Wiley-Interscience Series in Discrete Mathematics and Optimization

COMBINATORICS

SECOND EDITION

RUSSELL MERRIS

WWW.

Combinatorics

Second Edition

WILEY-INTERSCIENCE
SERIES IN DISCRETE MATHEMATICS AND OPTIMIZATION

ADVISORY EDITORS

A complete list of titles in this series appears at the end of this volume.

Combinatorics

SECOND EDITION

RUSSELL MERRIS
California State University, Hayward

A JOHN WILEY & SONS, INC., PUBLICATION

This book is printed on acid-free paper. ⊗

Published simultaneously in Canada.

For ordering and customer service, call 1-800-CALL-WILEY.

Library of Congress Cataloging-in-Publication Data:

Merris, Russell, 1943–
Combinatorics / Russell Merris.–2nd ed.
p. cm. – (Wiley series in discrete mathematics and optimization)
Includes bibliographical references and index.
ISBN-0-471-26296-X (acid-free paper)
1. Combinatorial analysis I. Title. II. Series.

QA164.M47 2003
511′.6–dc21 2002192250

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

This book is dedicated to my wife, Karen Diehl Merris.

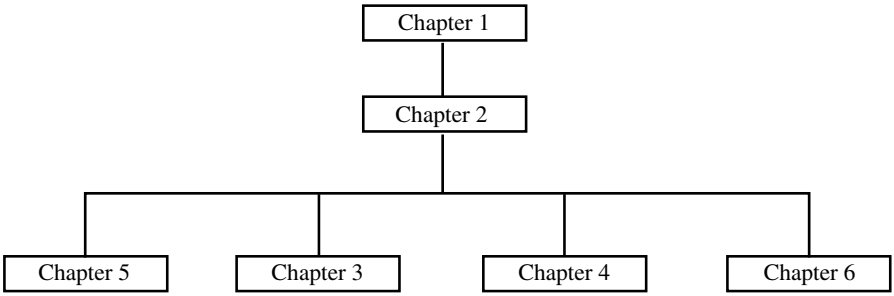
Contents

Note: Asterisks indicate optional sections that can be omitted without loss of continuity.

Preface

This book is intended to be used as the text for a course in combinatorics at the level of beginning upper division students. It has been shaped by two goals: to make some fairly deep mathematics accessible to students with a wide range of abilities, interests, and motivations and to create a pedagogical tool useful to the broad spectrum of instructors who bring a variety of perspectives and expectations to such a course.

The author's approach to the second goal has been to maximize flexibility. Following a basic foundation in Chapters 1 and 2, each instructor is free to pick and choose the most appropriate topics from the remaining four chapters. As summarized in the chart below, Chapters 3–6 are *completely independent of each other.* Flexibility is further enhanced by optional sections and appendices, by weaving some topics into the exercise sets of multiple sections, and by identifying various points of departure from each of the final four chapters. (The price of this flexibility is some redundancy, e.g., several definitions can be found in more than one place.)



Turning to the first goal, students using this book are expected to have been exposed to, even if they cannot recall them, such notions as equivalence relations, partial fractions, the Maclaurin series expansion for e^x, elementary row operations, determinants, and matrix inverses. A course designed around this book should have as specific prerequisites those portions of calculus and linear algebra commonly found among the lower division requirements for majors in the mathematical and computer sciences. Beyond these general prerequisites, the last two sections of Chapter 5 presume the reader to be familiar with the *definitions* of classical adjoint

(adjugate) and characteristic roots (eigenvalues) of real matrices, and the first two sections of Chapter 6 make use of reduced row-echelon form, bases, dimension, rank, nullity, and orthogonality. (All of these topics are reviewed in Appendix A3.)

Strategies that promote student engagement are a lively writing style, timely and appropriate examples, interesting historical anecdotes, a variety of exercises (tempered and enlivened by suitable hints and answers), and judicious use of footnotes and appendices to touch on topics better suited to more advanced students. These are things about which there is general agreement, at least in principle.

There is less agreement about how to focus student energies on attainable objectives, in part because focusing on some things inevitably means neglecting others. If the course is approached as a *last chance* to expose students to this marvelous subject, it probably will be. If approached more invitingly, as a *first* course in combinatorics, it may be. To give some specific examples, highlighted in this book are binomial coefficients, Stirling numbers, Bell numbers, and partition numbers. These topics appear and reappear throughout the text. Beyond reinforcement in the service of retention, the tactic of overarching themes helps foster an image of combinatorics as a unified mathematical discipline. While other celebrated examples, e.g., Bernoulli numbers, Catalan numbers, and Fibonacci numbers, are generously represented, they appear almost entirely in the exercises. For the sake of argument, let us stipulate that these roles could just as well have been reversed. The issue is that beginning upper division students cannot be expected to absorb, much less appreciate, *all* of these special arrays and sequences in a single semester. On the other hand, the flexibility is there for willing admirers to rescue one or more of these justly famous combinatorial sequences from the relative obscurity of the exercises.

While the overall framework of the first edition has been retained, everything else has been revised, corrected, smoothed, or polished. The focus of many sections has been clarified, e.g., by eliminating peripheral topics or moving them to the exercises. Material new to the second edition includes an optional section on algorithms, several new examples, and many new exercises, some designed to guide students to discover and prove nontrivial results for themselves. Finally, the section of hints and answers has been expanded by an order of magnitude.

The material in Chapter 3, Pólya's theory of enumeration, is typically found closer to the end of comparable books, perhaps reflecting the notion that it is the *last* thing that should be taught in a junior-level course. The author has aspired, not only to make this theory accessible to students taking a first upper division mathematics course, but to make it possible for the subject to be addressed right after Chapter 2. Its placement in the middle of the book is intended to signal that it *can* be fitted in there, not that it must be. If it seems desirable to cover some but not all of Chapter 3, there are many natural places to exit in favor of something else, e.g., after the application of Bell numbers to transitivity in Section 3.3, after enumerating the overall number of color patterns in Section 3.5, after *stating* Pólya's theorem in Section 3.6, or after proving the theorem at the end of Section 3.6.

Optional Sections 1.3 and 1.10 can be omitted with the understanding that exercises in subsequent sections involving probability or algorithms should be assigned with discretion. With the same caveat, Section 1.4 can be omitted by those not

intending to go on to Sections 6.1, 6.2, or 6.4. The material in Section 6.3, touching on mutually orthogonal Latin squares and their connection to finite projective planes, can be covered independently of Sections 1.4, 6.1, and 6.2.

The book contains much more material then can be covered in a single semester. Among the possible syllabi for a one semester course are the following:

- Chapters 1, 2, and 4 and Sections 3.1–3.3
- Chapters 1 (omitting Sections 1.3, 1.4, & 1.10), 2, and 3, and Sections 5.1 & 5.2
- Chapters 1 (omitting Sections 1.3 & 1.10), 2, and 6 and Sections 4.1 – 4.4
- Chapters 1 (omitting Sections 1.4 & 1.10) and 2 and Sections 3.1 – 3.3, 4.1 – 4.3, & 6.3
- Chapters 1 (omitting Sections 1.3 & 1.4) and 2 and Sections 4.1 – 4.3, 5.1, & 5.3–5.7
- Chapters 1 (omitting Sections 1.3, 1.4, & 1.10) and 2 and Sections 4.1 – 4.3, 5.1, 5.3–5.5, & 6.3

Many people have contributed observations, suggestions, corrections, and constructive criticisms at various stages of this project. Among those deserving special mention are former students David Abad, Darryl Allen, Steve Baldzikowski, Dale Baxley, Stanley Cheuk, Marla Dresch, Dane Franchi, Philip Horowitz, Rhian Merris, Todd Mullanix, Cedide Olcay, Glenn Orr, Hitesh Patel, Margaret Slack, Rob Smedfjeld, and Masahiro Yamaguchi; sometime collaborators Bob Grone, Tom Roby, and Bill Watkins; correspondents Mark Hunacek and Gerhard Ringel; reviewers Rob Beezer, John Emert, Myron Hood, Herbert Kasube, André Kézdy, Charles Landraitis, John Lawlor, and Wiley editors Heather Bergman, Christine Punzo, and Steve Quigley. I am especially grateful for the tireless assistance of Cynthia Johnson and Ken Rebman.

Despite everyone's best intentions, no book seems complete without some errors. An up-to-date errata, accessible from the Internet, will be maintained at URL

http://www.sci.csuhayward.edu/∼rmerris

Appropriate acknowledgment will be extended to the first person who communicates the specifics of a previously unlisted error to the author, preferably by e-mail addressed to

merris@csuhayward.edu

Hayward California RUSSELL MERRIS

1

The Mathematics of Choice

> It seems that mathematical ideas are arranged somehow in strata, the ideas in each stratum being linked by a complex of relations both among themselves and with those above and below. The lower the stratum, the deeper (and in general the more difficult) the idea. Thus, the idea of an irrational is deeper than the idea of an integer.
>
> — G. H. Hardy (*A Mathematician's Apology*)

Roughly speaking, the first chapter of this book is the top stratum, the surface layer of combinatorics. Even so, it is far from superficial. While the first main result, the so-called fundamental counting principle, is nearly self-evident, it has enormous implications throughout combinatorial enumeration. In the version presented here, one is faced with a sequence of decisions, each of which involves some number of choices. It is from situations like this that the chapter derives its name.

To the uninitiated, mathematics may appear to be "just so many numbers and formulas." In fact, the numbers and formulas should be regarded as shorthand notes, summarizing *ideas*. Some ideas from the first section are summarized by an algebraic formula for multinomial coefficients. Special cases of these numbers are addressed from a combinatorial perspective in Section 1.2.

Section 1.3 is an optional discussion of probability theory which can be omitted if probabilistic exercises in subsequent sections are approached with caution. Section 1.4 is an optional excursion into the theory of binary codes which can be omitted by those not planning to visit Chapter 6. Sections 1.3 and 1.4 are partly motivational, illustrating that even the most basic combinatorial ideas have real-life applications.

In Section 1.5, ideas behind the formulas for sums of powers of positive integers motivate the study of relations among binomial coefficients. Choice is again the topic in Section 1.6, this time with or without replacement, where order does or doesn't matter.

To better organize and understand the multinomial theorem from Section 1.7, one is led to symmetric polynomials and, in Section 1.8, to partitions of n. Elementary symmetric functions and their association with power sums lie at the

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

heart of Section 1.9. The final section of the chapter is an optional introduction to algorithms, the flavor of which can be sampled by venturing only as far as Algorithm 1.10.3. Those desiring not less but more attention to algorithms can find it in Appendix A2.

1.1. THE FUNDAMENTAL COUNTING PRINCIPLE

How many different four-letter words, including nonsense words, can be produced by rearranging the letters in LUCK? In the absence of a more inspired approach, there is always the brute-force strategy: Make a systematic list.

Once we become convinced that Fig. 1.1.1 accounts for every possible rearrangement and that no "word" is listed twice, the solution is obtained by counting the 24 words on the list.

While finding the brute-force strategy was effortless, implementing it required some work. Such an approach may be fine for an isolated problem, the *like* of which one does not expect to see again. But, just for the sake of argument, imagine yourself in the situation of having to solve a great many thinly disguised variations of this same problem. In that case, it would make sense to invest some effort in finding a strategy that requires less work to implement. Among the most powerful tools in this regard is the following commonsense principle.

1.1.1 Fundamental Counting Principle. Consider a (finite) sequence of decisions. Suppose the number of choices for each individual decision is independent of decisions made previously in the sequence. Then the number of ways to make the whole sequence of decisions is the product of these numbers of choices.

To state the principle symbolically, suppose c_i is the number of choices for decision i. If, for $1 \leq i < n$, c_{i+1} does not depend on which choices are made in

LUCK	LUKC	LCUK	LCKU	LKUC	LKCU
ULCK	ULKC	UCLK	UCKL	UKLC	UKCL
CLUK	CLKU	CULK	CUKL	CKLU	CKUL
KLUC	KLCU	KULC	KUCL	KCLU	KCUL

Figure 1.1.1. The rearrangements of LUCK.

decisions $1, \ldots, i$, then the number of different ways to make the sequence of decisions is $c_1 \times c_2 \times \cdots \times c_n$.

Let's apply this principle to the word problem we just solved. Imagine yourself in the midst of making the brute-force list. Writing down one of the words involves a sequence of four decisions. Decision 1 is which of the four letters to write first, so $c_1 = 4$. (It is no accident that Fig. 1.1.1 consists of four rows!) For each way of making decision 1, there are $c_2 = 3$ choices for decision 2, namely which letter to write second. Notice that the specific letters comprising these three choices depend on how decision 1 was made, but their *number* does not. That is what is meant by the number of choices for decision 2 being independent of how the previous decision is made. Of course, $c_3 = 2$, but what about c_4? Facing no alternative, is it correct to say there is "no choice" for the last decision? If that were literally true, then c_4 would be zero. In fact, $c_4 = 1$. So, by the fundamental counting principle, the number of ways to make the sequence of decisions, i.e., the number of words on the final list, is

$$c_1 \times c_2 \times c_3 \times c_4 = 4 \times 3 \times 2 \times 1.$$

The product $n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1$ is commonly written n! and read *n-factorial*.* The number of four-letter words that can be made up by rearranging the letters in the word LUCK is $4! = 24$.

What if the word had been LUCKY? The number of five-letter words that can be produced by rearranging the letters of the word LUCKY is $5! = 120$. A systematic list might consist of five rows each containing $4! = 24$ words.

