up with a reasonable lower bound.

13. Relate the coefficients of $p(K_n, k)$ to a family of numbers studied elsewhere in this book.

14. The coefficients of the chromatic polynomial of a graph G start $1, -e(G)$. Prove that they continue alternating positive/negative until at some point they reach 0 and stay 0. In other words, any chromatic polynomial can be written in the form $p(G,k) = \sum_{i=m}^{n} (-1)^{n-i} a_i k^i$ where m is an integer satisfying $1 \leqslant m \leqslant n$ and $a_i > 0$ for all i satisfying $m \leqslant i \leqslant n$.

15. In the chromatic polynomial of a graph G, prove that if k^m is the smallest power of k that has a nonzero coefficient, then G has m components.

16. This exercise concerns a characterization of the chromatic polynomial of a tree.

   (a) Prove by induction: if T is a tree on n vertices, then $p(T,k) = k(k-1)^{n-1}$.

   (b) Prove: if G is a graph and $p(G,k) = k(k-1)^{n-1}$, then G is a tree.

   (c) How many labeled graphs have chromatic polynomial equal to $k(k-1)^{50}$?

Travel Notes

Kenneth Appel and Wolfgang Haken's proof of the four-color theorem used a computer to check a large number of cases (so-called "reducible configurations") and therefore was enumerative in nature. Their 1976 result settled a problem that stood for well over 100 years, but it was met with skepticism by some mathematicians who reacted negatively to the use of a computer in a proof. The original published paper Appel & Haken (1977) is 139 pages. More recently, Robertson, Sanders, Seymour & Thomas (1996) announced a new proof of the four-color theorem that uses the same general idea of Appel & Haken but avoids some of the technicalities they encountered.

Chromatic polynomials were introduced by Birkhoff in 1912 as a possible approach to proving the four-color theorem. That approach did not pan out, but they were further explored in Birkhoff & Lewis (1946).

6.4 Ramsey theory

To understand how non-mathematicians sometimes view the work of mathematicians, look no farther than this letter to Ann Landers that appeared in *The Washington Post* on June 22, 1993.

> **DEAR ANN LANDERS:** I am sure many members of Congress read your column. I hope they will see this, because it's the best way I can think of to get their attention.
>
> I am enclosing an article from the *Rochester Democrat & Chronicle* so you will know I am not making this up.
>
> Two professors, one from Rochester, the other from Australia, have worked for three years, used 110 computers and communicated 10,000 miles by electronic mail, and finally have learned the answer to a question that has baffled scientists for 63 years. The question is this: If you are having a party and want to invite at least four people who know each other and five who don't, how many people should you invite? The answer is 25. Mathematicians and scientists in countries worldwide have sent messages of congratulations.
>
> I don't want to take anything away from this spectacular achievement, but it seems to me that the time and money spent on this project could have been better used had they put it toward finding ways to get food to the millions of starving children in war-torn countries around the world.—B.V.B., Rochester, N.Y.

Unfortunately, the letter-writer stated the question incorrectly in their third paragraph. The correct version is: If you are having a party and want to *guarantee* that no matter who you invite there will either be four people who all know each other or five people who all don't know each other, then what is the least number of people you must invite?

But the bigger issue as implied by the letter-writer's sarcasm is, Should we care? Here are two reasons to say "yes," both involving the 17th century mathematician Pierre de Fermat. First, a particular piece of theory may not prove its worth in applications until long after its discovery. Exhibit A in support of this is Fermat's little theorem of 1640, which Rivest, Shamir, & Adelman famously employed in 1978 to devise a method for secure digital communication now known as RSA encryption. Fermat could not have anticipated this application.

Second, the journey of solving a difficult mathematical problem is often more important than the end result. Exhibit B is Fermat's last theorem, the truth of which has not yet led to any earth-shaking applications. But the 350-year journey from first statement by Fermat

to final proof by Andrew Wiles in 1995 produced so much deep, powerful, and applicable mathematics that these by-products have eclipsed the theorem itself.

In this section we study the sort of problems to which the Ann Landers letter-writer referred. This is the field of graph Ramsey theory, a notoriously difficult area of combinatorics where the questions are easy to explain but the answers are hard to find.

Party problems, edge coloring, and Ramsey problems

The following question about people at a party is known as the

(3, 3) **Party problem:** What is the fewest number of people you can invite to a party to guarantee that there are either three mutual acquaintances or three mutual strangers?

"Three mutual acquaintances" means that any two people in that group of three have met, and "three mutual strangers" means that no two people in that group of three have met. Now here is a question about coloring the edges of a graph.

(3, 3) **Ramsey problem:** What is the smallest value of n so that every red-blue coloring of the edges of K_n contains either an all-red K_3 subgraph or an all-blue K_3 subgraph?

A "red-blue coloring of the edges" means that every edge is painted either red or blue.

These two problems are equivalent: identify the vertices of K_n with the invited guests and then connect each pair of guests with either a red or blue edge according to whether they are acquainted or not acquainted, respectively. We shall work with edge coloring from now on. Also, we'll use the abbreviations "red-blue coloring of K_n" and "red K_3" with the understanding that we're referring to coloring the edges.

The problem spoken of at the beginning of this section is the

(4, 5) **Ramsey problem:** What is the smallest value of n so that every red-blue coloring of K_n contains either a red K_4 or a blue K_5?

As mentioned in the letter, the answer to this problem is 25. This means two things: (1) every possible red-blue coloring of the edges of K_{25} will produce either an all-red K_4 or an all-blue K_5 or perhaps both; and (2), there is an example of a red-blue coloring of the edges of K_{24} that contains neither an all-red K_4 nor an all-blue K_5.

The graph coloring problems are called Ramsey problems because they fit into the more general framework of a theorem proved by Frank Ramsey in 1930. Loosely speaking Ramsey's theorem says that

- in a large structure
  (in the (4, 5) Ramsey problem this structure is K_{25})
- that is constructed randomly
  (each edge of K_{25} is colored red or blue in any manner),
- there is a non-random substructure
  (an all-red K_4 or an all-blue K_5).

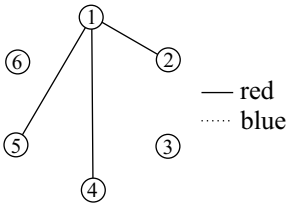
T. S. Motzkin's famous quote—"Complete disorder is impossible"—is often used to describe Ramsey theory.

The easiest Ramsey problem

The $(3,3)$ Ramsey problem asks for the smallest value of n guaranteeing that every red-blue coloring of K_n contains either a red K_3 or a blue K_3. The answer is six. This requires showing two things.

1. Every red-blue coloring of K_6 contains a red K_3 or a blue K_3.
2. There exists an example of a red-blue coloring of K_5 that contains neither a red K_3 nor a blue K_3.

To prove #1, suppose the vertex set is [6]. The first step of the proof is the most important. Of the five edges incident to vertex 1, there must be three of the same color. Without loss of generality, say that edges 12, 14, and 15 are red:



Now examine the edges among vertices 2, 4, and 5. If any one of them is red, we have found our red K_3. For example, if edge 25 is red then edges 12, 15, and 25 form a red K_3. Otherwise all three of them are blue and therefore edges 24, 25, and 45 form a blue K_3. This exhausts the cases and completes the proof.

To prove #2, we need to exhibit a red-blue coloring of K_5 having neither a red K_3 nor a blue K_3.

Question 257 *Give an example of such a coloring of* K_5.

Ramsey arrow notation

Let $R(a,b)$ denote the answer to the

(a,b) **Ramsey problem:** What is the smallest value of n so that every red-blue coloring of K_n contains either a red K_a or a blue K_b?

We just showed that $R(3,3) = 6$.

Question 258 *Explain why* $R(a,b) = R(b,a)$*, always.*

The numbers $R(a,b)$ have been the subject of intense study yet very few of them are known. Ramsey's theorem shows only that the numbers $R(a,b)$ are well-defined. It does not give any insight into how to determine their value. In this section we will find a few of them. At the end, we give all known values of $R(a,b)$ as well as the best known upper and lower bounds on some of the other numbers.

We write $6 \to (3,3)$ to indicate that every red-blue coloring of K_6 has a red K_3 or a blue K_3. We also write $5 \not\to (3,3)$ to indicate that not every red-blue coloring of K_5 has a red K_3 or a blue K_3. In general, $n \to (a,b)$ means that every red-blue coloring of K_n has a red K_a or a blue K_b. This is sometimes expressed as, "n has the (a,b) Ramsey property."

Question 259 *Suppose* $n \to (a,b)$*. Explain why* $p \to (a,b)$ *for all* $p > n$.

Therefore, $R(a,b)$ is the least positive integer n for which $n \to (a,b)$. Therefore, $R(a,b) = n$ if and only if $n \to (a,b)$ and $n-1 \not\to (a,b)$.

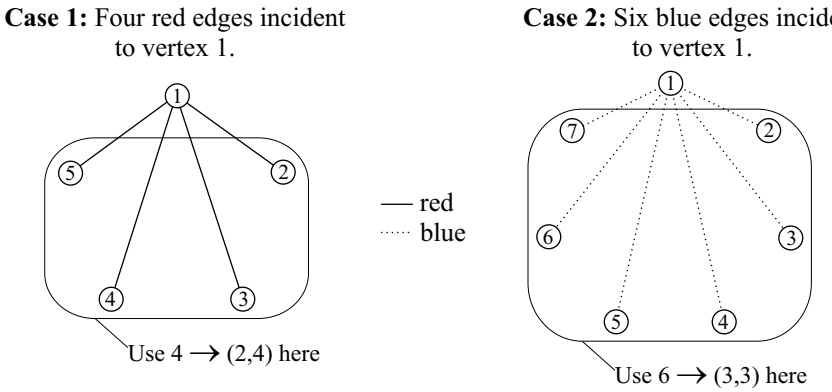


Figure 6.9. The two cases in the proof that $10 \to (3,4)$.

Trivial Ramsey problems

The Ramsey numbers $R(2,b)$ are easy to determine. We seek the smallest value of n for which every red-blue coloring of K_n contains either a red K_2 or a blue K_b. Note that a red K_2 is just a single red edge. Obviously $b \to (2,b)$ because any red-blue coloring of K_b either contains only blue edges or else contains at least one red edge.

Question 260 *Show that $b-1 \not\to (2,b)$. That is, give an example of a red-blue coloring of K_{b-1} that contains neither a red K_2 nor a blue K_b.*

Therefore $R(2,b) = b$ for all $b \geqslant 2$.

The next easiest Ramsey problem

Now that we know $R(3,3) = 6$, we next tackle $R(3,4)$. To illustrate both the difficulty of finding Ramsey numbers as well as the interesting aspects of the journey involved in doing so, we will first determine an upper bound, then a lower bound, and then finally a better upper bound.

Proof that $10 \to (3,4)$

We prove an upper bound $R(3,4) \leqslant 10$ by proving $10 \to (3,4)$. To show that any red-blue coloring of K_{10} has either a red K_3 or a blue K_4, we see if we can modify the argument used to prove $6 \to (3,3)$. Consider any coloring of K_{10} and examine the edges incident to vertex 1. We consider two cases. See Figure 6.9 for an illustration.

Case 1: There are at least four red edges incident to vertex 1. Without loss of generality, assume red edges join vertex 1 to vertices 2-5. Look at the K_4 subgraph induced by vertices 2-5. Since $4 \to (2,4)$, this subgraph contains a red K_2 or a blue K_4. If it contains a blue K_4, then we have found a blue K_4 in our larger K_{10}. Else it contains a red K_2, so that those two vertices and vertex 1 form a red K_3 in the larger graph K_{10}. Therefore $10 \to (3,4)$ in this case.

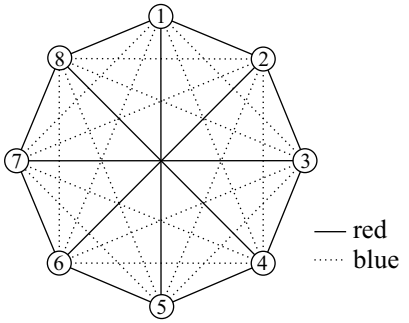
Case 2: There are at most three red edges, and therefore at least six blue edges, incident to vertex 1. Without loss of generality, assume blue edges join vertex 1 to vertices 2-7. Look at the K_6 subgraph induced by vertices 2-7. Since $6 \to (3,3)$, this subgraph contains a red K_3 or a blue K_3. If it contains a red K_3, then we have found a red K_3 in our

larger graph K_{10}. Else it contains a blue K_3, so that those three vertices and vertex 1 form a blue K_4 in the larger graph K_{10}. Therefore $10 \to (3,4)$ in this case as well.

These two cases are exhaustive, so $10 \to (3,4)$ and therefore $R(3,4) \leqslant 10$.

Proof that $8 \not\to (3,4)$

To show $8 \not\to (3,4)$ we must find a red-blue coloring of K_8 having neither a red K_3 nor a blue K_4. Here is such a graph:



And the winner is...

At this point we know $9 \leqslant R(3,4) \leqslant 10$. So does $9 \to (3,4)$ or does $9 \not\to (3,4)$?

Let's see if we can improve upon the proof that $10 \to (3,4)$. Consider any red-blue coloring of K_9. Ignore the blue edges for the moment and consider the 9-vertex graph involving just the red edges. Since this graph has an odd number of vertices, there exists a vertex of *even* degree. Without loss of generality let's assume that vertex 1 is such a vertex, so that it has an even number of red edges incident to it. Now go back to the original red-blue coloring of K_9. Each vertex has degree 8, not 9, so we modify Case 1 as follows.

Case 1: There are at least three red edges incident to vertex 1. But vertex 1 has an even number of red edges incident to it, so there must be at least four red edges incident to vertex 1. This case now proceeds as before.

Case 2: There are at most two red edges, and therefore at least six blue edges, incident to vertex 1. This case is identical to Case 2 of the previous proof.

In each case the conclusion is $9 \to (3,4)$. We have now determined the value of $R(3,4)$.

Theorem 6.4.1 $R(3,4) = 9$.

Two upper bounds

Why did we show the proof that $10 \to (3,4)$ when in fact we know that $9 \to (3,4)$? Upon careful inspection, the proof that $10 \to (3,4)$ actually proves that

$$R(3,4) \leqslant R(2,4) + R(3,3).$$

The same argument works to give an upper bound on any Ramsey number $R(a,b)$.

Theorem 6.4.2 *If $a, b \geqslant 3$, then $R(a,b) \leqslant R(a-1,b) + R(a,b-1)$.*

Proof: Assume $a, b \geqslant 3$. Define $n := R(a-1,b) + R(a,b-1)$. We prove the theorem by showing that $n \to (a,b)$.

Consider any red-blue coloring of K_n and look at the edges incident with vertex 1. There are $n-1 = R(a-1,b) + R(a,b-1) - 1$ such edges. We consider two cases.

Case 1: There are at least $R(a-1,b)$ red edges incident to vertex 1. Consider the subgraph induced by the endpoints of any $R(a-1,b)$ such edges. It contains either a red K_{a-1} or a blue K_b. If it contains a blue K_b, then the K_n contains a blue K_b. If it contains a red K_{a-1}, then those $a-1$ vertices plus vertex 1 form a red K_a. Therefore $n \to (a,b)$ in this case.

Case 2: There are at least $R(a,b-1)$ blue edges incident to vertex 1. See the question after the proof.

In either case $n \to (a,b)$. Therefore $R(a,b) \leqslant n = R(a-1,b) + R(a,b-1)$. ■

Question 261 *Why must there be either $R(a-1,b)$ red edges or $R(a,b-1)$ blue edges incident to vertex 1? Also, provide the details of Case 2.*

We have not yet proved that the Ramsey numbers $R(a,b)$ for $a,b \geqslant 2$ are well-defined (i.e., exist and are finite), but we can do so with the aid of Theorem 6.4.2. We prove by induction on $a+b$. For the base case, since $R(2,b) = R(b,2) = b$ for all $b \geqslant 2$ these numbers are well-defined. Now assume $a,b \geqslant 3$ and that $R(p,q)$ is well-defined for whenever $p+q < a+b$. This implies that $R(a-1,b)$ and $R(a,b-1)$ are well-defined. The argument used to prove Theorem 6.4.2 shows that $R(a,b) \leqslant R(a-1,b)+R(a,b-1)$. Therefore $R(a,b)$ has a well-defined upper bound, and so $R(a,b)$, being the least positive integer n for which $n \to (a,b)$, is well-defined.

The bound of the following theorem can also be proved using Theorem 6.4.2 and induction (see Exercise 4).

Theorem 6.4.3 *If $a,b \geqslant 2$, then* $R(a,b) \leqslant \binom{a+b-2}{a-1}$.

Question 262 *Find upper bounds on $R(a,b)$ for $a,b = 3,4,5,6$ using Theorems 6.4.2 and 6.4.3.*

A lower bound

We next turn our attention to a lower bound on $R(a,a)$. Let's first see how this works in the case of $R(5,5)$. The general case is no more difficult.

What condition on n would allow us to conclude that $R(5,5) > n$? We would need to show that there is a red-blue coloring of K_n with neither a red K_5 nor a blue K_5. Let's try to count the complement—the colorings of K_n having either a red K_5 or a blue K_5. If S is any 5-subset of vertices of K_n, let A_S be the set of red-blue colorings of K_n in which the subgraph induced by S is all-red or all-blue. The size of this set is

$$|A_S| = 2 \cdot 2^{\binom{n}{2}-\binom{5}{2}}$$

because there are two ways to color the edges in the subgraph induced by S (all red or all blue), and then $2^{\binom{n}{2}-\binom{5}{2}}$ ways to color the remaining $\binom{n}{2} - \binom{5}{2}$ edges of K_n.

The number of colorings of K_n having a red K_5 or a blue K_5 is then the size of the union of the A_S

$$[\#\text{ colorings with red } K_5 \text{ or blue } K_5] = \left| \bigcup_{S:|S|=5} A_S \right|.$$

An easy upper bound on the union is the sum of the sizes of the sets:

$$\left| \bigcup_{S:|S|=5} A_S \right| \leqslant \sum_{S:|S|=5} |A_S|.$$

Use the formula for $|A_S|$ to write

$$\sum_{S:|S|=5} |A_S| = \sum_{S:|S|=5} 2 \cdot 2^{\binom{n}{2}-\binom{5}{2}} = \binom{n}{5} \cdot 2 \cdot 2^{\binom{n}{2}-\binom{5}{2}}.$$

We have shown that

$$[\#\text{ colorings with red } K_5 \text{ or blue } K_5] \leqslant \binom{n}{5} \cdot 2 \cdot 2^{\binom{n}{2}-\binom{5}{2}}.$$

Now comes the key observation: *If the number on the right is less than the total number of red-blue colorings of K_n, then there will be a coloring containing neither a red K_5 nor a blue K_5.* The total number of red-blue colorings of K_n is $2^{\binom{n}{2}}$, and

$$\binom{n}{5} \cdot 2 \cdot 2^{\binom{n}{2}-\binom{5}{2}} < 2^{\binom{n}{2}}$$

is true if and only if

$$\binom{n}{5} < 2^{\binom{5}{2}-1}.$$

This inequality is the condition we sought at the outset: If n satisfies $\binom{n}{5} < 2^{\binom{5}{2}-1}$, then $R(5,5) > n$.

Theorem 6.4.4 *If n is an integer satisfying*

$$\binom{n}{a} < 2^{\binom{a}{2}-1}$$

then $R(a,a) > n$.

Question 263 *Prove the theorem by generalizing the argument for $R(5,5) > n$.*

The lower bound provided by Theorem 6.4.4 is not very tight in most cases.

Question 264 *Find a lower bound on $R(a,a)$ for $a = 3,4,5,6$ using the theorem.*

How hard are the Ramsey problems?

The famous Hungarian mathematician Paul Erdős (1913–1996) once made this analogy about the relative difficulty of finding $R(5,5)$ and $R(6,6)$. Suppose an all-powerful and invincible alien comes to Earth and asks a single question. Answer correctly and the alien will spare the planet. Answer incorrectly and it will instantly destroy humanity. If the alien asks for the value of $R(5,5)$, then according to Erdős our best strategy is to get every mathematician to drop what they're doing and work on finding the answer. If instead the

$a\downarrow\ b\rightarrow$	3	4	5	6	7	8	9
3	6	9	14	18	23	28	36
4		18	25	35;41	49;61	56;84	73;115
5			43;49	58;87	80;143	101;216	125;316
6				102;165	113;298	127;495	169;780
7					205;540	216;1031	233;1713
8						282;1870	317;3583
9							565;6588

Table 6.1. Best known bounds on Ramsey numbers $R(a,b)$ for $3 \leqslant a \leqslant b \leqslant 9$.

alien asks for $R(6,6)$, then Erdős says our best strategy is to try to figure out how to destroy the alien.

Table 6.1 shows the best known information for the nontrivial Ramsey numbers $R(a,b)$ satisfying $3 \leqslant a \leqslant b \leqslant 9$. Only nine values of $R(a,b)$ are known with certainty; in all other cases the table shows the best known lower and upper bounds.

Question 265 *Compare your upper and lower bounds found in Questions 262 and 264 with those of Table 6.1.*

The most recent discovery was $R(4,5) = 25$, which prompted the letter shown at the beginning of this section. Here is the timeline of the quest to find $R(4,5)$.

- 1955: First upper bound $R(4,5) \leqslant 31$.
- 1965: First lower bound and improved upper bound $25 \leqslant R(4,5) \leqslant 30$.
- 1968: Improved upper bound $R(4,5) \leqslant 29$.
- 1971: Improved upper bound $R(4,5) \leqslant 28$.
- 1991: Improved upper bound $R(4,5) \leqslant 27$.
- 1992: Improved upper bound $R(4,5) \leqslant 26$.
- 1993: Improved upper bound $R(4,5) \leqslant 25$ and proof that $R(4,5) = 25$.

Given the time and difficulty involved in each step, perhaps determining even $R(4,7)$ is insurmountable given the current bounds $49 \leqslant R(4,7) \leqslant 61$.

Other Ramsey numbers

One generalization of the Ramsey number $R(a,b)$ involves adding more colors. Define $R(a,b,c)$ to be the least positive integer n such that any red-blue-green coloring of K_n has either a red K_a or a blue K_b or a green K_c. In this case there is only one nontrivial number known: $R(3,3,3) = 17$. In the case of four colors, none of the numbers $R(a,b,c,d)$ are known.

Question 266 *Determine $R(2,3,3)$. What can you say about $R(2,b,c)$?*

Another generalization of $R(a,b)$ involves looking for monochromatic subgraphs other than complete graphs. For any graphs G and H, define $R(G,H)$ to be least positive integer n such that any red-blue coloring of K_n either contains a red G or a blue H as a subgraph. For example, $R(C_4, K_5 - e)$ is the least positive integer n such that any red-blue coloring of K_n contains either a red C_4 (i.e., a red 4-cycle) or a blue $K_5 - e$ (a blue K_5 with an edge deleted). In this new notation, $R(a,b)$ is $R(K_a, K_b)$. See the Exercises.

Summary

The Ramsey number $R(a, b)$ equals the least positive integer n for which every red-blue coloring of the edges of K_n contains either an all-red K_a or an all-blue K_b. Ramsey numbers are difficult to compute. Only nine nontrivial Ramsey numbers are known: $R(3, b)$ for $b = 3, 4, \ldots, 9$ as well as $R(4, 4)$ and $R(4, 5)$. Work on determining $R(4, 5)$ spanned almost 40 years and required a great deal of computation in addition to mathematical ingenuity.

Exercises

1. True or false?
   (a) $n \to (a, b)$ if and only if $R(a, b) \leqslant n$.
   (b) $n \not\to (a, b)$ if and only if $R(a, b) \geqslant n$.
   (c) There is a red-blue coloring of K_{300} with neither a red K_6 nor a blue K_7.
   (d) One way to determine an upper bound on $R(a, b)$ is to exhibit a coloring of a complete graph that has either a red K_a or a blue K_b.
2. Prove the following version of Theorem 6.4.2 that gives a tighter bound in a special case: if $a, b \geqslant 3$ and $R(a-1, b)$ and $R(a, b-1)$ are both even, then $R(a, b) \leqslant R(a-1, b) + R(a, b-1) - 1$.
3. Consider any five points in the plane such that no three lie on the same line. Prove that there exist four points that form the vertices of a convex quadrilateral.
4. Prove Theorem 6.4.3 by induction on $a + b$. (Alternatively, you could prove using double induction on a and b.)
5. Find a red-blue coloring of K_{13} containing neither a red K_3 nor a blue K_5.
6. Determine the following generalized Ramsey numbers.
   (a) $R(K_3 - e, K_b)$ for all $b \geqslant 3$
   (b) $R(K_{1,3}, K_{1,4})$
   (c) $R(C_4, C_4)$
   (d) $R(K_3, C_4)$
7. Give a direct, combinatorial proof of Theorem 6.4.3.

Travel Notes

Graham, Rothschild & Spencer (1980) is an excellent survey of Ramsey theory and also contains some interesting history. Frank Ramsey expressed his original theorem in the context of sets, not graphs, and he was interested in a problem in mathematical logic. Nonetheless his paper Ramsey (1930) has sparked a great deal of research in combinatorics and graph theory. Ramsey worked in philosophy, mathematical logic, and economics and made important contributions to each field before his death at the age of only 27.

The two mathematicians mentioned in the letter at the beginning of this section are Brendan McKay and Stanisław Radziszowski, and their result appeared in McKay & Radziszowski (1995). Radziszowski also maintains an article called "Small Ramsey numbers," published in the *Electronic Journal of Combinatorics*, that contains the best known bounds on all sorts of Ramsey numbers including those shown in Table 6.1. The latest update is August 2006.

CHAPTER 7

Designs and Codes

In this chapter we visit two application areas of combinatorics that at first appear unrelated. One area involves error-correcting codes. An error-correcting code provides a way to transmit a message so that the original message can be recovered even when some errors are introduced in transmission. You need only think of today's technology (cell phones, DVD players, spacecraft) as well as the ways in which transmission problems occur (communications satellite or cell phone tower problems, bumping the player or scratching the disc, various kinds of interference) to recognize the importance of this application.

The other area involves combinatorial designs. One of the first needs for designs arose in constructing statistical experiments, especially in agriculture and medicine. Classical examples include studies to test the efficacy of fertilizer-seed variety combinations, drugs, or even automotive tires. In order to make valid conclusions, the experimenter must control non-experimental effects that can confound the outcome. For example, each possible fertilizer-seed combination should be tested in a variety of soils and climates so that the success of a particular combination is not dependent on either of those factors. Combinatorial designs provide prescribed experimental layouts that accomplish this objective.

Since those initial applications of combinatorial designs, they have proved their worth in a host of other settings. These include tournament scheduling and, as it turns out, error-correcting codes.

7.1 Construction methods for designs

We begin our study of combinatorial designs by trying to construct a few specific designs. After experiencing some of the issues therein, we derive a few properties and then explore more methods of construction.

The $(7, 7, 3, 3, 1)$ design

A recreational softball league commissioner needs to schedule games for a seven-team round-robin tournament. In such a tournament, each team plays each other team exactly once. The commissioner wants to send three teams to the field each day. While two teams play, the third supplies the umpires, and then they rotate so that a total of three games are played. How might we construct such a schedule?

Each team needs to play a total of six games. On any day a team comes to the field,

they play two games. Therefore, in an ideal schedule, each team would come to the field on $6/2 = 3$ days. Also notice that a total of $\binom{7}{2} = 21$ games must be played. In an ideal schedule, this would take $21/3 = 7$ days to accomplish because three games are played per day.

Let's try to make such a schedule. Label the teams 1 through 7 and attempt to group them in "blocks" of three teams that meet the requirements. Let's send teams 1-3 to the field on day 1. Team 1 also needs to play teams 4-7, so start by defining the three blocks

$$B_1 = \{1, 2, 3\} \qquad B_2 = \{1, 4, 5\} \qquad B_3 = \{1, 6, 7\}.$$

This ensures team 1 plays each other team once.

Team 2 has already played teams 1 and 3 and still needs to play teams 4-7. We won't include the block $\{2, 4, 5\}$ because teams 4 and 5 already play in B_2. (Each pair of teams must play exactly once.) Thus we choose $B_4 = \{2, 4, 6\}$. Team 2 still needs to play teams 5 and 7, so let's try $B_5 = \{2, 5, 7\}$. This completes team 2's required games. Noting that team 3 still needs to play teams 4-7, we set $B_6 = \{3, 4, 7\}$ and $B_7 = \{3, 5, 6\}$.

Question 267 *If you instead choose $B_4 = \{2, 4, 7\}$, what would the rest of the blocks be?*

The whole schedule, or design, is:

i	1	2	3	4	5	6	7
B_i	1,2,3	1,4,5	1,6,7	2,4,6	2,5,7	3,4,7	3,5,6

Each of the 21 pairs of teams indeed plays exactly once. For example, teams 3 and 6 appear together in B_7 and in no other blocks. Notice also that each team comes to the field on exactly three days.

This collection of seven blocks is known as a *balanced incomplete block design*. It contains the structure that the commissioner desired: each team appears in exactly three blocks, each block contains exactly three teams, and each pair of teams appears together in exactly one block. It is known as a $(7, 7, 3, 3, 1)$ design for reasons we'll explain shortly.

No such "ideal" design exists if instead there are six teams. The tournament would involve $\binom{6}{2} = 15$ games and so an ideal schedule would involve $15/3 = 5$ days. Starting with $B_1 = \{1, 2, 3\}$ and $B_2 = \{1, 4, 5\}$, there is no way to construct a block $B_3 = \{1, ?, 6\}$ that avoids team 1 playing a team it has already played. The commissioner should either be prepared to send teams to the field for the sole purpose of umpiring or else should explore another way to structure the tournament.

Question 268 *Does such a design exist if there are eight teams? Either construct one or explain why one doesn't exist.*

Balanced incomplete block designs

A ***combinatorial design*** or simply a ***design*** is a pair $(V, \mathcal{B})$ where V is a finite set of ***varieties*** and $\mathcal{B}$ is a multiset consisting of nonempty subsets of V. The subsets in $\mathcal{B}$ are the ***blocks*** of the design. The design we just constructed has

$$V = \{1, 2, 3, 4, 5, 6, 7\}$$
$$\mathcal{B} = \Big\{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\Big\}.$$

In this case there are no repeated blocks, so $\mathcal{B}$ is an ordinary set. Although we labeled the blocks $B_1, \ldots, B_7$ when we constructed this design, we did so for ease of reference. Blocks in a design are unlabeled.

A (b, v, r, k, λ) ***design*** has b blocks and v varieties such that each variety appears in exactly r blocks, each block contains exactly k varieties, and each pair of distinct varieties appears together in exactly λ blocks. Such designs are either ***complete*** or ***incomplete*** according to whether $k = v$ or $k < v$, respectively. A ***balanced incomplete block design (BIBD)*** is a (b, v, r, k, λ) design with $k < v$. The tournament schedule constructed above is a $(7, 7, 3, 3, 1)$ BIBD.

More generally, any design in which each variety appears in exactly r blocks is ***r-regular***. Any design in which each block has size k is ***k-uniform***. Any design in which each pair of distinct varieties appears in exactly λ blocks is ***λ-balanced***. Therefore, a BIBD is an incomplete, regular, uniform, balanced design. A design with

$$V = \{1, 2, 3, 4\}$$
$$\mathcal{B} = \Big\{\{1, 2\}, \{1, 2\}, \{3, 4\}, \{3, 4\}\Big\}$$

is not a BIBD because although it is incomplete, 2-regular, and 2-uniform, it is not balanced because varieties 1 and 2 appear together in two blocks while varieties 1 and 3 don't appear together in any blocks. Exercise 8 asks you to prove that any incomplete, uniform, and balanced design is necessarily regular and hence a BIBD.

Question 269 *Construct an example of a design with $V = \{1, 2, 3\}$ that is regular and balanced but not uniform.*

In a complete design each block consists of the entire set V of varieties. If such a design has b blocks, then the remaining parameters are easy to compute.

Question 270 *Determine the remaining parameters of a complete $(b, v, ?, ?, ?)$ design.*

The interesting work to be done on (b, v, r, k, λ) designs involves those whose parameters satisfy $1 < k < v$, because complete designs (having $k = v$) and designs with $k = 1$ are trivial.

Constructing a $(10, 6, 5, 3, 2)$ design

Pharmaceutical researchers wish to test six different pain relievers on chronic migraine sufferers. They recruit 10 subjects for their study. Ideally they would test all six drugs on each subject but this is not possible for both medical and practical reasons. Instead, they administer three different drugs to each subject and insist on testing every possible pair of drugs on two different subjects. If one drug is truly more effective than another, then that should be reflected in the independent experiences of two subjects.

The drugs comprise the $v = 6$ varieties. Each block corresponds to a group of three drugs that will be administered to a subject, so $k = 3$ and $b = 10$. In addition, each pair of drugs must appear together in $\lambda = 2$ blocks. The experiment calls for a $(10, 6, r, 3, 2)$ design. It turns out that each variety must appear in exactly five blocks, so $r = 5$ and we need to construct a $(10, 6, 5, 3, 2)$ design. (Shortly, we'll see why $r = 5$.)

Set $V := [6]$. Variety 1 must appear in $r = 5$ blocks so we place it in B_1 through B_5. Varieties 1 and 2 must appear together in $\lambda = 2$ blocks, so we place variety 2 in B_1 and

B_2. Variety 2 must also appear in five blocks total, so we place it in B_6 through B_8. Any other variety can go in B_1, so we choose to place variety 3 there. Our partially completed design is:

i	1	2	3	4	5	6	7	8	9	10
B_i	1,2,3	1,2,?	1,?,?	1,?,?	1,?,?	2,?,?	2,?,?	2,?,?	?,?,?	?,?,?

For our next move, varieties 1 and 3 need to appear together in two blocks. They already appear together in B_1 so we can place variety 3 in B_3.

Question 271 *Can the design be completed if instead we chose $B_1 = B_2 = \{1, 2, 3\}$? Support your answer. (Repeated blocks are allowed in a design, so if it cannot be completed then it will not be for that reason.)*

Varieties 2 and 3 also need to appear in the same block twice, so we place variety 3 in B_6. Variety 3 has now appeared with varieties 1 and 2 the required number of times. It needs to appear five times in all, so we must place it in B_9 and B_{10}. We now have:

i	1	2	3	4	5	6	7	8	9	10
B_i	1,2,3	1,2,?	1,3,?	1,?,?	1,?,?	2,3,?	2,?,?	2,?,?	3,?,?	3,?,?

Among blocks B_1 through B_5, we still need to place varieties 4-6 so that each of these varieties appears with variety 1 exactly two times. One way to do so is:

i	1	2	3	4	5	6	7	8	9	10
B_i	1,2,3	1,2,4	1,3,5	1,4,6	1,5,6	2,3,?	2,?,?	2,?,?	3,?,?	3,?,?

This completes the considerations involving variety 1. Among B_6 through B_8, which are the remaining blocks that contain variety 2, we still need the following pairs to appear:

pair	1,2	2,3	2,4	2,5	2,6
# blocks in which pair still needs to appear	0	0	1	2	2

Setting $B_6 = \{2, 3, 4\}$ forces $B_7 = B_8 = \{2, 5, 6\}$ which then causes varieties 5 and 6 to appear together three times in the design. We then try $B_6 = \{2, 3, 5\}$ but also find that we cannot complete the design.

Question 272 *Explain why at this point we cannot choose $B_6 = \{2, 3, 5\}$.*

Setting $B_6 = \{2, 3, 6\}$ forces $B_7 = \{2, 4, 5\}$ and $B_8 = \{2, 5, 6\}$. We are almost done:

i	1	2	3	4	5	6	7	8	9	10
B_i	1,2,3	1,2,4	1,3,5	1,4,6	1,5,6	2,3,6	2,4,5	2,5,6	3,?,?	3,?,?

Variety 3 has not yet appeared in the same block as variety 4, so we must put 4 in each of the last two blocks to get:

i	1	2	3	4	5	6	7	8	9	10
B_i	1,2,3	1,2,4	1,3,5	1,4,6	1,5,6	2,3,6	2,4,5	2,5,6	3,4,5	3,4,6

You should verify that this is indeed a $(10, 6, 5, 3, 2)$ design.

The basic necessary conditions

The somewhat *ad hoc* methods we used to construct the $(7, 7, 3, 3, 1)$ and $(10, 6, 5, 3, 2)$ designs become cumbersome if we wish to construct larger designs. Also, if a design doesn't exist, proving so using these construction methods takes great care.

Before we return to design construction methods, we derive two fundamental necessary conditions for the existence of a (b, v, r, k, λ) design.

Theorem 7.1.1 *If a (b, v, r, k, λ) design exists, then $bk = vr$ and $r(k-1) = \lambda(v-1)$.*

Combinatorial proof: Consider any (b, v, r, k, λ) design.

To prove $bk = vr$ we ask, How many 2-lists (B, x) are possible, where B is a block of the design and x is a variety appearing in that block?

Answer 1: Choose a block in b ways. Every block has size k, so there are k ways to select a variety in that block. By the product principle there are bk such 2-lists.

Answer 2: First choose a variety in v ways. Every variety appears in r blocks, so there are r ways to select a block containing that variety. There are vr such 2-lists.

To prove $r(k-1) = \lambda(v-1)$ we first fix any variety y and then ask, How many 2-lists (B, x) are possible, where $x, y \in B$ and $x \neq y$?

Answer 1: Since variety y appears in exactly r blocks, there are r ways to choose the block B. That block contains $k-1$ varieties other than y, so there are $k-1$ ways to choose the variety x. There are $r(k-1)$ such 2-lists.

Answer 2: There are $v-1$ ways to choose a variety x that is different from y. These two varieties appear together in exactly λ blocks, so there are λ ways to choose the block B. There are $\lambda(v-1)$ such 2-lists. ■

Question 273 *All of the BIBDs we have encountered so far have $r > \lambda$. Use the theorem to prove that this is true in general.*

If we apply the theorem to the $(10, 6, r, 3, 2)$ design of the previous example, we can use the condition $bk = vr$ to write $30 = 6r$, which implies $r = 5$. Generally, the theorem shows that the values of any three of the parameters in a (b, v, r, k, λ) design determine the values of the other two. For that reason, a (b, v, r, k, λ) design is often simply called a (v, k, λ) design. We will use both notations interchangeably.

In addition to determining missing parameters, we can also use the theorem to prove that certain designs don't exist. Some examples follow.

Example: do these designs exist?

What conclusion can you draw from Theorem 7.1.1 about the existence of designs with the following parameters?

(a) $(111, 111, 11, 11, 1)$

$\Longrightarrow$ A $(111, 111, 11, 11, 1)$ design indeed satisfies $bk = vr$ and $r(k-1) = \lambda(v-1)$. The theorem doesn't rule out the existence of such a design, but neither does it help us construct one.

(b) $(4, 4, 3, 3, 2)$

$\Longrightarrow$ A $(4, 4, 3, 3, 2)$ design also satisfies $bk = vr$ and $r(k-1) = \lambda(v-1)$, so again the theorem does not rule out its existence. In fact, such a design is easy to construct. Set $V = [4]$ and let $\mathcal{B}$ consist of the 3-subsets of V.

Question 274 *Construct a design with* $(v, k, \lambda) = (5, 3, 3)$ *by using a similar construction technique.*

(c) $(v, k, \lambda) = (11, 3, 2)$

$\Longrightarrow$ If a $(b, 11, r, 3, 2)$ design were to exist, then it would satisfy $3b = 11r$ and $2r = 20$. This means $r = 10$, which implies $3b = 110$. But then b is not an integer, so no such design exists.

(d) a softball schedule as described at the beginning of this section, but involving v teams

$\Longrightarrow$ This reduces to determining the values of v for which a $(b, v, r, 3, 1)$ design exists. We need $2r = v - 1$ or $r = (v - 1)/2$. We also need $3b = v(v - 1)/2$ or $b = v(v - 1)/6$. Therefore, if such a design exists involving v teams, it must be the case that v is odd and $v(v - 1)$ is divisible by 6. The theorem gives no insight into whether these conditions are sufficient.

Two basic construction methods

The equations of Theorem 7.1.1 are necessary conditions for the existence of a design. Unfortunately they are not sufficient, and part (a) of the last example is a case in point. In 1988, a group of researchers used a CRAY supercomputer to determine that no (111, 111, 11, 11, 1) design exists. See Lam (1991) for their story. On the other hand, the conditions of the theorem may also be sufficient, as they are with part (d) of the example. A $(b, v, r, 3, 1)$ design is called a ***Steiner triple system***. The name has stuck despite the fact that Kirkman (1847) provided the exact conditions for their existence earlier than Steiner who in 1853, unaware of Kirkman's work, merely conjectured that the necessary conditions were sufficient. We consider Steiner triple systems in Section 7.3.

We devote the remainder of this section to three construction methods. In the next two sections we return to the study of necessary conditions.

Method 1: repeat blocks

From a (b, v, r, k, λ) design, create a new design by writing each block t times. The result is a $(tb, v, tr, k, t\lambda)$ design. For example, we know that a (21, 7, 9, 3, 3) design exists because we can simply include three copies of each block of the (7, 7, 3, 3, 1) design.

Question 275 *Explain how to construct a* (170, 6, 85, 3, 34) *design.*

Method 2: find the complementary design

A natural way to build a new design from an existing one is to take the complement of each block relative to the set of varieties. This is called the ***complementary design***. If $\mathcal{D}$ is a design, then $\mathcal{D}^c$ denotes its complementary design.

Here is the (7, 7, 3, 3, 1) design and its complementary design:

i	1	2	3	4	5	6	7
B_i	1,2,3	1,4,5	1,6,7	2,4,6	2,5,7	3,4,7	3,5,6

i	1	2	3	4	5	6	7
B_i^c	4,5,6,7	2,3,6,7	2,3,4,5	1,3,5,7	1,3,4,6	1,2,5,6	1,2,4,7

Notice that the complementary design is a BIBD with parameters (7, 7, 4, 4, 2).

Question 276 *Find the complementary design of the* $(10, 6, 5, 3, 2)$ *design given earlier. Is it a BIBD? What are its parameters?*

What is the relationship between the parameters of a design and of its complementary design? Suppose that $\mathcal{D}$ is a (b, v, r, k, λ) BIBD. One can quickly see that $\mathcal{D}^c$ is a $(b, v, b-r, v-k, ?)$ design.

Question 277 *Justify these first four parameters. Also, why should we not consider finding the complementary design of a complete design?*

Does each pair of distinct varieties appear together in the same number of blocks of the complementary design? The answer is yes and proving it requires a quick application of inclusion-exclusion. First notice that varieties i and j appear together in a block of $\mathcal{D}^c$ if and only if *neither one* appears in the corresponding block of $\mathcal{D}$. The number of blocks of $\mathcal{D}$ in which neither i nor j appears is

$$b - r - r + \lambda = b - 2r + \lambda$$

because there are b total blocks, r blocks containing i, r blocks containing j, and λ blocks containing both i and j. This proves the first statement in the following theorem. The theorem's second sentence follows by observing that $(\mathcal{D}^c)^c = \mathcal{D}$.

Theorem 7.1.2 *Given a* (b, v, r, k, λ) *BIBD, the complementary design is a* $(b, v, b-r, v-k, b-2r+\lambda)$ *BIBD. Moreover, there exists a* (b, v, r, k, λ) *design if and only if there exists a* $(b, v, b-r, v-k, b-2r+\lambda)$ *design.*

Constructing cyclic designs

The last construction technique of this section involves modular arithmetic, and our first illustration of it involves constructing a 3-uniform design on 13 varieties. Instead of using $V = [13]$, we use $V = \{0, 1, 2, \ldots, 12\}$, the set of residues modulo 13. Begin with the "base blocks" $\{1, 3, 9\}$ and $\{2, 5, 6\}$ and add the residues modulo 13 to the varieties in each base block in turn.