Suppose the word had been LOOT? How many four-letter words, including nonsense words, can be constructed by rearranging the letters in LOOT? Why not apply the fundamental counting principle? Once again, imagine yourself in the midst of making a brute-force list. Writing down one of the words involves a sequence of four decisions. Decision 1 is which of the three letters L, O, or T to write first. This time, $c_1 = 3$. But, what about c_2? In this case, the number of choices for decision 2 depends on how decision 1 was made! If, e.g., *L* were chosen to be the first letter, then there would be two choices for the second letter, namely O or T. If, however, O were chosen first, then there would be three choices for the second decision, L, (the second) O, or T. Do we take $c_2 = 2$ or $c_2 = 3$? The answer is that *the fundamental counting principle does not apply to this problem* (at least not directly). The fundamental counting principle applies *only* when the *number* of choices for decision $i + 1$ is *independent* of how the previous i decisions are made.

To enumerate all possible rearrangements of the letters in LOOT, begin by distinguishing the two O's. maybe write the word as LOoT. Applying the fundamental counting principle, we find that there are $4! = 24$ different-*looking* four-letter words that can be made up from L, O, o, and T.

*The exclamation mark is used, not for emphasis, but because it is a convenient symbol common to most keyboards.

LOoT	LOTo	LoOT	LoTO	LTOo	LToO
OLoT	OLTo	OoLT	OoTL	OTLo	OToL
oLOT	oLTO	oOLT	oOTL	oTLO	oTOL
TLOo	TLoO	TOLo	TOoL	ToLO	ToOL

Figure 1.1.2. Rearrangements of LOoT.

Among the words in Fig. 1.1.2 are pairs like OLoT and oLOT, which look different only because the two O's have been distinguished. In fact, every word in the list occurs twice, once with "big O" coming before "little o", and once the other way around. Evidently, the number of different words (with indistinguishable O's) that can be produced from the letters in LOOT is not 4! but $4!/2 = 12$.

What about TOOT? First write it as TOot. Deduce that in any list of all possible rearrangements of the letters T, O, o, and t, there would be $4! = 24$ different-looking words. Dividing by 2 makes up for the fact that two of the letters are O's. Dividing by 2 again makes up for the two T's. The result, $24/(2 \times 2) = 6$, is the number of different words that can be made up by rearranging the letters in TOOT. Here they are

TTOO TOTO TOOT OTTO OTOT OOTT

All right, what if the word had been LULL? How many words can be produced by rearranging the letters in LULL? Is it too early to guess a pattern? Could the number we're looking for be $4!/3 = 8$? No. It is easy to see that the correct answer must be 4. Once the position of the letter U is known, the word is completely determined. Every other position is filled with an L. A complete list is ULLL, LULL, LLUL, LLLU.

To find out why 4!/3 is wrong, let's proceed as we did before. Begin by distinguishing the three L's, say L_1, L_2, and L_3. There are 4! different-looking words that can be made up by rearranging the four letters L_1, L_2, L_3, and U. If we were to make a list of these 24 words and then erase all the subscripts, how many times would, say, LLLU appear? The answer to this question can be obtained from the fundamental counting principle! There are three decisions: decision 1 has three choices, namely which of the three L's to write first. There are two choices for decision 2 (which of the two remaining L's to write second) and one choice for the third decision, which L to put last. Once the subscripts are erased, LLLU would appear 3! times on the list. We should divide $4! = 24$, not by 3, but by $3! = 6$. Indeed, $4!/3! = 4$ is the correct answer.

Whoops! if the answer corresponding to LULL is 4!/3!, why didn't we get 4!/2! for the answer to LOOT? In fact, we did: $2! = 2$.

Are you ready for MISSISSIPPI? It's the same problem! If the letters were all different, the answer would be 11!. Dividing 11! by 4! makes up for the fact that there are four I's. Dividing the quotient by another 4! compensates for the four S's.

Dividing that quotient by 2! makes up for the two P's. In fact, no harm is done if that quotient is divided by $1! = 1$ in honor of the single M. The result is

$$\frac{11!}{4!\,4!\,2!\,1!} = 34,650.$$

(Confirm the arithmetic.) The 11 letters in MISSISSIPPI can be (re)arranged in 34,650 different ways.*

There is a special notation that summarizes the solution to what we might call the "MISSISSIPPI problem."

1.1.2 Definition. The *multinomial coefficient*

$$\binom{n}{r_1, r_2, \ldots, r_k} = \frac{n!}{r_1!r_2!\cdots r_k!},$$

where $r_1 + r_2 + \cdots + r_k = n$.

So, "multinomial coefficient" is a *name* for the answer to the question, how many n-letter "words" can be assembled using r_1 copies of one letter, r_2 copies of a second (different) letter, r_3 copies of a third letter, ..., and r_k copies of a kth letter?

1.1.3 Example. After cancellation,

$$\begin{aligned}\binom{9}{4,3,1,1} &= \frac{9\times 8\times 7\times 6\times 5\times 4\times 3\times 2\times 1}{4\times 3\times 2\times 1\times 3\times 2\times 1\times 1\times 1} \\ &= 9\times 8\times 7\times 5 = 2520.\end{aligned}$$

Therefore, 2520 different words can be manufactured by rearranging the nine letters in the word SASSAFRAS. □

In real-life applications, the words need not be assembled from the English alphabet. Consider, e.g., POSTNET† barcodes commonly attached to U.S. mail by the Postal Service. In this scheme, various numerical delivery codes‡ are represented by "words" whose letters, or *bits*, come from the alphabet $\{|, \,\}$. Corresponding, e.g., to a ZIP + 4 code is a 52-bit barcode that begins and ends with $|$. The 50-bit middle part is partitioned into ten 5-bit zones. The first nine of these zones are for the digits that comprise the ZIP + 4 code. The last zone accommodates a *parity*

* This number is roughly equal to the number of members of the Mathematical Association of America (MAA), the largest professional organization for mathematicians in the United States.

† Postal Numeric Encoding Technique.

‡ The original five-digit Zoning Improvement Plan (ZIP) code was introduced in 1964; ZIP+4 codes followed about 25 years later. The 11-digit Delivery Point Barcode (DPBC) is a more recent variation.

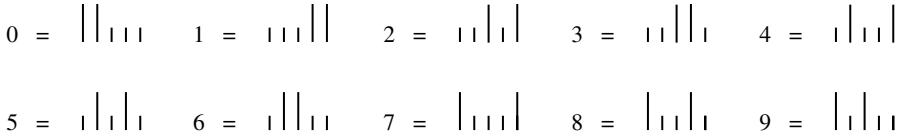


Figure 1.1.3. POSTNET barcodes.

check digit, chosen so that the sum of all ten digits is a multiple of 10. Finally, each digit is represented by one of the 5-bit barcodes in Fig. 1.1.3. Consider, e.g., the ZIP +4 code 20090-0973, for the Mathematical Association of America. Because the sum of these digits is 30, the parity check digit is 0. The corresponding 52-bit word can be found in Fig. 1.1.4.

20090-0973

Figure 1.1.4

We conclude this section with another application of the fundamental counting principle.

1.1.4 Example. Suppose you wanted to determine the number of positive integers that exactly divide $n = 12$. That isn't much of a problem; there are six of them, namely, 1, 2, 3, 4, 6, and 12. What about the analogous problem for $n = 360$ or for $n = 360,000$? Solving even the first of these by brute-force list making would be a lot of work. Having already found another strategy whose implementation requires a lot less work, let's take advantage of it.

Consider $360 = 2^3 \times 3^2 \times 5$, for example. If $360 = dq$ for positive integers d and q, then, by the uniqueness part of the *fundamental theorem of arithmetic*, the prime factors of d, together with the prime factors of q, are precisely the prime factors of 360, multiplicities included. It follows that the prime factorization of d must be of the form $d = 2^a \times 3^b \times 5^c$, where $0 \le a \le 3$, $0 \le b \le 2$, and $0 \le c \le 1$. Evidently, there are four choices for a (namely 0, 1, 2, or 3), three choices for b, and two choices for c. So, the number of possibile d's is $4 \times 3 \times 2 = 24$. □

1.1. EXERCISES

1 The Hawaiian alphabet consists of 12 letters, the vowels a, e, i, o, u and the consonants h, k, l, m, n, p, w.

(a) Show that 20,736 different 4-letter "words" could be constructed using the 12-letter Hawaiian alphabet.

(b) Show that 456,976 different 4-letter "words" could be produced using the 26-letter English alphabet.*

(c) How many four-letter "words" can be assembled using the Hawaiian alphabet if the second and last letters are vowels and the other 2 are consonants?

(d) How many four-letter "words" can be produced from the Hawaiian alphabet if the second and last letters are vowels but there are no restrictions on the other 2 letters?

2 Show that

(a) $3! \times 5! = 6!$.

(b) $6! \times 7! = 10!$.

(c) $(n+1) \times (n!) = (n+1)!$.

(d) $n^2 = n![1/(n-1)! + 1/(n-2)!]$.

(e) $n^3 = n![1/(n-1)! + 3/(n-2)! + 1/(n-3)!]$.

3 One brand of electric garage door opener permits the owner to select his or her own electronic "combination" by setting six different switches either in the "up" or the "down" position. How many different combinations are possible?

4 One generation back you have two ancestors, your (biological) parents. Two generations back you have four ancestors, your grandparents. Estimating 2^{10} as 10^3, approximately how many ancestors do you have

(a) 20 generations back?

(b) 40 generations back?

(c) In round numbers, what do you estimate is the total population of the planet?

(d) What's wrong?

5 Make a list of all the "words" that can be made up by rearranging the letters in

(a) TO. **(b)** TOO. **(c)** TWO.

6 Evaluate multinomial coefficient

(a) $\binom{6}{4,1,1}$. **(b)** $\binom{6}{3,3}$. **(c)** $\binom{6}{2,2,2}$.

*Based on these calculations, might it be reasonable to expect Hawaiian words, on average, to be longer than their English counterparts? Certainly such a conclusion would be warranted if both languages had the same vocabulary and both were equally "efficient" in avoiding long words when short ones are available. How efficient is English? Given that the total number of words defined in a typical "unabridged dictionary" is at most 350,000, one could, at least in principle, construct a new language with the same vocabulary as English but in which every word has four letters—and there would be 100,000 words to spare!

(d) $\binom{6}{3,2,1}$. **(e)** $\binom{6}{1,3,2}$. **(f)** $\binom{6}{1,1,1,1,1,1}$.

7 How many different "words" can be constructed by rearranging the letters in

(a) ALLELE? **(b)** BANANA? **(c)** PAPAYA?

(d) BUBBLE? **(e)** ALABAMA? **(f)** TENNESSEE?

(g) HALEAKALA? **(h)** KAMEHAMEHA? **(i)** MATHEMATICS?

8 Prove that

(a) $1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1$.

(b) $1 \times 1! + 2 \times 2! + 3 \times 3! + \cdots + n \times n! = (n+1)! - 1$.

(c) $(2n)!/2^n$ is an integer.

9 Show that the barcodes in Fig. 1.1.3 comprise *all possible* five-letter words consisting of two |'s and three |'s.

10 Explain how the following barcodes fail the POSTNET standard:

(a) 

(b) 

(c) 

11 "Read" the ZIP+4 Code

(a) 

(b) 

12 Given that the first nine zones correspond to the ZIP+4 delivery code 94542-2520, determine the parity check digit and the two "hidden digits" in the 62-bit DPBC

(*Hint:* Do you need to be told that the parity check digit is last?)

13 Write out the 52-bit POSTNET barcode for 20742-2461, the ZIP+4 code at the University of Maryland used by the Association for Women in Mathematics.

14 Write out all 24 divisors of 360. (See Example 1.1.4.)

15 Compute the number of positive integer divisors of

(a) 2^{10}. **(b)** 10^{10}. **(c)** 12^{10}. **(d)** 31^{10}.

(e) 360,000. **(f)** 10!.

16 Prove that the positive integer n has an odd number of positive-integer divisors if and only if it is a perfect square.

17 Let $D = \{d_1, d_2, d_3, d_4\}$ and $R = \{r_1, r_2, r_3, r_4, r_5, r_6\}$. Compute the number

(a) of different functions $f : D \to R$.

(b) of one-to-one functions $f : D \to R$.

18 The latest automobile license plates issued by the California Department of Motor Vehicles begin with a single numeric digit, followed by three letters, followed by three more digits. How many different license "numbers" are available using this scheme?

19 One brand of padlocks uses combinations consisting of three (not necessarily different) numbers chosen from $\{0, 1, 2, \ldots, 39\}$. If it takes five seconds to "dial in" a three-number combination, how long would it take to try all possible combinations?

20 The *International Standard Book Number* (ISBN) is a 10-digit numerical code for identifying books. The groupings of the digits (by means of hyphens) varies from one book to another. The first grouping indicates where the book was published. In ISBN 0-88175-083-2, the zero shows that the book was published in the English-speaking world. The code for the Netherlands is "90" as, e.g., in ISBN 90-5699-078-0. Like POSTNET, ISBN employs a check digit scheme. The first nine digits (ignoring hyphens) are multiplied, respectively, by 10, 9, 8, ..., 2, and the resulting products summed to obtain S. In 0-88175-083-2, e.g.,

$$S = 10 \times 0 + 9 \times 8 + 8 \times 8 + 7 \times 1 + 6 \times 7 + 5 \times 5 + 4 \times 0 + 3 \times 8 + 2 \times 3 = 240.$$

The last (check) digit, L, is chosen so that $S + L$ is a multiple of 11. (In our example, $L = 2$ and $S + L = 242 = 11 \times 22$.)

(a) Show that, when S is divided by 11, the quotient Q and remainder R satisfy $S = 11Q + R$.

(b) Show that $L = 11 - R$. (When $R = 1$, the check digit is X.)

(c) What is the value of the check digit, L, in ISBN 0-534-95154-L?

(d) Unlike POSTNET, the more sophisticated ISBN system can not only detect common errors, it can sometimes "correct" them. Suppose, e.g., that a single digit is wrong in ISBN 90-5599-078-0. Assuming the check digit is correct, can you identify the position of the erroneous digit?

(e) Now that you know the position of the (single) erroneous digit in part (d), can you recover the correct ISBN?

(f) What if it were expected that exactly two digits were wrong in part (d). Which two digits might they be?

21 A total of $9! = 362,880$ different nine-letter "words" can be produced by rearranging the letters in FULBRIGHT. Of these, how many contain the four-letter sequence GRIT?

22 In how many different ways can eight coins be arranged on an 8×8 checkerboard so that no two coins lie in the same row or column?

23 If A is a finite set, its *cardinality*, $o(A)$, is the number of elements in A. Compute

(a) $o(A)$ when A is the set consisting of all five-digit integers, each digit of which is 1, 2, or 3.

(b) $o(B)$, where $B = \{x \in A : \text{each of } 1, 2, \text{and } 3 \text{ is among the digits of } x\}$ and A is the set in part (a).

1.2. PASCAL'S TRIANGLE

Mathematics is the art of giving the same name to different things.

— Henri Poincaré (1854–1912)

In how many different ways can an r-element subset be chosen from an n-element set S? Denote the number by $C(n, r)$. Pronounced "n-choose-r", $C(n, r)$ is just a name for the answer. Let's find the number represented by this name.

Some facts about $C(n, r)$ are clear right away, e.g., the nature of the elements of S is immaterial. All that matters is that there are n of them. Because the only way to choose an n-element subset from S is to choose all of its elements, $C(n, n) = 1$. Having n single elements, S has n single-element subsets, i.e., $C(n, 1) = n$. For essentially the same reason, $C(n, n-1) = n$: A subset of S that contains all but one element is uniquely determined by the one element that is left out. Indeed, this idea has a nice generalization. A subset of S that contains all but r elements is uniquely determined by the r elements that are left out. This natural one-to-one correspondence between subsets and their complements yields the following *symmetry property*:

$$C(n, n-r) = C(n, r).$$

1.2.1 Example. By definition, there are $C(5, 2)$ ways to select two elements from $\{A, B, C, D, E\}$. One of these corresponds to the two-element subset $\{A, B\}$. The complement of $\{A, B\}$ is $\{C, D, E\}$. This pair is listed first in the following one-to-one correspondence between two-element subsets and their three-element complements:

$$\{A,B\} \leftrightarrow \{C,D,E\}, \qquad \{B,D\} \leftrightarrow \{A,C,E\};$$
$$\{A,C\} \leftrightarrow \{B,D,E\}, \qquad \{B,E\} \leftrightarrow \{A,C,D\};$$
$$\{A,D\} \leftrightarrow \{B,C,E\}, \qquad \{C,D\} \leftrightarrow \{A,B,E\};$$
$$\{A,E\} \leftrightarrow \{B,C,D\}, \qquad \{C,E\} \leftrightarrow \{A,B,D\};$$
$$\{B,C\} \leftrightarrow \{A,D,E\}, \qquad \{D,E\} \leftrightarrow \{A,B,C\}.$$

By counting these pairs, we find that $C(5,2) = C(5,3) = 10$. □

A special case of symmetry is $C(n,0) = C(n,n) = 1$. Given n objects, there is just one way to reject all of them and, hence, just one way to choose none of them. What if $n = 0$? How many ways are there to choose no elements from the empty set? To avoid a deep philosophical discussion, let us simply adopt as a convention that $C(0,0) = 1$.

A less obvious fact about choosing these numbers is the following.

1.2.2 Theorem (Pascal's Relation). *If $1 \le r \le n$, then*

$$C(n+1,r) = C(n,r-1) + C(n,r). \tag{1.1}$$

Together with Example 1.2.1, Pascal's relation implies, e.g., that $C(6,3) = C(5,2) + C(5,3) = 20$.

Proof. Consider the $(n+1)$-element set $\{x_1, x_2, \ldots, x_n, y\}$. Its r-element subsets can be partitioned into two families, those that contain y and those that do not. To count the subsets that contain y, simply observe that the remaining $r-1$ elements can be chosen from $\{x_1, x_2, \ldots, x_n\}$ in $C(n,r-1)$ ways. The r-element subsets that do not contain y are precisely the r-element subsets of $\{x_1, x_2, \ldots, x_n\}$, of which there are $C(n,r)$. ■

The proof of Theorem 1.2.2 used another self-evident fact that is worth mentioning explicitly. (A much deeper extension of this result will be discussed in Chapter 2.)

1.2.3 The Second Counting Principle. If a set can be expressed as the disjoint union of two (or more) subsets, then the number of elements in the set is the sum of the numbers of elements in the subsets.

So far, we have been viewing $C(n,r)$ as a single number. There are some advantages to looking at these choosing numbers collectively, as in Fig. 1.2.1. The triangular shape of this array is a consequence of not bothering to write $0 = C(n,r)$, $r > n$. Filling in the entries we know, i.e., $C(n,0) = C(n,n) = 1$, $C(n,1) = n = C(n,n-1)$, $C(5,2) = C(5,3) = 10$, and $C(6,3) = 20$, we obtain Fig. 1.2.2.

n \ r	0	1	2	3	4	5	6	7
0	$C(0,0)$							
1	$C(1,0)$	$C(1,1)$						
2	$C(2,0)$	$C(2,1)$	$C(2,2)$					
3	$C(3,0)$	$C(3,1)$	$C(3,2)$	$C(3,3)$				
4	$C(4,0)$	$C(4,1)$	$C(4,2)$	$C(4,3)$	$C(4,4)$			
5	$C(5,0)$	$C(5,1)$	$C(5,2)$	$C(5,3)$	$C(5,4)$	$C(5,5)$		
6	$C(6,0)$	$C(6,1)$	$C(6,2)$	$C(6,3)$	$C(6,4)$	$C(6,5)$	$C(6,6)$	
7	$C(7,0)$	$C(7,1)$	$C(7,2)$	$C(7,3)$	$C(7,4)$	$C(7,5)$	$C(7,6)$	$C(7,7)$
				⋯				

Figure 1.2.1. $C(n, r)$.

Given the fourth row of the array (corresponding to $n = 3$), we can use Pascal's relation to compute $C(4, 2) = C(3, 1) + C(3, 2) = 3 + 3 = 6$. Similarly, $C(6, 4) = C(6, 2) = C(5, 1) + C(5, 2) = 5 + 10 = 15$. Continuing in this way, one row at a time, we can complete as much of the array as we like.

n \ r	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	$C(4,2)$	4	1			
5	1	5	10	10	5	1		
6	1	6	$C(6,2)$	20	$C(6,4)$	6	1	
7	1	7	$C(7,2)$	$C(7,3)$	$C(7,4)$	$C(7,5)$	7	1
				⋯				

Figure 1.2.2

Following Western tradition, we refer to the array in Fig. 1.2.3 as *Pascal's triangle.*[*] (Take care not to forget, e.g., that $C(6, 3) = 20$ appears, not in the third column of the sixth row, but in the fourth column of the seventh!)

Pascal's triangle is the source of many interesting identities. One of these concerns the sum of the entries in each row:

$$\begin{aligned} 1 + 1 &= 2, \\ 1 + 2 + 1 &= 4, \\ 1 + 3 + 3 + 1 &= 8, \\ 1 + 4 + 6 + 4 + 1 &= 16, \end{aligned} \tag{1.2}$$

[*]After Blaise Pascal (1623–1662), who described it in the book *Traité du triangle arithmétique*. Rumored to have been included in a lost mathematical work by Omar Khayyam (ca. 1050–1130), author of the *Rubaiyat*, the triangle is also found in surviving works by the Arab astronomer al-Tusi (1265), the Chinese mathematician Chu Shih-Chieh (1303), and the Hindu writer Narayana Pandita (1365). The first European author to mention it was Petrus Apianus (1495–1552), who put it on the title page of his 1527 book, *Rechnung*.

n \ r	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
				...				

Figure 1.2.3. Pascal's triangle.

and so on. Why should each row sum to a power of 2? In

$$C(n,0) + C(n,1) + \cdots + C(n,n) = \sum_{r=0}^{n} C(n,r),$$

$C(n,0)$ is the number of subsets of $S = \{x_1, x_2, \ldots, x_n\}$ that have no elements; $C(n,1)$ is the number of one-element subsets of S; $C(n,2)$ is the number of two-element subsets, and so on. Evidently, the sum of the numbers in row n of Pascal's triangle is the total number of subsets of S (even when $n = 0$ and $S = \varnothing$). The empirical evidence from Equations (1.2) suggests that an n-element set has a total of 2^n subsets. How might one go about proving this conjecture?

One way to do it is by mathematical induction. There is, however, another approach that is both easier and more revealing. Imagine youself in the process of listing the subsets of $S = \{x_1, x_2, \ldots, x_n\}$. Specifying a subset involves a sequence of decisions. Decision 1 is whether to include x_1. There are two choices, *Yes* or *No*. Decision 2, whether to put x_2 into the subset, also has two choices. Indeed, there are two choices for each of the n decisions. So, by the fundamental counting principle, S has a total of $2 \times 2 \times \cdots \times 2 = 2^n$ subsets.

There is more. Suppose, for example, that $n = 9$. Consider the sequence of decisions that produces the subset $\{x_2, x_3, x_6, x_8\}$, a sequence that might be recorded as NYYNNYNYN. The first letter of this word corresponds to *No*, as in "no to x_1"; the second letter corresponds to *Yes*, as in "yes to x_2"; because x_3 is in the subset, the third letter is Y; and so on for each of the nine letters. Similarly, $\{x_1, x_2, x_3\}$ corresponds to the nine-leter word YYYNNNNNN. In general, there is a one-to-one correspondence between subsets of $\{x_1, x_2, \ldots, x_n\}$, and n-letter words assembled from the alphabet $\{\mathrm{N}, \mathrm{Y}\}$. Moreover, in this correspondence, r-element subsets correspond to words with r Y's and $n - r$ N's.

We seem to have discovered a new way to think about $C(n,r)$. It is the number of n-letter words that can be produced by (re)arranging r Y's and $n - r$ N's. This interpretation can be verified directly. An n-letter word consists of n spaces, or locations, occupied by letters. Each of the words we are discussing is completely determined once the r locations of the Y's have been chosen (the remaining $n - r$ spaces being occupied by N's).

The significance of this new perspective is that we know how to count the number of n-letter words with r Y's and $n-r$ N's. That's the MISSISSIPPI problem! The answer is multinomial coefficient $\binom{n}{r,n-r}$. Evidently,

$$C(n,r) = \binom{n}{r, n-r} = \frac{n!}{r!(n-r)!}.$$

For things to work out properly when $r = 0$ and $r = n$, we need to adopt another convention. Define $0! = 1$. (So, 0! is *not* equal to the nonsensical $0 \times (0-1) \times (0-2) \times \cdots \times 1$.)

It is common in the mathematical literature to write $\binom{n}{r}$ instead of $\binom{n}{r,n-r}$, one justification being that the information conveyed by "$n-r$" is redundant. It can be computed from n and r. The same thing could, of course, be said about *any* multinomial coefficient. The last number in the second row is always redundant. So, that particular argument is not especially compelling. The honest reason for writing $\binom{n}{r}$ is tradition.

We now have two ways to look at $C(n,r) = \binom{n}{r}$. One is what we might call the *combinatorial definition*: n-choose-r is the number of ways to choose r things from a collection of n things. The alternative, what we might call the *algebraic definition*, is

$$C(n,r) = \frac{n!}{r!(n-r)!}.$$

Don't make the mistake of asuming, just because it is more familiar, that the algebraic definition will always be easiest. (Try giving an algebraic proof of the identity $\sum_{r=0}^{n} C(n,r) = 2^n$.) Some applications are easier to approach using algebraic methods, while the combinatorial definition is easier for others. Only by becoming familiar with both will you be in a position to choose the easiest approach in every situation!

1.2.4 Example. In the basic version of poker, each player is dealt five cards (as in Fig. 1.2.4) from a standard 52-card deck (no joker). How many different five-card poker hands are there? Because someone (in a fair game it might be *Lady Luck*) chooses five cards from the deck, the answer is $C(52,5)$. The ways to find the number behind this name are: (1) Make an exhaustive list of all possible hands, (2) work out 52 rows of Pascal's triangle, or (3) use the algebraic definition

$$\begin{aligned} C(52,5) &= \frac{52!}{5!\,47!} \\ &= \frac{52 \times 51 \times 50 \times 49 \times 48 \times 47!}{5 \times 4 \times 3 \times 2 \times 1 \times 47!} \\ &= \frac{52 \times 51 \times 50 \times 49 \times 48}{5 \times 4 \times 3 \times 2 \times 1} \\ &= 52 \times 51 \times 10 \times 49 \times 2 \\ &= 2,598,960. \end{aligned}$$

□

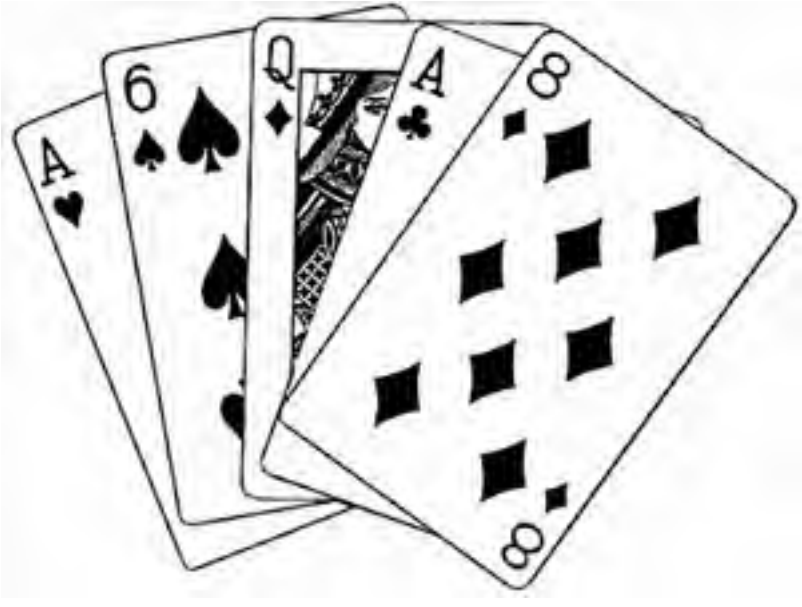


Figure 1.2.4. A five-card poker hand.