This is done in Figure 7.1 where the base blocks appear at the top of each column. The notation $\{1, 3, 9\} \oplus 5$, for example, means to add 5 to each element of $\{1, 3, 9\}$ and then

$$\begin{aligned}
B_1 &= \{1,3,9\} \oplus 0 = \{1,3,9\} & B_{14} &= \{2,5,6\} \oplus 0 = \{2,5,6\}\\
B_2 &= \{1,3,9\} \oplus 1 = \{2,4,10\} & B_{15} &= \{2,5,6\} \oplus 1 = \{3,6,7\}\\
B_3 &= \{1,3,9\} \oplus 2 = \{3,5,11\} & B_{16} &= \{2,5,6\} \oplus 2 = \{4,7,8\}\\
B_4 &= \{1,3,9\} \oplus 3 = \{4,6,12\} & B_{17} &= \{2,5,6\} \oplus 3 = \{5,8,9\}\\
B_5 &= \{1,3,9\} \oplus 4 = \{5,7,0\} & B_{18} &= \{2,5,6\} \oplus 4 = \{6,9,10\}\\
B_6 &= \{1,3,9\} \oplus 5 = \{6,8,1\} & B_{19} &= \{2,5,6\} \oplus 5 = \{7,10,11\}\\
B_7 &= \{1,3,9\} \oplus 6 = \{7,9,2\} & B_{20} &= \{2,5,6\} \oplus 6 = \{8,11,12\}\\
B_8 &= \{1,3,9\} \oplus 7 = \{8,10,3\} & B_{21} &= \{2,5,6\} \oplus 7 = \{9,12,0\}\\
B_9 &= \{1,3,9\} \oplus 8 = \{9,11,4\} & B_{22} &= \{2,5,6\} \oplus 8 = \{10,0,1\}\\
B_{10} &= \{1,3,9\} \oplus 9 = \{10,12,5\} & B_{23} &= \{2,5,6\} \oplus 9 = \{11,1,2\}\\
B_{11} &= \{1,3,9\} \oplus 10 = \{11,0,6\} & B_{24} &= \{2,5,6\} \oplus 10 = \{12,2,3\}\\
B_{12} &= \{1,3,9\} \oplus 11 = \{12,1,7\} & B_{25} &= \{2,5,6\} \oplus 11 = \{0,3,4\}\\
B_{13} &= \{1,3,9\} \oplus 12 = \{0,2,8\} & B_{26} &= \{2,5,6\} \oplus 12 = \{1,4,5\}
\end{aligned}$$

Figure 7.1. A cyclic $(26, 13, 6, 3, 1)$ design.

reduce modulo 13:

$$\begin{aligned}\{1,3,9\} \oplus 5 &= \big\{(1+5) \bmod 13,\ (3+5) \bmod 13,\ (9+5) \bmod 13\big\} \\ &= \{6,8,1\}.\end{aligned}$$

This produces (check!) a $(26, 13, 6, 3, 1)$ design.

Question 278 *Let $V = \{0, 1, 2, 3, 4, 5, 6\}$ be the set of residues modulo 7 and consider the single base block $\{0, 1, 3\}$. Construct a cyclic design on seven blocks by finding $\{0, 1, 3\} \oplus i$ for each $i \in V$. What are the parameters of the resulting design?*

Characterizing cyclic designs

It turns out that not every choice of base blocks produces a (b, v, r, k, λ) design via the cyclic method. Why do some base blocks work and others don't?

Question 279 *Re-do Question 278 but use the base block $\{0, 1, 2\}$. Why is the resulting design not a BIBD?*

Fortunately, there is a complete answer to the question of whether a given set of base blocks generates a BIBD. The key lies in the pairwise differences between elements in the same base block.

For the $(26, 13, 6, 3, 1)$ design, we used the base blocks $\{1, 3, 9\}$ and $\{2, 5, 6\}$. Look at all of the pairwise differences modulo 13 between elements of the same block. In the table below, the top half shows the differences within the block $\{1, 3, 9\}$ and the bottom half the differences within $\{2, 5, 6\}$:

$1-3 = -2 \equiv 11$	$1-9 = -8 \equiv 5$	$3-9 = -6 \equiv 7$
$3-1 = 2 \equiv 2$	$9-1 = 8 \equiv 8$	$9-3 = 6 \equiv 6$
$2-5 = -3 \equiv 10$	$2-6 = -4 \equiv 9$	$5-6 = -1 \equiv 12$
$5-2 = 3 \equiv 3$	$6-2 = 4 \equiv 4$	$6-5 = 1 \equiv 1$

(We write $-2 \equiv 11$, for example, as an abbreviation for $-2 \equiv 11 \pmod{13}$.) Notice that each of the 12 nonzero residues modulo 13 occurs exactly once on this list.

Question 280 *For the design of Question 278, compute the pairwise differences within the block $\{0, 1, 3\}$. Does each nonzero residue modulo 7 occur exactly once?*

The following theorem gives a complete characterization of cyclic designs in terms of base blocks.

Theorem 7.1.3 *Suppose $\mathcal{C}$ is a set of k-subsets of the v-set $\{0, 1, \ldots, v-1\}$ of residues modulo v, where $v \geq k \geq 2$. Then $\mathcal{C}$ contains the base blocks of a cyclic (v, k, λ) design if and only if the following procedure produces a list that contains each nonzero residue modulo v exactly λ times:*

For each block $C = \{c_1, \ldots, c_k\}$ of $\mathcal{C}$, calculate

$$(c_i - c_j) \bmod v$$

for each ordered pair (c_i, c_j) of unequal elements of C.

The proof involves applying the properties of modular arithmetic and we leave it to Exercise 19. We now give one more example, this time with $\lambda = 3$. Let $v = 15$ and $k = 7$, and consider the base block $\{0, 1, 2, 4, 5, 8, 10\}$ as a subset of the residues modulo 15. The

$$
\begin{array}{lll}
0-1=-1\equiv 14 & 0-2=-2\equiv 13 & 0-4=-4\equiv 11 \\
1-0=1\equiv 1 & 2-0=2\equiv 2 & 4-0=4\equiv 4 \\
0-5=-5\equiv 10 & 0-8=-8\equiv 7 & 0-10=-10\equiv 5 \\
5-0=5\equiv 5 & 8-0=8\equiv 8 & 10-0=10\equiv 10 \\
1-2=-1\equiv 14 & 1-4=-3\equiv 12 & 1-5=-4\equiv 11 \\
2-1=1\equiv 1 & 4-1=3\equiv 3 & 5-1=4\equiv 4 \\
1-8=-7\equiv 8 & 1-10=-9\equiv 6 & 2-4=-2\equiv 13 \\
8-1=7\equiv 7 & 10-1=9\equiv 9 & 4-2=2\equiv 2 \\
2-5=-3\equiv 12 & 2-8=-6\equiv 9 & 2-10=-8\equiv 7 \\
5-2=3\equiv 3 & 8-2=6\equiv 6 & 10-2=8\equiv 8 \\
4-5=-1\equiv 14 & 4-8=-4\equiv 11 & 4-10=-6\equiv 9 \\
5-4=1\equiv 1 & 8-4=4\equiv 4 & 10-4=6\equiv 6 \\
5-8=-3\equiv 12 & 5-10=-5\equiv 10 & 8-10=-2\equiv 13 \\
8-5=3\equiv 3 & 10-5=5\equiv 5 & 10-8=2\equiv 2
\end{array}
$$

Figure 7.2. Pairwise differences within the block $\{0, 1, 2, 4, 5, 8, 10\}$.

block contains seven varieties, so there are $7 \cdot 6 = 42$ pairwise differences to compute. They appear in Figure 7.2. Each of the residues $1, 2, \ldots, 14$ appears exactly three times so this meets the conditions of the theorem. When found, the resulting design is a $(15, 15, 7, 7, 3)$ BIBD.

Question 281 *Construct this design.*

Not all designs are cyclic, but this method (and generalizations of it) are prolific at producing designs. See Exercise 17 for some basic necessary conditions for cyclic designs.

Summary

A (b, v, r, k, λ) design involves a set of varieties and a multiset of blocks. Each block is a subset of varieties. The parameters have the following meaning:

Parameter	Meaning
b	the number of blocks
v	the number of varieties
r	each variety appears in exactly r blocks
k	each block contains exactly k varieties
λ	each pair of varieties appears together in exactly λ blocks

A balanced incomplete block design (BIBD) has $k < v$.

Any (b, v, r, k, λ) design, if it exists, necessarily satisfies $bk = vr$ and $r(k-1) = \lambda(v-1)$. However, these conditions are not sufficient for existence. We explored methods that construct designs from scratch (*ad hoc* methods, the method of cyclic designs) as well as those that build a design from another design (repeating blocks, the complementary design).

Exercises

1. Suppose that you know three of the five parameters in a (b, v, r, k, λ) design. In each case below, derive a formula for the remaining parameters.

(a) b, v, and r known

(b) v, k, and λ known

(c) r, k, and λ known

2. Describe all possible $(b, v, r, 2, 1)$ designs.

3. Let $n \geqslant 3$. Explain how to construct an $(n, n, n-1, n-1, n-2)$ design.

4. Prove that there is only one $(7, 7, 3, 3, 1)$ design up to relabeling the vertices. (The order in which the blocks are listed doesn't matter either.)

5. Let $V = [n]$ and let $\mathcal{B}$ consist of all of the k-subsets of V, where $1 < k < n$. Determine whether this is a BIBD. If it is, give its parameters.

6. (graph theory) Explain how K_n, the complete graph on n vertices, can be thought of as a design. Give its parameters. Also, explain why a non-complete graph is not a design.

7. Explain combinatorially why in any (b, v, r, k, λ) design, we have $b = \dfrac{\lambda\binom{v}{2}}{\binom{k}{2}}$.

8. Let $\mathcal{D}$ be an incomplete design that is k-uniform and λ-balanced. Prove that $\mathcal{D}$ is regular. (Hint: Revisit the proof of Theorem 7.1.1.)

9. Find a base for a cyclic $(10, 5, 4, 2, 1)$ design.

10. Construct a cyclic $(11, 11, 5, 5, 2)$ design.

11. Construct a cyclic $(18, 9, 8, 4, 3)$ design. (Hint: Use two base blocks.)

12. Construct a $(14, 8, 7, 3, 3)$ design.

13. Suppose $\mathcal{D}$ is a cyclic design modulo v, with the set $\mathcal{C}$ containing the base blocks. Find a set of base blocks for the complementary design $\mathcal{D}^c$ and prove that you are correct.

14. Prove that $r \leqslant \frac{b+\lambda}{2}$ in any (b, v, r, k, λ) design.

15. You enter a lottery by picking a subset of three numbers from [14]. You win a prize if you match at least two of the numbers on the winning ticket.

    (a) Show that it is possible to guarantee a win by buying 14 tickets. (Hint: Use the $(7, 7, 3, 3, 1)$ design.)

    (b) Would an analogous strategy work if instead you had to pick three numbers from [21]? Explain.

    (This is called the "Transylvania lottery" and appears to be of unknown origin.)

16. Show that the set $\mathcal{C} = \Big\{\{0, 1, 3\}, \{2, 6, 7\}, \{4, 8, 11\}, \{5, 10, 12\}\Big\}$ contains the base blocks of a cyclic design modulo 13. Construct the design and give its parameters.

17. (a) Explain why a $(10, 6, 5, 3, 2)$ design cannot be cyclic.

    (b) Prove that in a cyclic design, there exists an integer c for which $b = cv$, $ck(k-1) = \lambda(v-1)$, and $r = ck$. What is the significance of c in terms of the design?

    (c) Can a $(305, 61, 20, 4, 1)$ design be cyclic?

18. Here is an illustration of how to construct a cyclic design using modulo 2 arithmetic. Let V be the set of 4-digit binary numbers. Using the base block

$$B_1 = \{0001, 0010, 0100, 1000, 0011, 1100\},$$

construct the design by finding the blocks $B_1 \oplus \mathbf{v}$ for each $\mathbf{v} \in V$. What are the parameters of this design?

19. Prove Theorem 7.1.3.

Travel Notes

With designs, as sometimes happens with other concepts in mathematics, the recreational problem came before the practical application. In 1847, Kirkman published a solution to the question now known as

Kirkman's schoolgirls problem. If once every day for a week 15 schoolgirls are to walk in five rows of three girls each, is it possible for each girl to be in a row with each other girl exactly once?

This problem calls for a $(15, 3, 1)$ design that has an additional property: resolvability. In a ***resolvable*** design, the blocks can be arranged into groups so that each group partitions the set of varieties. It was the eminent statistician Fisher who in the 1930s-1940s showed how designs could be of use in statistical experiments. Much of his terminology (varieties, blocks) stays with us today. Bose, an Indian mathematician, developed many construction methods for designs in a 1939 paper, among them the method of cyclic designs.

7.2 The incidence matrix and symmetric designs

Any (b, v, r, k, λ) design must satisfy $bk = vr$ and $r(k-1) = \lambda(v-1)$. In addition, any BIBD has $k < v$ and therefore $\lambda < r$. We devote this section to the study of symmetric designs which are designs with an equal number of varieties and blocks. We begin by studying the incidence matrix which is an important tool in design theory.

The incidence matrix of a design

Another way to represent a design is with its incidence matrix. The ***incidence matrix*** of a design $(V, \mathcal{B})$ is that $v \times b$ matrix A whose (i, j)-entry is

$$a_{ij} = \begin{cases} 1 & \text{if variety } i \text{ is in block } B_j \\ 0 & \text{otherwise.} \end{cases} \tag{7.1}$$

Implicit in this definition is a pre-chosen ordering of both the varieties and the blocks. For example, the incidence matrix for the $(7, 7, 3, 3, 1)$ design with the following labeling

i	1	2	3	4	5	6	7
B_i	1,2,3	1,4,5	1,6,7	2,4,6	2,5,7	3,4,7	3,5,6

is the 7×7 matrix

$$A_1 := \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{ccccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \end{array}.$$

The rows and columns are labeled with the chosen ordering of varieties and blocks. Any other ordering will do because the only requirement is that equation (7.1) hold.

As another example, the incidence matrix of the $(10, 5, 6, 3, 3)$ design consisting of the 3-subsets of $[5]$, namely

i	1	2	3	4	5	6	7	8	9	10
B_i	1,2,3	1,2,4	1,2,5	1,3,4	1,3,5	1,4,5	2,3,4	2,3,5	2,4,5	3,4,5

is the 5×10 matrix

$$A_2 := \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array} \begin{array}{c} \begin{array}{cccccccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 & B_8 & B_9 & B_{10} \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \end{array}.$$

Question 282 *How many rows and columns does the incidence matrix for a* $(28, 4, 1)$ *design have?*

Two properties of the incidence matrix

The incidence matrix leads to important theorems in design theory. Let's pave the way for that work with two preliminary results.

To anticipate the first result, examine the following matrix products involving the incidence matrices of the $(7, 7, 3, 3, 1)$ and $(10, 5, 6, 3, 3)$ designs shown earlier:

$$A_1 A_1^T = \begin{pmatrix} 3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 3 \end{pmatrix} \qquad A_2 A_2^T = \begin{pmatrix} 6 & 3 & 3 & 3 & 3 \\ 3 & 6 & 3 & 3 & 3 \\ 3 & 3 & 6 & 3 & 3 \\ 3 & 3 & 3 & 6 & 3 \\ 3 & 3 & 3 & 3 & 6 \end{pmatrix}.$$

Something is going on here: the diagonal entries equal r and the others equal λ.

The definition of matrix multiplication explains this. If A is the incidence matrix of a (b, v, r, k, λ) design, then A is $v \times b$ and the product AA^T is $v \times v$. Any diagonal entry of

AA^T equals

$$\begin{aligned}(AA^T)_{ii} &= (i\text{-th row of } A)\cdot(i\text{-th column of } A^T)\\ &= (i\text{-th row of } A)\cdot(i\text{-th row of } A)\\ &= \text{number of 1s in row } i \text{ of } A\\ &= \text{number of blocks in which variety } i \text{ appears}\\ &= r.\end{aligned}$$

Any off-diagonal entry of AA^T equals (assume $i \neq j$)

$$\begin{aligned}(AA^T)_{ij} &= (i\text{-th row of } A)\cdot(j\text{-th column of } A^T)\\ &= (i\text{-th row of } A)\cdot(j\text{-th row of } A)\\ &= \text{number of columns of } A \text{ in which both row } i \text{ and row } j \text{ have a 1}\\ &= \text{number of blocks in which varieties } i \text{ and } j \text{ appear together}\\ &= \lambda.\end{aligned}$$

So indeed AA^T has r on the diagonal and λ on the off-diagonal.

Question 283 *If A_3 is the incidence matrix of a* $(28, 4, 1)$ *design, then what is $A_3 A_3^T$?*

A useful way to write the product of the incidence matrix with its transpose is as a sum of I and J matrices, where I is an identity matrix and J is a matrix of all 1s, each of appropriate size:

$$AA^T = \begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & r \end{pmatrix} = (r-\lambda)I + \lambda J.$$

The second result we wish to prove involves the determinant of AA^T. We'll content ourselves with computing it in the special case $v = 4$ as the general case is completely analogous. When $v = 4$,

$$AA^T = \begin{pmatrix} r & \lambda & \lambda & \lambda \\ \lambda & r & \lambda & \lambda \\ \lambda & \lambda & r & \lambda \\ \lambda & \lambda & \lambda & r \end{pmatrix}.$$

Recall two basic facts about the determinant: (1) the determinant of a matrix remains unchanged if we use an "add a nonzero multiple of a row/column to another row/column" operation; (2) the determinant of a triangular matrix equals the product of its diagonal entries.

To calculate the determinant, begin by replacing row i by row i minus row 1, for $i = 2, 3, 4$, obtaining

$$\det AA^T = \begin{vmatrix} r & \lambda & \lambda & \lambda \\ \lambda & r & \lambda & \lambda \\ \lambda & \lambda & r & \lambda \\ \lambda & \lambda & \lambda & r \end{vmatrix} = \begin{vmatrix} r & \lambda & \lambda & \lambda \\ \lambda - r & r-\lambda & 0 & 0 \\ \lambda - r & 0 & r-\lambda & 0 \\ \lambda - r & 0 & 0 & r-\lambda \end{vmatrix}.$$

To get it to triangular form replace column 1 by column i plus column 1, for $i = 2, 3, 4$:

$$\det AA^T = \begin{vmatrix} r+3\lambda & \lambda & \lambda & \lambda \\ 0 & r-\lambda & 0 & 0 \\ 0 & 0 & r-\lambda & 0 \\ 0 & 0 & 0 & r-\lambda \end{vmatrix} = (r+3\lambda)(r-\lambda)^3.$$

The last equality follows because the matrix is now (upper) triangular.

Question 284 *For the design of Question 283, guess the determinant of* $A_3 A_3^T$.

The general formula involving v varieties follows easily, and the following theorem states the two results involving the incidence matrix.

Theorem 7.2.1 *If A is the incidence matrix of a (b, v, r, k, λ) design, then*

$$AA^T = (r-\lambda)I + \lambda J$$

and $\det AA^T = \big[r + (v-1)\lambda\big](r-\lambda)^{v-1}$.

Question 285 *Explain why* $\det AA^T = rk(r-\lambda)^{v-1}$ *as well.*

Symmetric designs and the Bruck-Ryser-Chowla theorem

A design is ***symmetric*** provided the number of blocks equals the number of varieties ($b = v$). The formula $bk = vr$ implies that any (b, v, r, k, λ) design with $b = v$ also has $r = k$ and therefore is a (v, v, k, k, λ) design. The familiar $(7, 7, 3, 3, 1)$ design is symmetric.

One of the most celebrated and powerful results in design theory is the Bruck-Ryser-Chowla (BRC) theorem on symmetric designs. It provides a necessary condition for a symmetric design's existence. After giving a partial proof, we explore some consequences.

Theorem 7.2.2 (Bruck-Ryser-Chowla) *If a symmetric (v, k, λ) design exists, then*

- *if v is even, then $k - \lambda$ is a perfect square; and*
- *if v is odd, then the equation*

$$x^2 = (k-\lambda)y^2 + (-1)^{(v-1)/2}\lambda z^2$$

has a nontrivial solution in integers x, y, z.

Partial proof: We prove the theorem only in the case that v is even, since the other case requires a comparatively intricate, number-theoretic argument.

Assume that we have a symmetric (v, k, λ) design with v even and with incidence matrix A. Theorem 7.2.1 and its subsequent Question tell us that

$$\det AA^T = rk(r-\lambda)^{v-1}.$$

Since the design is symmetric, A is square and so $\det AA^T = (\det A)(\det A^T) = (\det A)^2$. In addition, $r = k$ in a symmetric design. Applying this to the above equation shows

$$(\det A)^2 = k^2(k-\lambda)^{v-1}.$$

The left side is a perfect square so the right side is also. Since k^2 is a perfect square, $(k-\lambda)^{v-1}$ is also. But v is even, so $v-1$ is odd and thus $k-\lambda$ is a perfect square. ■

Example: do these designs exist?

What conclusion can you draw from the Bruck-Ryser-Chowla theorem about the existence of designs with the following parameters?

(a) $(111, 111, 11, 11, 1)$

$\Longrightarrow$ Suppose a $(111, 111, 11, 11, 1)$ design exists. Since the number of varieties is odd, the BRC theorem implies that there is a nontrivial solution to

$$x^2 = (11-1)y^2 + (-1)^{(111-1)/2} \cdot 1 \cdot z^2$$

or $x^2 = 10y^2 - z^2$. There is: $(x, y, z) = (3, 1, 1)$. The BRC theorem does not allow us to conclude whether such a design exists. (As mentioned in Section 7.1, such a design does not exist.)

(b) $(22, 22, 7, 7, 2)$

$\Longrightarrow$ Suppose a $(22, 22, 7, 7, 2)$ design exists. Since v is even, the BRC theorem implies that $k - \lambda = 7 - 2 = 5$ is a perfect square. This is a contradiction, so no such design exists. (It is worth noting that $bk = vr$ and $r(k-1) = \lambda(v-1)$, so that the basic necessary conditions do not imply the nonexistence of such a design.)

Question 286 *What does the BRC theorem say about the existence of a* $(16, 6, 2)$ *design?*

Example: does this design exist?

Does a $(43, 43, 7, 7, 1)$ design exist?

Suppose it did. In that case the BRC theorem implies that there exists integers x, y, and z, not all zero, such that $x^2 = 6y^2 - z^2$. Without loss of generality, we may assume that the three integers do not share a common factor. Rewriting as $x^2 + z^2 = 6y^2$, we see that $x^2 + z^2$ must be even. That forces x^2 and z^2, and therefore x and z, to be both even or both odd.

If x and z are both even, then $x = 2k$ and $z = 2l$ for some integers k and l. That implies $(2k)^2 + (2l)^2 = 6y^2$ or $2k^2 + 2l^2 = 3y^2$. Therefore $3y^2$ is even which forces y to be even. Now x, y, and z are all even, but this is a contradiction because they don't share a common factor.

Therefore x and z are both odd. Write $x = 2m + 1$ and $y = 2n + 1$ for some integers m and n. The equation $x^2 + z^2 = 6y^2$ now becomes $(2m+1)^2 + (2n+1)^2 = 6y^2$ or

$$2(m^2 + m + n^2 + n) + 1 = 3y^2.$$

This implies that y is odd, so $y = 2p + 1$ for some integer p. Making that substitution leads to the equation

$$m(m+1) + n(n+1) = 6p^2 + 6p + 1.$$

This is also a contradiction because the left side is even and the right side is odd.

Question 287 *Fill in the missing details (algebraic, logical) in the above proof.*

This exhausts our cases. No nontrivial solution to $x^2 = 6y^2 - z^2$ exists and hence no $(43, 43, 7, 7, 1)$ design exists.

v	k	λ	Parameters	Exists?	Reason
7	3	1	(7, 7, 3, 3, 1)	yes	Section 7.1
7	4	2	(7, 7, 4, 4, 2)	yes	complement of (7, 7, 3, 3, 1)
13	4	1	(13, 13, 4, 4, 1)	yes	cyclic
11	5	2	(11, 11, 5, 5, 2)	yes	Exercise 10, Section 7.1
21	5	1	(21, 21, 5, 5, 1)	yes	cyclic
11	6	3	(11, 11, 6, 6, 3)	yes	complement of (11, 11, 5, 5, 2)
16	6	2	(16, 16, 6, 6, 2)	yes	Exercise 18, Section 7.1
31	6	1	(31, 31, 6, 6, 1)	yes	cyclic
15	7	3	(15, 15, 7, 7, 3)	yes	Section 7.1
22	7	2	(22, 22, 7, 7, 2)	no	BRC theorem (this section)
43	7	1	(43, 43, 7, 7, 1)	no	BRC theorem (this section)
15	8	4	(15, 15, 8, 8, 4)	yes	complement of (15, 15, 7, 7, 3)
29	8	2	(29, 29, 8, 8, 2)	no	BRC theorem (Exercise 2)
57	8	1	(57, 57, 8, 8, 1)	yes	cyclic
13	9	6	(13, 13, 9, 9, 6)	yes	complement of (13, 13, 4, 4, 1)
19	9	4	(19, 19, 9, 9, 4)	yes	cyclic
25	9	3	(25, 25, 9, 9, 3)	yes	see Travel Notes
37	9	2	(37, 37, 9, 9, 2)	yes	cyclic
73	9	1	(73, 73, 9, 9, 1)	yes	cyclic

Table 7.1. All possible nontrivial symmetric designs for $3 \leqslant k \leqslant 9$.

Symmetric designs with $3 \leqslant k \leqslant 9$

It is interesting to investigate the possibility of symmetric designs for relatively small block sizes. Table 7.1 summarizes these possibilities for $3 \leqslant k \leqslant 9$. Notice that a symmetric (v, v, k, k, λ) design has $\lambda = \frac{k(k-1)}{v-1}$, so a choice for v and k automatically determines λ. Thus, for each value of k satisfying $3 \leqslant k \leqslant 9$, the table includes only those values of v for which $\frac{k(k-1)}{v-1}$ is an integer. One exception is when $v = k + 1$. In that case the design is a $(k + 1, k + 1, k, k, k - 1)$ design which is easily constructed. See Exercise 3 of Section 7.1.

For example, when the block size is $k = 8$ the only values of v (assuming of course that $v \geqslant 8$) for which

$$\lambda = \frac{8(8-1)}{v-1} = \frac{56}{v-1}$$

is an integer are $v = 9, 15, 29, 57$. Since the $(9, 9, 8, 8, 7)$ design trivially exists, we only list the three corresponding to $v = 15, 29, 57$.

Question 288 *When $k = 10$, which values of v should be considered? What are the corresponding values of λ?*

Various researchers have settled the existence question for each of these designs. If we address the existence question for a particular design in this book, the table gives its

reference. The word "cyclic" indicates that the design can be constructed via the method of cyclic designs presented in Section 7.1.

The residual design and the derived design

We now explore two construction methods that apply to symmetric designs. Each method builds a non-symmetric design from a symmetric one and therefore adds support to the study of symmetric designs. First, we must understand a property of symmetric designs that justifies the methods.

Symmetric designs are linked

Notice that in the $(7, 7, 3, 3, 1)$ design

$$\{1,2,3\}\quad \{1,4,5\}\quad \{1,6,7\}\quad \{2,4,6\}\quad \{2,5,7\}\quad \{3,4,7\}\quad \{3,5,6\}$$

and in the $(15, 15, 7, 7, 3)$ you constructed in Question 281 on page 279, namely

$$\begin{array}{lll}
\{0,1,2,4,5,8,10\} & \{5,6,7,9,10,13,0\} & \{10,11,12,14,0,3,5\} \\
\{1,2,3,5,6,9,11\} & \{6,7,8,10,11,14,1\} & \{11,12,13,0,1,4,6\} \\
\{2,3,4,6,7,10,12\} & \{7,8,9,11,12,0,2\} & \{12,13,14,1,2,5,7\} \\
\{3,4,5,7,8,11,13\} & \{8,9,10,12,13,1,3\} & \{13,14,0,2,3,6,8\} \\
\{4,5,6,8,9,12,14\} & \{9,10,11,13,14,2,4\} & \{14,0,1,3,4,7,9\},
\end{array} \tag{7.2}$$

any pair of unequal blocks has exactly λ varieties in common. This requires checking $\binom{7}{2} = 21$ pairs in the first design and $\binom{15}{2} = 105$ pairs in the second.

In general, a design is ***l*-linked** provided that $|B_i \cap B_j| = l$ for all blocks B_i and B_j with $i \neq j$. The property observed in the two examples of the previous paragraph happens in general. The proof, asked for in Exercise 12, works with the incidence matrix.

Theorem 7.2.3 *If a BIBD is symmetric, then it is linked. That is, given any symmetric (v, k, λ) BIBD, it follows that every pair of unequal blocks has exactly λ varieties in common.*

The theorem is trivially true in the case of a complete design.

The residual design

Given a symmetric BIBD, we construct the ***residual design*** by (1) choosing any block B_0; (2) deleting B_0; and (3) deleting the varieties in B_0 from the remaining blocks.

For example, the choice of $B_0 := \{9, 10, 11, 13, 14, 2, 4\}$ in the $(15, 15, 7, 7, 3)$ design shown in (7.2) produces the residual design having the following blocks:

$$\begin{array}{lll}
\{0,1,5,8\} & \{5,6,7,0\} & \{12,0,3,5\} \\
\{1,3,5,6\} & \{6,7,8,1\} & \{12,0,1,6\} \\
\{3,6,7,12\} & \{7,8,12,0\} & \{12,1,5,7\} \\
\{3,5,7,8\} & \{8,12,1,3\} & \{0,3,6,8\} \\
\{5,6,8,12\} & & \{0,1,3,7\}.
\end{array}$$

It is a $(14, 8, 7, 4, 3)$ design.

Question 289 *Find the residual design that results from choosing $B_0 := \{1, 6, 7\}$ in the $(7, 7, 3, 3, 1)$ design. Then do the same but choose $B_0 := \{3, 4, 7\}$. Explain why any two residual designs are essentially the same no matter the choice of B_0.*

In general, if we start with a symmetric (v, k, λ) BIBD, the residual design is a $(v - 1, v - k, k, k - \lambda, \lambda)$ design. To justify these parameters, assume we delete the block B_0. This leaves $v - 1$ blocks. When we remove the k varieties in B_0 from the remaining blocks, this leaves $v-k$ varieties. Since the design is λ-linked, each block has λ varieties in common with B_0, so the residual design contains blocks of size $k - \lambda$. Finally, the residual design remains k-uniform and λ-balanced because these properties are inherited from the original, symmetric design.

The derived design

Given a symmetric BIBD, we construct the ***derived design*** by (1) choosing any block B_0; (2) deleting B_0; and (3) replacing each remaining block by its intersection with B_0.

For example, the choice of $B_0 := \{9, 10, 11, 13, 14, 2, 4\}$ in the $(15, 15, 7, 7, 3)$ design leads to the derived design having the following blocks:

$$\begin{array}{lll} \{2,4,10\} & \{9,10,13\} & \{10,11,14\} \\ \{2,9,11\} & \{10,11,14\} & \{11,13,4\} \\ \{2,4,10\} & \{9,11,2\} & \{13,14,2\} \\ \{4,11,13\} & \{9,10,13\} & \{13,14,2\} \\ \{4,9,14\} & & \{14,4,9\}. \end{array}$$

It is a $(14, 7, 6, 3, 2)$ design.

In general, if we start with a symmetric (v, k, λ) BIBD, the derived design is a $(v - 1, k, k - 1, \lambda, \lambda - 1)$ BIBD.

Question 290 *Justify the value of each of these parameters. When do you need the fact that a symmetric design is linked?*

The following theorem summarizes the basic facts about the residual and derived designs.

Theorem 7.2.4 *Given a symmetric (v, k, λ) BIBD,*

- *the residual design is a $(v - 1, v - k, k, k - \lambda, \lambda)$ design, and*
- *the derived design is a $(v - 1, k, k - 1, \lambda, \lambda - 1)$ design.*

In other words, if there exists a symmetric (v, k, λ) BIBD, then there exists both a $(v - 1, v - k, k, k - \lambda, \lambda)$ and a $(v - 1, k, k - 1, \lambda, \lambda - 1)$ design.

It is natural to ask whether the converse is true, as it is in Theorem 7.1.2 on the complementary design. For example, if a $(v - 1, v - k, k, k - \lambda, \lambda)$ design exists, can we always "undo" the process of constructing the residual design to conclude that a symmetric (v, k, λ) design exists? The answer is no. Bhattacharya (1944) gave an example of a $(24, 16, 9, 6, 3)$ design which cannot be embedded as the residual of a symmetric $(25, 9, 3)$ design. See Exercise 13. However, some conditions are known under which such an embedding is possible. See Chapter 16 of Hall (1986).

Example: residual and derived designs

Given a symmetric $(16, 6, 2)$ design, what designs can be constructed from it?

With $(v, k, \lambda) = (16, 6, 2)$, the residual design is a

$$(v - 1, v - k, k, k - \lambda, \lambda) = (15, 10, 6, 4, 2)$$

design and the derived design is a

$$(v-1, k, k-1, \lambda, \lambda-1) = (15, 6, 5, 2, 1)$$

design. We can also construct the complementary design in each case. This gives six designs (including the original one) and they have the following parameters:

$$\begin{array}{lll} (16,16,6,6,2) & (15,10,6,4,2) & (15,6,5,2,1) \\ (16,16,10,10,6) & (15,10,9,6,5) & (15,6,10,4,6). \end{array}$$

Summary

In a symmetric design, the number of blocks equals the number of varieties. They form a well-studied class of BIBDs and many existence/non-existence results are known for them. The Bruck-Ryser-Chowla theorem gives necessary conditions for the existence of symmetric designs, and it has proven to be a rather effective tool for researchers. Symmetric designs are also a source of non-symmetric designs via the methods of the residual design and the derived design.

Linear algebra, and in particular the incidence matrix, plays an important role in the results of this section and indeed the rest of this chapter.

Exercises

1. Find the smallest value of r (where $r > 1$) for which a $(b, v, r, 6, 1)$ design might exist according to all necessary conditions studied so far. Determine b and v for that value of r, and then also determine two more values of r for which such a design might exist.
2. Use the Bruck-Ryser-Chowla theorem to prove that a $(29, 29, 8, 8, 2)$ design does not exist. (Hint: Start off in a similar manner to the example in this section involving a $(43, 7, 1)$ design.)
3. Determine whether a symmetric $(43, 36, 30)$ design exists.
4. Suppose $n \geqslant 2$. What does the BRC theorem say about the existence of a $(n^2 + n + 1, n + 1, 1)$ design? Find two different values of n for which such designs do not exist.
5. Prove that if a design is symmetric with $\lambda = 1$, then there exists an integer n such that the design has parameters $(n^2 + n + 1, n^2 + n + 1, n + 1, n + 1, 1)$. (Such a design is called a ***projective plane***.)
6. You need to construct an $(8, 2, 1)$ design. Can it be constructed by finding the residual or derived design of an appropriate symmetric design? Justify.
7. Construct a $(14, 7, 8, 4, 4)$ design.
8. Consider a symmetric (v, k, λ) BIBD. Show that the residual design of its complementary design has the same parameters as the complementary design of its derived design.
9. Let $\mathcal{D}$ be a design with incidence matrix A. Define the ***dual design of*** $\mathcal{D}$ to be that design with incidence matrix A^T. We use $\mathcal{D}^T$ to denote the dual design.

   Assume that $\mathcal{D}$ is a (b, v, r, k, λ) BIBD. Find a sufficient condition for $\mathcal{D}^T$ to be a BIBD and prove that you are correct. Also, find the parameters of $\mathcal{D}^T$.

10. A ***biplane*** is a symmetric $(v, k, 2)$ design.
    (a) Prove that the parameters of a biplane must satisfy $v = \frac{k(k-1)}{2} + 1$.
    (b) Use any known necessary conditions to determine whether a biplane could exist for each value of k satisfying $3 \leqslant k \leqslant 11$.
11. Prove that no biplane with $k = 12$ exists. (See previous exercise.)
12. Prove Theorem 7.2.3. (Hint: Observe that $AJ = kJ$ and $JA = kJ$ where A is the incidence matrix and J is the all-1s matrix. Justify why A^{-1} exists, then use $AA^T = (k - \lambda)I + \lambda J$ to prove that $A^T A = (k - \lambda)I + \lambda J$ as well.)
13. (based on Hall (1986)) Here is the $(24, 16, 9, 6, 3)$ design of Bhattacharya that we mentioned in this section:

1, 2, 7, 8, 14, 15	3, 5, 7, 8, 11, 13	2, 3, 8, 9, 13, 16
3, 5, 8, 9, 12, 14	1, 6, 7, 9, 12, 13	2, 5, 7, 10, 13, 15
3, 4, 7, 10, 12, 16	3, 4, 6, 13, 14, 15	4, 5, 7, 9, 12, 15
2, 4, 9, 10, 11, 13	3, 6, 7, 10, 11, 14	1, 2, 3, 4, 5, 6
1, 4, 7, 8, 11, 16	2, 4, 8, 10, 12, 14	5, 6, 8, 10, 15, 16
1, 6, 8, 10, 12, 13	1, 2, 3, 11, 12, 15	2, 6, 7, 9, 14, 16
1, 4, 5, 13, 14, 16	2, 5, 6, 11, 12, 16	1, 3, 9, 10, 15, 16
4, 6, 8, 9, 11, 15	1, 5, 9, 10, 11, 14	11, 12, 13, 14, 15, 16

    Find two blocks that have four elements in common, and then use that to explain why this design cannot be the residual of a symmetric $(25, 9, 3)$ design.

Travel Notes

As we will see in Section 7.5, the incidence matrix of a design proves useful in the theory of error-correcting codes as the rows of incidence matrices form such a code. Good references for the reader interested in the complete proof of the Bruck-Ryser-Chowla theorem are Hall (1986) and Van Lint & Wilson (1992). The theorem was first proved for symmetric designs with $\lambda = 1$ in 1949 by Bruck and Ryser. In 1950, Chowla and Ryser completed the proof for general λ. Concerning the note in Table 7.1, see Appendix I of Hall (1986) for an example of a symmetric $(25, 9, 3)$ design.

7.3 Fisher's inequality and Steiner systems

In this section we prove one last necessary condition for the existence of a BIBD and then investigate Steiner triple systems. From there, we generalize the idea of a design to that of a t-design and then introduce general Steiner systems.

Fisher's inequality

In all BIBDs we have encountered so far, the number of varieties does not exceed the number of blocks. This is true in general and was proved by the statistician Fisher (1940). The proof we present uses the incidence matrix and the following facts from linear algebra.

1. If B is $n \times n$ and $\det B \neq 0$, then $\operatorname{rank} B = n$. (Any square matrix with nonzero determinant has full rank.)

2. The inequality $\operatorname{rank} CD \leqslant \operatorname{rank} C$ holds for any matrices C and D, provided CD is defined. (This is sometimes known as the rank-of-products inequality.)
3. The rank of a matrix is at most the number of columns.

Fisher's inequality applies to BIBDs and says $b \geqslant v$, or that the number of blocks is at least as great as the number of varieties.

Question 291 *Give an example to show that Fisher's inequality doesn't necessarily hold for complete designs.*

Theorem 7.3.1 (Fisher's inequality) *In any (b, v, r, k, λ) BIBD, $b \geqslant v$ and $r \geqslant k$.*

Proof: Consider any (b, v, r, k, λ) BIBD with incidence matrix A. By Theorem 7.2.1, we know $\det(AA^T) = rk(r-\lambda)^{v-1}$. But Question 273 shows that $r > \lambda$ in any BIBD, so $\det(AA^T) \neq 0$ and hence $\operatorname{rank} AA^T = v$. Using the facts mentioned before the theorem,

$$v = \operatorname{rank} AA^T \leqslant \operatorname{rank} A \leqslant b$$

which proves Fisher's inequality $b \geqslant v$. The equation $bk = vr$ then implies $r \geqslant k$. ■

Steiner triple systems

A ***triple system*** is 3-uniform design, that is, a $(v, 3, \lambda)$ design. The $(7, 7, 3, 3, 1)$ and $(10, 6, 5, 3, 2)$ designs are triple systems. A ***Steiner triple system*** is a 1-balanced triple system, that is, a $(v, 3, 1)$ design. The $(7, 7, 3, 3, 1)$ design and the $(26, 13, 6, 3, 1)$ design of Figure 7.1 on page 277 are Steiner triple systems. Since the number of varieties v determines the rest of the parameters in a Steiner triple system, a $(v, 3, 1)$ design is sometimes simply called an STS(v) design.

Triple systems are important in design theory for several reasons. For one, design theory began in the mid-1800s with the work of Kirkman and Steiner on the existence of what we now call Steiner triple systems. Also, having $k = 3$ is the smallest value of the block size k for which the existence and construction questions are, in general, nontrivial.

A necessary and sufficient condition

Any STS(v) design, if it exists, is a $(b, v, r, 3, 1)$ design. In the example following Theorem 7.1.1 in Section 7.1, we found that a necessary condition for such a design to exist is $r = \frac{v-1}{2}$ and $b = \frac{v(v-1)}{6}$. That is, v must be odd and $v(v-1)$ must be divisible by 6.

To push this a little farther, divide v by 6 and write $v = 6q + s$ where q is an integer and s is an integer satisfying $0 \leqslant s < 6$. Since v is odd, $s = 1$, 3, or 5. It turns out that Theorem 7.1.1 eliminates the possibility that $s = 5$.

Question 292 *Assume $v = 6q + 5$ and then use $b = \frac{v(v-1)}{6}$ to derive a contradiction.*

This proves that any STS(v) design must have $v = 6q + 1$ or $v = 6q + 3$ for some integer q, which proves the necessary condition in the following theorem. We omit the proof of sufficiency and instead describe construction methods (one in this section, one in Section 7.5) that work in certain cases. A good reference for the proof is Chapter 15 of the book by Hall (1986).

Theorem 7.3.2 *Let $v \geqslant 3$. A Steiner triple system on v varieties exists if and only if either $v \equiv 1 \pmod 6$ or $v \equiv 3 \pmod 6$.*

In other words, a Steiner triple system exists exactly when the number of varieties belongs to the set $\{3, 7, 9, 13, 15, 19, 21, 25, 27, \ldots\}$. Notice that the STS(3) design is trivial. Table 7.2 contains a systematic list of the parameters of Steiner triple systems.

b	v	r	k	λ
1	3	1	3	1
7	7	3	3	1
12	9	4	3	1
26	13	6	3	1
35	15	7	3	1
57	19	9	3	1
70	21	10	3	1
100	25	12	3	1
117	27	13	3	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\frac{v(v-1)}{6}$	v	$\frac{v-1}{2}$	3	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 7.2. The parameters of Steiner triple systems.

A construction method for Steiner triple systems

We now present a method that creates an STS($v_1 v_2$) design from an STS(v_1) and an STS(v_2) design. For example, from an STS(9) and an STS(13) design, we can build an STS(117) design.

To illustrate, we will create an STS(21) design from the STS(3) design

$$V_1 = \{x, y, z\}$$
$$\mathcal{B}_1 = \Big\{\{x, y, z\}\Big\}$$

and the usual STS(7) design

$$V_2 = \{1, 2, 3, 4, 5, 6, 7\}$$
$$\mathcal{B}_2 = \Big\{\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}, \{3, 5, 6\}\Big\}.$$

Table 7.2 reminds us that an STS(21) design has 70 blocks.

The set of varieties of the new design is the set $V_1 \times V_2$, the Cartesian product of V_1 and V_2. To save space, write it as the following set of two-letter words:

$$V_1 \times V_2 = \{x1, x2, \ldots, x7, y1, y2, \ldots, y7, z1, z2, \ldots, z7\}.$$

Now for the blocks. They are constructed as follows.

- Type I: All blocks $\{cm, dm, em\}$ where $\{c, d, e\} \in \mathcal{B}_1$ and $m \in V_2$.
- Type II: All blocks $\{nf, ng, nh\}$ where $n \in V_1$ and $\{f, g, h\} \in \mathcal{B}_2$.
- Type III: All blocks $\{cf, dg, eh\}$ where $\{c, d, e\} \in \mathcal{B}_1$ and $\{f, g, h\} \in \mathcal{B}_2$.