1.2.5 Example. The game of bridge uses the same 52 cards as poker.* The number of different 13-card bridge hands is

$$\begin{aligned} C(52,13) &= \frac{52!}{13!\,39!} \\ &= \frac{52 \times 51 \times \cdots \times 40 \times 39!}{13! \times 39!} \\ &= \frac{52 \times 51 \times \cdots \times 40}{13!}, \end{aligned}$$

about 635,000,000,000. □

It may surprise you to learn that $C(52,13)$ is so much larger than $C(52,5)$. On the other hand, it does seem clear from Fig. 1.2.3 that the numbers in each row of Pascal's triangle increase, from left to right, up to the middle of the row and then decrease from the middle to the right-hand end. Rows for which this property holds are said to be *unimodal*.

1.2.6 Theorem. *The rows of Pascal's triangle are unimodal.*

*The actual, physical cards are typically slimmer to accommodate the larger, 13-card hands.

Proof. If $n > 2r + 1$, the ratio

$$\frac{C(n, r+1)}{C(n, r)} = \frac{r!(n-r)!}{(r+1)!(n-r-1)!} = \frac{n-r}{r+1} > 1,$$

implying that $C(n, r+1) > C(n, r)$. ■

1.2. EXERCISES

1 Compute

(a) $C(7, 4)$. **(b)** $C(10, 5)$. **(c)** $C(12, 4)$.

(d) $C(101, 2)$. **(e)** $C(101, 99)$. **(f)** $C(12, 6)$.

2 If n and r are integers satisfying $n > r \geq 0$, prove that

(a) $(r+1)C(n, r+1) = (n-r)C(n, r)$.

(b) $(r+1)C(n, r+1) = nC(n-1, r)$.

3 Write out rows 7 through 10 of Pascal's triangle and confirm that the sum of the numbers in the 10th row is $2^{10} = 1024$.

4 Consider the sequence of numbers 0, 0, 1, 3, 6, 10, 15, ... from the third $(r = 2)$ column of Pascal's triangle. Starting with $n = 0$, the nth term of the sequence is $a_n = C(n, 2)$. Prove that, for all $n \geq 0$,

(a) $a_{n+1} - a_n = n$. **(b)** $a_{n+1} + a_n = n^2$.

5 Consider the sequence $b_0, b_1, b_2, b_3, \ldots$, where $b_n = C(n, 3)$. Prove that, for all $n \geq 0$,

(a) $b_{n+1} - b_n = C(n, 2)$.

(b) $b_{n+2} - b_n$ is a perfect square.

6 Poker is sometimes played with a joker. How many different five-card poker hands can be "chosen" from a deck of 53 cards?

7 Phrobana is a game played with a deck of 48 cards (no aces). How many different 12-card phrobana hands are there?

8 Give the inductive proof that an n-element set has 2^n subsets.

9 Let r_i be a positive integer, $1 \leq i \leq k$. If $n = r_1 + r_2 + \cdots + r_k$, prove that

$$\binom{n}{r_1, r_2, \ldots, r_k} = \binom{n-1}{r_1 - 1, r_2, \ldots, r_k} + \binom{n-1}{r_1, r_2 - 1, \ldots, r_k} + \cdots + \binom{n-1}{r_1, r_2, \ldots, r_k - 1}$$

(a) using algebraic arguments.
(b) using combinatorial arguments.

10 Suppose n, k, and r are integers that satisfy $n \geq k \geq r \geq 0$ and $k > 0$. Prove that

(a) $C(n,k)C(k,r) = C(n,r)C(n-r,k-r)$.

(b) $C(n,k)C(k,r) = C(n,k-r)C(n-k+r,r)$.

(c) $\sum_{j=0}^{n} C(n,j)C(j,r) = C(n,r)2^{n-r}$.

(d) $\sum_{j=k}^{n} (-1)^{j+k}C(n,j) = C(n-1,k-1)$.

11 Prove that $\left[\sum_{r=0}^{n} C(n,r)\right]^2 = \sum_{s=0}^{2n} C(2n,s)$.

12 Prove that $C(2n,n)$, $n > 0$, is always even.

13 Probably first studied by Leonhard Euler (1707–1783), the *Catalan sequence*[*] 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, ... is defined by $c_n = C(2n,n)/(n+1)$, $n \geq 0$. Confirm that the Catalan numbers satisfy

(a) $c_2 = 2c_1$. **(b)** $c_3 = 3c_2 - c_1$.

(c) $c_4 = 4c_3 - 3c_2$. **(d)** $c_5 = 5c_4 - 6c_3 + c_2$.

(e) $c_6 = 6c_5 - 10c_4 + 4c_3$. **(f)** $c_7 = 7c_6 - 15c_5 + 10c_4 - c_3$.

(g) Speculate about the general form of these equations.

(h) Prove or disprove your speculations from part (g).

14 Show that the Catalan numbers (Exercise 13) satisfy

(a) $c_n = C(2n-1,n-1) - C(2n-1,n+1)$.

(b) $c_n = C(2n,n) - C(2n,n-1)$.

(c) $c_{n+1} = \dfrac{4n+2}{n+2}c_n$.

15 One way to illustrate an r-element subset S of $\{1,2,\ldots,n\}$ is this: Let P_0 be the origin of the xy-plane. Setting $x_0 = y_0 = 0$, define

$$P_k = (x_k, y_k) = \begin{cases} (x_{k-1}+1, y_{k-1}) & \text{if} \quad k \in S, \\ (x_{k-1}, y_{k-1}+1) & \text{if} \quad k \notin S. \end{cases}$$

Finally, connect successive points by unit segments (either horizontal or vertical) to form a "path". Figure 1.2.5 illustrates the path corresponding to $S = \{3,4,6,8\}$ and $n = 8$.

[*]Euler was so prolific that more than one topic has come to be named for the first person to work on it *after* Euler, in this case, Eugene Catalan (1814–1894).

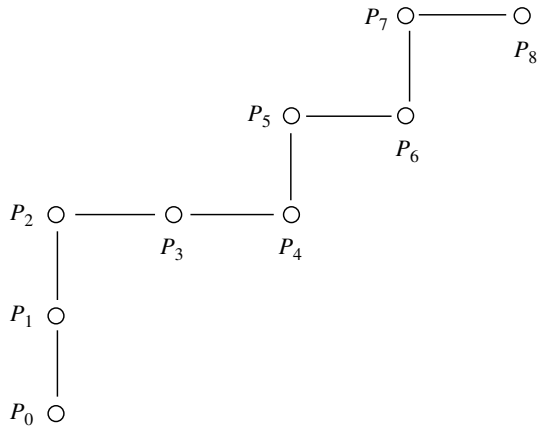


Figure 1.2.5

(a) Illustrate $E = \{2, 4, 6, 8\}$ when $n = 8$.

(b) Illustrate $E = \{2, 4, 6, 8\}$ when $n = 9$.

(c) Illustrate $D = \{1, 3, 5, 7\}$ when $n = 8$.

(d) Show that $P_n = (r, n - r)$ when S is an r-element set.

(e) A *lattice path* of *length* n in the xy-plane begins at the origin and consists of n unit "steps" each of which is either up or to the right. If r of the steps are to the right and $s = n - r$ of them are up, the lattice path terminates at the point (r, s). How many different lattice paths terminate at (r, s)?

16 Define $c_0 = 1$ and let c_n be the number of lattice paths of length $2n$ (Exercise 15) that terminate at (n, n) and never rise above the line $y = x$, i.e., such that $x_k \geq y_k$ for each point $P_k = (x_k, y_k)$. Show that

(a) $c_1 = 1$, $c_2 = 2$, and $c_3 = 5$.

(b) $c_{n+1} = \sum_{r=0}^{n} c_r c_{n-r}$. (*Hint:* Lattice paths "touch" the line $y = x$ for the last time at the point (n, n). Count those whose next-to-last touch is at the point (r, r)).

(c) c_n is the nth Catalan number of Exercises 13–14, $n \geq 1$.

17 Let X and Y be disjoint sets containing n and m elements, respectively. In how many different ways can an $(r + s)$-element subset Z be chosen from $X \cup Y$ if r of its elements must come from X and s of them from Y?

18 Packing for a vacation, a young man decides to take 3 long-sleeve shirts, 4 short-sleeve shirts, and 2 pairs of pants. If he owns 16 long-sleeve shirts, 20 short-sleeve shirts, and 13 pairs of pants, in how many different ways can he pack for the trip?

n \ r	0	1	2	3	4	5	6	7
0	$C(0,0)$							
1	$C(1,0)$	$C(1,1)$						
2	$C(2,0)$	$C(2,1)$	$C(2,2)$					
3	$C(3,0)$	$C(3,1)$	$C(3,2)$	$\boldsymbol{C(3,3)}$				
4	$C(4,0)$	$C(4,1)$	$\boldsymbol{C(4,2)}$	$C(4,3)$	$C(4,4)$			
5	$C(5,0)$	$\boldsymbol{C(5,1)}$	$C(5,2)$	$C(5,3)$	$C(5,4)$	$C(5,5)$		
6	$\boldsymbol{C(6,0)}$	$C(6,1)$	$C(6,2)$	$C(6,3)$	$C(6,4)$	$C(6,5)$	$C(6,6)$	
7	$C(7,0)$	$C(7,1)$	$C(7,2)$	$C(7,3)$	$C(7,4)$	$C(7,5)$	$C(7,6)$	$C(7,7)$
				$\cdots$				

Figure 1.2.6

19 Suppose n is a positive integer and let $k = \lfloor n/2 \rfloor$, the greatest integer not larger than $n/2$. Define

$$F_n = C(n,0) + C(n-1,1) + C(n-2,2) + \cdots + C(n-k,k).$$

Starting with $n = 0$, the sequence $\{F_n\}$ is

$$1, 1, 2, 3, 5, 8, 13, \ldots,$$

where, e.g., the $7th$ number in the sequence, $F_6 = 13$, is computed by summing the **boldface** numbers in Fig. 1.2.6.*

(a) Compute F_7 directly from the definition.

(b) Prove the recurrence $F_{n+2} = F_{n+1} + F_n$, $n \geq 0$.

(c) Compute F_7 using part (b) and the initial fragment of the sequence given above.

(d) Prove that $\sum_{i=0}^{n} F_i = F_{n+2} - 1$.

20 C. A. Tovey used the Fibonacci sequence (Exercise 19) to prove that infinitely many pairs (n,k) solve the equation $C(n,k) = C(n-1,k+1)$. The first pair is $C(2,0) = C(1,1)$. Find the second. (*Hint*: $n < 20$. Your solution need not make use of the Fibonacci sequence.)

21 The Buda side of the Danube is hilly and suburban while the Pest side is flat and urban. In short, Budapest is a divided city. Following the creation of a new commission on culture, suppose 6 candidates from Pest and 4 from Buda volunteer to serve. In how many ways can the mayor choose a 5-member commission.

*It was the French number theorist François Édouard Anatole Lucas (1842–1891) who named these numbers after Leonardo of Pisa (ca. 1180–1250), a man also known as Fibonacci.

(a) from the 10 candidates?

(b) if proportional representation dictates that 3 members come from Pest and 2 from Buda?

22 H. B. Mann and D. Shanks discovered a criterion for primality in terms of Pascal's triangle: Shift each of the $n + 1$ entries in row n to the right so that they begin in column $2n$. Circle the entries in row n that are multiples of n. Then r is prime if and only if all the entries in column r have been circled. Columns 0–11 are shown in Fig. 1.2.7. Continue the figure down to row 9 and out to column 20.

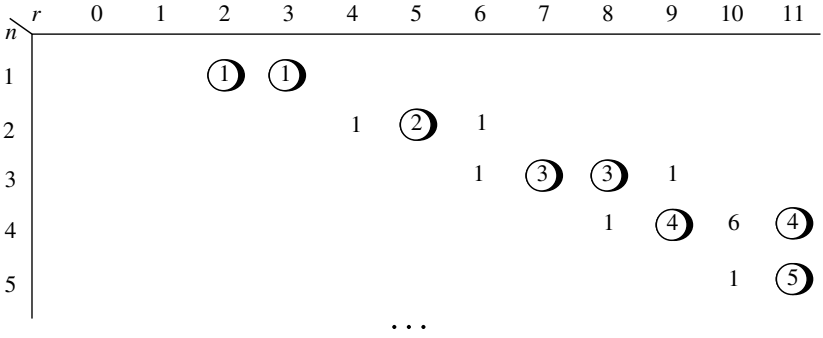


Figure 1.2.7

23 The superintendent of the Hardluck Elementary School District suggests that the Board of Education meet a \$5 million budget deficit by raising average class sizes, from 30 to 36 students, a 20% increase. A district teacher objects, pointing out that if the proposal is adopted, the potential for a *pair* of classmates to get into trouble will increase by 45%. What is the teacher talking about?

24 Strictly speaking, Theorem 1.2.6 establishes only half of the unimodality property. Prove the other half.

25 If n and r are nonnegative integers and x is an indeterminate, define $K(n, r) = (1 + x)^n x^r$.

(a) Show that $K(n + 1, r) = K(n, r) + K(n, r + 1)$.

(b) Compare and contrast the identity in part (a) with Pascal's relation.

(c) Since part (a) is a polynomial identity, it holds when numbers are substituted for x. Let $k(n, r)$ be the value of $K(n, r)$ when $x = 2$ and exhibit the numbers $k(n, r)$, $0 \leq n$, $r \leq 4$, in a 5×5 array, the rows of which are indexed by n and the columns by r. (*Hint:* Visually confirm that $k(n + 1, r) = k(n, r) + k(n, r + 1)$, $0 \leq n$, $r \leq 3$.)

26 Let S be an n-element set, where $n \geq 1$. If A is a subset of S, denote by $o(A)$ the *cardinality* of (number of elements in) A. Say that A is odd (even) if $o(A)$ is odd (even). Prove that the number of odd subsets of S is equal to the number of its even subsets.

27 Show that there are exactly seven different ways to factor $n = 63{,}000$ as a product of two relatively prime integers, each greater than one.

28 Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes. Prove that there are exactly $2^{r-1} - 1$ different ways to factor n as a product of two relatively prime integers, each greater than one.

*1.3. ELEMENTARY PROBABILITY

> The theory of probabilities is basically only common sense reduced to calculation; it makes us appreciate with precision what reasonable minds feel by a kind of instinct, often being unable to account for it. ... It is remarkable that [this] science, which began with the consideration of games of chance, should have become the most important object of human knowledge.
>
> — Pierre Simon, Marquis de Laplace (1749–1827)

Elementary probability theory begins with the consideration of D equally likely "events" (or "outcomes"). If N of these are "noteworthy", then the probability of a noteworthy event is the fraction N/D. Maybe a brown paper bag contains a dozen jelly beans, say, 1 red, 2 orange, 2 blue, 3 green, and 4 purple. If a jelly bean is chosen at random from the bag, the probability that it will be blue is $\frac{2}{12} = \frac{1}{6}$; the probability that it will be green is $\frac{3}{12} = \frac{1}{4}$; the probability that it will be blue or green is $(2+3)/12 = \frac{5}{12}$; and the probability that it will be blue and green is $\frac{0}{12} = 0$.

Dice are commonly associated with games of chance. In a dice game, one is typically interested only in the numbers that rise to the top. If a single die is rolled, there are just six outcomes; if the die is "fair", each of them is equally likely. In computing the probability, say, of rolling a number greater than 4 with a single fair die, the denominator is $D = 6$. Since there are $N = 2$ noteworthy outcomes, namely 5 and 6, the probability we want is $P = \frac{2}{6} = \frac{1}{3}$.

The situation is more complicated when two dice are rolled. If all we care about is their sum, then there are 11 possible outcomes, anything from 2 to 12. But, the probability of rolling a sum, say, of 7 is not $\frac{1}{11}$ because these 11 outcomes are not equally likely. To help facilitate the discussion, assume that one of the dice is green and the other is red. Each time the dice are rolled, Lady Luck makes two decisions, choosing a number for the green die, and one for the red. Since there are 6 choices for each of them, the two decisions can be made in any one of $6^2 = 36$ ways. If both dice are fair, then *each of these* 36 *outcomes is equally likely.* Glancing at Fig. 1.3.1,

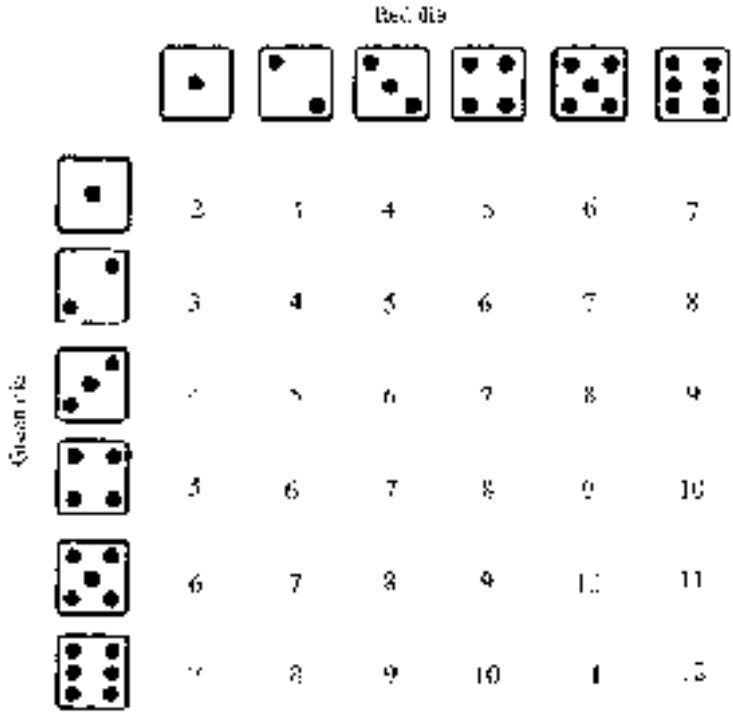


Figure 1.3.1. The 36 outcomes of rolling two dice.

one sees that there are six ways the dice can sum to 7, namely, a green 1 and a red 6, a green 2 and a red 5, a green 3 and a red 4, and so on. So, the probability of rolling a (sum of) 7 is not $\frac{1}{11}$ but $\frac{6}{36} = \frac{1}{6}$.

1.3.1 Example. Denote by $P(n)$ the probability of rolling (a sum of) n with two fair dice. Using Fig. 1.3.1, it is easy to see that $P(2) = \frac{1}{36} = P(12)$, $P(3) = \frac{2}{36} = \frac{1}{18} = P(11)$, $P(4) = \frac{3}{36} = \frac{1}{12} = P(10)$, and so on. What about $P(1)$? Since 1 is not among the outcomes, $P(1) = \frac{0}{36} = 0$. In fact, if P is some probability (any probability at all), then $0 \leq P \leq 1$. □

1.3.2 Example. A popular game at charity fundraisers is Chuck-a-Luck. The apparatus for the game consists of three dice housed in an hourglass-shaped cage. Once the patrons have placed their bets, the operator turns the cage and the dice roll to the bottom. If none of the dice comes up 1, the bets are lost. Otherwise, the operator matches, doubles, or triples each wager depending on the number of "aces" (1's) showing on the three dice.

Let's compute probabilities for various numbers of 1's. By the fundamental counting principle, there are $6^3 = 216$ possible outcomes (all of which are equally

Number of 1's	0	1	2	3
Probability	$\frac{125}{216}$	$\frac{75}{216}$	$\frac{15}{216}$	$\frac{1}{216}$

Figure 1.3.2. Chuck-a-Luck probabilities.

likely if the dice are fair). Of these 216 outcomes, only one consists of three 1's. Thus, the probability that the bets will have to be tripled is $\frac{1}{216}$.

In how many ways can two 1's come up? Think of it as a sequence of two decisions. The first is which die should produce a number different from 1. The second is what number should appear on that die. There are three choices for the first decision and five for the second. So, there are $3 \times 5 = 15$ ways for the three dice to produce exactly two 1's. The probability that the bets will have to be doubled is $\frac{15}{216}$.

What about a single ace? This case can be approached as a sequence of three decisions. Decision 1 is which die should produce the 1 (three choices). The second decision is what number should appear on the second die (five choices, anything but 1). The third decision is the number on the third die (also five choices). Evidently, there are $3 \times 5 \times 5 = 75$ ways to get exactly one ace. So far, we have accounted for $1 + 15 + 75 = 91$ of the 216 possible outcomes. (In other words, the probability of getting *at least* one ace is $\frac{91}{216}$.) In the remaining $216 - 91 = 125$ outcomes, three are no 1's at all. These results are tabulated in Fig. 1.3.2. □

Some things, like determining which team kicks off to start a football game, are decided by tossing a coin. A fair coin is one in which each of the two possible outcomes, heads or tails, is equally likely. When a fair coin is tossed, the probability that it will come up heads is $\frac{1}{2}$.

Suppose four (fair) coins are tossed. What is the probability that half of them will be heads and half tails? Is it obvious that the answer is $\frac{3}{8}$? Once again, Lady Luck has a sequence of decisions to make, this time four of them. Since there are two choices for each decision, $D = 2^4$. With the noteworthies in **boldface**, these 16 outcomes are arrayed in Fig. 1.3.3. By inspection, $N = 6$, so the probability we seek is $\frac{6}{16} = \frac{3}{8}$.

HHHH	HTHH	THHH	**TTHH**
HHHT	**HTHT**	**THHT**	TTHT
HHTH	**HTTH**	**THTH**	TTTH
HHTT	HTTT	THTT	TTTT

Figure 1.3.3

1.3.3 Example. If 10 (fair) coins are tossed, what is the probability that half of them will be heads and half tails? Ten decisions, each with two choices, yields $D = 2^{10} = 1024$. To compute the numerator, imagine a systematic list analogous to Fig. 1.3.3. In the case of 10 coins, the noteworthy outcomes correspond to

10-letter "words" with five H's and five T's, so $N = \binom{10}{5,5} = C(10,5) = 252$, and the desired probability is $\frac{252}{1024} \doteq 0.246$. More generally, if n coins are tossed, the probability that exactly r of them will come up heads is $C(n,r)/2^n$.

What about the probability that *at most* r of them will come up heads? That's easy enough: $P = N/2^n$, where $N = N(n,r) = C(n,0) + C(n,1) + \cdots + C(n,r)$ is the number of n-letter words that can be assembled from the alphabet $\{H,T\}$ and that contain at most r H's. □

Here is a different kind of problem: Suppose two fair coins are tossed, say a dime and a quarter. If you are told (only) that one of them is heads, what is the probability that the other one is also heads? (Don't just guess, think about it.)

May we assume, without loss of generality, that the dime is heads? If so, because the quarter has a head of its own, so to speak, the answer should be $\frac{1}{2}$. To see why this is wrong, consider the equally likely outcomes when two fair coins are tossed, namely, HH, HT, TH, and TT. If all we know is that one (at least) of the coins is heads, then TT is eliminated. Since the remaining three possibilities are still equally likely, $D = 3$, and the answer is $\frac{1}{3}$.

There are two "morals" here. One is that the most reliable guide to navigating probability theory is *equal likelihood*. The other is that finding a correct answer often depends on having a precise understanding of the question, and that requires precise language.

1.3.4 Definition. A nonempty finite set E of equally likely outcomes is called a *sample space*. The number of elements in E is denoted $o(E)$. For any subset A of E, the probability of A is $P(A) = o(A)/o(E)$. If B is a subset of E, then $P(A \text{ or } B) = P(A \cup B)$, and $P(A \text{ and } B) = P(A \cap B)$.

In mathematical writing, an unqualified "or" is inclusive, as in "A or B or both".*

1.3.5 Theorem. *Let E be a fixed but arbitrary sample space. If A and B are subsets of E, then*

$$P(A \text{ or } B) = P(A) + P(B) - P(A \text{ and } B).$$

Proof. The sum $o(A) + o(B)$ counts all the elements of A and all the elements of B. It even counts some elements twice, namely those in $A \cap B$. Subtracting $o(A \cap B)$ compensates for this double counting and yields

$$o(A \cup B) = o(A) + o(B) - o(A \cap B).$$

(Notice that this formula generalizes the second counting principle; it is a special case of the even more general principle of inclusion and exclusion, to be discussed in Chapter 2.) It remains to divide both sides by $o(E)$ and use Definition 1.3.4.

■

*The exclusive "or" can be expressed using phrases like "either A or B" or "A or B but not both".

1.3.6 Corollary. *Let E be a fixed but arbitrary sample space. If A and B are subsets of E, then $P(A \text{ or } B) \leq P(A) + P(B)$ with equality if and only if A and B are disjoint.*

Proof. $P(A \text{ and } B) = 0$ if and only if $o(A \cap B) = 0$ if and only if $A \cap B = \varnothing$. ■

A special case of this corollary involves the *complement*, $A^c = \{x \in E : x \notin A\}$. Since $A \cup A^c = E$ and $A \cap A^c = \varnothing$, $o(A) + o(A^c) = o(E)$. Dividing both sides of this equation by $o(E)$ yields the useful identity

$$P(A) + P(A^c) = 1.$$

1.3.7 Example. Suppose two fair dice are rolled, say a red one and a green one. What is the probability of rolling a 3 on the red die, call it a red 3, or a green 2? Let's abbreviate by setting $R3 = \text{red } 3$ and $G2 = \text{green } 2$ so that, e.g., $P(R3) = \frac{1}{6} = P(G2)$.