In our example, we include $1 \cdot 7 = 7$ blocks of Type I:

$$\begin{array}{llll} \{x1, y1, z1\} & \{x2, y2, z2\} & \{x3, y3, z3\} & \{x4, y4, z4\} \\ \{x5, y5, z5\} & \{x6, y6, z6\} & \{x7, y7, z7\} & \end{array} \tag{7.3}$$

We include $3 \cdot 7 = 21$ of Type II:

$$\begin{array}{lll} \{x1, x2, x3\} & \{y1, y2, y3\} & \{z1, z2, z3\} \\ \{x1, x4, x5\} & \{y1, y4, y5\} & \{z1, z4, z5\} \\ \{x1, x6, x7\} & \{y1, y6, y7\} & \{z1, z6, z7\} \\ \{x2, x4, x6\} & \{y2, y4, y6\} & \{z2, z4, z6\} \\ \{x2, x5, x7\} & \{y2, y5, y7\} & \{z2, z5, z7\} \\ \{x3, x4, x7\} & \{y3, y4, y7\} & \{z3, z4, z7\} \\ \{x3, x5, x6\} & \{y3, y5, y6\} & \{z3, z5, z6\} \end{array} \tag{7.4}$$

Type III blocks require clarification. We must include all blocks $\{cf, dg, eh\}$ over *all possible permutations* of the varieties in the block $\{c, d, e\}$ and in the block $\{f, g, h\}$. Equivalently, we can fix a particular order of the varieties in the block from $\mathcal{B}_1$ and then include all permutations of the three varieties in each block from $\mathcal{B}_2$. We thus include $1 \cdot 7 \cdot 3! = 42$ blocks of the third type:

$$\begin{array}{lll} \{x1, y2, z3\} & \{x1, y3, z2\} & \{x2, y1, z3\} \\ \{x2, y3, z1\} & \{x3, y1, z2\} & \{x3, y2, z1\} \\ \{x1, y4, z5\} & \{x1, y5, z4\} & \{x4, y1, z5\} \\ \{x4, y5, z1\} & \{x5, y1, z4\} & \{x5, y4, z1\} \\ \{x1, y6, z7\} & \{x1, y7, z6\} & \{x6, y1, z7\} \\ \{x6, y7, z1\} & \{x7, y1, z6\} & \{x7, y6, z1\} \\ \vdots & \vdots & \vdots \\ \{x3, y5, z6\} & \{x3, y6, z5\} & \{x5, y3, z6\} \\ \{x5, y6, z3\} & \{x6, y3, z5\} & \{x6, y5, z3\}. \end{array} \tag{7.5}$$

In total there are $7 + 21 + 42 = 70$ blocks among (7.3), (7.4), and (7.5), and these comprise our new design.

At this point we have a design with $b = 70$, $v = 21$, and $k = 3$. To complete the proof that it is an STS(21) design, we must show that $r = 10$ and $\lambda = 1$ per Table 7.2.

To show $r = 10$, we take a generic variety wi belonging to $V_1 \times V_2$. It appears in Type I blocks exactly one time, in Type II blocks exactly three times, and in Type III blocks exactly $1 \cdot 3! = 6$ times. Thus this variety appears $1 + 3 + 6 = 10$ times total.

Question 293 *Verify that $\lambda = 1$ by taking a generic pair of varieties wi, uj and showing that they appear together exactly once in the new design. (Consider cases based on whether $w = u$, $i = j$, or $w \neq u$ and $i \neq j$.)*

This procedure works in general and proves the existence of many STS(v) designs. For example, since we have constructed STS(3) and STS(7) designs, we know that an STS($3^m 7^n$) design exists for nonnegative integers m and n, not both zero.

Theorem 7.3.3 *If a Steiner triple system on v_1 varieties exists and so does one on v_2 varieties, then a Steiner triple system on $v_1 v_2$ varieties exists.*

t-designs

In a (b, v, r, k, λ) design, any two varieties appear together in exactly λ blocks. One natural generalization of this idea would require instead that any three varieties, or any four varieties, or more, appear together in exactly λ blocks.

In general, we define a t-(v, k, λ) ***design*** to be a design on v varieties and having size-k blocks such that any t varieties appear together in exactly λ blocks. Often this is shortened to just ***t-design***.

Our work from the beginning of this chapter until now has involved 2-designs. That is, any (b, v, r, k, λ) design is a 2-(v, k, λ) design.

Here is an example of a 3-design, specifically a 3-(10, 4, 1) design. It has 10 varieties, 30 blocks of size 4, and every triple of varieties appears together in exactly one block:

$$\begin{array}{lllll} \{1,5,6,10\} & \{1,2,8,9\} & \{2,3,6,7\} & \{3,4,9,10\} & \{4,5,7,8\} \\ \{1,3,4,7\} & \{4,6,8,9\} & \{2,7,8,10\} & \{2,3,5,9\} & \{2,4,5,10\} \\ \{5,6,7,9\} & \{3,6,8,10\} & \{1,3,5,8\} & \{1,7,9,10\} & \{1,2,4,6\} \\ \{2,3,4,8\} & \{2,4,7,9\} & \{3,7,8,9\} & \{3,4,5,6\} & \{3,5,7,10\} \\ \{4,6,7,10\} & \{1,4,5,9\} & \{1,4,8,10\} & \{5,8,9,10\} & \{1,2,5,7\} \\ \{2,5,6,8\} & \{1,6,7,8\} & \{1,2,3,10\} & \{1,3,6,9\} & \{2,6,9,10\}. \end{array} \tag{7.6}$$

At this point, you'll either have to take that latter statement on faith or else check for yourself that it is true for each of the $\binom{8}{3} = 56$ possible 3-subsets of varieties. Exercise 7 provides an interesting way around this and also shows how this particular design was constructed.

Question 294 *The* $(7, 3, 1)$ *design is a* 2-$(7, 3, 1)$ *design. Is it a* t*-design for any other value of* t*? Explain.*

Basic properties of t-designs

Examine the 3-(10, 4, 1) design shown in (7.6). We can determine that such a design must have 30 blocks as follows. There are $\binom{v}{t} = \binom{10}{3}$ possible 3-subsets of varieties, and each must appear in exactly $\lambda = 1$ blocks of the design. This means that there are $\lambda\binom{v}{t} = 1 \cdot \binom{10}{3}$ total 3-subsets to "cover" among the blocks of the design. Each size-4 block contains $\binom{k}{t} = \binom{4}{3}$ possible 3-subsets of varieties. This means that

$$\begin{aligned} b &= \text{number of blocks} \\ &= \frac{\text{total number of } t\text{-subsets to "cover"}}{\text{number of } t\text{-subsets "covered" per block}} \\ &= \frac{\lambda\binom{v}{t}}{\binom{k}{t}} \\ &= \frac{1 \cdot \binom{10}{3}}{\binom{4}{3}} \\ &= 30. \end{aligned}$$

It is also possible to prove that $b\binom{k}{t} = \lambda\binom{v}{t}$ using a combinatorial proof that generalizes the idea used in the proof of Theorem 7.1.1 of Section 7.1.

Question 295 *Provide this proof. (Count pairs of the form* (B, T) *where* B *is a block and* T *is a* t*-subset of* B*.)*

We also can determine that a 3-(10, 4, 1) design has $r = 12$ using a modification of the proof of Theorem 7.1.1. We ask the question: For a fixed variety y, how many pairs (B, T) are possible where B is a block containing y and T is a 3-subset of B containing y?

There are r ways to choose a block B containing variety y. For each such choice, there are $\binom{k-1}{t-1} = \binom{3}{2}$ ways to choose the $t-1=2$ other varieties from B to complete the subset T. Therefore there are $r\binom{k-1}{t-1} = r\binom{3}{2}$ pairs in all.

On the other hand, there are $\binom{v-1}{t-1} = \binom{9}{2}$ ways to choose $t-1=2$ varieties to include with y in the subset T. For each such choice, there is $\lambda = 1$ way to choose a block B containing the varieties in T. Therefore there are $\lambda\binom{v-1}{t-1} = 1 \cdot \binom{9}{2}$ pairs in all.

Setting $r\binom{3}{2} = 1 \cdot \binom{9}{2}$ gives $r = 12$. In the course of our discussion, we have proved the following more general version of Theorem 7.1.1.

Theorem 7.3.4 *If a t-(v,k,λ) design exists, then $b\binom{k}{t} = \lambda\binom{v}{t}$ and $r\binom{k-1}{t-1} = \lambda\binom{v-1}{t-1}$.*

Much more work can be done. In fact, any t-design is also an i-design for all $i < t$. For example, the 3-design we showed earlier is also a 2-design and hence an ordinary BIBD.

Question 296 *When treated as a 2-design, what are the parameters (b,v,r,k,λ) of the 3-$(10,4,1)$ design shown in (7.6)?*

The following result, sometimes called the *parameter theorem*, makes this precise. One possible proof follows a line of reasoning similar to that used in the proof of Theorem 7.3.4. We leave it to Exercise 10.

Theorem 7.3.5 (parameter theorem) *If $\mathcal{D}$ is a t-(v,k,λ) design and i satisfies $0 \leqslant i < t$, then $\mathcal{D}$ is also an i-(v,k,λ_i) design where λ_i satisfies $\lambda_i\binom{k-i}{t-i} = \lambda\binom{v-i}{t-i}$.*

Question 297 *In the statement of the theorem, what are λ_0 and λ_1 in terms of more familiar design parameters?*

Two examples follow that illustrate this theorem.

Example: a 2-design from a 3-design

Suppose we have a 3-$(8,4,1)$ design. (See Exercise 6 for an example of one.) When considered a 2-design, what are its parameters?

The parameter theorem implies that it is a 2-$(8,4,\lambda_2)$ design where λ_2 satisfies

$$\lambda_2\binom{4-2}{3-2} = 1 \cdot \binom{8-2}{3-2}$$

which gives $\lambda_2 = 3$. Therefore it is a 2-$(8,4,3)$ design, or equivalently a $(14,8,7,4,3)$ BIBD.

Example: does this design exist?

What do the necessary conditions of Theorems 7.3.4 and 7.3.5 imply about the existence of a 4-$(20,6,10)$ design?

If such a design exists, then by Theorem 7.3.4 it would have

$$b = \frac{\lambda\binom{v}{t}}{\binom{k}{t}} = \frac{10 \cdot \binom{20}{4}}{\binom{6}{4}} = 3230$$

and

$$r = \frac{\lambda\binom{v-1}{t-1}}{\binom{k-1}{t-1}} = \frac{10\binom{19}{3}}{\binom{5}{3}} = 969.$$

That is, it would have 3230 blocks and each variety would appear in exactly 969 blocks. Since each of these numbers is an integer, this does not rule out the existence of this design.

By Theorem 7.3.5, the design would also be a 3-$(20, 6, \lambda_3)$ design, where

$$\lambda_3 = \frac{\lambda\binom{v-3}{t-3}}{\binom{k-3}{t-3}} = \frac{10 \cdot \binom{17}{1}}{\binom{3}{1}} = \frac{170}{3}.$$

Since λ_3 is not an integer, we conclude that no 4-$(20, 6, 10)$ design exists.

Steiner systems

To close, we briefly mention an important and well-studied class of t-designs. A ***Steiner system*** is a t-design with $\lambda = 1$. In other words, a Steiner system is a t-$(v, k, 1)$ design. This is usually abbreviated $\mathrm{S}(t, k, v)$. The all-purpose $(7, 3, 1)$ design is an $\mathrm{S}(2, 3, 7)$ design, and indeed any Steiner triple system is an $\mathrm{S}(2, 3, v)$ design. The design shown in (7.6) is an $\mathrm{S}(3, 4, 10)$ design.

Unlike Theorem 7.3.2, which gives a necessary and sufficient condition for the existence of a Steiner triple system, no comparable theorem is known for more general Steiner systems. We have seen examples of an $\mathrm{S}(t, k, v)$ design for $t = 2, 3$. Examples exist for $t = 4, 5$ but this is the end of our knowledge—the question of whether one exists for $t > 5$ remains an open problem. The largest (in terms of the number of blocks) known Steiner system with $t = 5$ is an $\mathrm{S}(5, 6, 84)$ design.

Question 298 *What are b and r for an* $\mathrm{S}(5, 6, 84)$ *design?*

As we will see in Section 7.5, error-correcting codes can be a source of Steiner systems.

Summary

Fisher's inequality rounds out the list of basic relationships that are necessary for the existence of a BIBD: $bk = vr$, $r(k-1) = \lambda(v-1)$, $b \geq v$, $r \geq k$, $v > k$, and $r > \lambda$. A generalization of a (v, k, λ) design is a t-(v, k, λ) design, wherein every t-subset of varieties appears in exactly λ blocks. A Steiner system is a t-design with $\lambda = 1$. While a complete answer is known to the existence question concerning Steiner triple systems, which are 2-$(v, 3, 1)$ designs, the construction of Steiner systems for $t > 2$ is a much more complicated problem.

Exercises

1. How many symmetric Steiner triple systems are there? Justify your answer.
2. Construct an $\mathrm{STS}(9)$ design.
3. Find all values of λ for which a triple system on six varieties exists. For each such value of λ, either give a design or explain how to construct it.
4. (graph theory) Prove that there exists an $\mathrm{STS}(v)$ design if and only if it is possible to partition the edges of the complete graph K_v into edge-disjoint subgraphs each of which is K_3.
5. Prove Theorem 7.3.3 by generalizing the argument given for the $v_1 = 3$ and $v_2 = 7$ example in the text.

6. Consider the $(7, 3, 1)$ design of Section 7.1. Define a new design $\mathcal{D}$ as follows. It has eight varieties and 14 blocks, where the blocks are of two types: (I) the blocks of the $(7, 3, 1)$ design but with variety 8 added to each; (II) the blocks of the complementary design to the $(7, 3, 1)$ design.

   Prove that this is an $S(3, 4, 8)$ design. (When you prove $\lambda = 1$, do so by using the structure of the $(7, 3, 1)$ design and its complement; do not check all $\binom{8}{3}$ possible 3-subsets of V by brute force.)

7. (graph theory) Here is a way to construct the 3-$(10, 4, 1)$ design shown in this section. Draw the complete graph K_5 and label its edges 1-10. The varieties for the design are the edges: $V = [10]$. The blocks are of three types: (I) edges in a subgraph isomorphic to $K_{1,4}$; (II) edges in a subgraph isomorphic to $K_2 \cup C_3$; (III) edges in a subgraph isomorphic to C_4.

   (a) List all of the blocks. How many of each type are there?

   (b) Using the graph structure, prove that this is a 3-design with $\lambda = 1$.

8. (graph theory) Along the lines of the previous example, consider the following design. The varieties are the (labeled) edges of the complete graph K_6. The blocks are of two types: (I) edges in a perfect matching[1]; (II) edges in a subgraph isomorphic to C_3. Determine the parameters so that this design is a t-(v, k, λ) design and prove that you are correct.

9. Might a 3-$(16, 6, 2)$ design exist according to the necessary conditions of Theorems 7.3.4 and 7.3.5? Explain.

10. Prove the parameter theorem (Theorem 7.3.5).

Travel Notes

For further reading, Hall (1986) is an excellent advanced reference on design theory. It includes a comprehensive list of known results on the existence/nonexistence of BIBDs with $3 \leqslant r \leqslant 20$.

7.4 Perfect binary codes

For the moment we leave the field of design theory and take up the study of error-correcting codes. Our goal in this section is to understand the construction of a certain type of error-correcting code. Let's jump right in and see how such a code works.

The Hamming $(7, 2^4, 3)$ code

A probe sent to the farthest reaches of our solar system transmits pictures back to Earth. Each picture is a grayscale image made of pixels where each pixel has an intensity value from 0 (black) to 15 (white).[2] Picture transmission is a "one-shot" affair: we get one and only one chance to transmit each picture so it must be done accurately. The remote location

[1] A ***perfect matching*** in a graph G with n vertices is a set of $n/2$ edges, no two of which meet at a vertex.

[2] This small range of values suits to illustrate the idea. Grayscale values 0–63 or 0–255 are more typical in applications.

of the probe and its limited power supply prevent us from repairing it or retransmitting an image.

With the agreement that each picture requires accurate transmission comes the sober realization that errors in transmission can happen. Problems may occur with the probe's equipment, with the equipment here on Earth, or even in between such as interference from atmospheric or cosmic effects. Many of these are beyond the control of scientists and engineers. Can a transmission method guard against them?

The code shown in Table 7.3 provides an ingenious way to do so. It contains a list of some 7-digit binary numbers, called *codewords*, along with their grayscale equivalents. This code is called the Hamming $(7, 2^4, 3)$ code. The first parameter indicates that each codeword has length 7 and the second that there are 2^4 codewords. The third indicates that the code has minimum distance 3, and we shall see what this means later in this section. To transmit a pixel having grayscale value 11, the probe sends `1011010`. To transmit grayscale 3, it sends `0011001`.

Codeword	Intensity (grayscale)	Codeword	Intensity (grayscale)
0000000	0	1000011	8
0001111	1	1001100	9
0010110	2	1010101	10
0011001	3	1011010	11
0100101	4	1100110	12
0101010	5	1101001	13
0110011	6	1110000	14
0111100	7	1111111	15

Table 7.3. The Hamming $(7, 2^4, 3)$ code applied to transmitting a grayscale image.

Imagine the probe sends a certain grayscale value and Earth receives `1010001`. This word does not appear on the list of codewords so it has no grayscale equivalent. But it is *close* to codeword `1010101` which corresponds to grayscale 10; in fact the two words only differ by one digit. Similarly, the non-codeword `1101011` differs from `1101001` (grayscale 13) by only one digit.

What makes the code ingenious is the following remarkable property: each of the $2^7 = 128$ possible 7-digit binary numbers is either one of the 16 codewords or else differs from a unique codeword in *exactly one* digit. In our application this means that Earth can receive the exact image the probe originally sent even when one error is made in transmitting each grayscale value. If Earth receives a 7-digit binary number that is not on the codeword list, simply replace it by the codeword closest to that number. Under the assumption that at most one error is made in transmitting each grayscale value, this decoding method ensures the correct reception of the original image.

Of course all bets are off under the possibility of more than one error in the transmission of a single grayscale value. For example, suppose at most two errors are made in transmitting each grayscale value. If Earth receives `1010000`, then did the probe originally send `0000000` (grayscale 0) or `1010101` (grayscale 10) or `1110000` (grayscale 14)? These correspond to black, light gray, and almost white, respectively, so this affects picture accuracy significantly.

An improved code would correct more errors but the ability to correct even just one error is a worthy achievement. Intuitively, the ability to correct more than one error would necessitate longer codewords. However, shorter codewords are certainly desirable inasmuch as they require less storage space and allow for faster transmission.

The mathematical properties and trade-offs of error-correcting codes are just as interesting as the practical considerations that arise from the applications themselves. For one, we shall see that so-called perfect binary codes, of which the Hamming $(7, 2^4, 3)$ code is one example, are rather rare. We focus on the existence and construction questions involving perfect codes and leave the all-important and equally interesting field of decoding to other sources.

Binary codes

Let $\mathbb{B}^n$ be the set of all n-digit binary numbers. A ***binary code*** is any nonempty subset of $\mathbb{B}^n$, and the elements of this set are called ***codewords***. Any point in $\mathbb{B}^n$ that is not a codeword is called a ***word***. In the context of sending messages, the ***codewords*** are just those points in $\mathbb{B}^n$ to which we have attached a meaning. All other words have no meaning and result from the faulty transmission of a codeword. The Hamming $(7, 2^4, 3)$ code is a binary code on $\mathbb{B}^7$.

We will need ways of combining, scaling, and measuring distance between codewords, so really we treat $\mathbb{B}^n$ as a vector space with the familiar operations of addition and scalar multiplication, but taken component-wise modulo 2. An example of addition in $\mathbb{B}^6$ is

$$101110 \oplus 011000 = 110110.$$

The $\oplus$ operator reminds us we are performing addition modulo 2 in each component. The rules are: $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$, and $1 + 1 = 0$. The scalar multiplication operation is also easy: for example, $0(101110) = 000000$ and $1(101110) = 101110$.

Hamming distance

The key concept that drives both the error-correcting abilities and the decoding method is that of distance. The ***Hamming distance*** between words $\mathbf{v}$ and $\mathbf{w}$ in $\mathbb{B}^n$ is defined as

$$h(\mathbf{v}, \mathbf{w}) := \text{number of components in which } \mathbf{v} \text{ and } \mathbf{w} \text{ differ.}$$

For example, in $\mathbb{B}^6$ we have $h(101110, 011000) = 4$ and $h(000000, 010001) = 2$.

Question 299 *Let* $\mathbf{v}$ *and* $\mathbf{w}$ *be words in* $\mathbb{B}^n$*, and let* $\mathbf{0}$ *be the all-0 word. Explain why* $h(\mathbf{v}, \mathbf{w})$ *equals the number of 1s in* $\mathbf{v} \oplus \mathbf{w}$*. Then, explain why* $h(\mathbf{v}, \mathbf{w}) = h(\mathbf{0}, \mathbf{v} \oplus \mathbf{w})$.

The Hamming distance h satisfies the mathematical properties of a ***metric***. These properties are as follows.

M1 For each $\mathbf{v}, \mathbf{w} \in \mathbb{B}^n$ we have $h(\mathbf{v}, \mathbf{w}) \geqslant 0$. In addition, $h(\mathbf{v}, \mathbf{w}) = 0$ if and only if $\mathbf{v} = \mathbf{w}$.

M2 For each $\mathbf{v}, \mathbf{w} \in \mathbb{B}^n$ we have $h(\mathbf{v}, \mathbf{w}) = h(\mathbf{w}, \mathbf{v})$.

M3 For each $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{B}^n$ we have $h(\mathbf{u}, \mathbf{w}) \leqslant h(\mathbf{u}, \mathbf{v}) + h(\mathbf{v}, \mathbf{w})$.

The familiar Euclidean distance formula used in algebra and calculus as well as the absolute value function are other examples of metrics. Properties M1 and M2 follow easily

from the definition of Hamming distance. Property M3, known as the triangle inequality, follows by component-wise analysis. See Exercise 2.

The ***weight*** of a word in $\mathbb{B}^n$ is the number of 1s in that word. We use $\mathrm{wt}(\mathbf{v})$ to denote the weight of $\mathbf{v}$. For example, $\mathrm{wt}(010111) = 4$.

Question 300 *Express* $\mathrm{wt}(\mathbf{v})$ *in terms of the Hamming distance metric. Then express* $h(\mathbf{v}, \mathbf{w})$ *in terms of the weight function.*

Spheres

At the beginning of this section, we claimed that the Hamming $(7, 2^4, 3)$ code had the property that each word in $\mathbb{B}^7$ is within distance 1 of exactly one codeword. The concept of a sphere helps us visualize and analyze this idea.

For a given word $\mathbf{v} \in \mathbb{B}^n$ and a nonnegative integer r, the ***sphere of radius*** r ***centered at*** $\mathbf{v}$ contains all words in $\mathbb{B}^n$ within distance r of $\mathbf{v}$. That is,

$$S_r(\mathbf{v}) := \left\{\mathbf{w} \in \mathbb{B}^n : h(\mathbf{v}, \mathbf{w}) \leqslant r\right\}.$$

For example, in $\mathbb{B}^6$ we have

$$S_0(010111) = \{010111\}$$
$$S_1(010111) = \{010111, 110111, 000111, 011111, 010011, 010101, 010110\}.$$

Also notice that $S_6(010111) = \mathbb{B}^6$ because any word in $\mathbb{B}^6$ is within distance 6 of any other word.

Question 301 *How many words are in* $S_2(010111)$*? In* $S_3(010111)$*? Count them by a method other than listing them all out.*

Figure 7.3 shows a partial visualization of the spheres of radius 1 around each codeword of the Hamming $(7, 2^4, 3)$ code. Each of the three complete spheres shown contains its corresponding codeword in bold as well as the the other seven words in $\mathbb{B}^7$ that are distance 1 from the codeword. Indeed, the 16 spheres of radius 1 partition the set $\mathbb{B}^7$ into 16 blocks. We will prove this later.

Error-correcting capability

As we focus on how to construct a code in order to achieve certain guarantees on its error-correcting abilities, we next seek to understand the relationship between the number of errors a code can correct and the distance between codewords. Intuitively, the codewords should be sufficiently "spread out" so that their corresponding spheres don't overlap. The method of decoding a message by replacing each word by the codeword closest to it is called ***minimum distance decoding***.

In the Hamming $(7, 2^4, 3)$ code of Table 7.3, the minimum distance between any two codewords is 3. Proving so requires two things, namely

- checking that $h(\mathbf{c}_1, \mathbf{c}_2) \geqslant 3$ for all distinct codewords $\mathbf{c}_1$ and $\mathbf{c}_2$, and
- finding two codewords that are exactly distance 3 apart.

The first part involves $\binom{16}{2} = 120$ pairs which is tedious but possible. Once accomplished, the second part follows by observing, say, that $h(0000000, 0010110) = 3$.

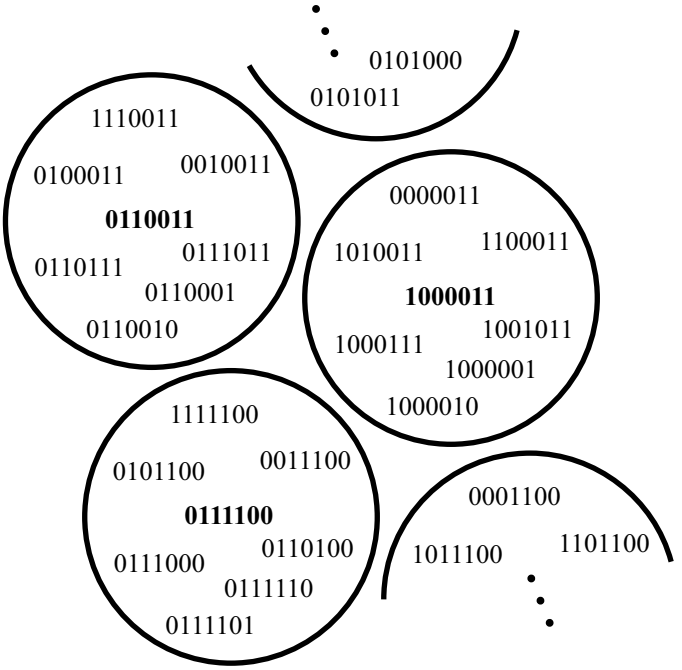


Figure 7.3. Some radius-1 spheres of the Hamming $(7, 2^4, 3)$ code.

Given a binary code $\mathcal{C}$, we say it has ***minimum distance*** d provided that d is the minimum value of the Hamming distance between any two codewords:

$$d := \min\left\{h(\mathbf{c}, \mathbf{c}') : \mathbf{c}, \mathbf{c}' \in \mathcal{C} \text{ and } \mathbf{c} \neq \mathbf{c}'\right\}.$$

We refer to a code using the triple

(length of codewords, number of codewords, minimum distance).

So if $\mathcal{C}$ is a code on $\mathbb{B}^n$ with minimum distance d, we call it a $(n, |\mathcal{C}|, d)$ ***binary code***, where $|\mathcal{C}|$ is the size of the set $\mathcal{C}$.

Once we know the minimum distance of a code, the following theorem tells us its error-correcting capability.

Theorem 7.4.1 *If $\mathcal{C}$ is a binary code and the minimum distance between any two codewords is d, then $\mathcal{C}$ can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors using minimum distance decoding. Furthermore, this is best possible.*

Proof: Assume that $\mathcal{C}$ is a code on $\mathbb{B}^n$ that has minimum distance d. Suppose the codeword $\mathbf{c} \in \mathcal{C}$ is sent, the word $\mathbf{v} \in \mathbb{B}^n$ is received, and at most $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors are made in transmission. This means that the distance between $\mathbf{c}$ and $\mathbf{v}$ satisfies

$$h(\mathbf{c}, \mathbf{v}) \leqslant \left\lfloor \frac{d-1}{2} \right\rfloor,$$

so that $\mathbf{v}$ is in the sphere of radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ centered at the codeword $\mathbf{c}$.

We must show that this word $\mathbf{v}$ does not belong to any other sphere of radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ centered at any other codeword. To this end, let $\mathbf{c}'$ be any codeword other than $\mathbf{c}$. By assumption, $h(\mathbf{c}, \mathbf{c}') \geqslant d$. By the triangle inequality, $h(\mathbf{c}, \mathbf{c}') \leqslant h(\mathbf{c}, \mathbf{v}) + h(\mathbf{v}, \mathbf{c}')$. Therefore

$$\begin{aligned} h(\mathbf{v}, \mathbf{c}') &\geqslant h(\mathbf{c}, \mathbf{c}') - h(\mathbf{c}, \mathbf{v}) \\ &\geqslant d - h(\mathbf{c}, \mathbf{v}) && \text{since } h(\mathbf{c}, \mathbf{c}') \geqslant d \\ &\geqslant d - \frac{d-1}{2} && \text{since } h(\mathbf{c}, \mathbf{v}) \leqslant \left\lfloor \frac{d-1}{2} \right\rfloor \leqslant \frac{d-1}{2} \\ &= \frac{d+1}{2} \\ &> \left\lfloor \frac{d-1}{2} \right\rfloor. \end{aligned}$$

This proves $h(\mathbf{v}, \mathbf{c}') > \left\lfloor \frac{d-1}{2} \right\rfloor$ and so $\mathbf{v}$ does not belong to any sphere of radius $\left\lfloor \frac{d-1}{2} \right\rfloor$ centered at a codeword other than $\mathbf{c}$. This completes the proof that $\mathcal{C}$ can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. We defer the proof that this is best possible—that it cannot correct more than this many errors—to Exercise 9. ■

Another way to state this theorem is: If $\mathcal{C}$ is a binary code and the minimum distance between any two codewords is $2e + 1$, then $\mathcal{C}$ can correct up to e errors using minimum distance decoding.

Question 302 *Consider the following code on* $\mathbb{B}^4$*:*

$$\mathcal{C} = \{0000, 1100, 0110, 0011, 1111\}.$$

What is its minimum distance? How many errors can it correct? Draw a diagram like Figure 7.3 but containing all 16 words in $\mathbb{B}^4$ *along with the five codeword spheres.*

The sphere packing bound and perfect codes

We next derive a condition that will limit our search for so-called perfect codes significantly. It involves a counting argument.

If $\mathcal{C}$ is a code on $\mathbb{B}^n$, then the number of words in any sphere of radius e centered at a codeword $\mathbf{c}$ is

$$\sum_{i=0}^{e} \binom{n}{i}$$

because there are $\binom{n}{0}$ words that differ from $\mathbf{c}$ in zero places, $\binom{n}{1}$ words that differ from $\mathbf{c}$ in exactly one place, and so on up to $\binom{n}{e}$ that differ in exactly e places. (In Question 301, your answers should have been $\binom{6}{0} + \binom{6}{1} + \binom{6}{2} = 22$ and $\binom{6}{0} + \binom{6}{1} + \binom{6}{2} + \binom{6}{3} = 42$, respectively.) In Figure 7.3, each radius-1 sphere contains $\binom{7}{0} + \binom{7}{1} = 8$ words.

If the code corrects up to e errors, then the radius-e spheres centered at the codewords are disjoint. Taken together, they cannot contain more than the whole set of words $\mathbb{B}^n$.

Therefore,

$$|\mathcal{C}| \cdot \sum_{i=0}^{e} \binom{n}{i} \leqslant 2^n \qquad \text{or} \qquad |\mathcal{C}| \leqslant \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}}. \tag{7.7}$$

This is called the ***sphere packing bound*** or sometimes the ***Hamming bound*** because it limits the number of codewords based on the disjoint-spheres requirement. Any code for which the sphere packing bound (7.7) holds at equality is a ***perfect code***. The following theorem is immediate.

Theorem 7.4.2 (sphere packing bound) *If $\mathcal{C}$ is a perfect code on $\mathbb{B}^n$ that corrects up to e errors, then $\sum_{i=0}^{e} \binom{n}{i}$ must be a power of 2. In that case, $\mathcal{C}$ contains $\frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}}$ codewords.*

Trivial and nontrivial codes

A code on $\mathbb{B}^n$ that corrects either 0 or n errors is a ***trivial code***. Any other code is a ***nontrivial code***. The following question asks you to explain why trivial codes deserve their name.

Question 303 *Define the following codes on $\mathbb{B}^3$:*

$$\mathcal{C}_1 = \{000, 001, 010, 100, 011, 101, 110, 111\}$$
$$\mathcal{C}_2 = \{000\}.$$

Explain why the first one corrects zero errors and the second corrects three errors. Then, explain why both are useless for the purpose of transmitting information in the error-correcting context.

Example: existence of a nontrivial perfect code

Can a nontrivial perfect code exist on $\mathbb{B}^6$?

Suppose one did. Theorem 7.4.2 implies that $\sum_{i=0}^{e} \binom{6}{i}$ is a power of 2 for some e satisfying $1 \leqslant e \leqslant 5$. (Remember, $e = 0$ and $e = 6$ correspond to trivial codes.) Since

$$\begin{aligned}
\tbinom{6}{0} + \tbinom{6}{1} &= 7 \\
\tbinom{6}{0} + \tbinom{6}{1} + \tbinom{6}{2} &= 22 \\
\tbinom{6}{0} + \tbinom{6}{1} + \tbinom{6}{2} + \tbinom{6}{3} &= 42 \\
\tbinom{6}{0} + \tbinom{6}{1} + \tbinom{6}{2} + \tbinom{6}{3} + \tbinom{6}{4} &= 57 \\
\tbinom{6}{0} + \tbinom{6}{1} + \tbinom{6}{2} + \tbinom{6}{3} + \tbinom{6}{4} + \tbinom{6}{5} &= 63
\end{aligned}$$

and none of these is a power of 2, we have a contradiction. No nontrivial perfect code on $\mathbb{B}^6$ exists.

Question 304 *Might a nontrivial perfect code on $\mathbb{B}^{15}$ exist according to Theorem 7.4.2? If so, how many errors would it correct?*

Necessary conditions for perfect 1-error-correcting binary codes

If a perfect binary code can correct $e = 1$ error, then by Theorem 7.4.2 it contains

$$\frac{2^n}{\binom{n}{0} + \binom{n}{1}} = \frac{2^n}{1 + n}$$

codewords, where $1 + n$ is a power of 2. Writing $1 + n = 2^m$ for some integer m gives $n = 2^m - 1$. Therefore if a perfect 1-error-correcting code exists, it must exist in $\mathbb{B}^{2^m-1}$ where m is some integer. In that case the number of codewords is

$$\frac{2^n}{1+n} = \frac{2^{2^m-1}}{1+2^m-1} = 2^{2^m-m-1}.$$

This code would need to achieve a minimum distance of $d = 2e + 1 = 3$ between codewords. If it exists, we shall refer to this as a $(2^m - 1, 2^{2^m-m-1}, 3)$ binary code. When $m = 3$, we have the familiar $(7, 2^4, 3)$ binary code.

Construction of perfect 1-error-correcting binary codes

We now show that $(2^m - 1, 2^{2^m-m-1}, 3)$ binary codes exist for all $m \geqslant 2$ and therefore prove that the necessary conditions just derived are also sufficient. These codes will be perfect 1-error-correcting codes. We will construct them using a matrix.

Linear codes and generator matrices

A ***linear code*** on $\mathbb{B}^n$ is a vector subspace of $\mathbb{B}^n$. Equivalently, a linear code on $\mathbb{B}^n$ is the set of all linear combinations of the rows of a $k \times n$ matrix, each entry being 0 or1. That matrix is called a ***generator matrix*** for the code.

An examination of the Hamming $(7, 4, 3)$ code of Table 7.3 reveals that if we chop off the last three digits of each codeword, a list of all 16 four-digit binary numbers remains. To construct this code via linear combinations of the rows of a matrix, then, it makes sense to start with the matrix

$$G_7 := \begin{pmatrix} 1 & 0 & 0 & 0 & * & * & * \\ 0 & 1 & 0 & 0 & * & * & * \\ 0 & 0 & 1 & 0 & * & * & * \\ 0 & 0 & 0 & 1 & * & * & * \end{pmatrix}$$

where the $*$'s are to be determined. The presence of the 4×4 identity matrix makes encoding easy.

Question 305 *Assuming the $*$'s in the matrix G_7 have been correctly determined, how would you write 1011010 as a linear combination of the rows of G_7? How would you write 0010110?*

Now we must determine the $*$'s so the code can correct up to one error. The relationship between error correction and minimum distance described in Theorem 7.4.1 tells us that the distance between any two codewords must be at least 3. So, it not only has to be the case that the distance between any two rows of G_7 is at least 3 (for each row will be one of the codewords), the same has to be true for all 16 possible linear combinations of the rows.

First observe that no row of G_7 can have fewer than three 1s. This is because $\mathbf{0} = 0000000$ is a codeword (it equals the all-0 linear combination) and the distance between $\mathbf{0}$ and any word equals the number of 1s in that word. Therefore in each row, at least two of the three $*$'s must be 1s. So the $***$ portion of each row of G_7 must be chosen from 011, 101, 110, and 111.

Question 306 *Why is the minimum distance requirement not satisfied if the same 3-digit number occupies the $***$ portion portion of two different rows of G_7?*

This forces us into using each of 011, 101, 110, and 111 exactly once. We choose

$$G_7 := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{7.8}$$

But if we generate all 16 possible codewords via linear combinations of these four rows, will we achieve the minimum distance requirement? The following theorem equates the problem of finding the minimum distance with the (typically easier) problem of finding a nonzero linear combination of minimum weight. We postpone the proof until we illustrate how to apply it to the matrix G_7 shown above.

Theorem 7.4.3 *If G is a 0-1 matrix and $\mathcal{L}$ is the set of all linear combinations of the rows of G, working modulo 2, then the minimum Hamming distance between any two elements of $\mathcal{L}$ equals the minimum weight of a nonzero element of $\mathcal{L}$.*

Here is how the theorem allows us to conclude that the code generated by the matrix G_7 has minimum distance 3: it is enough to consider every possible nonzero linear combination of the rows of G_7 and make sure that the result is a word of weight at least 3. A representative linear combination looks like

$$a_1 R_1 \oplus a_2 R_2 \oplus a_3 R_3 \oplus a_4 R_4$$

where R_i is row i of G_7 and each of the coefficients a_i is 0 or 1. Actually, the latter requirement effectively means that each row is either "in" (coefficient 1) or "out" (coefficient 0) of the linear combination. (This is a convenience enjoyed only by binary codes. We shall see examples of non-binary codes in Section 7.5.)

First observe that each row (i.e., linear combination with exactly one coefficient equal to 1) has weight at least 3. For any linear combination involving two rows, there will be two 1s among the first four columns and at least one 1 among the last three, so the weight is at least 3. For any involving three or more rows, there will be at least three 1s among the first three columns, and hence the weight will be at least 3. Therefore all nonzero linear combinations produce elements of weight at least 3. Observing that the first row of G_7 has weight exactly 3, we conclude that the minimum weight of a nonzero linear combination is 3. By the theorem, the minimum distance between any two codewords is 3.

Question 307 *Define*

$$G := \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

The code generated by linear combinations of its rows has $2^3 = 8$ codewords. What is the minimum distance between codewords? How many errors can this code correct?

Proof of the theorem

Proof of Theorem 7.4.3: Assume A is a 0-1 matrix and $\mathcal{L}$ is the set of all linear combinations of its rows, working modulo 2. Let d be the minimum Hamming distance between any two elements of $\mathcal{L}$, and let w be the minimum weight of a nonzero element of $\mathcal{L}$. We must show that $w = d$.

Let $\mathbf{u}, \mathbf{v} \in \mathcal{L}$ satisfy $h(\mathbf{u}, \mathbf{v}) = d$. Then $\text{wt}(\mathbf{u} \oplus \mathbf{v}) = d$ as well (see Question 300). Since $\mathcal{L}$ is closed under addition, $\mathbf{u} \oplus \mathbf{v}$ is also an element of $\mathcal{L}$. This implies $w \leqslant d$ because $\mathbf{u} \oplus \mathbf{v}$ is a nonzero element of $\mathcal{L}$ having weight d, and w is the minimum weight over all nonzero elements of $\mathcal{L}$.

For sake of contradiction, assume that $w < d$. Then there exists a nonzero element $\mathbf{x} \in \mathcal{L}$ for which $\text{wt}(\mathbf{x}) = w < d$. But then $h(\mathbf{0}, \mathbf{x}) = w < d$ and so there are two elements in $\mathcal{L}$ that are closer than d units apart. This contradicts the fact that d is the minimum distance. Therefore $w \geqslant d$ and this completes the proof. ■

The Hamming codes

The generator matrix construction of the Hamming $(7, 2^4, 3)$ code easily generalizes to build perfect $(2^m - 1, 2^{2^m - m - 1}, 3)$ binary codes. These codes are called ***Hamming codes*** after their founder Richard Hamming.

Theorem 7.4.4 (Hamming) *For any integer m with $m \geqslant 2$, there exists a perfect $(2^m - 1, 2^{2^m - m - 1}, 3)$ code. This code is a 1-error-correcting code on $\mathbb{B}^{2^m - 1}$ containing $2^{2^m - m - 1}$ codewords.*

Proof: Assume $m \geqslant 2$. Define the matrix

$$G := [\, I \mid A \,]$$

where

- I is the $(2^m - m - 1) \times (2^m - m - 1)$ identity matrix.
- A is any $(2^m - m - 1) \times m$ matrix whose rows contain all those words in $\mathbb{B}^m$ with at least two 1s.

Notice that $\mathbb{B}^m$ contains one word with zero 1s and m words with exactly one 1, so indeed $2^m - m - 1$ words in $\mathbb{B}^m$ have at least two 1s.

We claim that G generates a perfect $(2^m - 1, 2^{2^m - m - 1}, 3)$ code. The rows of G contain $2^m - m - 1 + m = 2^m - 1$ entries and hence are in $\mathbb{B}^{2^m - 1}$. Because of the presence of the $(2^m - m - 1) \times (2^m - m - 1)$ identity matrix on the left of G, each of the $2^{2^m - m - 1}$ possible linear combinations of rows of G produces a different codeword, so there are indeed $2^{2^m - m - 1}$ codewords in this code.

We now show that every nonzero codeword has weight at least 3. Any codeword that is a single row of G has one 1 among the first $2^m - m - 1$ entries and at least two 1s among the remaining m entries. Its weight is at least 3.

Any codeword formed by adding two rows of G will have two 1s among the first $2^m - m - 1$ entries and at least one 1 among the remaining m entries. The latter is true because all the rows of A are different. The weight of this codeword is also at least 3.

Finally, any codeword formed by adding together three or more rows of G will have at least three 1s among the first $2^m - m - 1$ entries. Its weight is at least 3.

Therefore every nonzero codeword has weight at least 3. Any row of A that has exactly two 1s will correspond to a row of G having exactly three 1s, so in fact the minimum weight of any nonzero codeword is 3. Theorem 7.4.3 implies that the minimum distance between any two codewords is 3. We have created a binary code with parameters $(2^m - 1, 2^{2^m - m - 1}, 3)$. It is a perfect code because it achieves the sphere packing bound. ■

Question 308 *Write a generator matrix for the Hamming* $(15, 2^{11}, 3)$ *code.*

Summary

An error-correcting code provides a method for accurate communication despite errors in transmission. We showed how to construct a family of binary codes using linear combinations of the rows of a generator matrix. These codes are perfect 1-error-correcting codes because, under the assumption that at most one error is made in the transmission of each codeword, they provide for completely accurate communication. Such codes exist exactly when the length of the codewords is one less than a power of two: 3, 7, 15, 31, 63, and so on.

Exercises

1. Decode the following 4×4 "image" of grayscale values sent according to the 1-error-correcting code of Table 7.3.

$$\begin{array}{cccc} 0100111 & 1110110 & 1010101 & 1011001 \\ 0100111 & 1000001 & 1000000 & 0111101 \\ 1101001 & 0101011 & 0101010 & 1110000 \\ 0110011 & 0110010 & 0110010 & 0001111 \end{array}$$

   Assuming that at most one error was made in transmitting each codeword, how many errors were actually made?

2. Prove the triangle inequality for the Hamming distance metric.

3. In $\mathbb{B}^8$, find the number of words in $S_4(01110110)$. Then find the number of words $\mathbf{v}$ for which $\mathrm{wt}(01110110 \oplus \mathbf{v}) \leqslant 4$.

4. Define the following operation on words in $\mathbb{B}^n$:

$$\mathbf{v} * \mathbf{w} := (v_1 w_1, v_2 w_2, \ldots, v_n w_n)$$

   where the products are taken modulo 2.

   Prove: If $\mathbf{v}, \mathbf{w} \in \mathbb{B}^n$, then $\mathrm{wt}(\mathbf{v} \oplus \mathbf{w}) = \mathrm{wt}(\mathbf{v}) + \mathrm{wt}(\mathbf{w}) - 2\mathrm{wt}(\mathbf{v} * \mathbf{w})$.

5. Prove that $\mathrm{wt}(\mathbf{v} \oplus \mathbf{w}) \geqslant \mathrm{wt}(\mathbf{v}) - \mathrm{wt}(\mathbf{w})$. Also, when does equality hold?

6. Prove that no perfect code on $\mathbb{B}^n$ that can correct up to $n - 1$ errors can exist.

7. You wish to use a perfect 1-error-correcting binary code to send a high-resolution image, where each pixel's grayscale value ranges from 0 to 65535. What is the smallest Hamming code you can use? How long is each codeword? What percentage of its codewords will you use to encode the grayscale values?

8. For each of the following generator matrices, how many errors can the resulting linear code correct? Support your answer.