Solution 1: When both dice are rolled, only one of the $6^2 = 36$ equally likely outcomes corresponds to $R3$ and $G2$, so $P(R3 \text{ and } G2) = \frac{1}{36}$. Thus, by Theorem 1.3.5,

$$\begin{aligned} P(R3 \text{ or } G2) &= P(R3) + P(G2) - P(R3 \text{ and } G2) \\ &= \tfrac{1}{6} + \tfrac{1}{6} - \tfrac{1}{36} \\ &= \tfrac{11}{36}. \end{aligned}$$

Solution 2: Let P_c be the complementary probability that neither $R3$ nor $G2$ occurs. Then $P_c = N/D$, where $D = 36$. The evaluation of N can be viewed in terms of a sequence of two decisions. There are five choices for the "red" decision, anything but number 3, and five for the "green" one, anything but number 2. Hence, $N = 5 \times 5 = 25$, and $P_c = \frac{25}{36}$, so the probability we want is

$$P(R3 \text{ or } G2) = 1 - P_c = \tfrac{11}{36}.$$

□

1.3.8 Example. Suppose a single (fair) die is rolled twice. What is the probability that the first roll is a 3 or the second roll is a 2? Solution: $\frac{11}{36}$. This problem is equivalent to the one in Example 1.3.7. □

1.3.9 Example. Suppose a single (fair) die is rolled twice. What is the probability of getting a 3 or a 2?

Solution 1: Of the $6 \times 6 = 36$ equally likely outcomes, $4 \times 4 = 16$ involve neither a 3 nor a 2. The complementary probability is $P(2 \text{ or } 3) = 1 - \frac{16}{36} = \frac{5}{9}$.

Solution 2: There are two ways to roll a 3 *and* a 2; either the 3 comes first followed by the 2 or the other way around. So, $P(3 \text{ and } 2) = \frac{2}{36} = \frac{1}{18}$. Using Theorem 1.3.5, $P(3 \text{ or } 2) = \frac{1}{6} + \frac{1}{6} - \frac{1}{18} = \frac{5}{18}$.

Whoops! Since $\frac{5}{9} \neq \frac{5}{18}$, one (at least) of these "solutions" is incorrect. The probability computed in solution 1 is greater than $\frac{1}{2}$, which *seems* too large. On the other hand, it is not hard to spot an error in solution 2, namely, the incorrect application of Theorem 1.3.5. The calculation $P(3) = \frac{1}{6}$ would be valid had the die been rolled only *once*. For this problem, the correct interpretation of $P(3)$ is the probability that the first roll is 3 or the second roll is 3. That should be identical to the probability determined in Example 1.3.8. (Why?) Using the (correct) values $P(3) = P(2) = \frac{11}{36}$ in solution 2, we obtain $P(2 \text{ or } 3) = \frac{11}{36} + \frac{11}{36} - \frac{1}{18} = \frac{5}{9}$.

The next time you get a chance, roll a couple of dice and see if you can avoid both 2's and 3's more than 44 times out of 99. □

Another approach to $P(A \text{ and } B)$ emerges from the notion of "conditional probability".

1.3.10 Definition. Let E be a fixed but arbitrary sample space. If A and B are subsets of E, the *conditional probability*

$$P(B|A) = \begin{cases} P(B) & \text{if } A = \varnothing, \\ o(A \cap B)/o(A) & \text{otherwise.} \end{cases}$$

When A is not empty, $P(B|A)$ may be viewed as the probability of B given that A is certain (e.g., known already to have occurred). The problem of tossing two fair coins, a dime and a quarter, involved conditional probabilities. If h and t represent heads and tails, respectively, for the dime and H and T for the quarter, then the sample space $E = \{hH, hT, tH, tT\}$. If $A = \{hH, hT, tH\}$ and $B = \{hH\}$, then $P(B|A) = \frac{1}{3}$ is the probability that both coins are heads given that one of them is. If $C = \{hH, hT\}$, then $P(B|C) = \frac{1}{2}$ is the probability that both coins are heads given that the dime is.

1.3.11 Theorem. *Let E be a fixed but arbitrary sample space. If A and B are subsets of E, then*

$$P(A \text{ and } B) = P(A)P(B|A).$$

Proof. Let $D = o(E)$, $a = o(A)$, and $N = o(A \cap B)$. If $a = 0$, there is nothing to prove. Otherwise, $P(A) = a/D$, $P(B|A) = N/a$, and $P(A)P(B|A) = (a/D)(N/a) = N/D = P(A \text{ and } B)$. ■

1.3.12 Corollary (Bayes's* First Rule). *Let E be a fixed but arbitrary sample space. If A and B are subsets of E, then $P(A)P(B|A) = P(B)P(A|B)$.*

Proof. Because $P(A \text{ and } B) = P(B \text{ and } A)$, the result is immediate from Theorem 1.3.11. ■

1.3.13 Definition. Suppose E is a fixed but arbitrary sample space. Let A and B be subsets of E. If $P(B|A) = P(B)$, then A and B are *independent*.

Definitions like this one are meant to associate a name with a phenomenon. In particular, Definition 1.3.13 is to be understood in the sense that A and B are independent if *and only if* $P(B|A) = P(B)$. (In statements of theorems, on the other hand, "if" should never be interpreted to mean "if and only if".)

In plain English, A and B are independent if $A = \varnothing$ or if $A \neq \varnothing$ and the probability of B is the same whether A is known to have occurred or not. It follows from Corollary 1.3.12 (and the definition) that $P(B|A) = P(B)$ if and only if $P(A|B) = P(A)$, i.e., A and B are independent if and only if B and A are independent. A combination of Definition 1.3.13 and Theorem 1.3.11 yields

$$P(A \text{ and } B) = P(A)P(B) \tag{1.3}$$

if and only if A and B are independent.

Equation (1.3) is analogous to the case of equality in Corollary 1.3.6, i.e., that

$$P(A \text{ or } B) = P(A) + P(B) \tag{1.4}$$

if and only if A and B are disjoint. Let's compare and contrast the words *independent* and *disjoint*.

1.3.14 Example. Suppose a card is drawn from a standard 52-card deck. Let K represent the outcome that the card is a king and C the outcome that it is a club.[†] Because $P(C) = \frac{13}{52} = \frac{1}{4} = P(C|K)$, these outcomes are independent and, as expected,

$$\begin{aligned} P(K)P(C) &= \left(\tfrac{1}{13}\right)\left(\tfrac{1}{4}\right) \\ &= \tfrac{1}{52} \\ &= P(\text{king of clubs}) \\ &= P(K \text{ and } C). \end{aligned}$$

Because $K \cap C = \{\text{king of clubs}\} \neq \varnothing$, K and C are not disjoint. As expected, $P(K \text{ or } C) = \frac{16}{52}$ differs from $P(K) + P(C) = \frac{4}{52} + \frac{13}{52} = \frac{17}{52}$ by $\frac{1}{52} = P(K \text{ and } C)$.

If Q is the outcome that the card is a queen, then K and Q are disjoint but not independent. In particular, $P(K \text{ or } Q) = \frac{8}{52} = P(K) + P(Q)$, but $P(Q) = \frac{4}{52} = \frac{1}{13}$ while $P(Q|K) = 0$.

[*] Thomas Bayes (1702–1761), an English mathematician and clergyman, was among those who defended Newton's calculus against the philosophical attack of Bishop Berkeley. He is better known, however, for his *Essay Towards Solving a Problem in the Doctrine of Chances*.

[†] Alternatively, let E be the set of all 52 cards, K the four-element subset of kings, and C the subset of all 13 clubs.

Finally, let F be the outcome that the chosen card is a "face card" (a king, queen, or jack). Because $K \cap F = K \neq \varnothing$, outcomes K and F are not disjoint. Since $P(F) = \frac{12}{52} = \frac{3}{13}$ while $P(F|K) = 1$, neither are they independent. □

1.3.15 Example. Imagine two copy editors independently proofreading the same manuscript. Suppose editor X finds x typographical errors while editor Y finds y. Denote by z the number of typos discovered by both editors so that, together, they identify a total of $x + y - z$ errors. George Pólya showed* how this information can be used to estimate the number of typographical errors overlooked by both editors! If the manuscript contains a total of t typos, then the empirical probability that editor X discovered (some randomly chosen) one of them is $P(X) = x/t$. If, on the other hand, one of the errors discovered by Y is chosen at random, the empirical probability that X found it is $P(X|Y) = z/y$. If X is a consistent, experienced worker, these two "productivity ratings" should be about the same. Setting $z/y \doteq x/t$ (i.e., assuming $P(X|Y) \doteq P(X)$) yields $t \doteq xy/z$. □

1.3.16 Example. In the popular game *Yahtzee*, five dice are rolled in hopes of obtaining various outcomes. Suppose you needed to roll three 4's to win the game. What is the probability of rolling exactly three 4's in a single throw of the five dice?

Solution: There are $C(5,3) = 10$ ways for Lady Luck to choose three dice to be the 4's, e.g., the "first" three dice might be 4's while the remaining two are not; dice 1, 2, and 5 might be 4's while dice 3 and 4 are not; and so on. Label these ten outcomes $A_1, A_2, \ldots, A_{10}$.

The computation of $P(A_1)$, say, is a classic application of Equation (1.3). The probability of rolling a 4 on one die is independent of the number rolled on any of the other dice. Since the probability that any one of the first three dice shows a 4 is $\frac{1}{6}$ and the probability that either one of the last two does not is $\frac{5}{6}$,

$$P(A_1) = \tfrac{1}{6} \times \tfrac{1}{6} \times \tfrac{1}{6} \times \tfrac{5}{6} \times \tfrac{5}{6}.$$

Similarly, $P(A_i) = \left(\frac{1}{6}\right)^3 \left(\frac{5}{6}\right)^2$, $2 \leq i \leq 10$.

If, e.g.,

$$A_1 = \{\text{dice } 1, 2, \text{ and } 3 \text{ are 4's while dice 4 and 5 are not}\}$$

and

$$A_3 = \{\text{dice } 1, 2, \text{ and } 5 \text{ are 4's while dice 3 and 4 are not}\},$$

*In a 1976 article published in the *American Mathematical Monthly.*

then the third die is a 4 in every outcome belonging to A_1 while it is anything but a 4 in each outcome of A_3, i.e., $A_1 \cap A_3 = \varnothing$. Similarly, A_i and A_j are disjoint for all $i \neq j$. Therefore, by Equation (1.4),

$$\begin{aligned} P(\text{three 4's}) &= P(A_1 \text{ or } A_2 \text{ or } \ldots \text{ or } A_{10}) \\ &= P(A_1) + P(A_2) + \cdots + P(A_{10}) \\ &= 10\left(\tfrac{1}{6}\right)^3\left(\tfrac{5}{6}\right)^2. \end{aligned}$$

So, the probability of rolling exactly three 4's in a single throw of five fair dice is

$$C(5,3)\left(\tfrac{1}{6}\right)^3\left(\tfrac{5}{6}\right)^2 = 0.032\cdots\ . \qquad \square$$

Example 1.3.16 illustrates a more general pattern. The probability of rolling exactly r 4's in a single throw of n fair dice is $C(n,r)\left(\frac{1}{6}\right)^r\left(\frac{5}{6}\right)^{n-r}$. If a single fair die is thrown n times, the probability of rolling exactly r 4's is the same: $C(n,r)\left(\frac{1}{6}\right)^r\left(\frac{5}{6}\right)^{n-r}$. A similar argument applies to n independent attempts to perform any other "trick". If the probability of a successful attempt is p, then the probability of an unsuccessful attempt is $q = 1 - p$, and the probability of being successful in exactly r of the n attempts is

$$P(r) = C(n,r)p^r q^{n-r}, \qquad 0 \leq r \leq n. \tag{1.5}$$

Equation (1.5) governs what has come to be known as a *binomial probability distribution*.

1.3. EXERCISES

1 According to an old adage, it is unsafe to eat shellfish during a month whose name does not contain the letter *R*. What is the probability that it is unsafe to eat shellfish (according to the adage) during a randomly chosen month of the year?

2 Suppose two fair dice are rolled. What is the probability that their sum is

(a) 5? **(b)** 6? **(c)** 8? **(d)** 9?

3 Suppose three fair dice are rolled. What is the probability that their sum is

(a) 5? **(b)** 9? **(c)** 12? **(d)** 15?

4 Suppose a fair coin is tossed 10 times and the result is 10 successive heads. What is the probability that heads will be the outcome the next time the coin is tossed? (If you didn't know the coin was fair, you might begin to suspect otherwise. The *chi-squared* statistic, which is beyond the scope of this book, affords a way to estimate the probability that a fair coin would produce discrepancies from expected behavior that are this bad or worse.)

5 Many game stores carry *dodecahedral* dice having 12 pentagonal faces numbered 1–12. Suppose a pair of fair dodecahedral dice are rolled. What is the probability that they will sum to

(a) 5? **(b)** 7? **(c)** 13? **(d)** 25?

6 In what fraction of six-child families are half the children girls and half boys? (Assume that boys and girls are equally likely.)

7 Suppose you learn that in a particular two-child family one (at least) of the children is a boy. What is the probability that the other child is a boy? (Assume that boys and girls are equally likely.)

8 Suppose the king and queen of hearts are shuffled together with the king and queen of spades and all four cards are placed face down on a table.

(a) If your roommate picks up two of the cards and says, "I have a king!" what is the probability that s/he has both kings? (Don't just guess. Work it out as if your life depended on getting the right answer.)

(b) If your roommate picks up two of the cards and says, "I have the king of spades", what is the probability that s/he has both kings?

9 In the Chuck-a-Luck game of Example 1.3.2, show how the fundamental counting principle can be used to enumerate the outcomes that don't contain any 1's at all.

10 Suppose that six dice are tossed. What is the probability of rolling exactly

(a) three 4's? **(b)** four 4's? **(c)** five 4's?

11 Suppose that five cards are chosen at random from a standard 52-card deck. Show that the probability they comprise a "flush" is about $\frac{1}{505}$. (A flush is a poker hand each card of which comes from the same suit.)