   (a) $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$

9. Finish the proof of Theorem 7.4.1 by showing that the code therein cannot correct more than $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors using minimum distance decoding. (Hint: One way to do this is to show that if the radius of the spheres were any larger, they would then "overlap.")

10. Suppose $\mathcal{C}$ is a code on $\mathbb{B}^n$ that corrects e errors, where $|\mathcal{C}| > 2$. Prove that $e < \frac{n-1}{2}$.

11. Here is a decoding method for the Hamming $(7, 2^4, 3)$ code. Define

$$\mathbf{d}_1 := 0001111 \qquad \mathbf{d}_2 := 0110011 \qquad \mathbf{d}_3 := 1010101.$$

When you receive the word $\mathbf{x}$, construct $c := (\mathbf{x}\cdot\mathbf{d}_1, \mathbf{x}\cdot\mathbf{d}_2, \mathbf{x}\cdot\mathbf{d}_3)$ where the dot products are computed modulo 2. This c is a 3-digit binary number, but when converted to decimal it identifies the position in $\mathbf{x}$ at which an error occurs.

For example, let $\mathbf{x} = 1001110$. Then $c = (1, 1, 0)$ and 110 in binary is 6 in decimal. An error occurs in position 6 of $\mathbf{x}$, and indeed 1001100 is the correct codeword. As another example, when $\mathbf{x} = 0110011$ then $c = (0, 0, 0)$ and 000 in binary is 0 in decimal—no error occurs because 0110011 is a codeword.

Justify this method of decoding. You may want to first prove that if $\mathbf{x}$ is a codeword then $c = (0, 0, 0)$. Then prove if $\mathbf{x}$ is not a codeword, then c identifies the position of the error.

Travel Notes

According to the account of Thompson (1983), Hamming's frustration in 1947 with a computer at Bell Telephone Laboratories provided the impetus for his discovery. It seems the computer, upon detecting an error during the course of running one of Hamming's programs, would completely abort the calculation with no chance for recovery. After cursing the computer, Hamming thought, "If the machine can detect an error, why can't it locate the position of the error and correct it?" The field of error-correcting codes was born.

Linear codes are often referred to as (n, k, d) codes, where k is the rank of the generator matrix. Thus the Hamming $(7, 2^4, 3)$ code is also called the Hamming $(7, 4, 3)$ code or sometimes just the Hamming $(7, 4)$ code.

7.5 Codes from designs, designs from codes

The Hamming codes of the last section are perfect, 1-error-correcting binary codes. In this section we address two main questions. One, are there any other perfect codes? Two, are there any codes (whether perfect or not) that correct more than one error? In answering these questions we will see the close relationship between combinatorial designs and error-correcting codes.

Symmetric designs generate codes

Consider again the symmetric $(7, 3, 1)$ design and let A_1 be its incidence matrix, which we showed at the beginning of Section 7.2:

$$A_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Make a code $\mathcal{C}_1$ on $\mathbb{B}^7$ by taking the rows of this matrix as our codewords. (We are *not* treating A_1 as a generator matrix; the rows of A_1 alone form the code.) Notice that the Hamming distance between any two rows of A_1 is exactly 4. Therefore $\mathcal{C}_1$ has minimum distance 4 and so it corrects up to $\left\lfloor \frac{4-1}{2} \right\rfloor = 1$ error by Theorem 7.4.1.

This does not represent improvement over our existing knowledge because we already know a *perfect* 1-error-correcting code on $\mathbb{B}^7$: the Hamming $(7, 2^4, 3)$ code. But don't let the term "perfect" cast a pall on any non-perfect code. In certain situations the code $\mathcal{C}_1$ may be preferable to the Hamming code. If we use $\mathcal{C}_1$ and receive 1101111, we know that more than one error has occurred because this word is not within distance 1 of any of the seven codewords shown in A_1. (Geometrically, it is not in *any* sphere centered at a codeword.) In that case we can ask for re-transmission.[3] The Hamming $(7, 2^4, 3)$ code, since it is perfect, places *every* word in $\mathbb{B}^7$ within distance 1 of a unique codeword. If two or more errors are made, the Hamming code will definitely decode incorrectly. If the same happens when using $\mathcal{C}_1$, we might be able to detect it.

Question 309 *How many words in $\mathbb{B}^7$ are contained among the seven radius-1 spheres centered at the rows of A_1? How many words, then, are not contained in any of these spheres?*

But watch what happens when we create a code from the incidence matrix of a bigger design, in this case a symmetric $(13, 4, 1)$ design. That code is on $\mathbb{B}^{13}$ and contains 13 codewords. Without writing down the incidence matrix, we can show that this code has minimum distance 6. Because symmetric designs are linked (see Theorem 7.2.3), any two rows of the matrix share a 1 in exactly $\lambda = 1$ place. Each row contains four 1s (because $r = k = 4$), so that means that there are $k - \lambda = 3$ places in which the first row has a 1 and the second row has a 0; it also means that there are $k - \lambda = 3$ places in which the second row has a 1 and the first row has a 0. Therefore, the Hamming distance between these two rows is $2(k - \lambda) = 6$. This holds for any pair of rows so the distance between any two codewords, and therefore the minimum distance, is 6. By Theorem 7.4.1, this code can correct up to

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{6-1}{2} \right\rfloor = 2$$

errors. Now we are getting somewhere. It is not a perfect code, but it corrects one more error than the family of Hamming codes.

[3] This is desirable in applications involving DVD players and other personal electronic devices where, unlike the space probe example, re-transmission costs are low.

This same analysis holds in general. The minimum distance between any two rows of the incidence matrix of a symmetric (v, k, λ) design is $d := 2(k - \lambda)$. Theorem 7.4.1 shows that the code corrects up to

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{2(k-\lambda)-1}{2} \right\rfloor = \left\lfloor k - \lambda - \frac{1}{2} \right\rfloor = k - \lambda - 1$$

errors.

Theorem 7.5.1 *If A is the incidence matrix of a symmetric (v, k, λ) design, then the rows of A form a code on $\mathbb{B}^v$ that contains v codewords and has minimum distance $2(k - \lambda)$. This code corrects up to $k - \lambda - 1$ errors.*

Perfect binary codes generate designs

Now that we have seen how certain designs produce codes, let's examine a way in which codes produce designs. In this case, we show how to build a Steiner triple system from a Hamming code. Since we know how to use a generator matrices to construct Hamming codes, this result gives us a new method of construction for Steiner triple systems. The proof is especially enlightening because it shows the interplay between the 1-balanced property of a design and the radius-1 sphere packing property of a perfect binary code.

Theorem 7.5.2 *If $\mathcal{C}$ is a Hamming $(2^m - 1, 2^{2^m - m - 1}, 3)$ code with $m \geqslant 3$, and A is the matrix whose columns contain the weight-3 codewords in $\mathcal{C}$, then A is the incidence matrix of a Steiner triple system on $2^m - 1$ varieties.*

Proof: Assume $\mathcal{C}$ and A are as stated in the hypothesis, and let $\mathcal{D}$ be the design that has A as its incidence matrix. An STS$(2^m - 1)$ design is a $(2^m - 1, 3, 1)$ design. Once we demonstrate that the design $\mathcal{D}$ is incomplete and has $v = 2^m - 1$, $k = 3$, $\lambda = 1$, our proof will be complete. This is because any incomplete, uniform, and balanced design is necessarily regular and therefore a BIBD. (See Exercise 8 of Section 7.1.)

Firstly, we observe that $\mathcal{D}$ is 3-uniform (i.e., $k = 3$) because each column of A, being a weight-3 codeword, corresponds to a size-3 block of $\mathcal{D}$. Next, we see that $\mathcal{D}$ is incomplete because $m \geqslant 3$ implies $v = 2^m - 1 \geqslant 7 > 3 = k$. Now, each codeword is an element of $\mathbb{B}^{2^m - 1}$ so the columns of A contain $2^m - 1$ entries. This is not yet enough to show that $v = 2^m - 1$ because we need to make sure that all varieties appear in $\mathcal{D}$. In other words, we need to rule out the possibility of an all-zero row in A. This will follow from the proof that $\lambda = 1$, which is the most interesting part.

To prove $\lambda = 1$, let i and j be two varieties of the design $\mathcal{D}$. We must prove that i and j appear together in exactly one block of $\mathcal{D}$. Equivalently, we need to show that A contains exactly one column in which row i and row j share 1. But each column of A is a weight-3 codeword of $\mathcal{C}$, so we just need to show that $\mathcal{C}$ contains exactly one codeword with a 1 in positions i and j.

Define $\mathbf{v}_{ij}$ to be that word in $\mathbb{B}^{2^m - 1}$ having 1 in positions i and j, and 0 in all other positions. This is a weight-2 word so it is not a codeword in $\mathcal{C}$. But $\mathcal{C}$ is a perfect code with minimum distance $d = 3$, so $\mathbf{v}_{ij}$ is within a radius-1 sphere of exactly one codeword, say $\mathbf{c}$. This must be a weight-3 codeword, for a weight-2 word is only within distance 1 of a weight-1 or weight-3 word, and $\mathcal{C}$ contains no weight-1 codewords. In addition, $\mathbf{c}$ must have 1 in positions i and j, for the only way to change $\mathbf{v}_{ij}$ into a weight-3 word is to

change a 0 to a 1. This completes the demonstration that $\lambda = 1$ and hence the proof of the theorem. ■

Exercise 1 concerns a generalization of this result to perfect e-error-correcting binary codes.

The only perfect binary codes are...

At this point we mention the first of two truly astonishing results regarding perfect codes. The first concerns perfect binary codes. The Hamming codes comprise a family of perfect 1-error-correcting binary codes with parameters $(2^m - 1, 2^{2^m-m-1}, 3)$. Recall the sphere-packing bound (7.7) which places an upper bound on the number of codewords in an e-error-correcting code on $\mathbb{B}^n$, namely

$$|\mathcal{C}| \leqslant \frac{2^n}{\sum_{i=0}^{e} \binom{n}{i}}.$$

Perfect binary codes are those that meet the sphere packing bound. So when m is an integer, $m \geqslant 2$, the pair $(n, e) = (2^m - 1, 1)$ implies that the denominator $\sum_{i=0}^{e} \binom{n}{i}$ is a power of 2 and hence that the upper bound is an integer.

Are there any other such pairs (n, e)? Surprisingly there are only two: $(n, e) = (23, 3)$ and $(n, e) = (90, 2)$.

Question 310 *Verify that $\sum_{i=0}^{e} \binom{n}{i}$ equals a power of 2 in each case. If the corresponding perfect codes exist, how many codewords does each have?*

It turns out that a code exists having the first set of parameters. This code, now called the Golay $(23, 2^{12}, 7)$ code, was published by Marcel Golay in 1949. However, no code exists having the second set of parameters. We will justify both of these assertions, but before we do so we mention the first surprising result. It says that the only possible parameters for perfect binary codes are those of the Hamming and Golay codes.

Theorem 7.5.3 *The only perfect 1-error-correcting binary codes that exist are codes with parameters $(2^m - 1, 2^{2^m-m-1}, 3)$. The only perfect 3-error-correcting binary code that exists is the Golay $(23, 2^{12}, 7)$ code. No other perfect e-error-correcting binary codes exist for any value of e.*

A note of clarification is in order. A set of parameters $(n, |\mathcal{C}|, d)$ does not necessarily determine a unique code. There are examples of *nonlinear codes* (which are those unable to be created via the generator matrix method) with the same parameters as the Hamming $(2^m - 1, 2^{2^m-m-1}, 3)$ codes. But the Golay code is indeed the only $(23, 2^{12}, 7)$ binary code. So this theorem tells us that a perfect binary code must either have the same parameters as one of the Hamming codes or else it must be the Golay $(23, 2^{12}, 7)$ code. There are no other possibilities.

The Golay $(23, 2^{12}, 7)$ code

We now sketch one possible construction method for Golay's perfect 3-error-correcting binary code. We begin by constructing the so-called extended Golay code $\mathcal{G}_{24}$ which is a code on $\mathbb{B}^{24}$ with parameters $(24, 2^{12}, 8)$. This code, though not a perfect code, is interesting in its own right because it contains a large Steiner system.

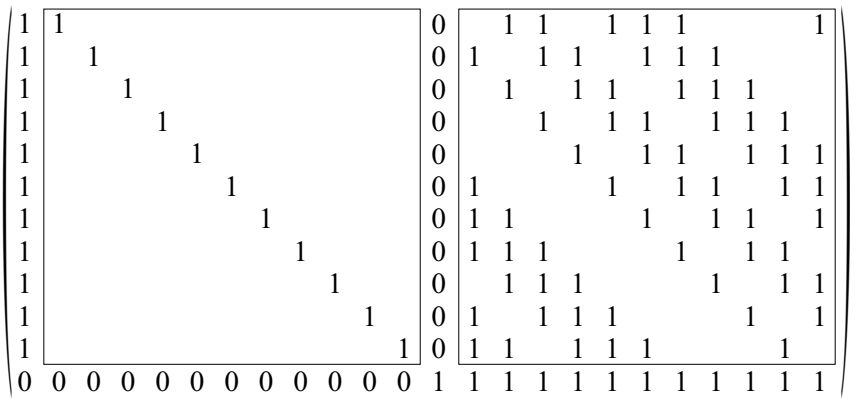


Figure 7.4. The generator matrix for the extended Golay code $\mathcal{G}_{24}$.

First we define a generating matrix for $\mathcal{G}_{24}$. It is the 12×24 matrix shown in Figure 7.4 and can be abbreviated as

$$G_{24} = \begin{pmatrix} 1 & & & 0 & & \\ \vdots & & I_{11} & \vdots & & A_{11} \\ 1 & & & 0 & & \\ 0 & 0 \cdots & 0 & 1 & 1 \cdots & 1 \end{pmatrix} \tag{7.9}$$

where I_{11} is the 11×11 identity matrix, and A_{11} is the incidence matrix of a symmetric $(11, 6, 3)$ design. The latter is the complement of a symmetric $(11, 5, 2)$ design; see Exercise 10 of Section 7.1.

It takes some work to show that the minimum distance is 8 for the code generated by the matrix G_{24}. By appealing to Theorem 7.4.3, it is enough to show that every nonzero codeword has weight at least 8. A glance at G_{24} shows that each of the first 11 rows has weight 8 while the last row has weight 12. Exercise 2 asks you to prove that the sum of any two rows has weight at least 8. In fact, one way to attack the problem of determining the minimum weight is to count the number of codewords of each possible weight. It turns out that among the 2^{12} codewords in $\mathcal{G}_{24}$ there are only five different weights, as shown in the table below. For a proof of this and some other results mentioned below, see MacWilliams & Sloane (1978).

weight w	0	8	12	16	24
# codewords $\mathbf{c}$ with $\text{wt}(\mathbf{c}) = w$	1	759	2576	759	1

Table 7.4. The weight distribution of codewords in $\mathcal{G}_{24}$.

Question 311 *What rows of G_{24} would you add to construct the one codeword of weight 24?*

Now that we know $\mathcal{G}_{24}$ to be a $(24, 2^{12}, 8)$ binary code, we mention two results that we also state without proof. First, if we delete any one column of G_{24}, the remaining 12×23 matrix is a generating matrix for a $(23, 2^{12}, 7)$ code. We know such a code to be perfect by our discussion in the last subsection. It is known as the Golay code $\mathcal{G}_{23}$. Moreover, it is unique.

Theorem 7.5.4 *The Golay code $\mathcal{G}_{23}$ is a perfect 3-error-correcting binary code with parameters* $(23, 2^{12}, 7)$. *Moreover, any other binary code with these parameters is equivalent to the Golay code.*

Second, the weight-8 codewords in $\mathcal{G}_{24}$ produce a $S(5, 8, 24)$ Steiner system. Recall that an $S(5, 8, 24)$ design is a 5-$(24, 8, 1)$ design, and so that each 5-subset of varieties appears in exactly one of the 759 blocks of this design. This would be a large and complicated design to construct without help from coding theory.

Theorem 7.5.5 *If A is the matrix whose columns are the weight-8 codewords of the Golay code $\mathcal{G}_{24}$, then A is the incidence matrix of an* $S(5, 8, 24)$ *design.*

No perfect code on $\mathbb{B}^{90}$ exists

Though $(n, e) = (90, 2)$ satisfies the sphere packing bound, we now prove that no perfect 2-error-correcting code on $\mathbb{B}^{90}$ exists. For sake of contradiction, assume that such a code exists and call it $\mathcal{C}$. It would be a $(90, 2^{78}, 5)$ code, for the sphere packing bound implies it contains

$$\frac{2^{90}}{\sum_{i=0}^{2}\binom{90}{i}} = \frac{2^{90}}{4096} = \frac{2^{90}}{2^{12}} = 2^{78}$$

codewords and has minimum distance $d = 2e + 1 = 5$.

Without loss of generality, assume that $\mathbf{0} \in \mathcal{C}$. Since $\mathcal{C}$ has minimum distance 5, every nonzero codeword has weight at least 5. Moreover, $\mathcal{C}$ must contain some weight-5 codewords. Our strategy for arriving at a contradiction involves constructing a particular set of weight-3 words and then examining how the spheres centered at weight-5 codewords partition this set.

To that end, consider the following 88 words in $\mathbb{B}^{90}$:

$$\begin{array}{rccccccccc}
\mathbf{w}^3 := & 1 & 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\
\mathbf{w}^4 := & 1 & 1 & 0 & 1 & 0 & \cdots & 0 & 0 \\
\mathbf{w}^5 := & 1 & 1 & 0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\mathbf{w}^{89} := & 1 & 1 & 0 & 0 & 0 & \cdots & 1 & 0 \\
\mathbf{w}^{90} := & 1 & 1 & 0 & 0 & 0 & \cdots & 0 & 1
\end{array}$$

That is, for $i = 3, 4, 5, \ldots, 90$, word $\mathbf{w}^i$ contains only 0s except for 1s in the first two positions as well as in position i.

Let $W = \{\mathbf{w}^3, \mathbf{w}^4, \mathbf{w}^5, \ldots, \mathbf{w}^{90}\}$. Consider two words in W equivalent if they belong to the same radius-2 sphere centered at a codeword of $\mathcal{C}$. This is an equivalence relation on W because $\mathcal{C}$ is a *perfect* code: every word in $\mathbb{B}^{90}$ is in exactly one sphere centered at a codeword.

Question 312 *Why must every word in W be in a sphere centered at a weight-5 codeword? In other words, why will no word in W be in a sphere centered at a codeword of weight other than 5?*

Since an equivalence relation induces a partition, let us examine each block of this partition of W. Consider the block containing $\mathbf{w}^3$. Let $\mathbf{c} \in \mathcal{C}$ be the (unique) weight-5 codeword such that $h(\mathbf{c}, \mathbf{w}^3) = 2$. Since $\mathbf{c}$ has weight 5 and is distance 2 from $\mathbf{w}^3$, this

$\mathbf{c}$ must have a 1 in the same positions that $\mathbf{w}^3$ does (namely, the first three positions) and then a 1 in two other positions. For sake of concreteness, let's say $\mathbf{c}$ has a 1 in positions 10 and 56.

Question 313 *Show then that* $h(\mathbf{c}, \mathbf{w}^{10}) = 2$ *and* $h(\mathbf{c}, \mathbf{w}^{56}) = 2$. *Also, explain why all other* $\mathbf{w}^i$ *have* $h(\mathbf{c}, \mathbf{w}^i) > 2$.

It follows that the block of the partition containing $\mathbf{w}^3$ has size 3. Indeed this argument applies not just to $\mathbf{w}^3$ but to any $\mathbf{w}^i \in W$, and demonstrates that every word in W is in a size-3 block of the partition. But herein lies our contradiction, for a size-88 set partitioned into blocks of size 3 would involve $88/3$ blocks. This rules out the possibility of a perfect $(90, 2^{78}, 5)$ binary code.

Theorem 7.5.6 *No perfect* $(90, 2^{78}, 5)$ *binary code exists.*

Ternary and other codes

What about non-binary codes? Can we construct larger codes that have better error-correcting properties? Are more perfect codes possible? We now generalize to non-binary codes.

Ternary codes

First let's consider an example of a ***ternary code***, which is a code in which each digit is 0, 1, or 2. Consider the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

As in the case of a binary code, we construct the code by finding all possible linear combinations of the rows of G. A generic linear combination is

$$a(1, 0, 2, 2) \oplus b(0, 1, 2, 1)$$

where $a, b \in \{0, 1, 2\}$. The notation $a(1, 0, 2, 2)$, for example, indicates component-wise scalar multiplication, modulo 3. The $\oplus$ operation indicates component-wise addition modulo 3. For example, when $a = 2$ and $b = 1$ we have

$$2(1, 0, 2, 2) \oplus 1(0, 1, 2, 1) = (2, 0, 1, 1) \oplus (0, 1, 2, 1) = (2, 1, 0, 2).$$

Question 314 *Find all nine codewords in this code generated by the matrix* G.

This code is an example of a $(4, 3^2, d)$ ternary code, where d is the minimum distance between two codewords. The Hamming distance between two words still equals the number of components in which the two words differ, and the weight of a word still equals the number of nonzero entries. For example, $h(1022, 0121) = 3$ and $\text{wt}(0102) = 2$.

Question 315 *What is the minimum distance for the code generated by the matrix* G *shown just above?*

In addition, for a linear code such as the one in the current example, its minimum distance still equals the minimum weight among the nonzero codewords. Indeed, most of the results of the last section that concern binary codes can be extended to ternary (and other) codes with little modification.

Finite fields and q-ary codes

For those familiar with both abstract and linear algebra, binary codes are codes over $GF(2)$ and ternary codes are codes over $GF(3)$. In general, a *q-ary code* is a subset of the vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q := GF(q)$ is a finite field on q elements. Further, the code is linear if it is a subspace of $\mathbb{F}_q^n$. It is well known that a field on q elements exists if and only if q is a power of a prime. Moreover, if a finite field on q elements exists, then it is unique up to isomorphism. The field $GF(q)$ is the ***Galois field of order*** q.

If p is a prime, then the field $GF(p)$ is isomorphic to the integers modulo p. So, for example, $GF(2)$ and $GF(3)$ behave like the integers modulo 2 and modulo 3, respectively. When we write $\mathbb{B}^n$ in this section and the previous one, we really mean $\mathbb{F}_2^n$.

It is possible to extend Hamming's perfect 1-error-correcting binary codes that we constructed in Section 7.4 to perfect 1-error-correcting q-ary codes for any q that is a power of a prime. This entire family of 1-error-correcting codes is given the name ***Hamming codes***.

The only perfect codes are...

With the door now open to non-binary codes comes the possibility of more perfect codes than the few we already know. But herein lies the second astonishing result. There is only one more perfect code, and it is a ternary code with parameters $(11, 3^6, 5)$ that was also discovered by Golay. The following theorem summarizes the work of several researchers working on the existence and uniqueness questions surrounding perfect codes.

Theorem 7.5.7 *If $\mathcal{C}$ is a perfect code over a finite field, then exactly one of the following is true of $\mathcal{C}$.*

- *It is a 1-error-correcting code that has the same parameters as one of the Hamming codes.*
- *It is equivalent to the 2-error-correcting Golay $(11, 3^6, 5)$ ternary code.*
- *It is equivalent to the 3-error-correcting Golay $(23, 2^{12}, 7)$ binary code.*

No other perfect codes exist.

Summary

This section introduced the interplay between designs and codes. We saw first that symmetric designs can be used to construct (usually non-perfect) error-correcting codes. We then saw that the Hamming binary codes are a source of Steiner triple systems. Both of these results are important because construction methods for symmetric designs and for Hamming codes are well-studied.

We closed this section with the answer to a major existence question in combinatorics and coding theory. Perfect codes are extremely rare and can only correct either one, two, or three errors. If a perfect code does not have the same parameters as one of the Hamming codes, then it must be either the 2- or 3-error-correcting Golay code.

Exercises

1. Let $\mathcal{C}$ be a perfect e-error-correcting code on $\mathbb{B}^n$, where e is odd. Prove that if A is the matrix whose columns are the weight-$(2e+1)$ codewords in $\mathcal{C}$, then A is the incidence matrix of an $S(e+1, 2e+1, n)$ Steiner system, that is, an $(e+1)$-$(n, 2e+1, 1)$ design.

2. Let $\mathbf{r}$ and $\mathbf{s}$ be two different rows of the matrix G_{24}. Prove that $\mathrm{wt}(\mathbf{r} \oplus \mathbf{s}) \geqslant 8$.
3. Prove that if $\mathcal{C}$ is a q-ary code containing codewords of length n that corrects up to e errors, then
$$|\mathcal{C}| \leqslant \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i}(q-1)^i}.$$
(This is the general sphere-packing bound.)
4. Let A be the 7×16 matrix whose columns are the codewords of the Hamming $(7, 2^4, 3)$ code. Define A' to be the 8×16 matrix obtained from A by adjoining an extra row, where the entries in this row are determined so that each column of A' contains an even number of 1s. Prove that A' is the incidence matrix of a 3-$(8, 4, 1)$ design.
5. Prove that in a linear binary code either every codeword has even weight or else half of the codewords have even weight and half have odd weight.

Travel Notes

By the 1950s the Hamming and Golay codes were known, but it was not until the early 1970s that it was proven that these are the only perfect codes possible. Theorem 7.5.7 represents the work of at least three researchers: Van Lint, who laid significant groundwork; Pless (1968), who proved that the Golay codes are unique; and Tietavainen (1973), who finished the proof that no other perfect codes exist. The books of MacWilliams & Sloane (1978) and Pless (1982) are classics and also treat the problem of decoding.

CHAPTER 8

Partially Ordered Sets

Partially ordered sets play a unifying role in combinatorial theory. So far we have studied ideas such as inclusion-exclusion, partitions of a set, counting under equivalence, and the chromatic polynomial of a graph in relative isolation. Our ultimate goal in this last chapter is to show how each of these ideas can be studied using partially ordered sets.

First we introduce partially ordered sets, their terminology and basic properties, and some important examples. We then prove two classical combinatorial results (Sperner's theorem and Dilworth's theorem) and study the concept of the dimension of a partially ordered set. To end our journey, we spend two sections studying the theory of Möbius inversion. It is this theory that provides the unifying framework.

8.1 Poset examples and vocabulary

A partially ordered set, or poset, is a set together with a relation that is reflexive and transitive (like an equivalence relation) but antisymmetric (unlike an equivalence relation).

Definition 8.1.1 *A **partially ordered set** or **poset** is an ordered pair* $\mathbf{P} = (X, \leqslant)$ *where* X *is a nonempty set and* $\leqslant$ *is a relation on* X *that is*

- ***reflexive:*** *if* $x \in X$*, then* $x \leqslant x$*;*
- ***antisymmetric:*** *if* $x, y \in X$ *and* $x \leqslant y$ *and* $y \leqslant x$*, then* $x = y$*; and*
- ***transitive:*** *if* $x, y, z \in X$ *and* $x \leqslant y$ *and* $y \leqslant z$*, then* $x \leqslant z$*.*

We sometimes say that X ***is ordered by*** $\leqslant$ to mean that $(X, \leqslant)$ is a poset. Sometimes we refer to X as the ***ground set*** of the poset. Until we get to Sections 8.5 and 8.6, we assume that the ground set is finite.

Using the symbol $\leqslant$ to denote the relation makes it convenient to write $x \leqslant y$ instead of $(x, y) \in \leqslant$. However, there are sometimes advantages to working explicitly with the ordered pairs in the relation. In that case, we typically write $\mathbf{P} = (X, R)$ to denote the poset so that $x \leqslant y$ becomes $(x, y) \in R$. We use both notations interchangeably.

Be warned that the symbol $\leqslant$ can be dangerous. When we write $x < y$ we mean that $x \leqslant y$ and $x \neq y$, just as with ordinary less-than. We also use $y \geqslant x$ to mean $x \leqslant y$, and use $y > x$ to mean $x < y$. But writing $x \not\leqslant y$ does NOT necessarily mean that $x > y$, as it would when comparing numbers using ordinary less-than-or-equal-to. It simply means that $x \leqslant y$ is false, i.e., the ordered pair (x, y) is not in the relation. Likewise, $x \not< y$ means only that $x < y$ is false and not necessarily that $x \geqslant y$.

Here is an everyday example of a poset. Imagine you are trying to rank a list of finalists for the purposes of determining who to hire for a job. In this case the ground set X is the set of candidates and the relation $\leqslant$ describes your preferences among them. If you can rank them in order from best to worst, then that is ideal. If not, then at least your ranking should satisfy the antisymmetric and transitive properties. Antisymmetry means that whenever x and y are different candidates, then you can't simultaneously prefer x to y and prefer y to x. Transitivity means that whenever you prefer x to y and also y to z, then you prefer x to z. In other words, these two properties ensure logical consistency among your preferences.

Sets ordered by inclusion

Any collection of sets ordered by the is-a-subset-of ($\subseteq$) relation is a poset. For example, consider the set of all subsets of [2], namely

$$2^{[2]} = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}.$$

The $\subseteq$ relation on this set is the following set of nine ordered pairs:

$$\{(\emptyset,\emptyset), (\emptyset,\{1\}), (\emptyset,\{2\}), (\emptyset,\{1,2\}), (\{1\},\{1\}), (\{1\},\{1,2\}),$$
$$(\{2\},\{2\}), (\{2\},\{1,2\}), (\{1,2\},\{1,2\})\}.$$

That is, (A, B) is in the relation if and only if $A \subseteq B$.

The subset relation is reflexive because $A \subseteq A$ for any set A. It is antisymmetric because if $A \subseteq B$ and $B \subseteq A$, then $A = B$. (In fact, this is the definition of set equality.) It is also transitive because if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$. Any poset involving the $\subseteq$ relation is said to be ***ordered by inclusion***.

The notation $\mathbf{2^n}$ denotes the subsets of $[n]$ ordered by inclusion. That is, $\mathbf{2^n} = (2^{[n]}, \subseteq)$. This poset is sometimes called a ***subset lattice***. We define lattice later in this section.

Question 316 *How many ordered pairs does the $\subseteq$ relation on $2^{[3]}$ have?*

Integers ordered by divisibility

Given a positive integer n, the ***divisibility lattice*** is the set of positive divisors of n ordered by the divisibility (is-a-divisor-of, or $|$) relation. We denote this poset $\mathbf{D_n}$. In other words, if we define

$$D_n := \{d \in \mathbb{Z} : d > 0 \text{ and } d|n\}$$

then $\mathbf{D_n} = (D_n, |)$. For example, $D_{18} = \{1, 2, 3, 6, 9, 18\}$ and so the divisibility relation on this set is

$$\{(1,1), (1,2), (1,3), (1,6), (1,9), (1,18), (2,2), (2,6), (2,18),$$
$$(3,3), (3,6), (3,9), (3,18), (6,6), (6,18), (9,9), (9,18), (18,18)\}.$$

Question 317 *Write the ordered pairs in the divisibility relation on D_{15} and on D_{16}.*

In general, let x, y, and z be positive integers. Since $x|x$ we have that $|$ is reflexive. Also, if $x|y$ and $y|x$, then $x = y$. Finally, if $x|y$ and $y|z$, then $x|z$ so $|$ is transitive. Each of these is easily verified using the definition of "divides": $a|b$ means $b = ka$ for some integer k.

Question 318 *Is the antisymmetric property true when x and y aren't both positive? Give a proof or counterexample.*

Total orders

Any set of real numbers ordered by less-than-or-equal-to is a poset. This is because $x \leqslant x$ for any real number x; if $x \leqslant y$ and $y \leqslant x$ then $x = y$; and if $x \leqslant y$ and $y \leqslant z$, then $x \leqslant z$. In fact, there is nothing "partial" about this partially ordered set. For any real numbers x and y, either $x \leqslant y$ or $y \leqslant x$ is true.

A ***totally ordered set*** or ***total order*** is a poset $(X, \leqslant)$ such that for each $x, y \in X$, either $x \leqslant y$ or $y \leqslant x$ is true. We define $\mathbf{n} := \big([n], \leqslant\big)$ to be the set $[n]$ ordered by $\leqslant$. As an example, the $\leqslant$ relation on [4] is

$$\big\{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\big\}.$$

As another example, the sets $\{a\}$, $\{a, b\}$, $\{a, b, d\}$, $\{a, b, d, e\}$ ordered by inclusion also form a total order. The poset $\mathbf{2^3}$ is not a total order because $\{1\} \not\subseteq \{2, 3\}$ and $\{2, 3\} \not\subseteq \{1\}$.

Question 319 *How many ordered pairs are in the $\leqslant$ relation on* [5]*? On* [6]*?*

Covering and the Hasse diagram

A convenient way to visualize a poset is with its Hasse diagram. For example, the Hasse diagrams of two subset lattices appear in Figure 8.1. In a Hasse diagram, we represent

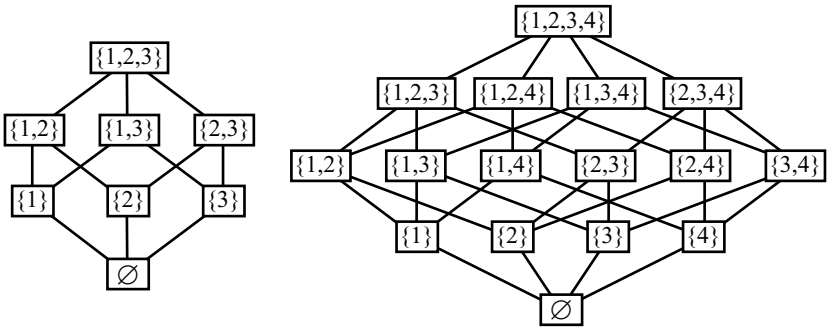


Figure 8.1. The subset lattices $\mathbf{2^3}$ and $\mathbf{2^4}$.

each element in the ground set by a symbol and then draw lines to indicate the relation. By convention, $x \leqslant y$ in the relation if and only if the following happens in the diagram: one, x appears below y on the page; two, there is a path from x to y that "travels upwards." The latter condition allows us to use an economy of lines for then we don't need to draw a line for each ordered pair in the relation.

For example, in the subset lattice $\mathbf{2^4}$, we know $\{1\} \subseteq \{1, 2, 3, 4\}$. In its Hasse diagram, we don't need to connect these two elements by a line because we can travel upwards from $\{1\}$ along, for example, the path $\{1\} \subseteq \{1, 2\} \subseteq \{1, 2, 4\} \subseteq \{1, 2, 3, 4\}$.

The idea of covering governs which lines we draw. We say that y ***covers*** x provided that $x < y$ and there is no z for which $x < z < y$. The notation $x \lessdot y$ indicates that y covers x. For example, $\{1, 3, 4\}$ covers $\{1, 3\}$ in the poset $\mathbf{2^4}$ because there is no set A for which $\{1, 3\} \subset A \subset \{1, 3, 4\}$. On the other hand, $\{1, 2, 3\}$ does not cover $\{2\}$.

Guidelines for drawing the Hasse diagram

To draw the ***Hasse diagram*** of the poset $\mathbf{P} = (X, \leqslant)$, follow these guidelines:

1. Represent each element of X by a symbol.
2. Draw a line connecting x and y only when $x \lessdot y$.
3. If $x \lessdot y$, then place y above x on the page.

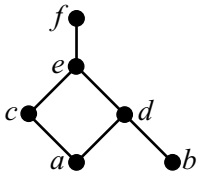
For example, consider the poset (X, R) with

$$X = \{a, b, c, d, e, f\}$$
$$R = \Big\{(a,a),\ (a,c),\ (a,d),\ (a,e),\ (a,f),\ (b,b),\ (b,d),(b,e),\ (b,f),$$
$$(c,c),\ (c,e),\ (c,f),\ (d,d),\ (d,e),\ (d,f),\ (e,e),\ (e,f),\ (f,f)\Big\}.$$

Drawing one line per ordered pair (x, y) with $x \neq y$ would require a jumble of 12 lines. As there are only six covering relations, namely

$$a \lessdot c \qquad a \lessdot d \qquad b \lessdot d \qquad c \lessdot e \qquad d \lessdot e \qquad e \lessdot f,$$

the Hasse diagram contains only six lines:



Question 320 *Draw the Hasse diagram of the poset with* $X = \{1, 2, 3, 4, 5\}$ *and* R *containing* (i, i) *for* $i = 1, 2, \ldots, 5$ *as well as* $(1, 2)$, $(1, 4)$, $(2, 4)$, $(3, 2)$, $(3, 4)$, *and* $(5, 4)$.

Hasse diagrams of the three divisibility lattices $\mathbf{D_{16}}$, $\mathbf{D_{18}}$, and $\mathbf{D_{24}}$ appear in Figure 8.2. Notice that $\mathbf{D_{16}}$ is a total order.

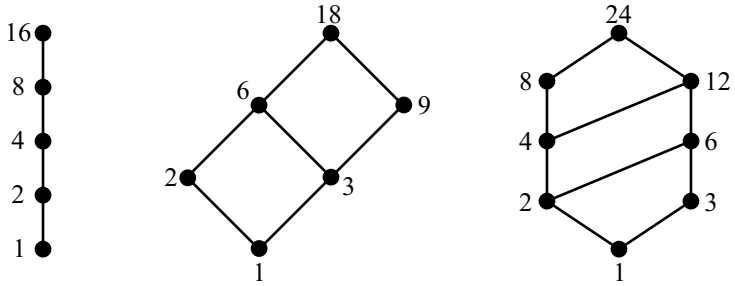


Figure 8.2. The divisibility lattices $\mathbf{D_{16}}$, $\mathbf{D_{18}}$, and $\mathbf{D_{24}}$.

Question 321 *Find a divisibility lattice whose Hasse diagram is essentially the same as that of* $\mathbf{D_{18}}$.

Poset vocabulary

For the purpose of introducing the vocabulary and notation of posets, we use the poset whose Hasse diagram appears in Figure 8.3.

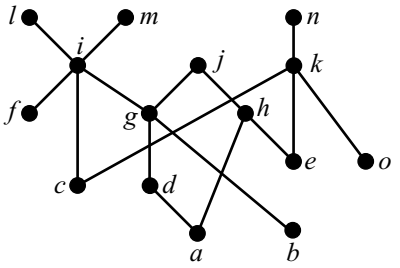


Figure 8.3. The Hasse diagram of a poset.

Comparable and incomparable

Let $\mathbf{P} = (X, \leqslant)$ be a poset. We say that x and y are ***comparable*** provided either $x \leqslant y$ or $y \leqslant x$. Failing that, x and y are ***incomparable*** and in that case we write $x \parallel y$. Any two elements in a poset are either comparable or incomparable. Since posets are reflexive, any element is comparable to itself. In a total order, any two elements are comparable.

Comparable means, quite literally, "able to be compared." It does not mean "equal" or "similar" as it might in everyday English. Incomparable means "unable to be compared."

In the poset shown in Figure 8.3, you should check that each of the following 10 statements is true:

$$\begin{array}{lllll} c \leqslant n & b \leqslant j & a \parallel b & g \parallel n & f < i \\ f \lessdot i & j > b & b \not< k & e \leqslant e & e \geqslant e. \end{array}$$

Chain and height

A ***chain*** of $\mathbf{P} = (X, \leqslant)$ is a nonempty subset of X containing pairwise comparable elements. That is, C is a chain of $\mathbf{P}$ provided $\emptyset \subset C \subseteq X$ and whenever $x, y \in C$ it follows that either $x \leqslant y$ or $y \leqslant x$. Among all possible chains of $\mathbf{P}$, if C^* is any chain of maximum size, then we define the ***height*** of the poset to be $|C^*|$.

For the poset of Figure 8.3, each of the following sets is a chain:

$$\begin{aligned} C_1 &= \{h\} \\ C_2 &= \{a, d, g, i, l\} \\ C_3 &= \{c, n\}. \end{aligned}$$

Since C_2 is a maximum-sized chain, we have height$(\mathbf{P}) = |C_2| = 5$. Notice that $\{a, d, g, i, m\}$ is also a maximum-sized chain. The set $\{f, i, l, m\}$ is not a chain because $l \parallel m$.

Antichain and width

An ***antichain*** of $\mathbf{P} = (X, \leqslant)$ is a nonempty subset of X containing pairwise incomparable elements (ignoring reflexivity). That is, A is an antichain of the poset $\mathbf{P}$ provided $\emptyset \subset A \subseteq X$ and whenever $x, y \in A$ with $x \neq y$, it follows that $x \parallel y$. Among all possible antichains of $\mathbf{P}$, if A^* is an antichain of maximum size, then we define the ***width*** of the poset to be $|A^*|$.

For the poset of Figure 8.3, each of the following sets is an antichain:

$$A_1 = \{h\}$$
$$A_2 = \{f, g, h, o\}$$
$$A_3 = \{c, f, g, h, o\}$$
$$A_4 = \{b, c, d, e, f, o\}.$$

Since A_4 is a maximum-sized antichain, we have width($\mathbf{P}$) $= |A_4| = 6$. Notice that $\{a, b, c, e, f, o\}$ is also a maximum-sized antichain. The set $\{e, f, g, h, o\}$ is not an antichain because $e \leqslant h$.

Notice that any singleton subset of X can be considered either a chain or an antichain.

Question 322 *Find the height and width of the posets* $\mathbf{2^3}$ *and* $\mathbf{2^4}$. *How many different maximum-sized chains are there in each poset?*

Extremal elements

An element $x \in X$ is ***maximal*** provided there is no $y \in X$ for which $x < y$. Informally, an element is maximal provided there is "nothing above" it. We define a ***minimal*** element in a similar manner. For the poset of Figure 8.3, the maximal elements are j, l, m, and n. The minimal elements are a, b, c, e, f, and o.

An element $x \in X$ is ***maximum*** provided $y \leqslant x$ for all $y \in X$. Informally, an element is maximum provided "everything else is below" that element. We define a ***minimum*** element in a similar manner. Notice that the existence of a maximum element implies that every element in the poset is comparable to that element. The same holds for a minimum element.

The poset of Figure 8.3, while having several maximal and minimal elements, has neither a maximum nor a minimum element. The concepts of maximal/maximum and minimal/minimum are easily confused so take care in using them.

Question 323 *Draw the Hasse diagram of a poset that is not a total order and that contains an element x with the following properties: x is comparable to every element of the poset, yet x is neither a maximum nor a minimum element.*

If a poset has a maximum element, then that that element is unique. To see this, let $\mathbf{P} = (X, \leqslant)$ be a poset and suppose x_1 and x_2 are maximum elements. Since x_1 is maximum, $y \leqslant x_1$ for all $y \in X$. In particular, $x_2 \leqslant x_1$. Now since x_2 is maximum, $y \leqslant x_2$ for all $y \in X$. In particular, $x_1 \leqslant x_2$. By antisymmetry of $\mathbf{P}$, $x_2 \leqslant x_1$ and $x_1 \leqslant x_2$ imply $x_1 = x_2$. Therefore a maximum element, if it exists, is unique. The same holds for a minimum element.

Theorem 8.1.2 *If a poset contains a maximum element, then there is only one such element. The same holds true for a minimum element.*

A poset needn't have a maximum element or a minimum element, but it must have at least one maximal element and at least one minimal element. We now prove this using a constructive approach.

Theorem 8.1.3 *If* $\mathbf{P} = (X, \leqslant)$ *is a poset, then it contains at least one maximal element and at least one minimal element.*

Proof: We prove only the existence of a maximal element, as the argument for a minimal element is entirely analogous. Let $\mathbf{P} = (X, \leqslant)$ be a poset and let $x \in X$. One of two things can happen:

- There is no $y \in X$ with $x < y$. If so, then x is maximal by definition. Stop.
- There is some $y \in X$ with $x < y$. If so, then x is not maximal but y might be. Start the procedure over with y.

This eventually stops because $\mathbf{P}$ is finite. The element at which it stops is maximal. ■

Subposet

In the poset $\mathbf{P}$ of Figure 8.3, the subposet containing a, g, h, and j is the poset with ground set $\{a, g, h, j\}$ and whose relation contains those ordered pairs appearing in $\mathbf{P}$ that contain only a, g, h, and j, namely

$$\big\{(a,a),(a,g),(a,h),(a,j),(g,g),(g,j),(h,h),(h,j),(j,j)\big\}.$$

We use $\mathbf{P}[Y]$ to denote this subposet, where $Y = \{a, g, h, j\}$.

In general, let $\mathbf{P} = (X, R)$ be a poset and let $Y \subseteq X$. Define

$$R[Y] := \big\{(y,z) : y, z \in Y \text{ and } (y,z) \in R\big\}.$$

Then $\mathbf{P}[Y] = \big(Y, R[Y]\big)$ is the ***subposet of*** $\mathbf{P}$ ***containing the elements of*** Y. We have not provided proof that $\mathbf{P}[Y]$ is indeed a poset but it is straightforward (Exercise 8).