12 Suppose some game of chance offers the possibility of winning one of a variety of prizes. Maybe there are n prizes with values $v_1, v_2, \ldots, v_n$. If the probability of winning the ith prizes is p_i, then the *expected value* of the game is

$$\sum_{i=1}^{n} v_i P_i.$$

Consider, e.g., a version of Chuck-a-Luck in which, on any given turn, you win \$1 for each ace.

(a) Show that the expected value of this game is 50 cents. (*Hint:* Figure 1.3.2.)

(b) What is the maximum amount anyone should be willing to pay for the privilege of playing this version each time the cage is turned?

(c) What is the maximum amount anyone should be willing to wager on this version each time the cage is turned? (The difference between "paying for the privilege of playing" and "wagering" is that, in the first case, your payment is lost, regardless of the outcome, whereas in the second case, you keep your wager unless the outcome is no aces at all.)

13 Does Chuck-a-Luck follow a binomial probability distribution? (Justify your answer.)

14 Suppose four fair coins are tossed. Let A be the set of outcomes in which at least two of the coins are heads, B the set in which at most two of the coins are heads, and C the set in which exactly two of the coins are heads. Compute

(a) $P(A)$. **(b)** $P(B)$. **(c)** $P(C)$.
(d) $P(A|B)$. **(d)** $P(A|C)$. **(e)** $P(A \text{ or } B)$.

15 In 1654, Antoine Gombaud, the Chevalier de Méré, played a game in which he bet that at least one 6 would result when four dice are rolled. What is the probability that de Méré won in any particular instance of this game? (Assume the dice were fair.)

16 Perhaps beause he could no longer find anyone to take his bets (see Exercise 15), the Chevalier de Méré switched to betting that, in any 24 consecutive rolls of two (fair) dice, "boxcars" (double 6's) would occur at least once. What is the probability that he won in any particular instance of this new game?

17 Suppose you toss a half-dollar coin n times. How large must n be to guarantee that your probability of getting heads at least once is better than 0.99?

18 The following problem was once posed by the diarist Samuel Pepys to Isaac Newton. "Who has the greatest chance of success: a man who throws six dice in hopes of obtaining at least one 6; a man who throws twelve dice in hopes of obtaining at least two 6's; or a man who throws eighteen dice in hopes of obtaining at least three 6's?" Compute the probability of success in each of the three cases posed by Pepys.

19 Are $P(A|B)$ and $P(B|A)$ always the same? (Justify your answer.)

20 Suppose that each of k people secretly chooses as integer between 1 and m (inclusive). Let P be the probability that some two of them choose the same number. Compute P (rounded to two decimal places) when

(a) $(m, k) = (10, 4)$ **(b)** $(m, k) = (20, 6)$ **(c)** $(m, k) = (365, 23)$

(*Hint:* Compute the complementary probability that everyone chooses different numbers.)

21 Suppose 23 people are chosen at random from a crowd. Show the probability that some two of them share the same birthday (just the day, not the day and year) is greater than $\frac{1}{2}$. (Assume that none of them was born on February 29.)

22 Let E be a fixed but arbitrary sample space. Let A and B be nonempty subsets of E. Prove that A and B cannot be both independent and disjoint.

23 The four alternate die numberings illustrated in Fig. 1.3.4 were discovered by Stanford statistician Bradley Efron. Note that when dice A and B are thrown together, die A beats (rolls a higher number than) die B with probability $\frac{2}{3}$. Compute the probability that

(a) die B beats die C.

(b) die C beats die D.

(c) die D beats die A.

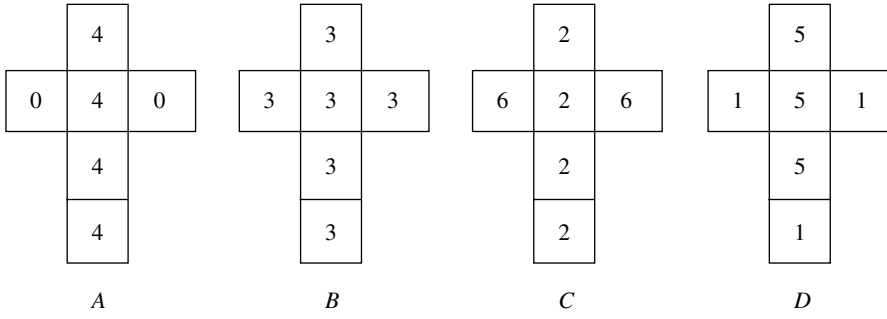


Figure 1.3.4. Efron dice.

24 One variation on the notion of a *random walk* takes place in the first quadrant of the xy-plane. Starting from the origin, the direction of each "step" is determined by the flip of a coin. If the kth coin flip is "heads", the kth step is one unit in the positive x-direction; if the coin flip is "tails", the step is one unit in the positive y-direction.

(a) Show that, after n steps, a random walker arrives at a point $P_n = (r, n - r)$, where $n \geq r \geq 0$. (*Hint:* Exercise 15, Section 1.2.)

(b) Assuming the coin is fair, compute the probability that the point $P_8 = (4, 4)$.

(c) Assuming the coin is fair, compute the probability that P_7 lies on the line $y = x$.

(d) Assuming the coin is fair, compute the probability that P_{2k} lies on the line $y = x$.

(e) Let r and n be fixed integers, $n \geq r \geq 0$. Assuming the coin comes up heads with probability p and tails with probability $q = 1 - p$, compute the probability that, after n steps, a random walker arrives at the point $P_n = (r, n - r)$.

25 Imagine having been bitten by an exotic, poisonous snake. Suppose the ER physician estimates that the probability you will die is $\frac{1}{3}$ unless you receive effective treatment immediately. At the moment, she can offer you a choice of experimental antivenins from two competing ''snake farms.'' Antivenin X has been administered to ten previous victims of the same type of snake bite and nine of them survived. Antivenin Y, on the other hand, has only been administered to four previous patients, but all of them survived. Unfortunately, mixing the two drugs in your body would create a toxic substance much deadlier than the venom from the snake. Under these circumstances, which antivenin would you choose, and why?

26 In California's *SuperLotto Plus* drawing of February 16, 2002, three winners shared a record $193 million jackpot. *SuperLotto Plus* players choose five numbers, ranging from 1 through 47 *Plus* a ''Mega'' number between 1 and 27 (inclusive). The winning numbers in the drawing of February 16 were 6, 11, 31, 32, and 39 *Plus* 20. (Order matters only to the extent that the Mega number is separate from the other five numbers.)

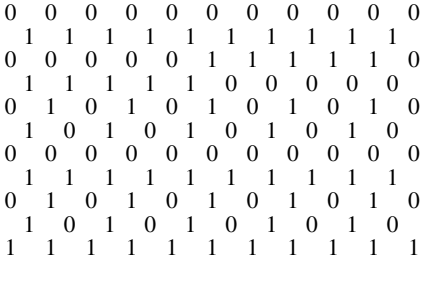
(a) Compute the probability of winning a share of the jackpot (with a single ticket).

(b) The jackpot is not the only prize awarded in the *SuperLotto* game. In the February 16 drawing, 56 tickets won $27,859 (each) by matching all five (ordinary) numbers but missing the Mega number. Compute the probability of correctly guessing all five (ordinary) numbers.

(c) Compute the probability of correctly guessing all five (ordinary) numbers and missing the Mega number.

(d) In the February 16 drawing, 496 ticket holders won $1572 (each) by correctly guessing the Mega number and four out of the other five. Compute the probability of winning this prize (with a single ticket).

*1.4. ERROR-CORRECTING CODES



The key to the connection between the combinatorial and algebraic definitions of $C(n, r) = \binom{n}{r}$ involves n-letter words constructed from two-letter alphabets. A binary code is a vocabulary comprised of such words. Binary codes have a wide

variety of applications ranging from stunning interplanetary images to everyday digital recordings. A common theme in these applications is the reliable movement of data through unreliable communication channels. The general problem is to detect and correct transmission errors that might arise from something as mundane as scratches on a CD to something as exotic as solar flares during an interplanetary voyage.

Our primary focus will be on words assembled using the alphabet $F = \{0, 1\}$, the letters of which are typically called *bits*.

1.4.1 Definition. An n-bit word is also known as a *binary word* of *length n*. The set of all 2^n binary words of length n will be denoted F^n. A *binary code* of *length n* is a nonempty subset of F^n.

A "good" code is one that can be used to transmit lots of information down a noisy channel, quickly and reliably. Consider, e.g., the code $\mathscr{C} = \{00000, 11111\} \subset F^5$, where 00000 might represent "yes" and 11111 might mean "no." Suppose one of these two codewords is sent down a noisy channel, only to have 000_0, or worse, 00010 come out the other end. While it is a binary word of length 5, 00010 is not a codeword. Thus, we *detect* an error. Just to make things interesting, suppose no further communication is possible. (Maybe the original message consisted of a single prerecorded burst.) Assuming it is more likely for any particular bit to be transmitted correctly than not, 00000 is more likely to have been the transmitted message than 11111. Thus, we might *correct* 00010 to 00000. Note that a binary word "corrected" in this way need not be correct in the sense that it was the transmitted codeword. It is just the legitimate codeword most likely to be correct.

1.4.2 Definition. Suppose b and w are binary words of length n. The *distance* between them, $d(b, w)$, is the number of places in which they differ.

Nearest-neighbor decoding refers to a process by which an erroneous binary word w is corrected to a legitimate codeword c in a way that minimizes $d(w, c)$. With the code $\mathscr{C} = \{00000, 11111\}$, it is possible to detect as many as four errors. With nearest-neighbor decoding, it is possible (correctly) to correct as many as two; $\mathscr{C}$ is a two-*error-correcting code*. (If 00000 were sent and 10101 received, nearest-neighbor decoding would produce 11111, the wrong message, Code $\mathscr{C}$ is not three-error correcting.)

1.4.3 Definition. An *r-error-correcting code* is one for which nearest-neighbor decoding reliably corrects as many as r errors.

Using the code $\mathscr{C} = \{100, 101\}$, suppose 100 is sent. If 110 is received, an error is detected. Because $d(110, 100) = 1 < 2 = d(110, 101)$ nearest-neighbor decoding corrects 110 to 100, the correct message. But, this is not enough to make $\mathscr{C}$ a one-error-correcting code. If 100 is sent and a single transmission error occurs, in the third bit, so that 101 is received, the error will not even be detected, much

less corrected. An r-error-correcting code must reliably correct r erroneous bits, no matter which r bits they happen to be.

Calling d a "distance" doesn't make it one. To be a distance , $d(b, w)$ should be zero whenever $b = w$, positive whenever $b \neq w$, symmetric in the sense that $d(b, w) = d(w, b)$ for all b and w, and it should satisfy the shortest-distance-between-two-points rule, also known as the *triangle inequality*. Of these conditions, only the last one is not obviously valid.

1.4.4 Lemma (Triangle Inequality). *If u, v, and w are fixed but arbitrary binary words of length n, then*

$$d(u, w) \leq d(u, v) + d(v, w).$$

Proof. The words u and w cannot differ from each other in a place where neither of them differs from v. Being binary words, they also cannot differ from each other in a place where both of them differ from v. It follows that $d(u, w)$ is the sum of the number of places where u differs from v but w does not, and the number of places where w differs from v but u does not. Because the first term in this sum is at most $d(u, v)$, the number of places where u differs from v, and the second is at most $d(w, v)$, the number of places where w differs from v, $d(u, w) \leq d(u, v) + d(w, v)$. ■

1.4.5 Definition. An (n, M, d) *code* consists of M binary words of length n, the minimum distance between any pair of which is d.

1.4.6 Example. The code $\{00000, 11111\}$, is evidently a (5, 2, 5) code. While it is easy to see that $n = 5$ and $M = 4$ for the code $\mathscr{C} = \{00000, 11101, 10011, 01110\}$, the value of d is less obvious. Computing the distances $d(00000, 11101) = 4$, $d(00000, 10011) = 3$, $d(00000, 01110) = 3$, $d(11101, 10011) = 3$, $d(11101, 01110) = 3$, and $d(10011, 01110) = 4$, between all $C(4, 2) = 6$ pairs of codewords, yields the minimum $d = 3$. So, $\mathscr{C}$ is a (5, 4, 3) code. □

An (n, M, d) code $\mathscr{C}$ can reliably detect as many as $d - 1$ errors. To determine how many erros $\mathscr{C}$ can reliably correct, consider the possibility that, for some erroneous binary word w, there is a tie for the codeword nearest w. Maybe $d(c, w) \geq r$ for every $c \in \mathscr{C}$, with equality for c_1 and c_2. In practice, such ties are broken by some predetermined rule. Because it can happen that this arbitrary rule dictates decoding w as c_1, even when c_2 was the transmitted codeword, no such code can *reliably* correct as many as r errors. However, by the triangle inequality, $d(c_1, w) = d(w, c_2) = r$ implies that $d(c_1, c_2) \leq 2r$, guaranteeing that no such situation can occur when $2r < d$. It seems we have proved the following.

1.4.7 Theorem. *An (n, M, d) code is r-error-correcting if and only if $2r + 1 \leq d$.*

Recall that our informal notion of a good code is one that can transmit lots of information down a noisy channel, quickly and reliably. So far, our discussion has focused on reliability. Let's talk about speed. For the sake of rapid transmission, one would like to have short words (small n) and a large vocabulary (big M). Because $M \leq 2^n$, these are conflicting requirements.

Suppose we fix n and d and ask how large M can be. The following notion is useful in addressing this question.

1.4.8 Definition. Let w be a binary word of length n. The *sphere* of *radius r centered at w* is

$$S_r(w) = \{b \in F^n : d(w, b) \leq r\},$$

the set of binary words that differ from w in at most r bits.