Question 324 *For the poset of Figure 8.3, draw the Hasse diagram of the subposet containing the elements of* $\{c, f, g, i, k, n\}$.

Another important example: partitions ordered by refinement

Recall from Section 2.3 that a partition of a set S is a collection of nonempty, disjoint sets whose union is S. Let Π_n denote the set of partitions of $[n]$. For example,

$$\begin{aligned}\Pi_3 &= \{123, 1.23, 2.13, 3.12, 1.2.3\}\\ \Pi_4 &= \{1234, 1.234, 2.134, 3.124, 4.123, 12.34, 13.24, 14.23, 1.2.34,\\ &\qquad 1.3.24, 1.4.23, 2.3.14, 2.4.13, 3.4.12, 1.2.3.4\}.\end{aligned}$$

The notation 2.4.13 is an abbreviation for the partition $\big\{\{2\},\{4\},\{1,3\}\big\}$. Order doesn't matter in a partition, so 2.4.13 and 2.13.4 and 31.4.2 all represent the same partition of [4]. Also, recall that the Bell number $B(n)$ counts the total number of partitions of an n-set. So $|\Pi_3| = B(3) = 5$ and $|\Pi_4| = B(4) = 15$.

We say that one partition is finer than another partition provided that each block of the first partition is a subset of a single block of the second partition. For example, 2.4.13 is finer than 24.13, and also 2.4.13 is finer than 2.134. We write $2.4.13 \preceq 24.13$ and $2.4.13 \preceq 2.134$ to indicate this. Every partition of [4] is finer than 1234, and 1.2.3.4 is finer than any partition of [4]. In other words, 1234 is the maximum element and 1.2.3.4 is the minimum element in the is-finer-than relation on Π_4.

Question 325 *Is* 4.123 *finer than* 14.23*? Is* 14.23 *finer than* 4.123*?*

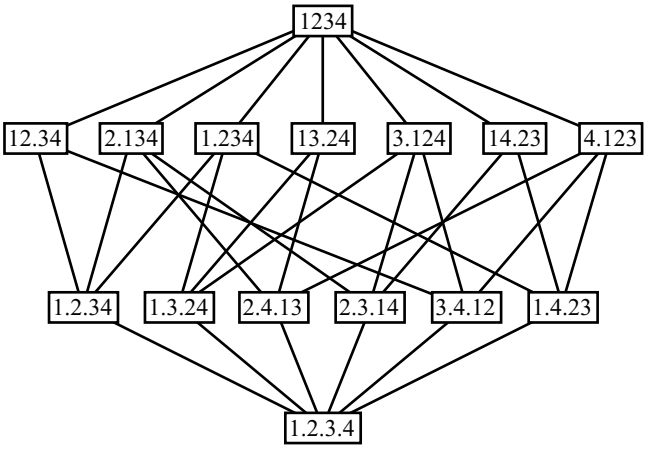


Figure 8.4. The poset $\mathbf{\Pi_4}$ of partitions of [4] ordered by refinement.

In general, let S be a set and let P_1 and P_2 be partitions of S, say

$$P_1 = \{B_1, \ldots, B_r\}$$
$$P_2 = \{C_1, \ldots, C_s\}.$$

That is, P_1 has r blocks and P_2 has s blocks. We say P_1 ***is finer than*** P_2, and write $P_1 \preceq P_2$, provided that for each block B_i of P_1, there exists some block C_j of P_2 such that $B_i \subseteq C_j$. The poset $\mathbf{\Pi_n} := (\Pi_n, \preceq)$ is the set of partitions of $[n]$ ordered by refinement. Exercise 9 asks for a proof that $\mathbf{\Pi_n}$ is indeed a poset. The Hasse diagram of the poset $\mathbf{\Pi_4}$ appears in Figure 8.4.

Question 326 *Draw the Hasse diagram of* $\mathbf{\Pi_3}$.

Lattices

We have already mentioned subset lattices and divisibility lattices so it is time to define the concept of lattice. A lattice is a poset for which every pair of elements has both a least upper bound and a greatest lower bound. Here is what these ideas mean.

Let $\mathbf{P} = (X, \leqslant)$ be a poset. Given elements x and y, we say that an element u is an ***upper bound of*** x ***and*** y provided $x \leqslant u$ and $y \leqslant u$. A ***least upper bound of*** x ***and*** y is an upper bound u^* for which $u^* \leqslant u$ for all upper bounds u of x and y. If a least upper bound of x and y exists, then obviously it is unique. It is also called the ***join of*** x ***and*** y and is denoted $x \vee y$.

In the poset of Figure 8.3, consider the elements d and f. Each of i, l, and m is an upper bound of d and f. Since $i \leqslant l$ and $i \leqslant m$, we also see that i is a least upper bound of d and f. That is, $d \vee f = i$. However, $i \vee j$ doesn't exist because there isn't even an element that is an upper bound of i and j.

Question 327 *Draw the Hasse diagram of a poset containing elements x and y such that these elements have at least one upper bound yet $x \vee y$ does not exist.*

An element l is a ***lower bound of*** x ***and*** y provided $l \leqslant x$ and $l \leqslant y$. A ***greatest lower bound of*** x ***and*** y is a lower bound l^* for which $l \leqslant l^*$ for all lower bounds l of x and y.

If a greatest lower bound exists then it is unique. It is also called the ***meet of*** x ***and*** y and is denoted $x \wedge y$.

In the poset of Figure 8.3, we have $g \wedge h = a$ while $g \wedge e$ doesn't exist.

Question 328 *In that same poset, find $d \wedge i$ and $i \wedge h$ and $b \wedge c$, if they exist.*

Formally, a ***lattice*** is a poset $\mathbf{P} = (X, \leqslant)$ such that for each $x, y \in X$, both $x \vee y$ and $x \wedge y$ are defined. Lattices enjoy a great deal more structure than ordinary posets and are important in many areas of mathematics.

Familiar lattices

The poset $\mathbf{2^n}$, which we called the subset lattice, does indeed satisfy the definition of lattice. In fact the join ($\vee$) and meet ($\wedge$) operations are union ($\cup$) and intersection ($\cap$). For example, in $\mathbf{2^4}$ we have $\{1,3,4\} \vee \{2,3\} = \{1,3,4\} \cup \{2,3\} = \{1,2,3,4\}$ and $\{1,3,4\} \wedge \{2,3\} = \{1,3,4\} \cap \{2,3\} = \{3\}$. Also, $\{1,3,4\} \wedge \{2\} = \emptyset$.

The same is true for the poset $\mathbf{D_n}$ of positive divisors of n ordered by divides. In this case, the join and meet operations are least common multiple and greatest common divisor, respectively. For example, in $\mathbf{D_{24}}$,

$$\begin{aligned} 3 \vee 6 &= \text{lcm}(3,6) = 6 \\ 4 \vee 6 &= \text{lcm}(4,6) = 12 \\ 8 \wedge 3 &= \gcd(8,3) = 1 \\ 12 \wedge 8 &= \gcd(12,8) = 4. \end{aligned}$$

Lattice properties

Any lattice has a maximum element and a minimum element. In addition, the join and meet operations satisfy several properties.

Theorem 8.1.4 *If $\mathbf{P} = (X, \leqslant)$ is a lattice, then $\mathbf{P}$ has a maximum element and a minimum element. In addition, the operations $\vee$ and $\wedge$ satisfy the following properties for each $x, y, z \in X$:*

- ***associative:*** $x \vee (y \vee z) = (x \vee y) \vee z$ *and* $x \wedge (y \wedge z) = (x \wedge y) \wedge z$*;*
- ***commutative:*** $x \vee y = y \vee x$ *and* $x \wedge y = y \wedge x$*;*
- ***idempotent:*** $x \vee x = x$ *and* $x \wedge x = x$*; and*
- ***absorption:*** $x \vee (x \wedge y) = x$ *and* $x \wedge (x \vee y) = x$.

Proof: Let $\mathbf{P} = (X, \leqslant)$ be a lattice. We prove the existence of a maximum element and the first absorption law and leave the rest to Questions and Exercises.

Let x^* be any maximal element guaranteed by Theorem 8.1.3. We prove that this x^* is in fact a maximum element by showing that $y \leqslant x^*$ for all $y \in X$. Let $y \in X$. Since $\mathbf{P}$ is a lattice, the join $y \vee x^*$ is defined. Define $u := y \vee x^*$. Since u is an upper bound of y and x^*, we have $y \leqslant u$ and $x^* \leqslant u$. In fact, it follows that $x^* = u$ because if $x^* < u$ then x^* wouldn't be maximal. But now $y \leqslant u$ and $u = x^*$ imply $y \leqslant x^*$. Therefore x^* is a maximum element.

We next prove the first absorption law and leave the remaining proofs to Exercise 8.1.4. To prove $x \vee (x \wedge y) = x$, we first define $l := x \wedge y$ and then prove $x \vee l = x$. Since l is a lower bound of x and y, we have $l \leqslant x$ and $l \leqslant y$. Now, x is certainly an upper

bound of x and l, because $x \leqslant x$ and $l \leqslant x$. Can x and l have an upper bound u satisfying $u < x$? No, because such an upper bound would satisfy $x \leqslant u$, which implies $x \leqslant u < x$ or $x < x$, a contradiction. Consequently $x \vee l = x$ and hence $x \vee (x \wedge y) = x$. ■

Question 329 *Prove that a lattice has a minimum element, and also prove the second absorption law.*

Summary

A poset is a set together with a relation that is reflexive, antisymmetric, and transitive. Posets arise frequently because familiar relations such as less-than-or-equal-to, is-a-subset-of, and divides possess these three properties. Important posets for combinatorial purposes include the total order $\mathbf{n}$, the subset lattice $\mathbf{2^n}$, the divisibility lattice $\mathbf{D_n}$, and partitions ordered by refinement $\mathbf{\Pi_n}$.

Exercises

1. Draw the Hasse diagram of $\mathbf{D_{60}}$.
2. Find, with proof, the height of the subset lattice $\mathbf{2^n}$. Then, count the number of maximum-sized chains in this poset.
3. Determine a necessary and sufficient condition for the divisibility lattice $\mathbf{D_n}$ to be a totally ordered set. Prove that you are correct.
4. Let $\mathbf{P} = (X, \leqslant)$ be a poset. Create a new poset by adding a new element x^* to X and the ordered pair (x^*, x^*) to the relation. Determine, with proof, the effects on the height, width, set of maximal elements, set of minimal elements, existence of a maximum, and existence of a minimum.
5. Let $\mathbf{P} = (X, \leqslant)$ be a poset. Define the poset $\hat{\mathbf{P}}$ by adding the new elements $\hat{0}$ and $\hat{1}$ to X, as well as the ordered pairs $(\hat{0}, \hat{0})$ and $(\hat{1}, \hat{1})$, as well as $(\hat{0}, x)$ and $(x, \hat{1})$ for all $x \in X$.
   (a) Prove that $\hat{\mathbf{P}}$ is indeed a poset.
   (b) Find, with proof, height($\hat{\mathbf{P}}$) and width($\hat{\mathbf{P}}$) in terms of height($\mathbf{P}$) and width($\mathbf{P}$).
6. Suppose $\mathbf{P}$ is a poset on n elements that is not a total order. What is the maximum number of ordered pairs in the relation? Prove that you are correct.
7. Find the number of ordered pairs in the subset relation in $\mathbf{2^n}$.
8. Prove that $\mathbf{P}[Y]$, the subposet of P containing the elements of Y, is a poset.
9. Prove that $\mathbf{\Pi_n}$, the partitions of $[n]$ ordered by refinement, is a poset. In addition, is it a lattice?
10. Let $\mathbf{P} = (X, \leqslant)$ be a poset. Let A be the set of all its minimal elements and B the set of all its maximal elements.
    (a) Are A and B always disjoint? Prove or give a counterexample.
    (b) Prove that each of A and B is an antichain.
11. Complete the proof of Theorem 8.1.4.
12. Prove that in a lattice, the following statements are equivalent: (1) $x \leqslant y$; (2) $x \vee y = y$; (3) $x \wedge y = x$.

13. Prove or disprove: in a lattice, any maximal chain is a maximum chain. (A maximal chain is a chain that can't be made larger through the addition of any element. A maximum chain is a chain of largest possible size.)
14. Let $\mathbf{P} = (X, \leqslant)$ be a poset that has a maximum element and for which the meet of every pair of elements is defined. Prove that $\mathbf{P}$ is a lattice.

Travel Notes

Poset terminology is relatively standard, but poset notation is less so. We choose to distinguish between the ground set X and the relation $\leqslant$, but many authors use a single letter for both the name of the poset and the relation.

8.2 Isomorphism and Sperner's theorem

In this section we first examine the notion of what it means for two posets to be "essentially the same." This notion is that of isomorphism which is pervasive in mathematics. In Chapter 6 we mentioned what it means for two graphs to be isomorphic and we now do the same for posets. We then prove Sperner's theorem which gives the width of the subset lattice $\mathbf{2^n}$.

Isomorphism

Consider the following two posets. The first is the divisibility lattice $\mathbf{D_{18}}$. The second poset is the set

$$\big\{\{1\}, \{1,2\}, \{1,3\}, \{1,3,9\}, \{1,2,3,6\}, \{1,2,3,6,9,18\}\big\}$$

ordered by inclusion. Figure 8.5 shows their Hasse diagrams.

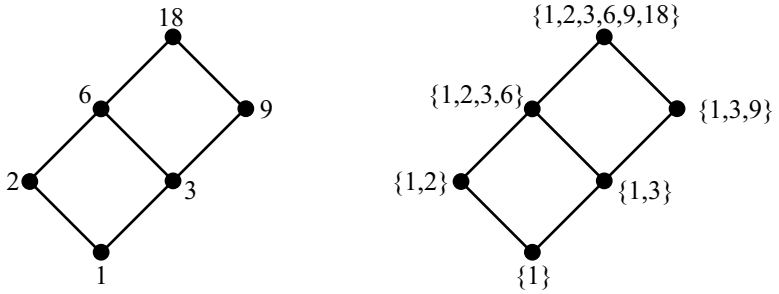


Figure 8.5. Two isomorphic posets.

These two posets are identical except for the labels attached to each element. More precisely, if ϕ is the function given by

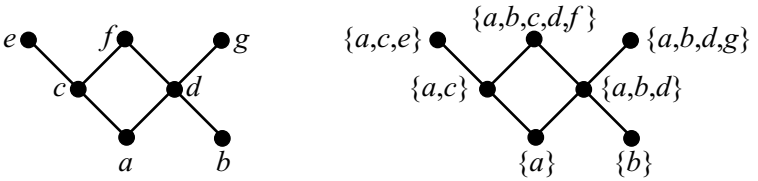
$$\begin{aligned} \phi(1) &= \{1\} & \phi(6) &= \{1,2,3,6\} \\ \phi(2) &= \{1,2\} & \phi(9) &= \{1,3,9\} \\ \phi(3) &= \{1,3\} & \phi(18) &= \{1,2,3,6,9,18\}, \end{aligned}$$

then $x|y$ in the first poset if and only if $\phi(x) \subseteq \phi(y)$ in the second poset. These two posets are isomorphic and the function ϕ is called an isomorphism.

Definition 8.2.1 *Let* $\mathbf{P} = (X, \leqslant)$ *and* $\mathbf{Q} = (Y, \preceq)$ *be posets. We say that* $\mathbf{P}$ ***is isomorphic to*** $\mathbf{Q}$*, and write* $\mathbf{P} \cong \mathbf{Q}$*, provided that there exists a bijection* $\phi : X \longrightarrow Y$ *with the following property: for each* $x_1, x_2 \in X$*, we have* $x_1 \leqslant x_2$ *if and only if* $\phi(x_1) \preceq \phi(x_2)$*. The bijection* ϕ *is called an* ***isomorphism****.*

Isomorphism and ordering by inclusion

We now prove that any poset can be expressed in terms of the is-a-subset-of relation. That is, any poset is isomorphic to a collection of sets ordered by inclusion. Figure 8.5 gives the first example of this. Here is another:



By now you probably have a guess about how to construct the correspondence. The key is to work with the "down-sets" of a poset. Given a poset $\mathbf{P} = (X, \leqslant)$ and an element $x \in X$, the ***down-set of*** x is the set of elements "at or below" x, i.e.,

$$D(x) := \{y \in X : y \leqslant x\}.$$

In the example above, the down-sets are

$$\begin{aligned} D(a) &= \{a\} & \qquad D(e) &= \{a, c, e\} \\ D(b) &= \{b\} & \qquad D(f) &= \{a, b, c, d, f\} \\ D(c) &= \{a, c\} & \qquad D(g) &= \{a, b, d, g\} \\ D(d) &= \{a, b, d\}. \end{aligned}$$

Question 330 *Give the down-set of each element in* $\mathbf{D_{24}}$*. In the context of the divides relation, how can you characterize what each down-set contains?*

In general, the function that maps each element to its down-set provides the isomorphism.

Theorem 8.2.2 *Any poset is isomorphic to a collection of sets ordered by inclusion. That is, if* $\mathbf{P}$ *is a poset, then* $\mathbf{P}$ *is isomorphic to the down-sets of* $\mathbf{P}$ *ordered by inclusion.*

Proof: Assume $\mathbf{P} = (X, \leqslant)$ is a poset. Let $\mathcal{D}$ be the set of the down-sets of $\mathbf{P}$ and let $\mathbf{Q} = (\mathcal{D}, \subseteq)$ be the down-sets of $\mathbf{P}$ ordered by inclusion. Define $\phi : X \longrightarrow \mathcal{D}$ by $\phi(x) = D(x)$. We prove that ϕ is an isomorphism.

To show that ϕ is one-to-one, assume that $\phi(x) = \phi(y)$, i.e., $D(x) = D(y)$. Certainly $x \in D(x)$, so it follows that $x \in D(y)$ because $D(x) = D(y)$. This means $x \leqslant y$. Since $y \in D(y)$, we can use a similar argument to conclude that $y \leqslant x$. By antisymmetry, $x = y$. Therefore ϕ is one-to-one. The function ϕ is onto by construction. Therefore ϕ is a bijection.

We now prove that $x \leqslant y$ if and only if $\phi(x) \subseteq \phi(y)$; that is, $x \leqslant y$ in $\mathbf{P}$ if and only if $D(x) \subseteq D(y)$ in $\mathbf{Q}$. First assume that $x \leqslant y$. Let $z \in D(x)$. This means $z \leqslant x$. Transitivity implies that $z \leqslant y$, so $z \in D(y)$. Therefore $D(x) \subseteq D(y)$.

Finally, assume that $D(x) \subseteq D(y)$. Since $x \in D(x)$, it follows that $x \in D(y)$. Therefore $x \leqslant y$, and this completes the proof that ϕ is an isomorphism. ■

Isomorphism and total orders

Any total order on n elements is isomorphic to the poset $\mathbf{n}$ consisting of the set $[n]$ ordered by ordinary less-than-or-equal-to. For example, the sets

$$\{2\},\ \{2,5,6\},\ \{2,4,5,6,7\},\ \{2,5\}$$

ordered by inclusion is a total order that is isomorphic to $\mathbf{4}$.

Theorem 8.2.3 *If* $\mathbf{P}$ *is a total order on n elements, then* $\mathbf{P} \cong \mathbf{n}$.

Though this result seems intuitively obvious, a rigorous proof takes some care (Exercise 6).

Question 331 *Give an example of a divisibility lattice* $\mathbf{D_n}$ *that is isomorphic to* $\mathbf{10}$. *That is, give a value of n for which* $\mathbf{D_n} \cong \mathbf{10}$.

Sperner's theorem

The Hasse diagrams of the subset lattices $\mathbf{2^3}$ and $\mathbf{2^4}$ appear in Figure 8.1 on page 319. The latter poset has width 6 and a maximum-sized antichain is

$$\big\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\big\}.$$

It contains the $\binom{4}{2}$ size-2 subsets of $[4]$. The poset $\mathbf{2^3}$ has width 3 and contains two maximum-sized antichains:

$$\big\{\{1\},\{2\},\{3\}\big\} \qquad \text{and} \qquad \big\{\{1,2\},\{1,3\},\{2,3\}\big\}.$$

The first contains the $\binom{3}{1}$ size-1 subsets and the second contains the $\binom{3}{2}$ size-2 subsets.

It appears that in any subset lattice $\mathbf{2^n}$, all of the subsets of $[n]$ of a fixed size form a *maximal* antichain—an antichain that cannot be made larger by adding an additional element. For example, if we take the size-6 antichain shown above for $\mathbf{2^4}$ and add any subset of size 0, 1, 3, or 4 to it, the result is no longer an antichain.

So in seeking an antichain of $\mathbf{2^n}$ of largest possible size, we could do worse than to start with the $\binom{n}{k}$ size-k subsets of $[n]$. The value of k that maximizes this is $k = \lfloor n/2 \rfloor$. Such an antichain is *maximal*. But is it *maximum*? Sperner's theorem, published in 1928, says that it is. The proof we present was published by Lubell (1966). It has become somewhat of a standard because it involves a nice counting argument.

Let's take a moment to illustrate the counting problem involved in the key step of the proof. In the subset lattice $\mathbf{2^5}$, how many maximum chains (i.e., chains of maximum size) contain $\{2,4,5\}$? Notice that such a chain starts with $\emptyset$ and ends with $[5]$, for example,

$$\underbrace{\emptyset \subseteq \{4\} \subseteq \{4,5\}}_{\text{below } \{2,4,5\}} \subseteq \{2,4,5\} \subseteq \underbrace{\{2,3,4,5\} \subseteq \{1,2,3,4,5\}}_{\text{above } \{2,4,5\}}.$$

Answering the counting question amounts to counting the ways we can specify the portion of the chain below $\{2,4,5\}$ and the portion of the chain above $\{2,4,5\}$. There are 3! ways to specify the "below" portion and 2! ways to specify the "above" portion. Therefore there are $3! \cdot 2!$ maximum chains containing $\{2,4,5\}$.

Question 332 *Justify the last two sentences. Now, let S be a k-subset of* $[n]$. *In the subset lattice* $\mathbf{2^n}$, *how many maximum chains contain S?*

Overall, there are $n!$ maximum chains in $\mathbf{2^n}$. We are now ready for the proof of Sperner's theorem.

Theorem 8.2.4 (Sperner) *The width of the subset lattice* $\mathbf{2^n}$ *is* $\binom{n}{\lfloor n/2 \rfloor}$.

Proof: Let $w := \text{width}(\mathbf{2^n})$. First we prove that there exists an antichain of size $\binom{n}{\lfloor n/2 \rfloor}$ and then we prove that no antichain of a larger size exists. That is, first we prove that $w \geqslant \binom{n}{\lfloor n/2 \rfloor}$ and then we prove that $w \leqslant \binom{n}{\lfloor n/2 \rfloor}$.

Consider the $\binom{n}{k}$ size-k subsets of $[n]$. This forms an antichain because if S_1 and S_2 are unequal subsets, each containing k elements, then $S_1 \not\subseteq S_2$ and $S_2 \not\subseteq S_1$. In particular, when $k = \lfloor n/2 \rfloor$ we obtain an antichain of size $\binom{n}{\lfloor n/2 \rfloor}$. Therefore $w \geqslant \binom{n}{\lfloor n/2 \rfloor}$.

Now let $\{S_1, S_2, \ldots, S_w\}$ be a maximum antichain in $\mathbf{2^n}$. For each $i \in [w]$, let $\mathcal{C}_i$ be the set of all maximum chains containing S_i. Notice that

$$|\mathcal{C}_i| = |S_i|! \cdot (n - |S_i|)!,$$

because there are $|S_i|!$ ways to specify the portion of the chain "below" S_i and $(n - |S_i|)!$ ways to specify the portion of the chain "above" S_i.

The sets $\mathcal{C}_i$ are disjoint and therefore the sum of the sizes of these sets is at most the total number of maximum chains in $\mathbf{2^n}$:

$$\sum_{i=1}^{w} |\mathcal{C}_i| = \sum_{i=1}^{w} |S_i|! \cdot (n - |S_i|)! \leqslant n! \qquad \text{or} \qquad \sum_{i=1}^{w} \frac{|S_i|! \cdot (n - |S_i|)!}{n!} \leqslant 1.$$

Rewrite the i-th term of the sum on the right to get

$$\sum_{i=1}^{w} \frac{1}{\binom{n}{|S_i|}} \leqslant 1.$$

Now, we know that $\binom{n}{k}$ is maximized when $k = \lfloor n/2 \rfloor$, so

$$\binom{n}{|S_i|} \leqslant \binom{n}{\lfloor n/2 \rfloor} \qquad \text{or} \qquad \frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \leqslant \frac{1}{\binom{n}{|S_i|}} \quad \text{for all } i.$$

Use this in the inequality to get

$$\sum_{i=1}^{w} \frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \leqslant 1$$

which implies $\dfrac{w}{\binom{n}{\lfloor n/2 \rfloor}} \leqslant 1$ or $w \leqslant \binom{n}{\lfloor n/2 \rfloor}$. This completes the proof. ■

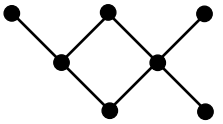
Besides an antichain consisting of all subsets of size $n/2$ (when n is even) or of size $(n-1)/2$ or $(n+1)/2$ (when n is odd), do other antichains exist? It has been proved (see Chapter 3 of the book by Erickson (1996)) that the answer is no: the only maximum-sized antichains in $\mathbf{2^n}$ are these "natural" ones. See Exercise 8 for a proof when n is even.

Summary

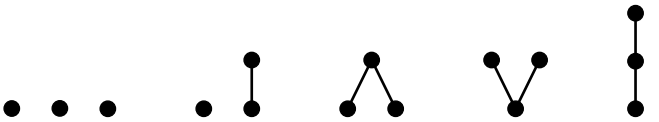
Poset isomorphism makes precise the idea of what it means for two posets to be equivalent up to the relabeling of the elements in their ground sets. We used this to prove that any poset can be thought of as a collection of sets ordered by inclusion. We then used a counting argument to prove Sperner's theorem, which says $\text{width}(\mathbf{2^n}) = \binom{n}{\lfloor n/2 \rfloor}$.

Exercises

1. Find a set of positive integers X so that X ordered by divisibility is isomorphic to the poset below, or else show that no such X exists.



2. Any 3-element poset must be isomorphic to one of the following posets:



   Determine how many nonisomorphic posets there are on four elements by drawing their Hasse diagrams.

3. Determine how many nonisomorphic lattices on five elements there are by drawing their Hasse diagrams.

4. Prove that poset isomorphism $\cong$ is an equivalence relation

5. Suppose $n = p^k$ for some prime p and some positive integer k. Prove that $\mathbf{D_n} \cong \mathbf{k+1}$.

6. Prove Theorem 8.2.3 by induction on n.

7. Let $\mathbb{B}^n$ be the set of all n-digit binary numbers. For two such numbers x and y, we say $x \leqslant y$ provided that $x_i \leqslant y_i$ for all $i = 1, 2, \ldots, n$. For example in $\mathbb{B}^4$, we have $0100 \leqslant 0101$ and $0110 \leqslant 1111$ but $0101 \not\leqslant 1110$.

   (a) Prove that $(\mathbb{B}^n, \leqslant)$ is a poset.

   (b) Find a familiar poset that is isomorphic to $(\mathbb{B}^n, \leqslant)$ and prove that you are correct.

8. The goal of this exercise is to prove that the only maximum antichain in $\mathbf{2^n}$ when n is even is that consisting of the size-$\frac{n}{2}$ subsets of $[n]$. Analyze the proof of Sperner's theorem to see when equality occurs in the upper bound on w, and then use that to argue why the maximum antichain $\{S_1, S_2, \ldots, S_w\}$ must consist of the size-$n/2$ subsets of $[n]$.

Travel Notes

Sperner's theorem is not to be confused with Sperner's lemma, which concerns triangulations and is intimately related to Brouwer's fixed-point theorem of topology.

Sperner's theorem is a basic result in the field of extremal set theory. A typical problem involves finding a largest possible collection of sets satisfying some specific constraints. The theorem can be re-stated in this framework as: if $S_1, S_2, \ldots, S_r$ is a collection of subsets of $[n]$ for which $S_i \not\subseteq S_j$ for all $i \neq j$, then $r \leqslant \binom{n}{\lfloor n/2 \rfloor}$.

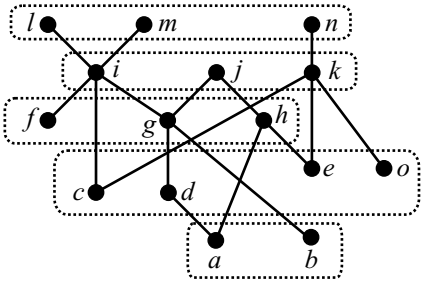
Another example of a result in extremal set theory is the Erdős-Ko-Rado theorem: if $S_1, S_2, \ldots, S_r$ is a collection of distinct, pairwise intersecting k-subsets of $[n]$, where $k \leqslant n/2$, then $r \leqslant \binom{n-1}{k-1}$. Pairwise intersecting means that $S_i \cap S_j \neq \emptyset$ for all i and j.

8.3 Dilworth's theorem

After Sperner's theorem, Dilworth's theorem is the second of the two classical combinatorial results on posets that we present. Dilworth's theorem says that when partitioning the ground set of a poset into chains or antichains, the smallest number of blocks in any such partition equals the width or height, respectively.

Antichain covers and Dilworth's theorem, part I

Consider partitioning the 15 elements of the poset in Figure 8.3 on page 321 (also shown below) such that each block of the partition is an antichain. We could put each of the 15 elements in its own block but we can certainly use fewer blocks. The following diagram represents a partition into five blocks where each block is an antichain.



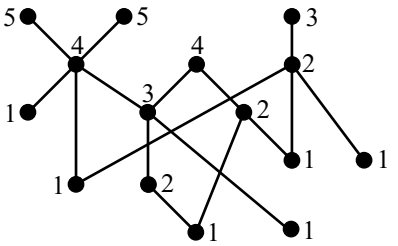
This partition of the ground set $X = \{a, b, c, \ldots, o\}$ into antichains is

$$\mathcal{A} = \big\{\{a, b\}, \{c, d, e, o\}, \{f, g, h\}, \{i, j, k\}, \{l, m, n\}\big\}$$

and is known as an antichain cover. Given any poset, an ***antichain cover*** is a partition of the ground set such that each block of the partition is an antichain.

Question 333 *Find an antichain cover with the fewest blocks possible for the subset lattices* $\mathbf{2^3}$ *and* $\mathbf{2^4}$.

What is the minimum size of an antichain cover? The way the dotted boxes were drawn on the Hasse diagram above suggests that perhaps there is a way to stratify the elements in the ground set so that an antichain cover is readily available. Define the ***height of an element*** to be the height of a largest chain in the poset that has that element as its maximum. Labeling each element in our current example with its height gives



This leads to a different partition of the ground set than given earlier but it contains the same number of antichains:

$$\mathcal{A}' = \big\{\{a, b, c, e, f, o\}, \{d, h, k\}, \{g, n\}, \{i, j\}, \{l, m\}\big\}.$$

Can we find an antichain cover of this poset using fewer than five antichains? No, because the height of the poset provides a lower bound on the number of antichains required to cover the ground set. Our current poset has height five, and

$$a < d < g < i < m$$

is a maximum chain. Since any two of these elements are comparable, any antichain cover must place each of these five elements in different blocks.

This suggests a constructive proof of our first "covering" result. We will consider it part of Dilworth's theorem even though his original theorem related chain covers to width and not antichain covers to height.

Theorem 8.3.1 *If* $\mathbf{P}$ *is a poset, then there exists a partition of the ground set into* height($\mathbf{P}$) *blocks, each of which is an antichain. Moreover, this is best possible.*

Proof: Assume $\mathbf{P} = (X, \leqslant)$ is a poset and height($\mathbf{P}$) $= h$. Notice that any antichain cover requires at least h antichains, for any two elements in a maximum chain are comparable and hence cannot be in the same block of the partition into antichains.

Now we show that an antichain cover of size h exists. For each $i \in [h]$, define A_i to be the set of elements of height i. That is,

$$A_i := \{x \in X : \text{height}(x) = i\}.$$

Recall that the height of an element x is the height of the largest chain in $\mathbf{P}$ whose maximum element is x.

We now verify that $\mathcal{A} := \{A_1, \ldots, A_h\}$ is an antichain cover. To show that $\mathcal{A}$ is a partition of X take any chain of height h, say

$$x_1 < \cdots < x_h.$$

Notice that $x_i \in A_i$, for $i \in [h]$, because a chain of height h is necessarily a maximum chain. Hence each block of $\mathcal{A}$ is nonempty. In addition, each element of X is in some block because the height of each element x is well-defined and if height(x) $= i$ then $x \in A_i$.

It remains to prove that each block of $\mathcal{A}$ is an antichain. For sake of contradiction, suppose that some block A_i were not an antichain. Then there would be elements $x, y \in A_i$ for which $x < y$. Since $x \in A_i$, by definition height(x) $= i$ and so there is a chain

$$x_1 < \cdots < x$$

of height i in $\mathbf{P}$. Since $y \in A_i$ we also have height(y) $= i$. But then

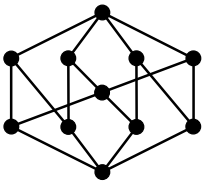
$$x_1 < \cdots < x < y$$

is a chain in $\mathbf{P}$ of height $i + 1$ which contradicts height(y) $= i$. Therefore each A_i is an antichain, and this completes the proof. ■

Example: determining height

The theorem provides an airtight way to prove that the height of a poset is h. Namely, exhibit a chain of size h as well as an antichain cover of that same size.

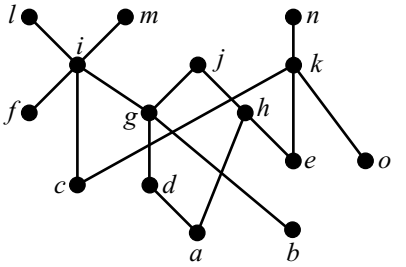
Question 334 *Use that method to determine the height of the poset shown below.*



Chain covers and Dilworth's theorem, part II

Just as the height of a poset determines the smallest size of an antichain cover, the width of a poset determines the smallest size of a chain cover. This result is Dilworth's original theorem.

Again, examine the poset of Figure 8.3 on page 321 but this time try to partition the ground set into chains. Here is one way to do it:



$C_1 = \{a, d, g, i, l\}$
$C_2 = \{f, m\}$
$C_3 = \{c, k, n\}$
$C_4 = \{b\}$
$C_5 = \{e, h, j\}$
$C_6 = \{o\}$

This time, the poset's width of 6 forces us to use at least six chains. This is because *any* antichain contains pairwise incomparable elements. Therefore, no two elements in the same antichain can be in the same chain.

Though exchanging "height" for "width" and "antichain" for "chain" in Theorem 8.3.1 produces Dilworth's original theorem, the proof is more intricate.

Theorem 8.3.2 (Dilworth) *If* $\mathbf{P}$ *is a poset, then there exists a partition of the ground set into* width($\mathbf{P}$) *blocks, each of which is a chain. Moreover, this is best possible.*

Proof: Our proof is by strong induction on the size of the ground set. When the ground set has one or two elements, you can check that the conclusion of the theorem is true for such posets.

Now assume that n is an integer, $n \geq 2$, and that the conclusion of the theorem is true for any poset on n or fewer elements. Let $\mathbf{P} = (X, R)$ be a poset with $|X| = n + 1$. Let C be any maximal chain of $\mathbf{P}$. We divide the analysis into two cases according to the width of the poset that results from deleting C from $\mathbf{P}$.

Case 1: *The induced subposet* $\mathbf{P}'$*, obtained from* $\mathbf{P}$ *by deleting the chain* C*, has* width($\mathbf{P}'$) $<$ width($\mathbf{P}$). Since $\mathbf{P}' := \Big(X - C, R[X - C]\Big)$ is a poset on n or fewer elements, the inductive hypothesis implies that there is a partition of its ground set into w' chains

$$X - C = C_1 \cup \cdots \cup C_{w'}$$

where $w' :=$ width($\mathbf{P}'$). But then

$$X = C_1 \cup \cdots \cup C_{w'} \cup C$$

is a partition of X into $w' + 1$ chains. If width($\mathbf{P}$) $= w' + 1$ then this case would be complete, for then we would have found a partition of X into the required number of chains. But this is indeed true. Any partition of X into chains requires at least width($\mathbf{P}$) chains. Since we have found a partition into $w' + 1$ chains, we have width($\mathbf{P}$) $\leq w' + 1$. Also, our assumption in this case is that width($\mathbf{P}'$) $<$ width($\mathbf{P}$), i.e., $w' <$ width($\mathbf{P}$) or $w' + 1 \leq$ width($\mathbf{P}$). Taken together, these two inequalities imply width($\mathbf{P}$) $= w' + 1$. This completes the inductive step in this case.

Case 2: *The induced subposet* $\mathbf{P}'$*, obtained from* $\mathbf{P}$ *by deleting the chain* C*, has* $\text{width}(\mathbf{P}') = \text{width}(\mathbf{P})$. First let's note that if we are in this case, then $|C| \geqslant 2$. For, if C only contains one element, then the fact that C is a maximal chain would mean that it is an "isolated point" (think in the context of the Hasse diagram). But then $\text{width}(\mathbf{P}') < \text{width}(\mathbf{P})$, contradicting our assumption.

In the poset $\mathbf{P}$, let x^+ and x^- be the maximum and minimum elements of C. Define $\mathbf{P}^*$ to be the induced subposet obtained from $\mathbf{P}$ by deleting x^+ and x^-. Notice that $\mathbf{P}^*$ is not empty because $\mathbf{P}$ has $n+1$ elements and we are assuming $n \geqslant 2$. It also has $\text{width}(\mathbf{P}^*) = \text{width}(\mathbf{P})$ because of our assumption in this case. Let A be an antichain of $\mathbf{P}^*$ having size w, where $w := \text{width}(\mathbf{P})$:

$$A = \{a_1, \ldots, a_w\}.$$

Certainly A is also an antichain of $\mathbf{P}$.

Define $\mathbf{D}$ to be the subposet of $\mathbf{P}$ induced by the elements at or below the antichain A. That is,

$$\mathbf{D} := \big(D(A), R[D(A)]\big)$$

where $D(A)$ is the down-set of A:

$$D(A) := \{x \in X : x \leqslant a \text{ for at least one } a \in A\}.$$

Analogously, define

$$\mathbf{U} := \big(U(A), R[U(A)]\big)$$

to be the subposet of $\mathbf{P}$ induced by the up-set of A:

$$U(A) := \{x \in X : a \leqslant x \text{ for at least one } a \in A\}.$$

We next show that we can partition X into three blocks as follows:

$$X = A \cup \Big(D(A) - A\Big) \cup \Big(U(A) - A\Big).$$

Clearly A is nonempty as are the other two sets, because $x^- \in D(A) - A$ and $x^+ \in U(A) - A$.

Question 335 *Verify these statements.*

Also, the three sets are pairwise disjoint. Obviously, the pair A and $D(A) - A$ and the pair A and $U(A) - A$ are disjoint. For the other, assume $x \in D(A) - A$ and $x \in U(A) - A$. Then $x \leqslant a$ for some $a \in A$ and $b \leqslant x$ for some $b \in A$. But then $b \leqslant a$, contradicting the fact that A is an antichain.

The rest of the proof involves first applying the induction hypothesis to the induced subposets on $D(A)$ and $U(A)$ and then combining the resulting chain partitions into a chain partition of $\mathbf{P}$. Define the posets

$$\mathbf{P}^- := \big(D(A), R[D(A)]\big)$$
$$\mathbf{P}^+ := \big(U(A), R[U(A)]\big).$$

Recall $\mathbf{P}$ has $n+1$ elements. Each of the two posets above has at most n elements because $x^+ \notin D(A)$ and $x^- \notin U(A)$. Therefore the inductive hypothesis implies that there exist chain partitions

$$D(A) = C_1 \cup \cdots \cup C_w$$
$$U(A) = D_1 \cup \cdots \cup D_w.$$

Note that A is an antichain of each of these subposets, so they both have width w. Possibly by re-indexing the blocks of each partition, we can assume that $a_i \in C_i \cap D_i$ for all $i \in [w]$. This is because A is a maximum antichain in each of $\mathbf{P}^-$ and $\mathbf{P}^+$, and so each $a_i \in A$ must appear in a different block of each of the two partitions. Also note that for all $i \in [w]$, the set $C_i \cup D_i$ is a chain.

Finally, "glue" together these chain partitions into a chain partition of X into $w = \text{width}(\mathbf{P})$ blocks, each of which is a chain:

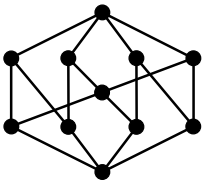
$$X = (C_1 \cup D_1) \cup \cdots \cup (C_w \cup D_w).$$

This completes the inductive step in this case, and hence the proof of the theorem. ■

Example: determining width

Like Theorem 8.3.1, Dilworth's theorem can be used to "certify" the width of a poset.

Question 336 *Use Dilworth's theorem to determine the width of the poset shown below.*



Summary

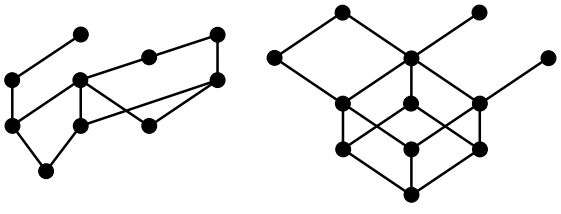
In this section we proved two results true of any poset: (1) the fewest number of antichains required to partition the ground set equals the height, and (2) the fewest number of chains required to partition the ground set equals the width. Each can be used to determine the height or width of a poset.

Exercises

1. Find the height and width of each of the following posets: $\mathbf{10}$, $\mathbf{D_{24}}$, and $\mathbf{\Pi_4}$. Use the appropriate version of Dilworth's theorem to certify your answers.

2. Draw the Hasse diagram of a height-2, width-8 poset that contains a maximum element. Draw the Hasse diagram of a height-8, width-2 poset containing no maximum or minimum element. Draw the Hasse diagram of a height-4, width-2 lattice.

3. Use Dilworth's theorem to determine the height and width of each poset:



4. Find an example of a nontrivial poset $\mathbf{P}$ for which width($\mathbf{P} - C$) = width($\mathbf{P}$) for all nonempty chains C of $\mathbf{P}$.
5. Let m and n be positive integers. Give an example of a height-m, width-n poset on mn elements.
6. Prove the following result, known as Dilworth's lemma: if $\mathbf{P}$ is a poset on $mn + 1$ elements, then either $\mathbf{P}$ contains a chain of size $m + 1$ or an antichain of size $n + 1$. (Hint: Can you make a connection with the Erdős-Szekeres theorem and its proof, in Section 1.5?)

Travel Notes

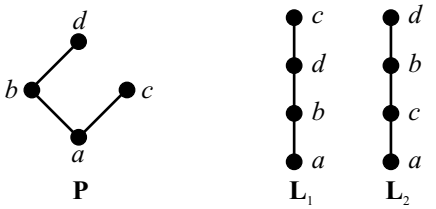
Several proofs of Dilworth's theorem have surfaced since the original publication of Dilworth (1950). Theorem 8.3.1, the easier half, was discovered 21 years later by Mirsky (1971). A good reference for Dilworth's theorem and for finite posets in general is the book by Anderson (2002).

Theorems 8.3.1 and 8.3.2 are known as *dual results*. Dual results pervade mathematics. Two that are closely related to Dilworth's theorem are the duality theorem of linear programming and the max-flow min-cut theorem of network flows. Each can be used to prove Dilworth's theorem.

8.4 Dimension

In the last section we analyzed a poset by tearing it down—by partitioning the ground set into simply-structured pieces, namely chains or antichains. In this section we instead examine how a poset can be built from simpler posets. Total orders serve as the building blocks and the set intersection operation does the building.

For a first example, consider the poset $\mathbf{P}$ below as well as the two total orders $\mathbf{L}_1$ and $\mathbf{L}_2$, all having the same ground set:



The poset $\mathbf{L}_1$ represents a so-called *extension of* $\mathbf{P}$ *to a total order*, or more briefly a *linear extension of* $\mathbf{P}$. By this we mean that whenever $x \leqslant y$ in $\mathbf{P}$, it follows that $x \leqslant y$ in $\mathbf{L}_1$. Specifically, the reflexive pairs $a \leqslant a$, $b \leqslant b$, $c \leqslant c$ and $d \leqslant d$, as well as the pairs

$$a < b \qquad a < d \qquad a < c \qquad b < d$$

are in both $\mathbf{P}$ and $\mathbf{L}_1$. The same holds for $\mathbf{L}_2$ so it is also a linear extension of $\mathbf{P}$.

Because of this it would be natural to write $\mathbf{P} \subseteq \mathbf{L}_1$ and $\mathbf{P} \subseteq \mathbf{L}_2$, and to consider $\mathbf{P}$ to be a subposet of each of its linear extensions. Of course, it is true that each linear extension includes more pairs than $\mathbf{P}$ does. We see that $b \parallel c$ in $\mathbf{P}$ while $b < c$ in $\mathbf{L}_1$ and $c < b$ in $\mathbf{L}_2$. Also, we observe $c \parallel d$ in $\mathbf{P}$ while $d < c$ in $\mathbf{L}_1$ and $c < d$ in $\mathbf{L}_2$.

However, the ordered pairs common to both $\mathbf{L}_1$ and $\mathbf{L}_2$ are exactly those in $\mathbf{P}$. Perhaps seeing the relations as sets makes it obvious:[1]

$$\begin{aligned}\mathbf{L}_1 &= \{(a,a),(a,b),(a,d),(a,c),(b,b),(b,d),(b,c),(d,d),(d,c),(c,c)\}\\ \mathbf{L}_2 &= \{(a,a),(a,c),(a,b),(a,d),(c,c),(c,b),(c,d),(b,b),(b,d),(d,d)\}\\ \mathbf{L}_1 \cap \mathbf{L}_2 &= \{(a,a),(a,b),(a,c),(a,d),(b,b),(b,d),(c,c),(d,d)\}\\ &= \mathbf{P}.\end{aligned}$$

The set $\{\mathbf{L}_1, \mathbf{L}_2\}$ is a *realizer of* $\mathbf{P}$. It is so called because the intersection of its member posets equals $\mathbf{P}$. It should be clear that it is not possible to realize $\mathbf{P}$ with only one linear extension for after all $\mathbf{P}$ is not a total order. We shall therefore say that the *dimension of* $\mathbf{P}$ is 2 because (1) it is possible to realize $\mathbf{P}$ with two linear extensions, and (2) no smaller realizer exists.

Question 337 *Recopy the Hasse diagram of* $\mathbf{P}$ *and then draw a line connecting* c *and* d. *Find a realizer of this new poset.*

At this point the concepts of linear extension, realizer, and dimension should raise a lot of questions. Where did the linear extensions $\mathbf{L}_1$ and $\mathbf{L}_2$ come from? Must every poset have a linear extension? Is the concept of dimension well-defined?

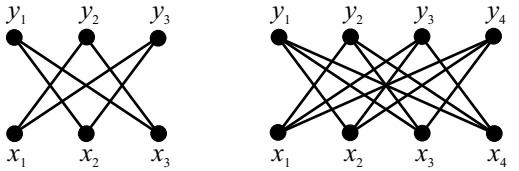
The best answer to the first question is trial and error. Constructing realizers often requires ad hoc methods that vary from poset to poset. The answer to both the second and third questions is yes. We postpone their discussion until the end of this section.

Two new posets

Before giving a formal definition of dimension, we introduce two posets that we'll use in this section.

$\mathbf{S_n}$: the standard example of an n-dimensional poset

The Hasse diagrams of the standard examples $\mathbf{S_3}$ and $\mathbf{S_4}$ appear below:



In general, for $n \geqslant 2$ let

$$X = \{x_1, x_2, \ldots, x_n\}$$
$$Y = \{y_1, y_2, \ldots, y_n\}.$$

Then define $\mathbf{S_n} := (X \cup Y, \leqslant)$ so that the only ordered pairs in the $\leqslant$ relation, besides those required to make it reflexive, are all those of the form $x_i \leqslant y_j$ for all $i \neq j$. Perhaps it is easier to see its construction as a Hasse diagram: put $x_1, x_2, \ldots, x_n$ in a row, put $y_1, y_2, \ldots, y_n$ in a row directly above that, and then connect each element in the bottom row to each element in the top row except the one directly above it.

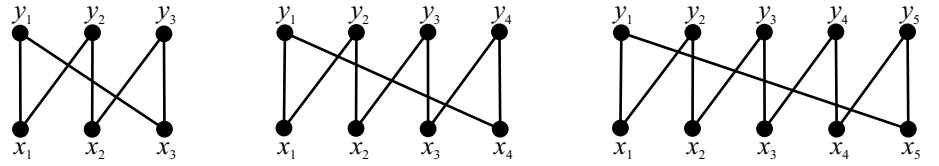
Question 338 *How many ordered pairs are in the relation for* $\mathbf{S_n}$*?*

Later, we'll prove that the dimension of $\mathbf{S_n}$ is n.

[1] It is an abuse of notation to say that a poset equals its relation, but the meaning should be clear since the ground set $X = \{a, b, c, d\}$ is understood.

$\mathbf{C_n}$: the crown

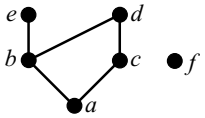
To construct the crown $\mathbf{C_n}$, use the same set $X \cup Y$ of the standard example poset just described but instead connect each x_i to just two elements: the elements y_i and y_{i+1}. (Wrap-around occurs at the end as the element x_n gets connected to y_n and y_1.) Here are the Hasse diagrams of the crowns $\mathbf{C_3}$, $\mathbf{C_4}$, and $\mathbf{C_5}$:



Linear extension, realizer, and dimension

Let $\mathbf{P} = (X, R)$ be a poset. By a ***linear extension of*** $\mathbf{P}$ we mean a totally ordered set of the form $\mathbf{L} = (X, R')$ where $R \subseteq R'$. That is, a linear extension of a poset is (1) itself a poset with the same ground set, (2) a total order, and (3) relation-preserving in the sense that any ordered pair present in the original poset is also present in the linear extension.

Question 339 *Is $a \leqslant f \leqslant b \leqslant d \leqslant e \leqslant c$ a linear extension of the poset shown on the right? Is $f \leqslant a \leqslant b \leqslant c \leqslant e \leqslant d$?*



A ***realizer of*** $\mathbf{P}$ is a set of linear extensions whose intersection is $\mathbf{P}$. An ***n-realizer*** is a realizer of size n. The ***dimension of*** $\mathbf{P}$ is the minimum value of n for which an n-realizer exists. We write $\dim(\mathbf{P}) = n$ to indicate that the dimension of $\mathbf{P}$ is n.

Any proof that the dimension of a poset is n requires two things: (1) an example of an n-realizer; and (2) a proof that no smaller realizer exists. We now give several examples of these types of arguments.

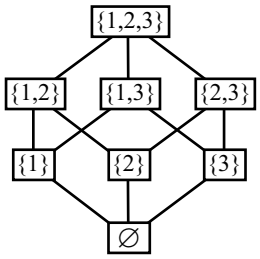
First examples of dimension

First we observe that $\dim(\mathbf{P}) = 1$ if and only if $\mathbf{P}$ is a total order, for any such poset serves as its own realizer. In a total order, every pair of elements is comparable. Might a poset in which every pair of distinct elements is incomparable (a "total unorder") have high dimension?

Question 340 *Find the dimension of the antichain of size 4. Then, extend your result to find the dimension of the antichain of size n, for $n \geqslant 2$.*

Example: the subset lattice $\mathbf{2^3}$

Next let's examine the subset lattice $\mathbf{2^3}$:



Certainly $\dim(\mathbf{2^3}) \geqslant 2$. Is its dimension equal to 2 or is it larger?

Let's begin by assuming that a 2-realizer exists (so that $\dim(\mathbf{2^3}) = 2$) and see what happens. Let $\mathcal{R} = \{\mathbf{L}_1, \mathbf{L}_2\}$ be a 2-realizer. Begin by noting that $\{1\} \parallel \{2,3\}$ in $\mathbf{2^3}$. Since the intersection of the two linear extensions equals $\mathbf{2^3}$, and since $\{1\}$ and $\{2,3\}$ are incomparable in that poset, then one of the linear extensions must place $\{1\}$ below $\{2,3\}$ and the other must place $\{2,3\}$ below $\{1\}$.

Without loss of generality, let's assume that $\{1\} <_1 \{2,3\}$ and $\{2,3\} <_2 \{1\}$, where to avoid confusion we use $\leqslant_1$ to denote the relation of $\mathbf{L}_1$ and $\leqslant_2$ to denote the relation of $\mathbf{L}_2$.

First we show that $\{2,3\} <_2 \{1\}$ forces $\{2\} <_2 \{1,3\}$. This is because

$$\{2\} <_2 \{2,3\} <_2 \{1\} <_2 \{1,3\}.$$

(The first and third inequalities follow because they are true in $\mathbf{2^3}$ and thus true in any of its linear extensions.) Similarly, $\{3\} <_2 \{1,2\}$.

Question 341 *Provide the details that show* $\{3\} <_2 \{1,2\}$.

Now, because $\{2\} \parallel \{1,3\}$ and $\{3\} \parallel \{1,2\}$ in $\mathbf{2^3}$, it follows that $\{1,3\} <_1 \{2\}$ and $\{1,2\} <_1 \{3\}$. But this in turn implies that

$$\{1,3\} <_1 \{2\} <_1 \{1,2\} \qquad \text{and} \qquad \{1,2\} <_1 \{3\} <_1 \{1,3\}.$$

That is, $\{1,3\} <_1 \{1,2\}$ and $\{1,2\} <_1 \{1,3\}$, which contradicts antisymmetry of the poset $\mathbf{L}_1$. Therefore, no 2-realizer exists for $\mathbf{2^3}$.

We have proved that $\dim(\mathbf{2^3}) \geqslant 3$. In order to conclude that $\dim(\mathbf{2^3}) = 3$ we need to find a 3-realizer. Here is one:

$$\begin{aligned}
\mathbf{L}_1 &: \quad \emptyset < \{1\} < \{2\} < \{1,2\} < \{3\} < \{1,3\} < \{2,3\} < \{1,2,3\} \\
\mathbf{L}_2 &: \quad \emptyset < \{1\} < \{3\} < \{1,3\} < \{2\} < \{1,2\} < \{2,3\} < \{1,2,3\} \\
\mathbf{L}_3 &: \quad \emptyset < \{2\} < \{3\} < \{2,3\} < \{1\} < \{1,2\} < \{1,3\} < \{1,2,3\}.
\end{aligned}$$

Proving that $\{\mathbf{L}_1, \mathbf{L}_2, \mathbf{L}_3\}$ is indeed a realizer involves a careful if tedious check of the following two facts:

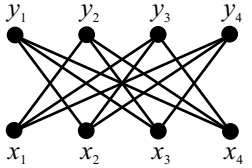
- If $A \subseteq B$ in $\mathbf{2^3}$, then $A \leqslant B$ in all three linear extensions.
- If $A \parallel B$ in $\mathbf{2^3}$, then there is some linear extension in which $A < B$ and some other linear extension in which $B < A$.

Question 342 *Check that these statements are true.*

This completes the demonstration that $\dim(\mathbf{2^3}) = 3$.

The dimension of the standard example $\mathbf{S_n}$

Next we prove that the standard example of an n-dimensional poset is indeed deserving of its name. Once you understand the proof for a special case (here, $n = 4$) it easily generalizes. The standard example $\mathbf{S_4}$ is shown below:



First we show that a realizer must consist of at least four linear extensions, and then we give a specific 4-realizer.

Consider any realizer of $\mathbf{S_4}$. Since $x_1 \parallel y_1$, we know that any realizer must contain a linear extension $\mathbf{L}_1$ with $y_1 < x_1$. Let's take a close look at what must happen in this linear extension. In $\mathbf{S_4}$ we have $x_2 < y_1$ and $x_1 < y_2$, so we must have these same relations preserved in any linear extension. This means that in $\mathbf{L}_1$, we have $x_2 < y_1 < x_1 < y_2$, i.e., $x_2 < y_2$. A similar argument shows that $x_3 < y_3$ and $x_4 < y_4$ in $\mathbf{L}_1$ as well.

We have shown that any linear extension of $\mathbf{S_4}$ which has $y_1 < x_1$ must also have $x_i < y_i$ for $i = 2, 3, 4$. In other words, placing $y_1 < x_1$ in a linear extension prevents us from placing $y_i < x_i$ for any other i. A similar result holds for other pairs, namely:

Any linear extension of $\mathbf{S_4}$ *which has* $y_j < x_j$ *must also have* $x_i < y_i$ *for all* i *with* $i \neq j$.

Therefore, any realizer of $\mathbf{S_4}$ must necessarily contain a linear extension $\mathbf{L}_1$ that has $y_1 < x_1$, a different linear extension $\mathbf{L}_2$ that has $y_2 < x_2$, and so on for $\mathbf{L}_3$ and $\mathbf{L}_4$. In other words, any realizer requires at least four linear extensions and so $\dim(\mathbf{S_4}) \geq 4$.

Now the question remains: does a 4-realizer exist? Yes, and one is pictured in Figure 8.6. The intersection of these four realizers is $\mathbf{S_4}$ because of the following.

- *Comparable pairs* $x_i < y_j$*:* Observe that $x_1 < y_j$ for $j = 2, 3, 4$ in all four linear extensions. Similarly, $x_2 < y_j$ for $j = 1, 3, 4$ and $x_3 < y_j$ for $j = 1, 2, 4$ and $x_4 < y_j$ for $j = 1, 2, 3$ in all four linear extensions.
- *Incomparable pairs* $x_i \parallel y_i$*:* Observe that $y_1 < x_1$ in $\mathbf{L}_1$ while $x_1 < y_1$ in all other linear extensions. Similarly, $y_2 < x_2$ in $\mathbf{L}_2$ while $x_2 < y_2$ in all other linear extensions, and so on.
- *Incomparable pairs* $x_i \parallel x_j$*:* Take two different elements x_i and x_j and assume $i < j$. Linear extension $\mathbf{L}_i$ has $x_j < x_i$ while all other linear extensions have $x_i < x_j$.

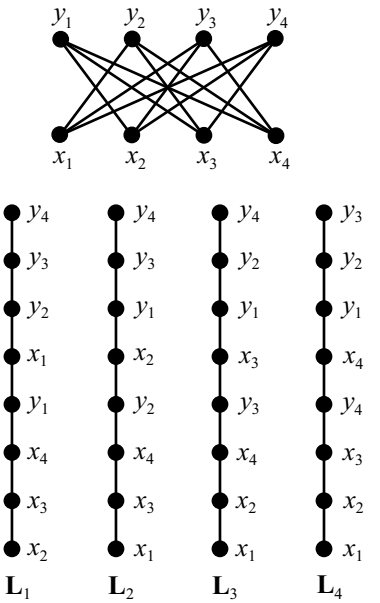


Figure 8.6. A 4-realizer of $\mathbf{S_4}$.

- *Incomparable pairs* $y_i \parallel y_j$*:* Take two different elements y_i and y_j and assume $i < j$. Linear extension $\mathbf{L}_j$ has $y_j < y_i$ while all other linear extensions have $y_i < y_j$.

Therefore, $\{\mathbf{L}_1, \mathbf{L}_2, \mathbf{L}_3, \mathbf{L}_4\}$ is a 4-realizer of $\mathbf{S_4}$ and so $\dim(\mathbf{S_4}) \leqslant 4$. This completes the proof that $\dim(\mathbf{S_4}) = 4$.

The argument that shows that any realizer must have at least size 4 and the construction of the specific 4-realizer can be generalized to $\mathbf{S_n}$ for any $n \geqslant 2$. Exercise 6 asks you to provide the details.

Theorem 8.4.1 *For $n \geqslant 2$, the dimension of the standard example $\mathbf{S_n}$ is n.*

The dimension of the crown $\mathbf{C_n}$

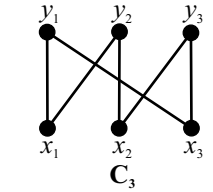
The crown $\mathbf{C_3}$ is the poset with Hasse diagram that appears at the top of Figure 8.7. Below it appears a 3-realizer, and to the right is verification that the three linear extensions are indeed a realizer. The first six lines of the table verify that the six comparable pairs present in $\mathbf{C_3}$ are also present in each linear extension. The last nine lines verify that for each incomparable pair $x \parallel y$ in $\mathbf{C_3}$, there is a linear extension containing $x < y$ and another containing $y < x$.

But this is just half of the story because it only proves that $\dim(\mathbf{C_3}) \leqslant 3$. We now prove that no 2-realizer exists. For sake of contradiction, suppose that $\{\mathbf{M}_1, \mathbf{M}_2\}$ is a realizer of $\mathbf{C_3}$. Since $x_1 \parallel y_3$ in $\mathbf{C_3}$, we assume without loss of generality that $x_1 <_1 y_3$ in $\mathbf{M}_1$ and $y_3 <_2 x_1$ in $\mathbf{M}_2$.

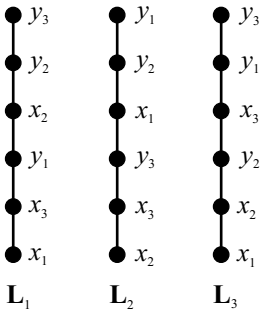
In $\mathbf{M}_2$ we have $x_3 <_2 y_2$ and $x_2 <_2 y_1$ because

$$x_3 < y_3 <_2 x_1 < y_2 \qquad \text{and} \qquad x_2 < y_3 <_2 x_1 < y_1.$$

These inequalities also show that $y_3 <_2 y_1$ and $y_3 <_2 y_2$ in $\mathbf{M}_2$. Since $y_1 \parallel y_3$ and $y_2 \parallel y_3$ in $\mathbf{C_3}$, it follows that these pairs must be reversed in the other linear extension:



$\mathbf{C_3}$



$\mathbf{L}_1$ $\mathbf{L}_2$ $\mathbf{L}_3$

In $\mathbf{C_3}$	In $\mathbf{L}_1$	In $\mathbf{L}_2$	In $\mathbf{L}_3$
$x_1 < y_1$	yes	yes	yes
$x_1 < y_2$	yes	yes	yes
$x_2 < y_2$	yes	yes	yes
$x_2 < y_3$	yes	yes	yes
$x_3 < y_3$	yes	yes	yes
$x_3 < y_1$	yes	yes	yes
$x_1 \parallel x_2$	$x_1 < x_2$	$x_2 < x_1$	
$x_1 \parallel x_3$	$x_1 < x_3$	$x_3 < x_1$	
$x_2 \parallel x_3$	$x_3 < x_2$	$x_2 < x_3$	
$y_1 \parallel y_2$	$y_1 < y_2$	$y_2 < y_1$	
$y_1 \parallel y_3$	$y_1 < y_3$	$y_3 < y_1$	
$y_2 \parallel y_3$	$y_2 < y_3$	$y_3 < y_2$	
$x_1 \parallel y_3$	$x_1 < y_3$	$y_3 < x_1$	
$x_2 \parallel y_1$	$y_1 < x_2$	$x_2 < y_1$	
$x_3 \parallel y_2$	$x_3 < y_2$		$y_2 < x_3$

Figure 8.7. A 3-realizer of the crown $\mathbf{C_3}$.

$y_1 <_1 y_3$ and $y_2 <_1 y_3$ in $\mathbf{M_1}$. Similarly, we have $y_1 <_1 x_2$ in $\mathbf{M_1}$. It then follows that

$$x_3 < y_1 <_1 x_2 < y_2$$

so $x_3 <_1 y_2$ in $\mathbf{M_1}$. This shows $x_3 <_1 y_2$ and $x_3 <_2 y_2$, which implies $x_3 < y_2$ in $\mathbf{C_3}$. But $x_3 \parallel y_2$ in $\mathbf{C_3}$, a contradiction. Therefore no 2-realizer of $\mathbf{C_3}$ exists.

Interestingly, and unlike the situation for $\mathbf{S_n}$, the dimension of the crown is always 3. The argument we gave for $\mathbf{C_3}$ does extend to prove the following result. See Exercises 7 and 8.

Theorem 8.4.2 *For $n \geqslant 3$, the dimension of the crown $\mathbf{C_n}$ is 3.*

Existence of linear extensions

To close this section, we discuss three results that show that the concept of poset dimension is well-defined.

The first says that any poset has a linear extension. Here is a constructive way to see this. Let x_1 be any minimial element of the poset. Delete x_1 from the poset, then let x_2 be any minimal element of the resulting poset. Delete x_2 from that poset, then let x_3 be any minimal element of the resulting poset. Continue until all elements of the original poset have been used. The desired linear extension is then $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$. Exercise 5 asks for a rigorous proof.

The second result is stronger than the first. It ensures that it is possible to create linear extensions that place incomparable pairs in certain positions. In constructing a realizer we know that if x and y are incomparable, then we must find a linear extension wherein $x < y$ and another wherein $y < x$. For example, in the subset lattice $\mathbf{2^3}$, it is possible to find a linear extension in which $\{2\} < \{1, 3\}$ and another linear extension in which $\{1, 3\} < \{2\}$.

Theorem 8.4.3 *If $\mathbf{P} = (X, \leqslant)$ is a poset and x' and y' are incomparable elements, then there exists a linear extension of $\mathbf{P}$ in which $x' < y'$.*

See Exercise 9 for an outline of a proof.

The third result is an immediate corollary of the previous theorem: any poset equals the intersection of all its linear extensions.

Question 343 *Give a quick proof using the previous theorem.*

Therefore any poset has a realizer—just use all of its linear extensions. Thus the dimension, being the minimum size of a realizer, is well-defined.

Summary

Any poset has a linear extension, which is a total order that contains all the relations present in the original poset. A realizer is a set of linear extensions whose intersection equals the original poset, and the dimension of a poset is the minimum size of a realizer.

Exercises

1. Consider the set $X = \{a, b, c, d, e\}$ ordered by the following relation:

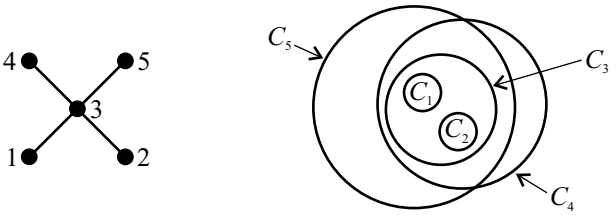
$$R = \big\{(a,a), (a,c), (a,d), (a,e), (b,b), (b,c), \\ (b,d), (b,e), (c,c), (c,d), (c,e), (d,d), (e,e)\big\}.$$

How many different linear extensions does this poset have?

2. Let $n \geqslant 3$ and let X be the set of 1-element and $(n-1)$-element subsets of $[n]$. Find a "named" poset that is isomorphic to $(X, \subseteq)$ and prove that you are correct.
3. Find the dimension of $\mathbf{\Pi_3}$, the set of partitions of [3] ordered by refinement.
4. Find the dimension of $\mathbf{2^4}$.
5. Prove that any poset has a linear extension. Do this by proving that the algorithm discussed at the end of this section is correct.
6. Extend the argument given in this section to prove that the dimension of $\mathbf{S_n}$ is n.
7. Verify that the following three linear extensions form a realizer of $\mathbf{C_4}$:

$$\begin{aligned} L_1: &\quad x_4 < x_3 < y_4 < x_2 < y_3 < x_1 < y_2 < y_1 \\ L_2: &\quad x_4 < x_1 < y_1 < x_2 < y_2 < x_3 < y_3 < y_4 \\ L_3: &\quad x_3 < x_2 < x_1 < y_3 < y_2 < x_4 < y_4 < y_1. \end{aligned}$$

   Then, complete the proof that $\dim(\mathbf{C_4}) = 3$ by proving that no 2-realizer exists.
8. Prove Theorem 8.4.2 by generalizing the arguments for $\mathbf{C_3}$ and $\mathbf{C_4}$.
9. Here is an outline of a proof of Theorem 8.4.3.
   (a) Let $\mathbf{P} = (X, R)$ be a poset and suppose $x' \parallel y'$. Create a new relation R' on X by adding to R the ordered pair (x', y') as well as some additional ordered pairs to ensure that R' remains reflexive, antisymmetric, and transitive. What ordered pairs do you think you have to add?
   (b) Prove that $\mathbf{P}' = (X, R')$ is indeed a poset, where R' is the relation from part (a).
   (c) Explain how to complete the proof of the theorem. (Hint: What if $\mathbf{P}'$ is a total order? What if it isn't?)
10. Prove that if $\mathbf{P}$ is a poset whose ground set contains at most five elements, then $\dim(\mathbf{P}) \leqslant 2$.
11. A ***circle order*** is a poset whose ground set consists of circular disks (circles with their interiors) in the xy-plane ordered by inclusion. Here is an example of a poset that is (i.e., is isomorphic to) a circle order:



   In other words $i \leqslant j$ in the poset on the left if and only if $C_i \subseteq C_j$ in the collection of circles on the right.
   Prove: if $\dim(\mathbf{P}) \leqslant 2$, then $\mathbf{P}$ can be expressed as a circle order.
12. A ***box order*** is similar to the idea of a circle order introduced in the previous exercise, but with rectangular boxes (rectangles with their interiors) instead of circular disks.
   (a) Represent each of $\mathbf{2^2}$ and $\mathbf{5}$ as a box order.

(b) Prove: if $\dim(\mathbf{P}) \leqslant 4$, then $\mathbf{P}$ can be expressed as a box order.

13. This exercise explains why "dimension" is a good name for the concept studied in this section. Let X be any set of points in $\mathbb{R}^n$. Define the ordering $\preceq$ on X by $x \preceq y$ whenever $x_i \leqslant y_i$ for all i. For example, when $x = (-4, 1.5, 13)$ and $y = (0, 100, 13)$ in $\mathbb{R}^3$, we have $x \preceq y$ because $-4 \leqslant 0$ and $1.5 \leqslant 100$ and $13 \leqslant 13$. On the other hand, $(-4, 1.5, 13) \not\preceq (0, 0, 15)$ because $1.5 \not\leqslant 0$.

A poset ***embeds in*** $\mathbb{R}^n$ provided it is isomorphic to a set of points in $\mathbb{R}^n$ ordered by the relation given above.

(a) Show that the 4-element poset shown at the beginning of this section embeds in $\mathbb{R}^2$. Show that $\mathbf{2^3}$ embeds in $\mathbb{R}^3$.

(b) Prove that $\mathbf{P}$ embeds in $\mathbb{R}^2$ if and only if $\dim(\mathbf{P}) \leqslant 2$, and also that $\mathbf{P}$ embeds in $\mathbb{R}^3$ if and only if $\dim(\mathbf{P}) \leqslant 3$.

(c) Generalize to prove that $\mathbf{P}$ embeds in $\mathbb{R}^n$ if and only if $\dim(\mathbf{P}) \leqslant n$.

In other words, the dimension of $\mathbf{P}$ is the least n for which $\mathbf{P}$ embeds in n-dimensional space $\mathbb{R}^n$.

Travel Notes

Dushnik & Miller (1941) introduced the concept of dimension. In that paper they also introduced the standard example of an n-dimensional poset. Trotter (1992) is the standard reference for dimension theory of finite posets.

Circle and box orders are examples of so-called geometric containment orders. There are some tantalizing open questions concerning such posets. Exercise 11 shows that 2-dimensional posets are circle orders. What about 3-dimensional posets? If we allow infinite posets, then the answer is no because there exists an example of a 3-dimensional infinite poset that is not a circle order. But in the case of finite posets, it is not known whether every 3-dimensional poset is a circle order. Yet there is a result that comes agonizingly close: every 3-dimensional poset is a regular n-gon order for all $n \geqslant 3$. A regular polygon with 100 trillion sides is practically a circle, is it not?!?

8.5 Möbius inversion, part I

The final two sections of this book introduce the theory and applications of Möbius inversion in order to unify some seemingly disparate topics and also to prepare the reader for further study in combinatorics. In this first section we use the example of inclusion-exclusion to understand the concepts of zeta function, Möbius function, and the Möbius inversion formula.

Our exposition essentially follows that of the classic papers of Rota (1964) and Bender & Goldman (1975). The former is a true milestone in combinatorics and the latter is a well-written summary of several combinatorial applications of Möbius inversion.

This section assumes that the reader has familiarity with matrix multiplication, the inverse of a matrix, and the determinant. One can in fact understand the principle of Möbius inversion without using matrices, but using them makes for good illustrations.

Revisiting inclusion-exclusion

Our first example in Section 3.1 concerned counting the integers in [100] that are divisible by none of 2, 3, and 5. We defined the universe $\mathcal{U}$ to be the set [100], and then defined property d_i to be "the integer is divisible by i" for $i = 2, 3, 5$. The answer to the problem is $N_=(\emptyset)$, which is the number of integers in $\mathcal{U}$ having none of the three properties. The inclusion-exclusion formula (Theorem 3.1.2, page 89) says

$$\begin{aligned} N_=(\emptyset) = {} & N_\geqslant(\emptyset) - N_\geqslant(d_2) - N_\geqslant(d_3) - N_\geqslant(d_5) \\ & + N_\geqslant(d_2d_3) + N_\geqslant(d_2d_5) + N_\geqslant(d_3d_5) - N_\geqslant(d_2d_3d_5). \end{aligned} \tag{8.1}$$

Recall that, for example, the notation $N_\geqslant(d_2d_3)$ stands for the number of integers in [100] that have the properties d_2 and d_3 and possibly others—the number of integers in [100] that are divisible by 2 and 3, and possibly by 5. This formula for $N_=(\emptyset)$ was useful because we could easily compute each of the $N_\geqslant$ values.

To count the integers in [100] divisible by 2 but by neither 3 nor 5, we could apply the more general inclusion-exclusion formula (Theorem 3.1.5, page 92) to get

$$N_=(d_2) = N_\geqslant(d_2) - N_\geqslant(d_2d_3) - N_\geqslant(d_2d_5) + N_\geqslant(d_2d_3d_5). \tag{8.2}$$

Linear systems

Both formulas of equations (8.1) and (8.2) can be derived by solving a linear system. Treat the values of $N_\geqslant$ as the "knowns" and the values of $N_=$ as the "unknowns." The following equation relates the known value $N_\geqslant(d_2)$ to some unknown values:

$$N_\geqslant(d_2) = N_=(d_2) + N_=(d_2d_3) + N_=(d_2d_5) + N_=(d_2d_3d_5). \tag{8.3}$$

That is, in counting the integers in [100] divisible by 2 (and possibly by 3 or 5), we can break up the analysis into four disjoint cases: those divisible by 2 alone; those divisible by 2 and 3 alone; those divisible by 2 and 5 alone; and those divisible by 2, 3, and 5. Similarly, we have

$$N_\geqslant(d_2d_5) = N_=(d_2d_5) + N_=(d_2d_3d_5). \tag{8.4}$$

These are just two of the eight equations we can write, one for each possible subset of the three properties. In matrix notation the entire linear system is

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} N_=(\emptyset) \\ N_=(d_2) \\ N_=(d_3) \\ N_=(d_5) \\ N_=(d_2d_3) \\ N_=(d_2d_5) \\ N_=(d_3d_5) \\ N_=(d_2d_3d_5) \end{pmatrix} = \begin{pmatrix} N_\geqslant(\emptyset) \\ N_\geqslant(d_2) \\ N_\geqslant(d_3) \\ N_\geqslant(d_5) \\ N_\geqslant(d_2d_3) \\ N_\geqslant(d_2d_5) \\ N_\geqslant(d_3d_5) \\ N_\geqslant(d_2d_3d_5) \end{pmatrix}.$$

Notice that equations (8.3) and (8.4) appear as the second and sixth rows, respectively.

Question 344 *The last row says $N_=(d_2d_3d_5) = N_\geqslant(d_2d_3d_5)$. Why is this true?*

Abbreviate this matrix equation as $ZN_= = N_\geqslant$ where Z is the 8×8 matrix on the left. We need to solve for the column vector $N_=$.

This linear system has a unique solution because the matrix Z is invertible: being upper triangular, its determinant equals the product of the diagonal entries, which is 1, and a nonzero determinant means the inverse exists. The solution is $N_= = Z^{-1}N_\geqslant$, or

$$\begin{pmatrix} N_=(\emptyset) \\ N_=(d_2) \\ N_=(d_3) \\ N_=(d_5) \\ N_=(d_2d_3) \\ N_=(d_2d_5) \\ N_=(d_3d_5) \\ N_=(d_2d_3d_5) \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\ 0 & 1 & 0 & 0 & -1 & -1 & 0 & 1 \\ 0 & 0 & 1 & 0 & -1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} N_\geqslant(\emptyset) \\ N_\geqslant(d_2) \\ N_\geqslant(d_3) \\ N_\geqslant(d_5) \\ N_\geqslant(d_2d_3) \\ N_\geqslant(d_2d_5) \\ N_\geqslant(d_3d_5) \\ N_\geqslant(d_2d_3d_5) \end{pmatrix}.$$

It is perhaps best to use a computer to calculate Z^{-1}.

Notice that all of the inclusion-exclusion formulas produced by Theorems 3.1.2 and 3.1.5 are presently available. Equation (8.1) is the first row of this matrix equation, equation (8.2) is the second row, etc.

The last important observation to take from this example is that the matrix Z came from a poset. Specifically, it came from the subsets of $\{d_2, d_3, d_5\}$ ordered by inclusion. If we index the rows and columns of Z according to the linear extension

$$\emptyset < \{d_2\} < \{d_3\} < \{d_5\} < \{d_2, d_3\} < \{d_2, d_5\} < \{d_3, d_5\} < \{d_2, d_3, d_5\}$$

of that poset, then Z_{ij} is 1 when row i's set is a subset of column j's subset, and Z_{ij} is 0 otherwise:

$$\begin{array}{c} \\ \emptyset \\ d_2 \\ d_3 \\ d_5 \\ d_2d_3 \\ d_2d_5 \\ d_3d_5 \\ d_2d_3d_5 \end{array} \begin{array}{c} \begin{array}{cccccccc} \emptyset & d_2 & d_3 & d_5 & d_2d_3 & d_2d_5 & d_3d_5 & d_2d_3d_5 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array} = Z.$$

(We write d_3d_5, for example, instead of $\{d_3, d_5\}$ to save space and avoid clutter.)

The zeta matrix and the Möbius matrix

The matrix Z shown above is called a zeta matrix. Given a poset $\mathbf{P} = (X, \leqslant)$ on n elements, let's say we have labeled the elements of X in a specific order as $x_1, x_2, \ldots, x_n$. The ***zeta matrix of*** $\mathbf{P}$ is that $n \times n$ matrix Z where

$$Z_{ij} = \begin{cases} 1 & \text{if } x_i \leqslant x_j \\ 0 & \text{otherwise.} \end{cases}$$

If you order the elements of X according to a linear extension of $\mathbf{P}$, as we did in the inclusion-exclusion example earlier, then indeed Z is an upper triangular matrix with 1s on the diagonal. (See Exercise 7.) The ***Möbius matrix of*** $\mathbf{P}$ is then defined as Z^{-1}, the inverse of the matrix Z.

Question 345 *Find the zeta matrix of the divisibility lattice* $\mathbf{D_{18}}$. *Label the rows and columns in the order 1, 2, 3, 6, 9, 18. Then find the Möbius matrix.*

The idea of Möbius inversion

Let's summarize what we learned from the inclusion-exclusion example. We wanted to answer a counting question and had two functions $N_{\geqslant}$ and $N_{=}$ to help us do so. These two functions were related by the equations

$$N_{\geqslant}(J) = \sum_{I:J\subseteq I} N_{=}(I) \qquad \text{for each } J \text{ satisfying } J \subseteq \{d_2, d_3, d_5\}. \tag{8.5}$$

The sum is to be interpreted as being over all sets I such that I contains J as a subset, i.e., over all supersets of J. These equations correspond to the system $ZN_{=} = N_{\geqslant}$ shown earlier.

This tells us how to express $N_{\geqslant}$ in terms of $N_{=}$, but the function $N_{=}$ contains the answer to our counting problem. We inverted equations (8.5) to obtain $N_{=}$ in terms of $N_{\geqslant}$. The answer is exactly that of Theorem 3.1.5 on page 92, namely

$$N_{=}(J) = \sum_{I:J\subseteq I} (-1)^{|I|-|J|} N_{\geqslant}(I) \qquad \text{for each } J \text{ satisfying } J \subseteq \{d_2, d_3, d_5\}.$$

In other words, these equations are exactly those expressed by $N_{=} = Z^{-1}N_{\geqslant}$.

When we first encountered inclusion-exclusion, the counting functions $N_{=}$ and $N_{\geqslant}$ were our main concern. We now see that there is a poset hiding behind the definitions of $N_{=}$ and $N_{\geqslant}$, namely the subsets of $\{d_2, d_3, d_5\}$ ordered by inclusion. In other words, the summation in equation (8.5) is over all elements I in that poset that are "above" the set J. In Möbius inversion we bring the underlying poset front and center.

At this point we will cease to speak of the zeta matrix and instead work with the zeta *function*. There are several advantages. For one, the somewhat unwieldy technical details of linear algebra (how to index rows and columns, upper triangular form, row reduction, determinants) disappear and this makes the theory much cleaner. For another, the results extend easily to certain classes of infinite posets.

The zeta function of a poset

Given a poset $\mathbf{P} = (X, \leqslant)$, the ***zeta function of*** $\mathbf{P}$ is that function $\zeta : X \times X \longrightarrow \mathbb{R}$ given by

$$\zeta(x, y) = \begin{cases} 1 & \text{if } x \leqslant y \\ 0 & \text{otherwise.} \end{cases}$$

This function replaces the zeta matrix Z and applies to any finite or infinite poset. In the inclusion-exclusion example we've been using, observe that the equation

$$N_{\geqslant}(J) = \sum_{I:J\subseteq I} N_{=}(I)$$

can also be written

$$N_{\geqslant}(J) = \sum_{I=\emptyset}^{\{d_2,d_3,d_5\}} \zeta(J, I)\, N_{=}(I)$$

where we interpret the sum to be over all possible subsets of $\{d_2, d_3, d_5\}$. This is because ζ, being the zeta function of the subsets of $\{d_2, d_3, d_5\}$ ordered by inclusion, satisfies $\zeta(J, I) = 1$ when $J \subseteq I$ and $\zeta(J, I) = 0$ otherwise.

The incidence algebra of a poset

We want to find the inverse of ζ, for that is what the Möbius function is, so next we need to understand what an inverse is in this context. In some sense it is just a generalization of the inverse of a matrix.

Let $\mathbf{P} = (X, \leqslant)$ be a poset. First of all, we restrict ourselves to functions $\alpha : X \times X \longrightarrow \mathbb{R}$ that satisfy $\alpha(x, y) = 0$ whenever $x \not\leqslant y$. Along with the operations of addition, scalar multiplication, and function multiplication that we will define shortly, this set of functions forms what is known as the ***incidence algebra of*** $\mathbf{P}$.

For two such functions α and β, their sum $\alpha + \beta$ is defined as usual: $(\alpha + \beta)(x, y) = \alpha(x, y) + \beta(x, y)$. This is the same way that matrix addition is defined—componentwise. If $c \in \mathbb{R}$, then the scalar multiplication $c\alpha$ is also no surprise: $(c\alpha)(x, y) = c \cdot \alpha(x, y)$. This is the same way that scalar-matrix multiplication is defined.

The function multiplication operation is the important one because the Möbius function is a multiplicative inverse of the zeta function. The product $\alpha\beta$ of two functions α and β is defined by

$$(\alpha\beta)(x, y) = \sum_{z : x \leqslant z \leqslant y} \alpha(x, z)\beta(z, y). \tag{8.6}$$

Let's take a moment to notice why this is similar to matrix multiplication in the case of a finite poset. For two $n \times n$ matrices A and B, their product AB is defined componentwise by

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

For finite posets this really is the same formula as equation (8.6), especially when we realize that the sum in that equation can be taken over all $z \in X$. This is because $\alpha(x, z) = 0$ whenever $x \not\leqslant z$ and $\beta(z, y) = 0$ whenever $z \not\leqslant y$.

Locally finite posets

A poset $\mathbf{P} = (X, \leqslant)$ is ***locally finite*** if for all $x, y \in X$ the set

$$[x, y] = \{z \in X : x \leqslant z \leqslant y\}$$

is finite. The set $[x, y]$ is called, quite naturally, the ***interval from*** x ***to*** y. For example, in the poset $\mathbf{D_{18}}$ we have

$$\begin{aligned} [3, 18] &= \{3, 6, 9, 18\} \\ [3, 9] &= \{3, 9\} \\ [6, 18] &= \{6, 18\} \\ [2, 2] &= \{2\}. \end{aligned}$$

Of course, finite posets are locally finite. But many infinite posets are locally finite as well, such as the positive integers ordered by divisibility and the subsets of positive integers ordered by inclusion.

The extension from finite to locally finite posets is an important one that requires little extra effort. The locally finite assumption guarantees that the sums we deal with, such as that of equation (8.6), are finite and thus convergent.

Question 346 *Give an example of a poset that is not locally finite.*

The Möbius function of a poset

The inverse of the zeta matrix Z was that matrix M for which $MZ = I$, the identity matrix. To find the inverse of the zeta function ζ, we seek a function μ so that $\mu\zeta$ is the identity function. In this case the incidence algebra's identity function is known as ***Kronecker delta***, which is that function $\delta : X \times X \longrightarrow \mathbb{R}$ given by

$$\delta(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise.} \end{cases}$$

Compare it with the identity matrix I.

Question 347 *Suppose that the zeta function of a poset equals δ shown above. What does the poset look like?*

We now define the Möbius function and then prove that it is an inverse of the zeta function.

Definition 8.5.1 *Given a locally finite poset $\mathbf{P} = (X, \leqslant)$, the **Möbius function of** $\mathbf{P}$ is that function $\mu : X \times X \longrightarrow \mathbb{R}$ defined by the following inductive procedure.*

1. *Set $\mu(x, y) := 0$ for all $x, y \in X$ with $x \not\leqslant y$.*
2. *Set $\mu(x, x) := 1$ for all $x \in X$.*
3. *Assuming $x < y$ and that $\mu(x, z)$ has already been defined for all z satisfying $x \leqslant z < y$, define*
$$\mu(x, y) := -\sum_{z : x \leqslant z < y} \mu(x, z).$$

The Möbius function is in the incidence algebra by virtue of #1, and the sum in #3 is well-defined because the poset is locally finite.

Theorem 8.5.2 *If $\mathbf{P} = (X, \leqslant)$ is a locally finite poset with zeta function ζ, then the Möbius function μ is an inverse of ζ. That is, $\mu\zeta = \delta$ where δ is the Kronecker delta function.*

Proof: Assume $\mathbf{P} = (X, \leqslant)$ is a locally finite poset with zeta function ζ. Let $x, y \in X$. Our goal is to show that $(\mu\zeta)(x, y) = \delta(x, y)$. By equation (8.6),

$$(\mu\zeta)(x, y) = \sum_{z : x \leqslant z \leqslant y} \mu(x, z)\, \zeta(z, y).$$

Case 1: If $x \not\leqslant y$, then the sum is empty and hence $(\mu\zeta)(x, y) = 0$. In addition, $\delta(x, y) = 0$ because $x \not\leqslant y$ implies $x \neq y$. Therefore $(\mu\zeta)(x, y) = \delta(x, y)$.

Case 2: If $x = y$, then

$$(\mu\zeta)(x, x) = \sum_{z : x \leqslant z \leqslant x} \mu(x, z)\, \zeta(z, x) = \mu(x, x)\, \zeta(x, x) = 1 \cdot 1 = 1.$$

Also, $\delta(x, x) = 1$, so therefore $(\mu\zeta)(x, x) = \delta(x, x)$.

Case 3: Finally, if $x < y$ we have

$$\begin{aligned}(\mu\zeta)(x,y) &= \sum_{z:x\leqslant z\leqslant y} \mu(x,z)\,\zeta(z,y)\\ &= \sum_{z:x\leqslant z\leqslant y} \mu(x,z)\\ &= \left(\sum_{z:x\leqslant z<y} \mu(x,z)\right) + \mu(x,y)\\ &= -\mu(x,y) + \mu(x,y)\\ &= 0.\end{aligned}$$

The second-to-last equality follows from #3 in Definition 8.5.1. Also, $\delta(x,y) = 0$ because $x < y$ implies $x \neq y$. Therefore $(\mu\zeta)(x,y) = \delta(x,y)$. ■

Example: computing a Möbius function

What is the Möbius function of the total order $\mathbf{5}$?

First we write the zeta function: for any $i, j \in [5]$ we have $\zeta(i,j) = 1$ when $i \leqslant j$, and $\zeta(i,j) = 0$ otherwise. Using step #2 of Definition 8.5.1, we set

$$\mu(1,1) = 1 \qquad \mu(2,2) = 1 \qquad \cdots \qquad \mu(5,5) = 1.$$

Next, use step #3 to get

$$\begin{aligned}\mu(1,2) &= -\mu(1,1) = -1\\ \mu(1,3) &= -\mu(1,1) - \mu(1,2) = -1 - (-1) = 0\\ \mu(1,4) &= -\mu(1,1) - \mu(1,2) - \mu(1,3) = -1 - (-1) - 0 = 0\\ \mu(1,5) &= -\mu(1,1) - \mu(1,2) - \mu(1,3) - \mu(1,4) = -1 - (-1) - 0 - 0 = 0.\end{aligned}$$

Then find

$$\begin{aligned}\mu(2,3) &= -\mu(2,2) = -1\\ \mu(2,4) &= -\mu(2,2) - \mu(2,3) = -1 - (-1) = 0\\ \mu(2,5) &= -\mu(2,2) - \mu(2,3) - \mu(2,4) = -1 - (-1) - 0 = 0.\end{aligned}$$

Continuing, we find that $\mu(i,i) = 1$ for all i, $\mu(i,i+1) = -1$ for $i = 1,2,3,4$, and $\mu(i,j) = 0$ otherwise.

The Möbius function of a total order

The previous example easily generalizes (Exercise 8) to a total order of any size. This result will play an important role in Section 8.6.

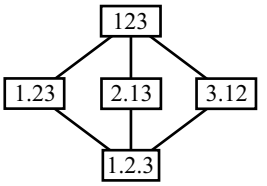
Theorem 8.5.3 *The Möbius function of the total order* $\mathbf{n}$ *is given by*

$$\mu(i,j) = \begin{cases} 1 & \text{if } i = j\\ -1 & \text{if } i+1 = j\\ 0 & \text{otherwise.}\end{cases}$$

Question 348 *Let* μ *be the Möbius function of the poset* $\mathbf{D_{16}}$. *Find* $\mu(2,8)$ *and* $\mu(4,8)$.

Example: the Möbius function of Π_3

Consider the partitions of [3] ordered by refinement:



We compute its Möbius function by first setting $\mu(P, P) = 1$ for all partitions P. Then

$$\mu(1.2.3, 1.23) = -\mu(1.2.3, 1.2.3) = -1$$

and similarly $\mu(1.2.3, 2.13) = 1$ and $\mu(1.2.3, 3.12) = 1$. Next,

$$\begin{aligned}\mu(1.2.3, 123) &= -\mu(1.2.3, 1.2.3) - \mu(1.2.3, 1.23) - \mu(1.2.3, 2.13) \\ &\quad - \mu(1.2.3, 3.12) \\ &= -1 - (-1) - (-1) - (-1) \\ &= 2.\end{aligned}$$

Finally, $\mu(1.23, 123) = -\mu(1.23, 1.23) = -1$ and similarly $\mu(2.13, 123) = -1$ and $\mu(3.12, 123) = -1$. Since we have computed $\mu(P, Q)$ for all partitions P and Q satisfying $P \preceq Q$, we are finished.

The principle of Möbius inversion, version I

We are ready to state the main result now that we know how to construct the Möbius function of a poset. Let $\mathbf{P} = (X, \leqslant)$ be a locally finite poset and let $N_=$ and $N_\geqslant$ be real-valued functions defined on the elements of this poset. The principle of Möbius inversion says that if $N_=$ and $N_\geqslant$ are related by the equations

$$N_\geqslant(x) = \sum_{y : x \leqslant y} N_=(y) \qquad \text{for each } x \in X,$$

then we can invert these equations to solve for $N_=$. The use of $N_=$ and $N_\geqslant$ is meant to hearken back to their meaning in the context of inclusion-exclusion.

Theorem 8.5.4 (Möbius inversion, I) *Suppose $\mathbf{P} = (X, \leqslant)$ is a locally finite poset with Möbius function μ. If $N_=$ and $N_\geqslant$ are functions $X \longrightarrow \mathbb{R}$ related by the equations*

$$N_\geqslant(x) = \sum_{y : x \leqslant y} N_=(y) \qquad \textit{for each } x \in X, \tag{8.7}$$

and where there exists some $u \in X$ for which $N_=(x) = 0$ unless $x \leqslant u$, then

$$N_=(x) = \sum_{y : x \leqslant y} \mu(x, y)\, N_\geqslant(y) \qquad \textit{for each } x \in X. \tag{8.8}$$

Comment: The condition "there exists some $u \in X$ for which $N_=(x) = 0$ unless $x \leqslant u$" ensures that the sums are finite in the case of an infinite poset. It will always be satisfied when applying the theorem to a finite poset.

Proof: Assume $\mathbf{P} = (X, \leqslant)$ is a locally finite poset and that $N_=$ and $N_\geqslant$ are related by the equations (8.7). Let $x \in X$. Begin with the sum in equation (8.8) and write $N_\geqslant(y)$ in terms of $N_=$ according to (8.7) to get

$$\sum_{y:x\leqslant y} N_\geqslant(y)\,\mu(x,y) = \sum_{y:x\leqslant y}\sum_{z:y\leqslant z} N_=(z)\,\mu(x,y).$$

Since $\zeta(y,z) = 0$ whenever $y \not\leqslant z$, use ζ to replace the inner sum by one over the entire set X. After this, switch the order of summation and rearrange to obtain

$$\begin{aligned}\sum_{y:x\leqslant y}\sum_{z:y\leqslant z} N_=(z)\,\mu(x,y) &= \sum_{y:x\leqslant y}\sum_{z\in X} \zeta(y,z)\,N_=(z)\,\mu(x,y)\\ &= \sum_{z\in X}\sum_{y:x\leqslant y} N_=(z)\,\mu(x,y)\,\zeta(y,z).\end{aligned}$$

To this last expression, factor $N_=(z)$ out of the inner sum and then restrict that sum over y satisfying $x \leqslant y \leqslant z$. There is no harm in doing so because $\zeta(y,z) = 0$ when $y \not\leqslant z$. This shows

$$\begin{aligned}\sum_{z\in X}\sum_{y:x\leqslant y} N_=(z)\,\mu(x,y)\,\zeta(y,z) &= \sum_{z\in X} N_=(z)\sum_{y:x\leqslant y}\mu(x,y)\,\zeta(y,z)\\ &= \sum_{z\in X} N_=(z)\sum_{y:x\leqslant y\leqslant z}\mu(x,y)\,\zeta(y,z).\end{aligned}$$

The inner sum in the last expression equals $(\mu\zeta)(x,z)$, which in turn equals $\delta(x,z)$ because $\mu\zeta = \delta$. Therefore

$$\begin{aligned}\sum_{z\in X} N_=(z)\sum_{y:x\leqslant y\leqslant z}\mu(x,y)\,\zeta(y,z) &= \sum_{z\in X} N_=(z)\,\delta(x,z)\\ &= N_=(x)\,\delta(x,x)\\ &= N_=(x).\end{aligned}$$

This completes the demonstration of equation (8.8), and hence the proof. ■

The principle of Möbius inversion, version II

In inclusion-exclusion and in the Möbius inversion formula of Theorem 8.5.4, we used the notation $N_\geqslant(x)$ to remind us to sum $N_=$ over all elements in the poset at or above x. This is the "greater than" version of the Möbius inversion formula (8.8). There is a corresponding "less than" version that we now state. We shall have occasion to use both versions in Section 8.6.

Theorem 8.5.5 (Möbius inversion, II) *Suppose $\mathbf{P} = (X, \leqslant)$ is a locally finite poset with Möbius function μ. If $N_=$ and $N_\leqslant$ are functions $X \longrightarrow \mathbb{R}$ related by the equations*

$$N_\leqslant(x) = \sum_{y:y\leqslant x} N_=(y) \qquad \text{for each } x \in X, \tag{8.9}$$

and where there exists some $l \in X$ for which $N_=(x) = 0$ unless $l \leqslant x$, then

$$N_=(x) = \sum_{y:y\leqslant x} \mu(y,x)\,N_\leqslant(y) \qquad \text{for each } x \in X. \tag{8.10}$$

Question 349 *Prove the theorem by making the necessary modifications to the proof of Theorem 8.5.4.*

Summary

Any poset (finite or locally finite) has a zeta function as well as a well-defined inverse of the zeta function called the Möbius function. The Möbius inversion formulas can be thought of as generalizations of inclusion-exclusion, and in Section 8.6 we show how it applies to several combinatorial problems.

Exercises

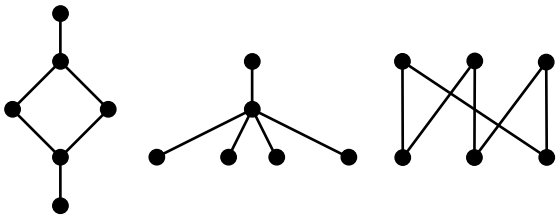
1. Determine, with explanation, which of the following statements are always true of the Möbius function of any poset.

   (a) If $\mu(x, y) = 0$, then $x \not\leq y$.

   (b) If $x \not\leq y$, then $\mu(x, y) = 0$.

2. Find $\mu(x, y)$ in the case that y covers x.

3. Compute the Möbius function of each of the three posets shown:



4. Let μ be the Möbius function of $\mathbf{\Pi_4}$, the partitions of [4] ordered by refinement whose Hasse diagram is shown in Figure 8.4 on page 324. Find $\mu(1.2.3.4, 1234)$ and $\mu(2.3.14, 1234)$.

5. Explain why M is the Möbius matrix of a poset, then the column sums of M always equal 0.

6. Show how to use Möbius inversion to solve the following equations for the x_i in terms of the s_i:

$$\begin{aligned} s_1 &= x_1 \\ s_2 &= x_1 + x_2 \\ s_3 &= x_1 + x_2 + x_3 \\ s_4 &= x_1 + x_2 + x_3 + x_4 \\ s_5 &= x_1 + x_2 + x_3 + x_4 + x_5. \end{aligned}$$

   In other words, what are $N_=$ and $N_\geqslant$, what is the underlying poset and its Möbius function, and how do you then find the solution?

7. Suppose $\mathbf{P} = (X, \leqslant)$ is a poset and that the elements of X have been labeled according to a linear extension: $x_1 < x_2 < \cdots < x_n$. Prove that if we label the rows and columns of the zeta matrix Z according to this linear extension, then Z has 1s on the diagonal and 0s below the diagonal.

8. Prove Theorem 8.5.3.

8.6 Möbius inversion, part II

In this final section we show how to apply the principle of Möbius inversion to derive the inclusion-exclusion formula and to solve a Pólya-type problem of counting under equivalence. We also sketch how to use it to solve the interesting problem of counting the connected labeled graphs on n vertices. These problems require knowing the Möbius function of the subset lattice, the divisibility lattice, and partitions ordered by refinement, respectively. First we develop a useful technique for computing Möbius functions.

Computing Möbius functions via poset products

Though the Möbius function of a poset can be found by using the inductive method of Definition 8.5.1, there are other techniques. The one we present here involves defining the product of two posets and then relating the Möbius function of the product to the Möbius function of each poset in the product. This is a simple relationship and it makes the method highly practical.

Given posets $\mathbf{P}_1 = (X_1, \leqslant_1)$ and $\mathbf{P}_2 = (X_2, \leqslant_2)$, we define their ***product*** as the poset

$$\mathbf{P}_1 \times \mathbf{P}_2 := (X_1 \times X_2, \leqslant),$$

where the relation $\leqslant$ on the ordered pairs in $X_1 \times X_2$ is defined for each $x_1, y_1 \in X_1$ and $x_2, y_2 \in X_2$ by

$$(x_1, x_2) \leqslant (y_1, y_2) \text{ if and only if } x_1 \leqslant_1 y_1 \text{ and } x_2 \leqslant_2 y_2.$$

The product of two posets is a poset (Exercise 2). Indeed the reflexive, antisymmetric, and transitive properties from $\mathbf{P}_1$ and $\mathbf{P}_2$ are directly inherited by the product. The idea easily extends to n-fold products $\mathbf{P}_1 \times \mathbf{P}_2 \times \cdots \times \mathbf{P}_n$.

Example: The subset lattice as a product

Let $\mathbf{B}^1 := \big(\{0, 1\}, \leqslant\big)$ be the totally ordered set on the integers 0 and 1. Then $\mathbf{B}^1 \times \mathbf{B}^1$ is the poset on the ordered pairs in the set

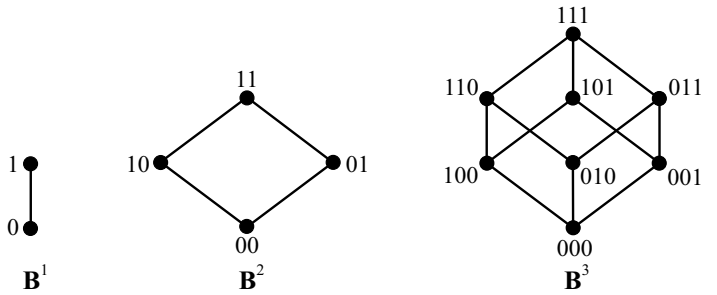
$$\{0, 1\} \times \{0, 1\} = \Big\{(0, 0), (0, 1), (1, 0), (1, 1)\Big\}$$

which we will just abbreviate as the set of 2-digit binary numbers $\{00, 01, 10, 11\}$. This product has $x_1x_2 \leqslant y_1y_2$ whenever $x_1 \leqslant y_1$ and $x_2 \leqslant y_2$. (For simplicity, we're using the $\leqslant$ symbol for both the relation on $\mathbf{B}^1$ as well as on $\mathbf{B}^1 \times \mathbf{B}^1$.) For example, in $\mathbf{B}^1 \times \mathbf{B}^1$ we have $10 \leqslant 11$ because the first digits satisfy $1 \leqslant 1$ in $\mathbf{B}$ and the second digits satisfy $0 \leqslant 1$ in $\mathbf{B}$. On the other hand, $10 \not\leqslant 01$ in the product.

The product $\mathbf{B}^1 \times \mathbf{B}^1 \times \mathbf{B}^1$ is defined similarly: it is on the set

$$\{000, 001, 010, 100, 011, 101, 110, 111\}$$

of 3-digit binary numbers where $x_1x_2x_3 \leqslant y_1y_2y_3$ if the $\leqslant$ relation is satisfied componentwise on the digits. The Hasse diagrams of $\mathbf{B}^1$, $\mathbf{B}^2$, and $\mathbf{B}^3$ are as follows:



These look familiar and indeed the n-fold product $\mathbf{B}^n$ is isomorphic to the subset lattice $\mathbf{2^n}$ for $n \geqslant 1$. The usual correspondence between subsets and binary numbers provides the isomorphism (Exercise 3).

The Möbius function of a product

The following theorem provides the specifics on how the Möbius function of a product relates to the Möbius function of each poset in the product. (See Exercise 7 for the proof.)

Theorem 8.6.1 *If $\mathbf{P}_1 = (X_1, \leqslant_1)$ and $\mathbf{P}_2 = (X_2, \leqslant_2)$ are posets with Möbius functions μ_1 and μ_2, respectively, then the Möbius function μ of the product $\mathbf{P}_1 \times \mathbf{P}_2$ satisfies*

$$\mu\Big((x_1, x_2), (y_1, y_2)\Big) = \mu_1(x_1, y_1)\,\mu(x_2, y_2)$$

for each $x_1, y_1 \in X_1$ and $x_2, y_2 \in X_2$.

For example, since $\mathbf{B^1}$ is a total order, the Möbius function μ_1 of $\mathbf{B^1}$ is

$$\begin{aligned}\mu_1(0,0) &= 1\\ \mu_1(0,1) &= -1\\ \mu_1(1,1) &= 1.\end{aligned}$$

To find the Möbius function μ_2 of $\mathbf{B}^2 = \mathbf{B}^1 \times \mathbf{B}^1$, we can compute it according to the theorem as

$$\begin{aligned}\mu_2(00,00) &= \mu_1(0,0)\,\mu_1(0,0) = (1)(1) = 1\\ \mu_2(00,01) &= \mu_1(0,0)\,\mu_1(0,1) = (1)(-1) = -1\\ \mu_2(00,10) &= \mu_1(0,1)\,\mu_1(0,0) = (-1)(1) = -1\\ \mu_2(00,11) &= \mu_1(0,1)\,\mu_1(0,1) = (-1)(-1) = 1\end{aligned}$$

and so on.

Question 350 *Finish computing μ_2. Why is it only necessary to find $\mu_2(x_1x_2, y_1y_2)$ when $x_1x_2 \leqslant y_1y_2$?*

Applying the principle of Möbius inversion

We are now ready to look at applications of Möbius inversion. Any such application needs the following two things.

- An underlying poset and its Möbius function.
- Numerical functions $N_=$ and $N_\geqslant$ (or $N_\leqslant$) defined on the poset that perform some sort of counting.

In our first application, we calculate the Möbius function of the subset lattice and then apply Möbius inversion to obtain the inclusion-exclusion formula. In the second, we calculate the Möbius function of the divisibility lattice and then apply Möbius inversion to answer a Pólya-type counting question.

The Möbius function of the subset lattice

For $n \geqslant 1$, we know that the subset lattice $\mathbf{2^n}$ is isomorphic to the poset $\mathbf{B}^n$. Since $\mathbf{B}^n$ is the n-fold product $\mathbf{B}^1 \times \mathbf{B}^1 \times \cdots \times \mathbf{B}^1$, we will use products to compute the Möbius function of $\mathbf{B}^n$.

First let's make an observation about μ_1, the Möbius function of $\mathbf{B}^1$. Since it is a total order, Theorem 8.5.3 tells us that

$$\begin{aligned}\mu_1(0,0) &= 1\\ \mu_1(0,1) &= -1\\ \mu_1(1,1) &= 1\end{aligned}$$

and this can be written in one stroke as $\mu_1(x, y) = (-1)^{y-x}$ whenever $x \leqslant y$ in $\mathbf{B}^1$.

Now let μ_n be the Möbius function of $\mathbf{B}^n$. By Theorem 8.6.1 and our formula for μ_1 we have, whenever $x_1x_2\cdots x_n \leqslant y_1y_2\cdots y_n$,

$$\begin{aligned}\mu_n(x_1x_2\cdots x_n, y_1y_2\cdots y_n) &= \mu_1(x_1, y_1)\,\mu_1(x_2, y_2)\cdots\mu_1(x_n, y_n)\\ &= (-1)^{y_1-x_1}\,(-1)^{y_2-x_2}\cdots(-1)^{y_n-x_n}\\ &= (-1)^{y_1+y_2+\cdots+y_n-(x_1+x_2+\cdots+x_n)}\\ &= (-1)^{\sum y_i-\sum x_i}.\end{aligned}$$

That is, for two n-digit binary numbers $x = x_1x_2\cdots x_n$ and $y = y_1y_2\cdots y_n$ with $x \leqslant y$, we have

$$\mu_n(x, y) = (-1)^{\sum y_i-\sum x_i} = (-1)^{(\#\text{ ones in } y)-(\#\text{ ones in } x)}.$$

Then using the usual correspondence between n-digit binary numbers and subsets of an n-set, we see that

$$\mu_n(I, J) = (-1)^{|J|-|I|} \qquad \text{for } I, J \subseteq [n] \text{ with } I \subseteq J. \tag{8.11}$$

This completes the computation of the Möbius function of the subset lattice $\mathbf{2^n}$.

Application: inclusion-exclusion

We now state the general principle of inclusion-exclusion in a slightly different manner than that of Theorem 3.1.5 on page 92. As stated, it is a direct translation of Theorem 8.5.4 into the language of inclusion-exclusion. Recall that 2^P denotes the power set of P, i.e., the set of all possible subsets of P.

Theorem 8.6.2 (inclusion-exclusion) *Let P be an n-set and consider the subsets of P ordered by containment. If $N_=$ and $N_\geqslant$ are real-valued functions defined on 2^P and are related by the equations*

$$N_\geqslant(I) = \sum_{J:I\subseteq J} N_=(J) \qquad \text{for each } I \in 2^P,$$

then

$$N_{=}(I) = \sum_{J:I\subseteq J} (-1)^{|J|-|I|} N_{\geqslant}(J) \qquad \text{for each } I \in 2^P.$$

The Möbius function of the divisibility lattice

Next we derive a formula for the Möbius function of the divisibility lattice $\mathbf{D_n}$. Actually, it turns out that it suffices to compute the Möbius function of the infinite, but locally finite, poset $\mathbf{D}$ of positive integers ordered by divisibility. This latter function is the so-called number theoretic Möbius function. When used in number theory it is written as a single-variable function $\mu(x)$ rather than as a bivariate function $\mu(x, y)$. The reason for doing so will become clear when we derive the formula. In preparation for this we first use the poset product to make a beautiful connection between divisibility lattices and prime factorization.

Prime factorization and poset products

The prime factorization of any integer n, $n \geqslant 2$, can be written

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

where the p_i are distinct primes and the α_i are positive integers. When $n = 24$ we have $24 = 2^3 \cdot 3^1$ so $t = 2$, $p_1 = 2$, $\alpha_1 = 3$, $p_2 = 3$ and $\alpha_2 = 1$. For each i, the divisibility lattice on the divisors of $p_i^{\alpha_i}$ is a total order. More importantly, the product of those t divisibility lattices is isomorphic to the divisibility lattice of divisors of n.

An illustration appears in Figure 8.8. Since each of 8 and 3 is a power of a single prime, the divisibility lattices $\mathbf{D_8}$ and $\mathbf{D_3}$ are total orders. Their product is shown in the middle of the figure and it is clearly isomorphic to $\mathbf{D_{24}}$ shown on the right. In fact, we can associate each (a, b) in the product with the integer $a \cdot b$ in $\mathbf{D_{24}}$. In that way, $(a, b) \leqslant (c, d)$ in $\mathbf{D_8} \times \mathbf{D_3}$ if and only if $a|c$ and $b|d$. This is equivalent to $ab|cd$ because a and b are relatively prime as are c and d.

In general, the prime factorization carries over to poset products in the following way. If

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

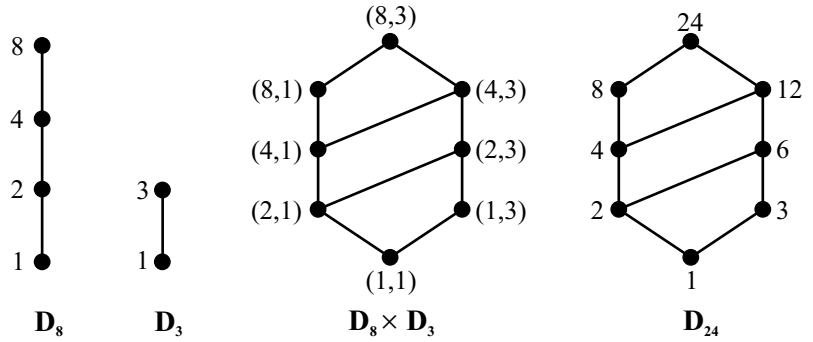


Figure 8.8. The divisibility lattice $\mathbf{D_{24}}$ as a product of $\mathbf{D_8}$ and $\mathbf{D_3}$.

is the prime factorization of n, then the set of divisors of n ordered by divides is isomorphic to the product of the total orders $\mathbf{D}_{\mathbf{p}_i^{\alpha_i}}$. That is,

$$\mathbf{D_n} \cong \mathbf{D}_{\mathbf{p}_1^{\alpha_1}} \times \mathbf{D}_{\mathbf{p}_2^{\alpha_2}} \times \cdots \times \mathbf{D}_{\mathbf{p}_t^{\alpha_t}}. \tag{8.12}$$

Of course this requires proof (Exercise 4). This is a beautiful extension of the Fundamental Theorem of Arithmetic with total orders playing the role of prime powers.

Question 351 *Factor* $\mathbf{D_{60}}$ *into a product of total orders and make an illustration like that of Figure 8.8.*

The number-theoretic Möbius function

The isomorphism shown in (8.12) above allows for easy computation of the Möbius function of $\mathbf{D_n}$ using Theorem 8.6.1. Here is how to find the Möbius function μ_{24} of $\mathbf{D_{24}}$ by using the isomorphism $\mathbf{D_{24}} \cong \mathbf{D_8} \times \mathbf{D_3}$.

Write the ground set of $\mathbf{D_8}$ as $\{2^0, 2^1, 2^2, 2^3\}$ instead of $\{1, 2, 4, 8\}$. Similarly, write the ground set of $\mathbf{D_3}$ as $\{3^0, 3^1\}$. Since each of these posets is a total order, a convenient way to write their Möbius functions is

$$\mu_8(2^i, 2^j) = \begin{cases} (-1)^{j-i} & \text{if } j - i \in \{0, 1\} \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mu_3(3^i, 3^j) = \begin{cases} (-1)^{j-i} & \text{if } j - i \in \{0, 1\} \\ 0 & \text{otherwise,} \end{cases}$$

according to Theorem 8.5.3.

Now we work on μ_{24} using Theorem 8.6.1. If a and b are divisors of 24, and $a|b$, then $a = 2^{i_1}3^{i_2}$ and $b = 2^{j_1}3^{j_2}$. Therefore

$$\begin{aligned} \mu_{24}(a, b) &= \mu_{24}(2^{i_1}3^{i_2}, 2^{j_1}2^{j_2}) \\ &= \mu_8(2^{i_1}, 2^{j_1})\, \mu_3(3^{i_2}, 3^{j_2}) \\ &= (-1)^{j_1-i_1}\, (-1)^{j_2-i_2} \\ &= (-1)^{\sum(j_k-i_k)}, \end{aligned}$$

where the second-to-last equality holds when $j_k - i_k \in \{0, 1\}$ for $k = 1, 2$; otherwise $\mu_{24}(a, b) = 0$. Notice next that the exponents $j_k - i_k$ also arise naturally in the prime factorization of $\frac{b}{a}$, specifically

$$\frac{b}{a} = \frac{2^{j_1}3^{j_2}}{2^{i_1}3^{i_2}} = 2^{j_1-i_1}3^{j_2-i_2}.$$

So, when $a|b$ we have $j_k - i_k \geqslant 0$ for $k = 1, 2$. In view of the fact that

$$\mu_{24}(a, b) = \begin{cases} (-1)^{\sum(j_k-i_k)} & \text{if } j_k - i_k \in \{0, 1\} \text{ for } k = 1, 2 \\ 0 & \text{otherwise,} \end{cases}$$

it follows that $\mu_{24}(a, b)$ just depends on the prime factorization of $\frac{b}{a}$. That is,

$$\mu_{24}(a, b) = \begin{cases} 1 & \text{if } a = b \\ (-1)^k & \text{if } \frac{b}{a} \text{ equals the product of } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

For example, $\mu_{24}(3, 24) = 0$ because $\frac{24}{3} = 8$ is not a product of distinct primes. However, $\mu_{24}(2, 12) = (-1)^2 = 1$ because $\frac{12}{2} = 6 = 2 \cdot 3$ is the product of $k = 2$ distinct primes. Note also that $\mu_{24}(4, 24) = \mu_{24}(1, 6) = 1$.

The ideas we used to find μ_{24} extend not only to the more general case of $\mathbf{D_n}$ but to the locally finite poset $\mathbf{D}$ of positive integers ordered by divisibility. To find $\mu(a, b)$ when $a|b$ in $\mathbf{D}$, it suffices to find the Möbius function of the lattice of divisors of $\frac{b}{a}$. This is because (1) the interval $[a, b]$ in $\mathbf{D}$ is isomorphic to the lattice of divisors of $\frac{b}{a}$, and (2) the Möbius function's values on an interval $[x, y]$ of any locally finite poset depend only on the structure of the subposet defined by that interval. The latter assertion is immediately evident from the inductive method of Definition 8.5.1. For the former, see Exercise 5.

Theorem 8.6.3 *The Möbius function μ of any finite divisibility lattice $\mathbf{D_n}$, and indeed of the infinite poset $\mathbf{D}$ of positive integers ordered by divisibility, is given by*

$$\mu(a, b) = \begin{cases} 1 & \text{if } a = b \\ (-1)^k & \text{if } \frac{b}{a} \text{ is the product of } k \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

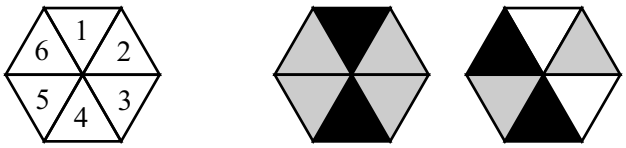
Because $\mu(a, b)$ only depends on the single quantity $\frac{b}{a}$, in number theory it is usually written as a univariate function: $\mu(\frac{b}{a}) := \mu(a, b)$ for all positive integers a, b with $a|b$. Equivalently, $\mu(m) := \mu(1, m)$ for any positive integer m.

Question 352 *Find $\mu(30)$ and $\mu(100)$. Also, if m is a positive integer then what is $\mu(m^2)$?*

Application: counting circular colorings

We next demonstrate how to use Möbius inversion to tackle a Pólya-type problem. On one hand, this approach is less direct than using the techniques of Chapter 5. On the other hand, it demonstrates the flexibility of Möbius inversion.

In how many ways can we color a spinner containing six regions if each region can be colored with one of three colors? An uncolored spinner with its regions labeled appears below at the left, and two possible colorings using black, gray, and white appear at the right.

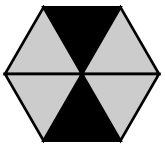


The spinner is free to rotate in the plane so its symmetry group is the cyclic group C_6.

Question 353 *Use the techniques of Chapter 5 to count the spinners. (You should get 130.)*

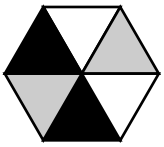
Let's approach this problem in a different way. If the spinner is not allowed to rotate then there are 3^6 possible colorings: each coloring can be specified by a 6-list where each letter is either B, G, or W. The two colorings shown earlier correspond to the lists BGG-BGG and WGWBGB. The question is how to deal with different 6-lists that correspond to equivalent spinner colorings.

Figure 8.9 illustrates some of the issues. The coloring shown at the top of the figure is equivalent to three different 6-lists while the coloring shown at the bottom is equivalent to



Three 6-lists are equivalent to this coloring:

BGGBGG
GGBGGB
GBGGBG



Six 6-lists are equivalent to this coloring:

WGWBGB	BGBWGW
GWBGBW	GBWGWB
WBGBWG	BWGWBG

Figure 8.9. Lists of period 3 and of period 6.

six different 6-lists. We shall say that the 6-lists shown at the top have period 3 while those shown at the bottom have period 6. In general, a list of any length has ***period*** d provided that d is the smallest positive number of rotations required to obtain the original list. A rotation shifts each element of the list to the left one place with wraparound occurring at the ends. (This corresponds to a counterclockwise rotation of the spinner.) A monochromatic coloring such as BBBBBB has period 1. To count the inequivalent spinners, we can just count the inequivalent 6-lists under this notion of equivalence.

The first key observation is that the period of any list must be either 1, 2, 3, or 6; that is, it must be a divisor of 6.

Question 354 *Why can't a 6-list have period 4, for example?*

Let $C(d)$ denote the number of "circular d-lists" with period d. By those we mean lists of length d *and* period d, where two lists are equivalent if one can be obtained from the other via rotations. The answer to our original question is

$$C(1) + C(2) + C(3) + C(6) \quad \text{or} \quad \sum_{d:d|6} C(d).$$

This is because any circular 6-list of period d, where $d|6$, can be created by first specifying a circular d-list of period d and then repeating that list the appropriate number of times to create a 6-list. For example, we know $C(2) = 3$ because the (inequivalent) circular 2-lists of period 2 are BG, BW, and GW. These correspond to the three (inequivalent) circular 6-lists of period 2, namely BGBGBG, BWBWBW, and GWGWGW. In general, for a spinner with n regions where each region can be colored with one of k colors the answer is

$$\sum_{d:d|n} C(d). \tag{8.13}$$

We shall compute $C(d)$ via Möbius inversion. (In our small example $C(1)$, $C(2)$, and $C(3)$ can be computed easily but $C(6)$ is more difficult.) What we need is a way to relate $C(d)$ to a known problem, and here it is:

$$3^6 = \sum_{d:d|6} d \cdot C(d).$$

We give a combinatorial proof. How many 6-lists, where each element is B, G, or W, are possible? One answer is 3^6. For the other answer, consider cases based on the period of

the 6-list when treated as a circular list. If the period is d, where $d|6$, then we select a circular d-list in $C(d)$ ways. There are then d choices for how to use this (circular) d-list to start the (non-circular) 6-list. For example, if $d = 3$ and we choose BWW, then this corresponds to the 6-lists BWWBWW, WWBWWB, and WBWWBW. There are $d \cdot C(d)$ having period d. Summing over all divisors of 6 gives the answer.

In general, the same reasoning applies to a spinner having n regions where each receives one of k colors. We have, for any positive divisor d of n,

$$k^d = \sum_{e:e|d} e \cdot C(e). \tag{8.14}$$

In the context of Theorem 8.5.5, the poset $\mathbf{P}$ is the divisibility lattice $\mathbf{D_n}$ so that the set X is the set of positive divisors of n. The functions $N_=$ and $N_\leqslant$ are

$$N_=(d) := d \cdot C(d)$$
$$N_\leqslant(d) := k^d.$$

According to the theorem the equation (8.14) can be inverted as

$$N_=(d) = \sum_{e:e|d} \mu(e,d)\, N_\leqslant(e) \qquad \text{or} \qquad d \cdot C(d) = \sum_{e:e|d} \mu(e,d)\, k^e.$$

Solving for $C(d)$ gives

$$C(d) = \frac{1}{d} \sum_{e:e|d} \mu(e,d)\, k^e$$

which can be written using the number-theoretic Möbius function as

$$C(d) = \frac{1}{d} \sum_{e:e|d} \mu\left(\frac{d}{e}\right) k^e \qquad \text{for every positive divisor } d \text{ of } n. \tag{8.15}$$

Therefore, in light of sum (8.13) there are

$$\sum_{d:d|n} \frac{1}{d} \sum_{e:e|d} \mu\left(\frac{d}{e}\right) k^e \tag{8.16}$$

different colorings of a spinner with n regions where each can receive one of k colors.

To find the solution to the original question ($n = 6$ and $k = 3$), first compute $C(d)$ for $d = 1, 2, 3, 6$. To get $C(6)$, calculate

$$\begin{aligned} C(6) &= \frac{1}{6} \sum_{e:e|6} \mu\left(\frac{6}{e}\right) 3^e \\ &= \frac{1}{6}\Big(\mu(6)\, 3^1 + \mu(3)\, 3^2 + \mu(2) 3^3 + \mu(1)\, 3^6\Big) \\ &= \frac{1}{6}\Big(1 \cdot 3 + (-1) \cdot 9 + (-1) \cdot 27 + 1 \cdot 729\Big) \\ &= 116. \end{aligned}$$

Question 355 *Use the formula to verify that* $C(1) = 3$, $C(2) = 3$, *and* $C(3) = 8$.

Therefore, there are

$$\sum_{d:d|6} C(d) = 3 + 3 + 8 + 116 = 130$$

different colorings of the spinner.

Two applications to graph theory

To close we briefly mention two applications of Möbius inversion in graph theory. One is a formula for the chromatic polynomial of a graph. It is not a practical formula but has been used to study graph coloring from a different, more general point of view.

The second is a formula for the number of connected labeled graphs on n vertices. In this case the pertinent Möbius function is that of the partitions of $[n]$ ordered by refinement. For such a partition π, let $N_=(\pi)$ equal the number of labeled graphs with vertex set $[n]$ and where the blocks of π correspond exactly to the vertex sets of the connected components of the graph. Let $\hat{1}$ denote the maximum element of the partition lattice, i.e., the partition of $[n]$ into one block. This means that the number of connected labeled graphs on n vertices is $N_=(\hat{1})$.

Defining $N_\leqslant(\hat{1}) = \sum_{\pi:\pi\leqslant\hat{1}} N_=(\pi)$, we have by Möbius inversion

$$N_=(\hat{1}) = \sum_{\pi:\pi\leqslant\hat{1}} \mu(\pi,\hat{1})\, N_\leqslant(\pi).$$

The values $N_\leqslant(\pi)$ are easy to find. For example, note that $N_\leqslant(\hat{1}) = 2^{\binom{n}{2}}$ because this is just the total number of labeled graphs on n vertices.

Question 356 *Suppose π is a partition of $[n]$ that has b_i blocks of size i, for $i = 1, 2, \ldots, n$. Explain why*

$$N_\leqslant(\pi) = \prod_{i=1}^{n} 2^{\binom{i}{2} b_i}.$$

The remainder of the work involves finding the Möbius function $\mu(\pi,\hat{1})$. If the partition π has k blocks, then it can be shown that

$$\mu(\pi,\hat{1}) = (-1)^{k-1}(k-1)!\,,$$

and so the number of connected labeled graphs on n vertices is

$$N_=(\hat{1}) = \sum_{\pi:\pi\leqslant\hat{1}} (-1)^{k-1}(k-1)! \prod_{i=1}^{n} 2^{\binom{i}{2} b_i}, \tag{8.17}$$

where for each partition π in the sum, k is its number of blocks and b_i is the number of blocks of size i. This formula is not terribly practical for computation because the sum is over all possible partitions of $[n]$. For example, when $n = 10$ the number of terms in the sum is the 10th Bell number $B(10) = 115{,}975$. It can be rewritten (Exercise 10) as a sum over all partitions of the *integer* n, which is a smaller number. When $n = 10$, this is the partition number $P(10) = 42$.

Summary

Möbius inversion, though not always the most practical or direct technique, is nonetheless an important piece of theory that unifies several combinatorial ideas that might otherwise appear unrelated. To each situation that it is applied, the technique brings the underlying poset to the fore. For inclusion-exclusion, that poset is the subset lattice; for counting circular lists, it is the divisibility lattice; and for counting connected labeled graphs, it is the partition lattice.

Exercises

1. Let μ be the number-theoretic Möbius function, and suppose k is a positive integer. Calculate $\mu(5^{k+1}-1)$ and $\mu(k^9+k^5+2k^3)$.
2. Prove that the product of two posets is a poset.
3. Let $n \geqslant 1$. Prove that $\mathbf{B}^n \cong \mathbf{2^n}$.
4. If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ is the prime factorization of n, then prove the isomorphism shown in (8.12).
5. Let $\mathbf{D}$ be the infinite poset of positive integers ordered by divisibility. Let a and b be positive integers with $a|b$. Prove that $\mathbf{D}$ restricted to the interval $[a, b]$ is isomorphic to $\mathbf{D}_{\frac{\mathbf{b}}{\mathbf{a}}}$.
6. Let $\mathbf{P} = (X, \leqslant)$ be a poset that has a minimum element $\hat{0}$ and a maximum element $\hat{1}$. Suppose also that there is an element $\hat{x} \in X$, different from $\hat{0}$ and $\hat{1}$, that is comparable to every element. Determine $\mu(\hat{0}, \hat{1})$.
7. Prove Theorem 8.6.1.
8. For any positive integer n, let $\phi(n)$ equal the number of positive integers in $[n]$ that are relatively prime to n. That is, $\phi(n) = \left|\{a \in [n] : \gcd(a, n) = 1\}\right|$. (This is the *Euler phi-function*.) Use Möbius inversion to derive the identity
$$\phi(n) = \sum_{d:d|n} \mu\left(\frac{n}{d}\right) d.$$
9. Use the identity of the previous exercise to prove that the sum shown in (8.16) can also be written as
$$\frac{1}{n} \sum_{d:d|n} \phi\left(\frac{n}{d}\right) k^d.$$
10. Rewrite formula (8.17) so that the sum is over the partitions of the integer n. (Hint: Consider type vectors of the partitions.) Then, use it to compute the number of connected labeled graphs on four vertices and on five vertices.

Travel Notes

We have Gian-Carlo Rota (1932–1999), a professor of mathematics at MIT, to thank for recognizing the importance of Möbius inversion in combinatorics. His 1964 paper, "On the foundations of combinatorial theory, I. Theory of Möbius functions," was recognized in 1988 by the American Mathematical Society's Leroy P. Steele prize for Seminal Contribution to Research. That paper, the prize's citation says, is "the single paper most responsible for the revolution that incorporated combinatorics into the mainstream of modern mathematics." Rota went on to write nine more "foundations" papers that continue to influence combinatorial research.

Bibliography

General references for combinatorics and graph theory

Bogart, K. P. (1990). *Introductory Combinatorics*, Harcourt Brace Jovanovich (Academic Press), San Diego.

Brualdi, R. A. (2004). *Introductory Combinatorics*, Prentice Hall, Upper Saddle River, NJ.

Chartrand, G. and Zhang, P. (2005). *Introduction to Graph Theory*, McGraw-Hill, Boston.

Erickson, M. J. (1996). *Introduction to Combinatorics*, John Wiley & Sons, New York.

Hall, M. J. (1986). *Combinatorial Theory*, John Wiley & Sons, New York.

van Lint, J. H. and Wilson, R. M. (1992). *A Course in Combinatorics*, Cambridge University Press, Cambridge, England.

Roberts, F. S. and Tesman, B. (2004). *Applied Combinatorics*, Pearson Prentice Hall, Upper Saddle River, NJ.

Stanley, R. P. (1986). *Enumerative Combinatorics: Volume I*, Wadsworth Brooks/Cole, Monterey, CA.

Tucker, A. (2006). *Applied Combinatorics*, John Wiley & Sons, New York.

West, D. B. (2001). *Introduction to Graph Theory*, Prentice Hall, Upper Saddle River, NJ.

Other references

Anderson, I. (2002). *Combinatorics of Finite Sets*, Dover Publications, Mineola, NY.

Andrews, G. E. and Eriksson, K. (2004). *Integer Partitions*, Cambridge University Press, Cambridge.

Appel, K. and Haken, W. (1977). "Every planar map is four-colorable," *Illinois Journal of Mathematics*, **21**, 429–567.

Benjamin, A. T. and Quinn, J. (2003). *Proofs that Really Count: The Art of Combinatorial Proof*, Dolciani Mathematical Expositions **27**, Mathematical Association of America.

Bhattacharya, K. N. (1944). "A new balanced incomplete block design," *Science and Culture*, **9**, 508.

Birkhoff, G. D. and Lewis, D. C. (1946). "Chromatic polynomials," *Transactions of the American Mathematical Society*, **60**, 355–451.

Brigham, R. C., Caron, R. M., Chinn, P. Z., and Grimaldi, R. P. (1996). "A tiling scheme for Fibonacci numbers," *Journal of Recreational Mathematics*, **28**, 10–17.

Cayley, A. (1889). "A theorem on trees," *Quarterly Journal of Pure and Applied Mathematics*, **23**, 376–378.

Cormen, T. H., Leiserson, C. E., and Rivest, R. L. (1990). *Introduction to Algorithms*, The MIT Press, Cambridge, MA.

Dilworth, R. P. (1950). "A decomposition theorem for partially ordered sets," *Annals of Mathematics*, **2**, 161–166.

Dunham, W. (1999). *Euler: The Master of Us All*, Dolciani Mathematical Expositions **22**, The Mathematical Association of America.

Dushnik, B. and Miller, E. W. (1941). "Partially ordered sets," *American Journal of Mathematics*, **63**, 600–610.

Erdős, P. and Szekeres, G. (1935). "A combinatorial problem in geometry," *Compositio Mathematica*, **2**, 463–470.

Fisher, R. A. (1940). An examination of the different possible solutions of a problem in incomplete blocks. *Annals of Eugenics*, **10**, 52–75.

Golay, M. J. E. (1949). "Notes on digital coding," *Proceedings of the IEEE*, **37**, 657.

Graham, R. L. , Rothschild, B. L., and Spencer, J. H. (1980). *Ramsey Theory*, John Wiley & Sons, New York.

Katz, V. J. (1996). "Combinatorics and induction in medieval Hebrew and Islamic mathematics," in *Vita Mathematica: Historical Research and Integration with Teaching* (R. Calinger, ed.), MAA Notes **40**, Mathematical Association of America.

Kirkman, T. (1847). "On a problem in combinations," *Cambridge and Dublin Mathematical Journal*, **2**, 191–204.

Lam, C. (1991). "The search for a finite projective plane of order 10," *American Mathematical Monthly*, **98**, 305–318.

Lubell, D. (1966). "A short proof of Sperner's lemma," *Journal of Combinatorial Theory*, **1**, 299.

MacWilliams, F. J. and Sloane, N. J. A. (1978). *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam.

McKay, B. D. and Radziszowski, S. P. (1995). $R(4, 5) = 25$," *Journal of Graph Theory*, **19**, 309–322.

Mirsky, L. (1971). "A dual of Dilworth's decomposition theorem," *American Mathematical Monthly*, **78**, 876–877.

Moon, J. W. (1967). "Various proofs of Cayley's formula for counting trees," in *A Seminar on Graph Theory* (F. Harary and L. W. Beineke, eds.), Holt, Rinehart & Winston, New York.

Neumann, P. M. (1979). "A lemma that is not Burnside's," *The Mathematical Scientist*, **4**, 133–141.

Niven, I. (1969). "Formal power series," *The American Mathematical Monthly*, **76**, 871-889.

Petkovšek, M., Wilf, H. S., and Zeilberger, D. (1996). $A = B$, A K Peters, Ltd., Wellesley, MA.

Pless, V. (1968). "On the uniqueness of the Golay codes," *Journal of Combinatorial Theory*, **5**, 215–228.

Pless, V. (1982) *Introduction to the Theory of Error-Correcting Codes*, John Wiley & Sons, New York.

Pólya, G. (1937). "Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemische Verbindungen," *Acta Mathematica*, **68**, 145–254.

Pólya, G. (1956). "On picture-writing," *American Mathematical Monthly*, **63**, 689–697.

Pólya, G. and Read, R. C. (1987). *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*, Springer-Verlag, New York.

Prüfer, H. (1918). "Neuer Beweis eines Satzes über Permutationen," *Archiv der Math. und Phys.*, **27**, 142–144.

Radziszowski, S. P. (1994). "Small Ramsey numbers," *The Electronic Journal of Combinatorics*, **1**. [*Dynamic Survey DS1* Revision #11: August 1, 2006]

Redfield, J. H. (1927). "The theory of group-reduced distributions," *American Journal of Mathematics*, **49**, 433–455.

Robertson, N., Sanders, D. P., Seymour, P. D., and Thomas, R. (1996). "A new proof of the four-color theorem," *Electronic Research Announcements of the American Mathematical Society*, **2**, 17–25.

Rota, G.-C. (1964). "On the foundations of combinatorial theory I. Theory of Möbius functions," *Zeitschrift fur Wahrscheinlichkeitstheorie*, **2**, 340–368.

Thompson, T. M. (1983). *From Error-Correcting Codes through Sphere Packings to Simple Groups*, The Carus Mathematical Monographs **21**, Mathematical Association of America.

Tietavainen, A. (1973). "On the nonexistence of perfect codes over finite fields," *SIAM Journal on Applied Mathematics*, **24**, 88–96.

Trotter, W. T. (1992). *Combinatorics and Partially Ordered Sets: Dimension Theory*, The Johns Hopkins University Press, Baltimore.

Hints and Answers to Selected Exercises

For selected Exercises in the text, either the final answer or a hint is given. In the case of final answers, they are left in terms of standard notation (e.g., $\binom{5}{2}$ rather than 10) and are given to help you check your work. Of course in most cases a final answer alone is not sufficient—you will want to explain it. Hints are given to help you through proofs or more involved problems, or to suggest how a special case might lead to the solution of the original problem. Use them only if you get stuck!

Section 1.1

1. (a) $\left(\!\binom{16}{6}\!\right)$
   (b) $\binom{25}{5}$
   (c) $(18)_4$
   The lottery with the fewest number of possible tickets offers the best chance of winning—which one is it?
2. (a) 2^{16}
   (b) $\binom{20}{10}$
3. (a) 3^n
   (b) 8^n
   (c) 16^n
5. $\left(\!\binom{4}{15}\!\right)$
7. There are n^4 passwords. Then solve $n^4 \geqslant 10^9$ to find n.
9. (a) 2^{10}
   (b) 2^{10}
   (c) $\binom{17}{10}$
11. $\left(\!\binom{6}{5}\!\right)$; $\binom{6}{5}$
13. Hint: Once you know which six numbers are in the permutation, how many ways are there to put them in increasing order?
15. $\left(\!\binom{5}{16-5}\!\right) = \left(\!\binom{5}{11}\!\right)$ is the answer to the first question.
17. Hint: Each solution corresponds to a 10-multiset taken from [3].
18. $\binom{8}{5}$
19. Hint: Any rectangle is uniquely specified by the two horizontal and two vertical grid lines that enclose it.

Section 1.2

1. (a) How many k-lists taken from $[n]$ have at least one repeated element?
   (c) How many n-digit binary numbers contain at least one 0 and at least one 1?
   (d) How many 5-digit ternary numbers (each digit is 0, 1, or 2) cannot also be considered 5-digit binary numbers?

3. One answer is $\sum_{k=3}^{20} \binom{20}{k}$ but it involves a sum of 18 terms. Find an answer that is easier to compute by hand.

5. Hint: Extend the example given in the text by first defining D to be the set of 8-character passwords that have no digits present.

7. $\left(\!\binom{n}{k}\!\right) - \binom{n}{k}$

9. Hint: The product of the elements is even exactly when the subset contains at least one even element.

11. Count the complement: $26^5 - 5 \cdot 26^3 \cdot 5$. (Assume that A, E, I, O, U are the only vowels.)

15. Hint: Start by answering the same question but for the integers from 1 to 100. Then see how this answer helps you answer the same question but for the integers from 1 to 1000. Then continue the pattern.

16. The answer to the first question is $4 \cdot (5)_3$.

17. Hint: Break into cases depending on the value of x_4.

18. (a) 4
    (c) $13 \cdot 48$
    (d) $13 \cdot \binom{4}{3} \cdot 12 \cdot \binom{4}{2}$
    (f) $10 \cdot 4^5 - 4 - 36$
    (h) $\binom{13}{2}\binom{4}{2}\binom{4}{2} \cdot 44$

Section 1.3

1. The answer to the first question is $\sum_{i=1}^{n-1} i$, but can you write it in closed (non-summation) form?

3. 10^7 because there are 10 choices for $f(1)$, then 10 choices for $f(2)$, and so on, up to 10 choices for $f(7)$.

5. Hint: Let f be the function that takes as its input a subset of $[n]$ and outputs an n-digit binary number that has 1s in the positions that correspond to the elements of the subset. Prove that this f is a bijection.

8. Hint: First explain why f^{-1} is a function and why its domain is B. For the one-to-one proof, assume $b_1, b_2 \in B$ and that $f^{-1}(b_1) = f^{-1}(b_2)$. Apply f to both sides and what happens?

9. Assume S_1 and S_2 are k-subsets of $[n]$, and that $h(S_1) = h(S_2)$. This means $S_1^c = S_2^c$ which implies $(S_1^c)^c = (S_2^c)^c$ or $S_1 = S_2$. Perhaps this proof is easier?

12. It is a bijection when n is odd. Why is it not a bijection when n is even?

Section 1.4

1. Each equivalence class contains eight permutations and there are three equivalence classes. One class contains the permutations 1234, 1243, 2134, 2143, 3412, 3421, 4312, 4321.
3. $\mathcal{E}^{-1} = \mathcal{E}$. To prove it, first prove $\mathcal{E}^{-1} \subseteq \mathcal{E}$ and then prove $\mathcal{E} \subseteq \mathcal{E}^{-1}$.
5. In the blank should be "it is the identity relation on A."
8. $\frac{10 \cdot 5 \cdot 4! \cdot 4!}{10} = 5 \cdot 4! \cdot 4!$
9. $\frac{10!}{10 \cdot 2}$
11. The answer to the second question is $\binom{n}{2}$. Why?
13. For the equivalence relation, consider two permutations of $[n]$ equivalent provided that the first k entries of each permutation are identical.
15. First do a complete enumeration of the $n = 4$ case if it helps.

Section 1.5

1. 6
3. Hint: Pair off the elements of $[2n]$ as $(1, 2n)$, $(2, 2n-1)$, $(3, 2n-2)$, and so on. Do you see how to use the pigeonhole principle where these pairs are the pigeonholes?
6. (a) Hint: Examine the parity (even/odd) of the two coordinates in each pair.
7. Hint: When $n = 3$, such a sequence is $3, 2, 1, 6, 5, 4, 9, 8, 7$.
9. Hint: Adapt the proof of Theorem 1.5.4.

Section 2.1

1. (a) How many permutations of $[n]$ are not in increasing order from left to right?
   (b) How many 4-lists taken from [20] have at least one repeated element?
   (c) Hint: See Combinatorial Proof #1 of this section.
2. $(15)_6 \cdot \binom{9}{4}$, or $\binom{15}{4} \cdot (11)_6$
4. (a) $9^7 - 9^6$
   (b) $8 \cdot (8)_6$
   (c) 4^7
6. (a) $5^5 - 4^5$
   (b) $(n-1)^n$
7. Hint: Use/extend the work in the "Counting onto functions" subsection.
12. This establishes that in order to count functions $[k] \longrightarrow [n]$, it is equivalent to count k-lists taken from $[n]$.
13. If F is the set of one-to-one functions $[k] \longrightarrow [n]$, then L is the set of k-permutations of $[n]$.
16. (a) Hint: Initially there are n ways to specify the location of customer 1, namely at the front of one of the n lines. Then there are $n+1$ ways to specify the location of customer 2: before customer 1 in line, after customer 1 in line, or at the front of one of the remaining $n-1$ lines. Continue.

Section 2.2

1. (a) How many n-digit binary numbers have at most two 1s?
   (b) How many ways are there to select a 5-person committee from a group of 10 people?
2. Hint: Given a group of 20 people, in how many ways can we form an 8-person committee, a 5-person subcommittee of that committee, and a 3-person task force of that subcommittee?
4. (a) Hint: How many n-digit ternary numbers are there? For Answer 2, condition on the number of 2s
   (e) Hint: From a store that sells n donut varieties, in how many ways can we order k donuts such that we order at least one variety of each type?
   (f) Hint: Count k-multisets from $[n]$. Condition on the largest element appearing in the multiset.
6. Hint: Use a similar proof to that of the binomial theorem, but instead count passwords with no repeated characters.
7. (a) $\left(\!\binom{4}{1}\!\right)$ or just 4
   (b) $\left(\!\binom{2}{8}\!\right)$
   (c) $\left(\!\binom{20}{401-20}\!\right) = \left(\!\binom{20}{381}\!\right)$
   (d) $\left(\!\binom{4}{12-1-1-2-2}\!\right) = \left(\!\binom{4}{6}\!\right)$
8. Hint: Any term is of the form $a^i b^j c^k$ where i, j, k are nonnegative integers. What must $i + j + k$ equal?
11. Hint: First count the ways to specify an unordered collection of k integers taken from $[n]$.
13. Hint: Solve a linear system. At some point you will want to look up "Vandermonde matrix" in a linear algebra book if you haven't encountered it before.

Section 2.3

1. $S(20, 3) = 580{,}606{,}446$ and $S(20, 1) + S(20, 2) + S(20, 3) = 581{,}130{,}734$
3. $S(8, 5) \cdot 5! = 126{,}000$
5. Hint: First specify the "missed" element, then specify an onto function involving the remaining elements.
7. Hint: Look at Section 1.4.
9. Hint: Any partition of $[n]$ into $n - 1$ blocks contains exactly one block of size 2 and the remaining blocks have size 1. Let f be the function that takes such a partition as its input and then outputs the block of size 2. Prove that this f is a bijection.
11. Hint: For Answer 2, condition on the number of elements that are not in the block containing n.
12. Hint: Apply Theorem 2.3.1 twice.
14. Hint: Trace what the program does on an example, say $S(7, 4)$. Use Stirling's triangle of the second kind to visualize.
18. (b) $\sum_{i=1}^{n} \beta(k, i)$
   (c) Hint: Use Exercise 16 of Section 2.1 and the equivalence principle.

Section 2.4

1. (a) $S(40, 10) \cdot 10!$
   (b) $\left(\!\binom{10}{40}\!\right)$
   (c) $\sum_{i=1}^{10} S(40, i)$
   (d) $P(40, 10)$
   (e) $(40)_{10}$
   (f) $\binom{40}{4} \cdot 9^{36}$

5. $P(n, n-2) = 2$ when $n \geqslant 4$, and $P(n, n-2) = 1$ when $n = 3$.

6. Apply Theorem 2.4.1 once to get $P(n, 2) = P(n-1, 1) + P(n-2, 2) = 1 + P(n-2, 2)$. Apply it again to $P(n-2, 2)$ and continue.

8. Hint: Given a partition of n, add 1 to each existing part and then append enough parts of size 1 to bring the total number of parts to n. For example, the partition $5 + 1 + 1$ of 7 turns into $6 + 2 + 2 + 1 + 1 + 1 + 1$. Prove that this function is a bijection.

11. How many partitions of n don't have any parts of size 1?

12. Hint: Instead prove the equivalent inequality $P(n+2) - P(n+1) \geqslant P(n+1) - P(n)$.

Section 3.1

1. The answer to the first question is 2666.

2. Hint: $\left\lfloor \frac{100}{4 \cdot 6} \right\rfloor$ does not equal the number of integers in [100] that are divisible by both 4 and 6.

4. (a) Hint: Define P_1 to be the property that the hand has no spades, P_2 the property that it has no clubs, etc. The answer is $\binom{52}{13} - \binom{4}{1}\binom{39}{13} + \binom{4}{2}\binom{26}{13} - \binom{4}{3}\binom{13}{13}$.
   (b) Hint: The number of hands void in spades is $N_=(P_1)$.

5. (a) $\sum_{j=0}^{6} \binom{6}{j}(-1)^j (6-j)!\,(6-j)!$

6. $D_n = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}$

7. (b) Use the alternating series remainder term theorem from calculus.

8. Let P_i be the property that recipient i receives six or more objects. The answer is $N_=(\emptyset)$ which is $\left(\!\binom{10}{20}\!\right) - \binom{10}{1}\left(\!\binom{10}{14}\!\right) + \binom{10}{2}\left(\!\binom{10}{8}\!\right) - \binom{10}{3}\left(\!\binom{10}{2}\!\right)$.

14. Hint: How many 0-subsets of $[n]$ are possible? Let p_i be the property that element i is in the subset, for $i \in [n]$.

17. Hint: There are $\binom{16}{10}$ paths from A to B.

Section 3.2

1. (a) Inductive step: Assume k is an integer, $k \geqslant 0$, and that $3^k - 1$ is divisible by 2. Then $3^{k+1} - 1 = 3(3^k) - 1 = 3(3^k) - 3 + 2 = 3(3^k - 1) + 2$. Each term is divisible by 2, so $3^{k+1} - 1$ is divisible by 2.

5. The formula is $(-1)^n \frac{n(n+1)}{2}$.

6. The formula is $\frac{n(n+1)(n+2)}{6}$.

9. (a) Hint: Start induction at $n = 3$. Adapt the proof given in the text.
   (b) Hint: Try proving $L_n \leqslant b^n$ and derive the smallest value of b that you can use in proving the inductive step. At some point you should solve $b + 1 = b^2$.

12. This is the Fundamental Theorem of Arithmetic!

Section 3.3

1. $\dfrac{1}{(1-x^2)(1-x^3)(1-x^6)(1-x^7)(1-x^8)}$

2. (a) coefficient of x^{14} in $(x + x^2)^{10}$
   (c) coefficient of x^{75} in $\dfrac{1}{(1-x^3)(1-x^5)(1-x^{10})(1-x^{12})}$
   (e) coefficient of x^{15} in $(1 + x + x^2 + \cdots + x^8)^3$

3. (a) $\left(\!\binom{23}{60}\!\right)$
   (c) $\left(\!\binom{8}{2}\!\right)$
   (d) $\left(\!\binom{3}{23}\!\right)$

6. Find the coefficient of x^{15} in $\dfrac{(1+x)^5}{(1-x)^3}$, which is $\sum_{k=0}^{5} \binom{5}{k} \left(\!\binom{3}{15-k}\!\right)$.

9. (a) Writing $\dfrac{1}{(1-x)(1-2x)} = \dfrac{A}{1-x} + \dfrac{B}{1-2x}$ gives $A = -1$ and $B = 2$. The coefficient of x^k is $2^{k+1} - 1$.

Section 3.4

1. Hint: Find the coefficient of x^{12} in $(x + x^2 + x^3 + x^4)^6$. Final answer is $\left(\!\binom{6}{6}\!\right) - \binom{6}{1}\left(\!\binom{6}{2}\!\right)$.

3. $\sum_{j=0}^{k} \binom{n}{j} \left(\!\binom{m}{k-j}\!\right)$

5. $\frac{a}{b}\left(-\frac{c}{b}\right)^k$

8. The coefficient of $\frac{x^n}{n!}$ in e^{3x} is 3^n, which equals the number of n-letter passwords using the letters A, B, C.

9. $c_n = 2^n - 2$

Section 3.5

1. (a) $a_n = 2^n - 1$, for $n \geqslant 0$
   (c) $c_n = (n+1)3^n$, for $n \geqslant 0$
   (d) $d_n = (n+1)2^n$, for $n \geqslant 0$
2. $a_n = (2-n)n!$
5. (a) $g_1 = 1$, $g_2 = 2$, and $g_5 = 10$

Section 3.6

1. $a_{30} = -257{,}363{,}915{,}118{,}311$
2. (a) $a_n = 4(2^n) - 1$, for $n \geqslant 0$
   (c) Hint: $r_1, r_2 = 1 \pm i$.
6. Your final answer should be $t_n = \frac{1}{2\sqrt{3}}\left(1+\sqrt{3}\right)^{n+1} - \frac{1}{2\sqrt{3}}\left(1-\sqrt{3}\right)^{n+1}$, for $n \geqslant 0$.

Section 4.1

1. (a) $\binom{16}{10,4,2}$
   (b) Hint: First specify a 12-digit sequence having 10 W's and 2 T's. Then specify a way to insert the four L's so that none of them are adjacent.
3. $\binom{120}{105}\dfrac{105!}{(2!)^{42}\cdot 42!\cdot (3!)^7\cdot 7!}$
5. $\binom{31}{12,9,10}$
8. Question: From a group of n people, how many ways are there to create an m-person committee and then create a task force of any size from the remaining $n-m$ people?
10. Combinatorial: Let $n \geqslant 2$. Given n people, in how many ways can we select a nonempty committee of any size and also designate one person as the chair and one person as the vice-chair? Non-combinatorial: Take two derivatives of $(1+x)^n$.
11. Your conjecture should be that the sum equals 4^n.
13. It equals $\binom{1/2}{n}(-8)^n$, but simplify it using the technique shown in this section.
15. The recurrence is $a_1 = 1$ and $a_n = \sum_{k=1}^{n-1} a_k a_{n-k}$ for $n \geqslant 2$.

Section 4.2

2. One formula is $F_{2n+1} = \sum_{k=0}^{n} F_{2k}$, and there is another one for F_{2n}.
3. Hint: You can write the error in terms of a Fibonacci number.
4. Hint: Prove by induction on n.
6. (a) Verify the base case for $n = 2$ and $n = 3$. Now assume n is an integer, $n \geqslant 3$, and that it's true for all k satisfying $2 \leqslant k \leqslant n$. We need to prove $3F_{n+1} = F_{n+3} - F_{n-1}$. By the Fibonacci recurrence $3F_{n+1} = 3(F_n + F_{n-1}) = 3F_n + 3F_{n-1}$. Apply the inductive hypothesis to each term and simplify.
11. Hint: Condition on whether the bracelet is open or closed.

Section 4.3

2. $3x^4 - 30x^3 + 69x^2 - 38x - 17$

4. (a) In any permutation of $[n]$ having $n-1$ cycles, there will be one 2-cycle and the remaining cycles are 1-cycles. There are $\binom{n}{2}$ ways to specify a 2-cycle, so $c(n, n-1) = \binom{n}{2}$.

   (b) A permutation of $[n]$ having only one cycle is equivalent to a circular seating of n people around a table, as we studied in Section 1.4. There are $\frac{n!}{n} = (n-1)!$.

5. Use separation of variables: $\frac{dy}{y} = f(x)\,dx$. Integrate both sides to obtain $\ln y = F(x) + C$ where F is an antiderivative of f. Solving for y gives $y = e^{F(x)+C}$.

8. Hint: Use the binomial theorem first on $(1+x)^n$, then substitute

$$x^k = \sum_{j=0}^{k} S(k, j)(x)_j$$

   and switch the order of summation.

11. Hint: The answer is $B(n-1)$.

12. $x^4 = \binom{x}{1} + 14\binom{x}{2} + 36\binom{x}{3} + 24\binom{x}{4}$

13. $\Delta(f(n) + g(n)) = f(n+1) + g(n+1) - (f(n) + g(n)) = (f(n+1) - f(n)) + (g(n+1) - g(n)) = \Delta f(n) + \Delta g(n)$

Section 4.4

1. There are k parts of size 2 and the rest (if any) are parts of size 1.

2. The idea is that $z_i - z_{i+1}$ equals the number of parts of size i in the conjugate, for $i = 1, 2, \ldots, k$. (Define $z_{k+1} := 0$.)

4. The solution is $A = C = \frac{1}{4}$ and $B = \frac{1}{2}$. Therefore $P(n, \text{at most two parts})$ equals the coefficient of x^n in $\frac{1/4}{1-x} + \frac{1/2}{(1-x)^2} + \frac{1/4}{1+x}$. From this you should get

$$P(n, \text{at most two parts}) = \frac{2n + 3 + (-1)^n}{4}.$$

   Then use $P(n, 2) = P(n-2, \text{at most two parts})$.

7. (a) Since $\lim_{n\to\infty} \frac{f(n)}{f(n)} = 1$ it follows that $f \sim f$. Also, if $f \sim g$ then

$$\lim_{n\to\infty} \frac{g(n)}{f(n)} = \lim_{n\to\infty} \frac{1}{\frac{f(n)}{g(n)}} = \frac{\lim_{n\to\infty} 1}{\lim_{n\to\infty} \frac{f(n)}{g(n)}} = \frac{1}{1} = 1,$$

   and so $g \sim f$. Now prove the transitive property.

9. (b) Hint: Prove by induction.

Section 5.2

1. four
3. (a) $\pi^{-1} = (1\ 5\ 3)(2)(4\ 6)$ and $\tau^{-1} = (1\ 2\ 3\ 4\ 5\ 6)$
   (b) $\pi \circ \tau = (1\ 4\ 5\ 6)(2\ 3)$ and $\tau \circ \pi = (1\ 2)(3\ 4\ 5\ 6)$
   (c) $\pi^{-1} \circ (\tau \circ \pi^2) = (1\ 6\ 3\ 4)(2\ 5)$
   (d) $\pi^{-2} = (1\ 3\ 5)(2)(4)(6)$ and $\tau^{-3} = (1\ 4)(2\ 5)(3\ 6)$
4. Hint: Not every element of $(\mathbb{R}, \cdot)$ has an inverse.
5. **Left-cancellation:** Assume $a, b, c \in G$ and $a * b = a * c$. Left-multiply by a^{-1} to get $a^{-1} * (a * b) = a^{-1} * (a * c)$. Use associativity to write $(a^{-1} * a) * b = (a^{-1} * a) * c$ which implies $e * b = e * c$, so $b = c$.
6. Hint: Prove by contradiction.
7. Hint: Revisit the proof of Theorem 5.2.4.
9. The symmetry group is the dihedral group D_4.

motion	product of disjoint cycles
I	(1)(2)(3)(4)(5)(6)(7)(8)(9)
R_1	(1 3 9 7)(2 6 8 4)(5)
R_2	(1 9)(2 8)(3 7)(4 6)(5)
R_3	(1 7 9 3)(2 4 8 6)(5)
F_1	(1)(2 4)(3 7)(5)(6 8)(9)
F_2	(1 3)(2)(4 6)(5)(7 9)(8)
F_3	(1 9)(2 6)(3)(4 8)(5)(7)
F_4	(1 7)(2 8)(3 9)(4)(5)(6)

15. (a) **One-to-one:** Assume $h_1a, h_2a \in Ha$. Then $f(h_1a) = f(h_2a)$ implies $h_1b = h_2b$, and right-cancellation implies $h_1 = h_2$. Right-multiplying by a shows $h_1a = h_2a$.

Section 5.3

1. (b) only the identity permutation
2. $\frac{1}{8}\left(k^9 + 4k^6 + k^5 + 2k^3\right)$
3. (b) Let a be the edge between 1 and 2, b the edge between 2 and 3, etc.

motion π	product of disjoint cycles	$\lvert\text{fix}_{D_4}(\pi)\rvert$
I	$(1)(2)(3)(4)(a)(b)(c)(d)$	2^9
R_1	$(1\ 2\ 3\ 4)(a\ b\ c\ d)$	2^2
R_2	$(1\ 3)(2\ 4)(a\ c)(b\ d)$	2^4
R_3	$(1\ 4\ 3\ 2)(a\ d\ c\ b)$	2^2
F_1	$(1)(2\ 4)(3)(a\ d)(b\ c)$	2^5
F_2	$(1\ 3)(2)(4)(a\ b)(c\ d)$	2^5
$F_{1,2}$	$(1\ 2)(3\ 4)(a)(b\ d)(c)$	2^5
$F_{2,3}$	$(1\ 4)(2\ 3)(a\ c)(b)(d)$	2^5

Answer: $\frac{1}{8}\left(2^9 + 4(2^5) + 2^4 + 2(2^2)\right) = 83$

5. (a) the cyclic group C_5
   (b) 5!
   (d) $\frac{1}{5}(5! + 0 + 0 + 0 + 0) = \frac{5!}{5}$, as we obtained in Section 1.4.
6. The symmetry group has size 2. The answer is $\frac{1}{2}(2^8 + 2^4) = 136$.

Section 5.4

1. Now the symmetry group only has size 2 and consists of the identity and one of the flip operations. The answer is $\frac{1}{2}(k^5 + k^3)$.
3. The answer to the first question is $\frac{1}{14}(2^7 + 7 \cdot 2^4 + 6 \cdot 2^1) = 18$. The answer to the second is $\frac{1}{14}\left(\binom{7}{3} + 6 \cdot 0 + 7 \cdot 3\right) = 4$.
7. The symmetry group is C_3. The answer is $\frac{1}{3}(3^{10} + 2 \cdot 3^4) = 19{,}737$.
9. The symmetry group is D_3. The answer is $\frac{1}{6}(4^6 3^6 + 2 \cdot 4^2 3^2 + 3 \cdot 4^4 3^4) = 508{,}080$.
11. For the 4×4 grid the answer is $\frac{1}{4}(2^{16} + 2^8 + 2 \cdot 2^4) = 16{,}456$.
13. One orbit contains 00000 and 11111. Another contains 00001, 00010, 00100, 01000, 10000, 11110, 11101, 11011, 10111, and 01111. A third contains 00011, 00110, 01100, 11000, 10001, 11100, 11001, 10011, 00111, and 01110. The fourth contains 00101, 01010, 10100, 01001, 10010, 11010, 10101, 01011, 10110, 01101.

Section 5.6

1. For S_3 it's $\frac{1}{6}(z_1^3 + 3z_1z_2 + 2z_3)$.
2. For C_4 it's $\frac{1}{4}(z_1^4 + z_2^2 + 2z_4)$.
3. $\frac{1}{p}(z_1^p + (p-1)z_p)$
6. The cycle index is $\frac{1}{14}(z_1^7 + 6z_7 + 7z_1z_2^3)$. Substitute $z_1 \longleftarrow a + b + c + d$, $z_2 \longleftarrow a^2 + b^2 + c^2 + d^2$, etc. into the cycle index. The terms we are interested in are $48ab^2c^2d^2 + 48a^2bc^2d^2 + 48a^2b^2cd^2 + 48a^2b^2c^2d$. The answer is $4 \cdot 48 = 192$.
9. The cycle index is $\frac{1}{3}(z_1^{10} + 2z_1z_3^3)$. Substitute $z_1 \longleftarrow r + g + w$ and $z_3 \longleftarrow r^3 + g^3 + w^3$ and expand. Add the coefficients on terms of the form $g^i w^j$ or $rg^i w^j$. The answer is 2064.

Section 6.1

1. $\binom{\binom{n}{2}}{m}$
3. Hint: Try a proof by contradiction.
5. It is not isomorphic to $K_{3,3}$. Why?
7. Hint: Consider a longest path in G.
9. (a) $e(Q_k) = k2^{k-1}$
10. (a) Hint: Count edges in K_n. For Answer 2, partition the vertices into a k-set and an $(n-k)$-set, then count edges within the k-set, between the k-set and the $(n-k)$-set, and within the $(n-k)$-set.

11. We proved this in Section 1.5.
12. (a) $B_{5,5}^{8} = 1235$
    (c) 36
15. Hint: A is the adjacency matrix of K_n, so count i-j walks in K_n.

Section 6.2

1. Hint: Each component of a forest is a tree, so use the tree-edge formula on each component.
2. Hint: One way to prove it involves deleting a vertex of degree Δ and analyzing what's left.
4. Hint: Split the spanning trees into two types, those containing e and those not containing e.
5. (a) $\tau(C_5) = 5$
   (b) $\tau(K_4) = 16$
   (c) Hint: $\tau(K_n - e) = \tau(K_n) - \tau(K_n \cdot e)$.
6. For K_4, the matrix M is $\begin{pmatrix} 3 & -1 & -1 & -1 \\ -1 & 3 & -1 & -1 \\ -1 & -1 & 3 & -1 \\ -1 & -1 & -1 & 3 \end{pmatrix}$ and its $(1,1)$ cofactor is
$$\det \begin{pmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{pmatrix} = 16.$$
8. (b) Hint: The sum you want is $\sum_{k=1}^{n-1} L(n,k)$.

Section 6.3

1. $\chi(T)$ is almost always 2. When is it not 2?
3. Hint: Get a palette of $\delta + 1$ colors and just start coloring one vertex at a time. Why will you never run into trouble?
5. The Petersen graph has $\chi = 3$ but the Grötsch graph has $\chi > 3$.
7. $\chi(G) = 4$, $e(G) = 9$, and $n(G) = 6$
9. (a) $p(K_{1,n}, k) = k(k-1)^{n-1}$
   (b) $p(K_{2,n}, k) = k(k-1)^{n-2} + k(k-1)(k-2)^{n-2}$ (Hint: Any proper k-coloring either has the vertices in the 2-vertex partite set colored the same or colored differently.)
   (c) Hint: $p(C_3 \cup P_4 \cup K_5, k) = p(C_3, k) \cdot p(P_4, k) \cdot p(K_5, k)$.
11. Hint: $p(K_n - e, k) = p(K_n, k) + p(K_n \cdot e, k)$.
13. Hint: $p(K_n, k) = (k)_n$.
15. Use induction and a similar approach to the proof of properties CP1-CP3 given in the section.

Section 6.4

1. (a) true
   (d) false
2. Hint: Generalize the argument used in the section to prove that $9 \to (3, 4)$.
4. Hint: Follow the approach suggested in the section. You will also want to use Pascal's identity.
5. Hint: Draw C_{13} and label its vertices 0-12 clockwise around it. Connect each vertex to two additional vertices: those that are distance 5 and 8 in the clockwise direction from the vertex. (So vertex 0 is adjacent to 1 and 13, and also to 5 and 8. Vertex 1 is adjacent to 2 and 0, and also to 6 and 9.) This graph represents the red edges. All other edges are blue.
6. (a) $R(K_3 - e, K_b) = 2b - 1$
   (c) $R(C_4, C_4) = 6$
   (d) $R(K_3, C_4) = 7$

Section 7.1

1. (a) $k = \frac{vr}{b}$ and $\lambda = \frac{r(vr-b)}{b(v-1)}$
   (b) $r = \frac{\lambda(v-1)}{k-1}$ and $b = \frac{\lambda v(v-1)}{k(k-1)}$
3. Take all $(n-1)$-subsets of $[n]$.
5. $b = \binom{n}{k}$, $v = n$, $r = \binom{n-1}{k-1}$, k, and $\lambda = \binom{n-2}{k-2}$
7. Hint: Use the equivalence principle to count the blocks. Notice that $\lambda\binom{v}{2}$ equals the number of ways first to select a pair of varieties and then to select a block that the pair belongs to.
10. Hint: $\{0, 1, 2, 6, 9\}$
11. Hint: Use $\{0, 1, 2, 4\}$ as one of the base blocks.
14. Hint: Find the parameters of the complementary design.
17. (a) When you construct a cyclic design, the number of blocks must be a multiple of the number of varieties. Why?
    (b) You need $b = cv$ by part (a). The other equations follow from this.
    (c) The basic necessary conditions as well as those from part (b) don't rule out its existence.

Section 7.2

1. You need $b = \frac{r(5r+1)}{6}$ and $v = 5r + 1$. Setting $r = 4$ results in parameters that meet all necessary conditions so far, as does $r = 6$ and $r = 7$. (Fisher's inequality in Section 7.3 eliminates the $r = 4$ possiblity.)
3. Hint: If this design exists, then its complementary design exists too.
5. Hint: Solve for b and v in terms of k and then put the parameters in the given form.
7. Hint: It is the residual of a certain symmetric design.

9. Hint: If $\mathcal{D}$ is symmetric, then $\mathcal{D}^T$ is a BIBD. Use the fact that symmetric designs are linked.

10. (b) Hint: Use the BRC theorem. You should find that it eliminates $k = 7, 8, 10$.

11. Hint: Find the parameters and use the BRC theorem.

Section 7.3

1. There is only one. What is it?

2. Hint: Use the construction method of Theorem 7.3.3.

3. If such a design exists, its parameters are $(2r, 6, r, 3, \frac{2r}{5})$. Determine what values r can take on, then use some results from Section 7.1.

7. (a) There are five of type I, 10 of type II, and 15 of type III.

9. Yes, all necessary conditions in those theorems are met so they do not rule out its existence.

Section 7.4

1. Ten errors were made.

3. The answer to both questions is $\binom{8}{0} + \binom{8}{1} + \binom{8}{2} + \binom{8}{3}$.

4. Hint: $\text{wt}(\mathbf{v} \oplus \mathbf{w})$ equals the number of positions in which the two words differ. Argue that the right side of the identity computes this as well, and note that $(\mathbf{v} * \mathbf{w})_i = 1$ if and only if $\mathbf{v}$ and $\mathbf{w}$ both have a 1 in their i-th position.

7. You need at least $65536 = 2^{16}$ codewords, so $2^m - m - 1 \geqslant 16$ if and only if $m \geqslant 5$. You should use the Hamming $(31, 2^{26}, 3)$ code. Each codeword is 31 bits long. The percentage of codewords you need relative to the number of codewords available in this code is $2^{16}/2^{26} \approx 0.1\%$.

8. (a) The minimum weight of a nonzero linear combination is 1, so the minimum distance is 1. This code does not correct any errors.

10. Hint: First explain why $|\mathcal{C}| > 2$ implies that there must be two codewords that agree in at least one place. What then does this imply about the minimum distance?

Section 7.5

2. Hint: You will need to use the fact that the submatrix A_{11} shown in (7.9) is the incidence matrix of a symmetric $(11, 6, 3)$ design and also that symmetric designs are linked. Treat the case when the last row is involved separately.

3. Hint: Revisit the proof of the sphere packing bound in Section 7.4.

Section 8.1

2. height($\mathbf{2^n}$) $= n + 1$ and the number of maximum-sized chains is $n!$.
3. $\mathbf{D_n}$ is a total order if and only if n is prime.
5. (b) height($\hat{\mathbf{P}}$) $= 2 +$ height($\mathbf{P}$) and width($\hat{\mathbf{P}}$) $=$ width($\mathbf{P}$)
7. Hint: The answer is 3^n. Break up the ordered pairs into cases according to the size of their first element. That is, count all (I, J) with $|I| = 0$, then count all (I, J) with $|I| = 1$, etc.
9. **Antisymmetric:** Assume $P_1 = \{B_1, \ldots, B_r\}$ and $P_2 = \{C_1, \ldots, C_s\}$ are partitions of $[n]$, and that $P_1 \preceq P_2$ and $P_2 \preceq P_1$. Consider any block $B_i \in P_1$. Since $P_1 \preceq P_2$, there is some block $C_j \in P_2$ for which $B_i \subseteq C_j$. Also, since $P_2 \preceq P_1$, there is some block $B_k \in P_1$ for which $C_j \subseteq B_k$. This means $B_i \subseteq C_j \subseteq B_k$, or that $B_i \subseteq B_k$. But P_1 is a partition of $[n]$, so $B_i = B_k$ which in turn means $B_i = C_j$. This proves that any block of P_1 is a block of P_2. A similar argument shows that any block of P_2 is a block of P_1. Therefore $P_1 = P_2$.

   Also, $\mathbf{\Pi_n}$ is a lattice.
10. (a) They are not necessarily disjoint.
    (b) Hint: Prove by contradiction.
13. This is false.

Section 8.2

1. $X = \{2, 3, 4, 6, 16, 18, 24\}$ is one set that works.
2. Hint: There are 16.
5. Hint: Write $D_{p^k} = \{p^0, p^1, \ldots, p^k\}$. Define $\phi : D_{p^k} \longrightarrow [k+1]$ by $\phi(p^i) = i + 1$, for all i satisfying $0 \leqslant i \leqslant k$. Prove that this is a bijection and then that $p^i | p^j$ if and only if $i + 1 \leqslant j + 1$.
7. (a) **Reflexive:** Let $x \in \mathbb{B}^n$. Since $x_i \leqslant x_i$ for all $i \in [n]$, it follows that $x \leqslant x$. **Antisymmetric:** Let $x, y \in \mathbb{B}^n$ and assume $x \leqslant y$ and $y \leqslant x$. This means that $x_i \leqslant y_i$ and $y_i \leqslant x_i$ for all $i \in [n]$. Therefore $x_i = y_i$ for all $i \in [n]$, so $x = y$. **Transitive:** Left for you.
   (b) $(\mathbb{B}^n, \leqslant) \cong \mathbf{2^n}$

Section 8.3

1. height($\mathbf{10}$) $= 10$ and width($\mathbf{10}$) $= 1$; height($\mathbf{\Pi_4}$) $= 4$ and width($\mathbf{\Pi_4}$) $= 7$. For $\mathbf{\Pi_4}$, use Figure 8.4 to give an antichain cover of size 4 and a chain cover of size 7.
2. For the first poset, draw a row of eight elements then add a ninth element above this row; connect that ninth element to each of the eight elements below it. For the second poset, use a total order but with a "Y" at the top and and upside-down "Y" at the bottom. For the third, the set $\{1, 2, 3, 12, 18, 36\}$ ordered by divisibility works.
3. The poset on the left has height 5 and width 3.

Section 8.4

1. Draw the Hasse diagram. Every linear extension must have $a \leqslant c \leqslant d \leqslant e$ and $b \leqslant c \leqslant d \leqslant e$. So this poset only has two linear extensions: $a \leqslant b \leqslant c \leqslant d \leqslant e$ and $b \leqslant a \leqslant c \leqslant d \leqslant e$.
2. Hint: Draw the Hasse diagram for the $n = 3$ and $n = 4$ cases.
3. $\dim(\mathbf{\Pi_3}) = 2$
5. Let $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$ be the linear extension created by the algorithm. For sake of contradiction, suppose $x_i \leqslant x_j$ in $\mathbf{P}$ but $x_j < x_i$ in the linear extension. This means that at the time x_j was added to the linear extension, (1) both x_j and x_i had not yet been deleted from the poset, and (2) x_j was a minimal element. But $x_i \leqslant x_j$ in $\mathbf{P}$, which means x_j is not minimal.
6. Hint: The argument we used to show that any realizer of $\mathbf{S_4}$ requires at least four linear extensions easily extends to $\mathbf{S_n}$. To find a realizer, extend the pattern of those in Figure 8.6.
9. (a) You need to put every element that is under x' below every element that is above y'. That is, add every ordered pair (w, z) where $w \leqslant x'$ and $y' \leqslant z$.
   (c) If $\mathbf{P}'$ is a total order, then it is a linear extension of $\mathbf{P}$ that has $x' \leqslant y'$, as desired. If it is not a total order, let x'' and y'' be two incomparable elements in $\mathbf{P}'$. Repeat the procedure until you get a total order.
12. (a) $\mathbf{5}$ can be represented by five concentric boxes.
   (b) Hint: Arrange the (up to four) linear extensions on the positive and negative x- and y-axes in a certain way. How then should you construct the box for each element?

Section 8.5

1. (a) false
   (b) true
3. For the poset on the left, label the minimum element 1, the one above that 2, then 3 and 4 on the left and right, then 5 and then label the maximum element 6. The Möbius matrix is

$$M = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & -1 & 1 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

4. $\mu(1.2.3.4, 1234) = -6$
6. The underlying poset is the total order $\mathbf{5}$ and its Möbius function is given in Theorem 8.5.3. After applying Möbius inversion, the solution is $x_1 = s_1$, $x_2 = s_2 - s_1$, $x_3 = s_3 - s_2$, $x_4 = s_4 - s_3$, $x_5 = s_5 - s_4$.

Section 8.6

1. Hint: First prove that each of $5^{k+1} - 1$ and $k^9 + k^5 + 2k^3$ is divisible by 4.
3. This is essentially the same as Exercise 7 of Section 8.2.
5. Hint: The idea is that if you divide each of the integers in the interval $[a, b]$ by a, then the interval $[a, b]$ in $\mathbf{D}$ looks exactly like the interval $[1, \frac{b}{a}]$ in $\mathbf{D}$. The isomorphism is $\phi : [a, b] \longrightarrow D_{\frac{b}{a}}$ given by $\phi(x) = \frac{x}{a}$.

List of Notation

This table includes most of the notational symbols used in the book as well as the page where they are defined.

Notation	Page
$[1^{p_1}\, 2^{p_2} \cdots n^{p_n}]$	76
2^A	5
$\mathbf{2^n}$	318
$a \equiv b \pmod{n}$	33
$A \times B$	25
$\{a_k\}_{k\geqslant 0}$	107
$B(n)$	68
$\mathbb{B}^n$	299
(b, v, r, k, λ)	273
C^A	201
C_n	229
$\mathbf{C_n}$	339
$\mathrm{co}(f)$	26
$\mathcal{D}^c$	276
$\delta(G)$	226
$\Delta(G)$	226
$d_G(v)$ or $d(v)$	226
$\dim(\mathbf{P})$	339
$\Delta^k f(n)$	171
$\mathbf{D_n}$	318
$\mathrm{dom}(f)$	26
$\delta(x, y)$	350
$e(G)$	226
$f : A \longrightarrow B$	25
$\mathrm{fix}_G(\pi)$	202
F_n	125, 152
$[\![f(x)]\!]_{x^k}$	114
$[\![f(x)]\!]_{x^k/k!}$	121
$G \cong H$	232
$h(\mathbf{v}, \mathbf{w})$	299

Notation	Page
K_n	228
$K_{r,s}$	228
L_n	99, 152
$\mu(x, y)$	350
$[n]$	2
$\mathbf{n}$	319
$n!$	7, 52
$N_{\geqslant}(\cdot)$ and $N_{=}(\cdot)$	86, 352
$n \longrightarrow (a, b)$	263
$n(G)$	226
n^k	4, 52
$(n)_k$	7, 52
$\binom{n}{k}$	9, 59
$\left(\!\binom{n}{k}\!\right)$	11, 60
$\binom{n}{t_1, t_2, \ldots, t_k}$	142
$\mathrm{orb}_G(f)$	202
$p(G, k)$	253
$P(n)$	77
$P(n, k)$	76
P_n	229
$\mathbf{\Pi_n}$	324
$\mathbf{P} \cong \mathbf{Q}$	328
$\mathbf{P} \times \mathbf{Q}$	355
$\mathbf{P} = (X, \leqslant)$	317
$\mathbf{P}[Y] = (Y, R[Y])$	323
$R(a, b)$	263
$\mathrm{rng}(f)$	26
$s(n, k)$	168
$S(n, k)$	67
$\mathbf{S_n}$	338

Index

About the Author

David R. Mazur is Associate Professor of Mathematics at Western New England College in Springfield, Massachusetts. He was born on October 23, 1971 in Washington, D.C. He received his undergraduate degree in mathematics from the University of Delaware in 1993, and also won the Department of Mathematical Sciences' William D. Clark prize for "unusual ability" in the major that year. He then received two fellowships for doctoral study in the Department of Mathematical Sciences (now the Department of Applied Mathematics and Statistics) at The Johns Hopkins University. From there he received his Master's in 1996 and his Ph.D. in 1999 under the direction of Leslie A. Hall, focusing on operations research, integer programming, and polyhedral combinatorics. His dissertation, *Integer Programming Approaches to a Multi-Facility Location Problem*, won first prize in the 1999 joint United Parcel Service/INFORMS Section on Location Analysis Dissertation Award Competition. The competition occurs once every two years to recognize outstanding dissertations in the field of location analysis.

Dave began teaching at Western New England College in 1999 and received tenure and promotion to Associate Professor in 2005. He was a 2000–2001 Project NExT fellow and continues to serve this program as a consultant. He is an active member of the Mathematical Association of America, having co-organized several sessions at national meetings. He currently serves on the MAA's Membership Committee. Dave lives with his wife and three children in Western Massachusetts.