Because it is a sphere together with its interior, "ball" might be a more appropriate name for $S_r(w)$.

1.4.9 Example. Let $\mathscr{C}$ be a $(10, M, 7)$ code and suppose $c \in \mathscr{C}$. Because there are 10 places in which a binary word can differ from c, there must be 10 binary words that differ from c in just 1 place. Similarly, $C(10, 2) = 45$ words differ from c in exactly 2 places and $C(10, 3) = 120$ words differ from it in 3 places. Evidently, including c itself, $S_3(c)$ contains a total of

$$1 + 10 + 45 + 120 = 176$$

binary words only one of which, namely, c, is a codeword.

If c_1 and c_2 are different codewords, then $S_3(c_1) \cap S_3(c_2) \neq \varnothing$ only if there is a binary word w such that $d(w, c_1) \leq 3$ and $d(w, c_2) \leq 3$, implying that

$$\begin{aligned} d(c_1, c_2) &\leq d(c_1, w) + d(w, c_2) \\ &\leq 6 \end{aligned}$$

and contradicting our assumption that the minimum distance between codewords is 7. In other words, if $c_1 \neq c_2$, then $S_3(c_1) \cap S_3(c_2) = \varnothing$.

One might think of $S_3(c)$ as a *sphere of influence* for c. Because different spheres of influence are disjoint and since each sphere contains 176 of the 1024 binary words of length 10, there is insufficient room in F^{10} for as many as six spheres of influence. (Check it: $6 \times 176 = 1056$.) Evidently, the vocabulary of a three-error-correcting binary code of length 10 can consist of no more than five words! If $\mathscr{C}$ is a (10, M, 7) code, then $M \leq 5$. □

Example 1.4.9 has the following natural generalization.

1.4.10 Theorem (Sphere-Packing Bound). *The vocabulary of an r-error-correcting code of length n contains no more than* $2^n / N(n, r)$ *codewords, where*

$$N(n, r) = C(n, 0) + C(n, 1) + \cdots + C(n, r).$$

Proof. Suppose $\mathscr{C} = \{c_1, c_2, \ldots, c_M\} \subset F^n$ is an r-error-correcting code. Let $S_r(c_i)$ be the sphere of influence centered at codeword c_i, $1 \leq i \leq M$. Since spheres corresponding to different codewords are disjoint and $o(S_r(c_i)) = N(n, r)$, $1 \leq i \leq M$, the number of different binary words of length n contained in the union of the M spheres is $M \times N(n, r)$, a number that cannot exceed the total number of binary words of length n. ■

1.4.11 Example. Suppose you were asked to design a three-error-correcting code capable of sending the four messages NORTH, EAST, WEST, or SOUTH. Among the easiest solutions is the (16, 4, 8) code

$$\{0000000000000000, 1111111100000000, 1111000011110000, 1111000000001111\}.$$

However, if speed (or professional pride) is an issue, you might want to hold this one in reserve and look for something better.

For a solution to be optmal, it should (at the very least) be an $(n, 4, 7)$ code with n as small as possible. According to Example 1.4.9, a three-error-correcting code of length 10 can have at most five codewords, which would be ample for our needs. Moreover, because $4 \times N(9, 3) = 4 \times (1 + 9 + 36 + 84) = 520 > 2^9$, there can be no (9, 4, 7) codes. So, the best we can hope to achieve is a (10, 4, 7) code.

Without loss of generality, we can choose $c_1 = 0000000000$. (Why?) Since it must differ from c_1 in (no fewer than) 7 places, we may as well let $c_2 = 1111111000$. To differ from c_1 in 7 places, c_3 must contain 7 (or more) 1's. But, c_3 can differ from c_2 in 7 places only if (at least) four of its first seven bits are 0's! It is, of course, asking too much of a 10-bit word that it contain at least four 0's and at least seven 1's. The same problem arises no matter which seven bits are set equal to 1 in c_2, and setting more than seven bits equal to 1 only makes matters worse! It seems there do not exist even three binary words of length 10 each differing from the other two in (at least) seven bits. (Evidently, the sphere-packing bound is not always attainable!)

If there are no (10, 3, 7) codes, there certainly cannot be any (10, 4, 7) codes. What about an (11, 4, 7) code? This time, the obvious choices, $c_1 = 00000000000$ and $c_2 = 11111110000$, leave room for $c_3 = 00001111111$, which differs from c_2 in eight places and from c_1 in seven. Because $c_4 = 11110001111$ differs from c_2 and c_3 in seven places and from c_1 in eight, $\mathscr{C} = \{c_1, c_2, c_3, c_4\}$ is an (11, 4, 7) code. □

Our discovery, in Example 1.4.11, that $M \leq 2$ in any $(10, M, 7)$ code is a little surprising. Because a sphere of radius 3 in F^{10} holds (only) 176 words, two nonoverlapping spheres contain little more than a third of the 1024 words in F^{10}! On the other hand, how many solid Euclidean balls of radius 3 will fit inside a Euclidean cube of volume 1024?*

*Even in the familiar world of three-dimensional Euclidean space, sphere-packing problems can be highly nontrivial. On the other hand, in at least one sense, packing Euclidean spheres in three-space is a bad analogy. Orange growers are interested in sphere packing because, without damaging the produce, they want to minimize the fraction of empty space in each "full" box of oranges. Apart from degenerate cases, equality is *never* achievable in the grower's version of the sphere-packing bound.

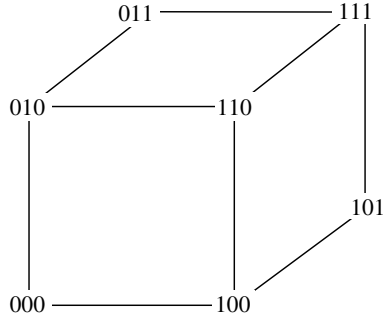


Figure 1.4.1. Three-dimensional binary space.

1.4.12 Example. As illustrated in Fig. 1.4.1, three-dimensional binary space F^3 is comparable, not to a Euclidean cube, but to the set consisting of its eight vertices! While packing the Euclidean cube with Euclidean spheres always results in "left-over" Euclidean points, F^3 is easily seen* to be the disjoint union of the spheres $S_1(000) = \{000, 100, 010, 001\}$ and $S_1(111) = \{111, 011, 101, 110\}$. (Note the two different ways in which $S_1(111)$ is "complementary" to $S_1(000)$.) □

1.4.13 Definition. An (n, M, d) code is *perfect* if $2^n = M \times [C(n, 0) + C(n, 1) + \cdots + C(n, r)]$, where $r = \lfloor (d-1)/2 \rfloor$ is the greatest integer not exceeding $(d-1)/2$.

So, an r-error-correcting code $\mathscr{C}$ is perfect if and only if its vocabulary achieves the sphere-packing bound, if and only if F^n is the disjoint union of the spheres $S_r(c)$ as c ranges over $\mathscr{C}$, if and only if every binary word of length n belongs to the sphere of influence of some (unique) codeword. In particular, a perfect code is as *efficient* as it is possible for codes to be.

It follows from Definition 1.4.13 that F^n, itself, is perfect. It is the disjoint union of the (degenerate) spheres $S_0(b)$, $b \in F^n$. Such trivial examples are uninteresting for a number of reasons, not the least of which is that F^n cannot detect, much less correct, even a single error. A nontrivial perfect code emerges from Example 1.4.12, namely, the one-error-correcting $(3, 2, 3)$ code $\{000, 111\}$. Might this be the only nontrivial example? No, $\{100, 011\}$ is another. All right, might the only nontrivial examples have parameters $(3, 2, 3)$?

1.4.14 Lemma. *Suppose $\mathscr{C}$ is an (n, M, d) code for which $r = \lfloor (d-1)/2 \rfloor = 1$. Then $\mathscr{C}$ is perfect if and only if there exists an integer $m \geq 2$ such that $n = 2^m - 1$ and $M = 2^{n-m}$.*

Proof. If $\mathscr{C}$ is perfect, then $2^n = M \times N(n, 1) = M(1 + n)$, so that $M = 2^n/(1 + n)$. Now, $1 + n$ exactly divides 2^n only if $1 + n = 2^m$ for some positive integer

*Because one vertex is hidden from view, "seen" may not be the most appropriate word to use here.

$m \leq n$, in which case $M = 2^n/2^m = 2^{n-m}$. Moreover, $2^m - 1 = n \geq d \geq 3$ implies $m \geq 2$.

Conversely, if $n = 2^m - 1$ and $M = 2^{n-m}$, then $M(1+n) = 2^{n-m} \times 2^m = 2^n$. ■

1.4.15 Example. The parameters of the perfect (3, 2, 3) code $\mathscr{C} = \{000, 111\}$ satisfy the conditions of Lemma 1.4.14 when $m = 2$.

Setting $d = 3$ and $m = 3$ in Lemma 1.4.14 shows that every (7, 16, 3) code is perfect. What it does not show is the existence of even one (7, 16, 3) code! However, as the reader may confirm, (7, 16, 3) is the triple of parameters for the so-called *Hamming code* $\mathscr{H}_3 = \{0000000, 1000011, 0100101, 0010110, 0001111, 1100110, 1010101, 1001100, 0110011, 0101010, 0011001, 0111100, 1011010, 1101001, 1110000, 1111111\}$. In Chapter 6, the existence of an $(n, M, 3)$ code that satisfies the conditions of Lemma 1.4.14 will be established for every $m \geq 4$. □

1.4. EXERCISES

1 What is the largest possible value for M in any $(8, M, 1)$ code?

2 How many errors can an $(n, M, 8)$ code

(a) detect? **(b)** correct?

3 Find the parameters (n, M, d) for the binary code

(a) $\mathscr{C}_1 = \{000, 011, 101, 110\}$.

(b) $\mathscr{C}_2 = \{000, 011, 101, 110, 111, 100, 010, 001\}$.

(c) $\mathscr{C}_3 = \{0000, 0110, 1010, 1100, 1111, 1001, 0101, 0011\}$.

(d) $\mathscr{C}_4 = \{11000, 00011, 00101, 00110, 01001, 01010, 01100, 10001, 10010, 10100\}$, (Compare $\mathscr{C}_4$ with the POSTNET barcodes of Fig. 1.1.3.)

4 Construct a code (or explain why none exists) with parameters

(a) (3, 4, 2). **(b)** (6, 4, 4). **(c)** (12, 4, 8).

(d) (4, 7, 2). **(e)** (8, 7, 4). **(f)** (8, 8, 4).

5 The *American Standard Code for Information Interchange* (ASCII) is a scheme for assigning numerical values from 0 through 255 to selected symbols. For example, the uppercase letters of the English alphabet correspond to 65 through 90, respectively. Why 256 symbols? Good question. The answer involves bits and bytes. Consisting of two four-bit ''zones'', a *byte* can store any binary numeral in the range 0 through 255.

Apart from representing binary numerals, bytes can also be viewed as codewords in $\mathscr{C} = F^8$. Because it corresponds to the base-2 numeral for 65, the codeword/byte 01000001 represents *A* (in the ASCII scheme). Similarly, *Z*, corresponding to 90, is represented by the codeword/byte 01011010.

(a) What is the ASCII number for the letter *S*?

(b) What byte represents *S*?

(c) What letter corresponds to ASCII number 76?

(d) What letter is represented by codeword/byte 01010101?

(e) The ASCII number for the square-root symbol is 251. What codeword/byte represents $\surd$?

(f) Decode the message 01001101-01000001-01010100-01001000.

6 The *complement* of a binary word b is the word b^* obtained from b by changing all if its zeros to ones and all of its ones to zeros. For any binary code $\mathscr{C}$, define $\mathscr{C}^* = \{c^* : c \in \mathscr{C}\}$.

(a) Show that $\mathscr{C}_2 = \mathscr{C}_1 \cup \mathscr{C}_1^*$, where $\mathscr{C}_1$ and $\mathscr{C}_2$ are the codes in Exercises 3(a) and (b), respectively.

(b) Find a code $\mathscr{C}$ of length 3 satisfying $\mathscr{C}^* = F^3 \backslash \mathscr{C}$, the set-theoretic complement of $\mathscr{C}$. (*Hint:* Example 1.4.12.)

(c) Find a code $\mathscr{C}$ of length 3 satisfying $\mathscr{C}^* = \mathscr{C}$.

(d) If $\mathscr{C}$ is an (n, M, d) code, prove or disprove that $\mathscr{C}^*$ has the same parameters.

(e) If $\mathscr{C}$ is an (n, M, d) code, prove or disprove that $F^n \backslash \mathscr{C}$ has the same parameters.

7 The *weight* of a binary word b, $\mathrm{wt}(b)$, is the number of bits of b equal to 1. A *constant-weight code* is one in which every codeword has the same weight.

(a) Show that $d \geq 2$ in any constant-weight (n, M, d) code (in which $n > 1$).

(b) Find a constant-weight $(8, M, d)$ code with $d > 2$.

(c) Find the largest possible value for M in a constant-weight (8, M, d) code.

8 Let $\mathscr{C}$ be the (8, 56, 2) code consisting of all binary words of length 8 and weight 5. (See Exercise 7.) Let $\mathscr{C}^*$ be the code consisting of the complements of the codewords of $\mathscr{C}$. (See Exercise 6.) Prove that $\mathscr{C} \cup \mathscr{C}^*$ is an (8, 112, 2) code.

9 M. Plotkin* proved that if $n < 2d$ in the (n, M, d) code $\mathscr{C}$, then $M \leq 2\lfloor d/(2d - n) \rfloor$, where $\lfloor x \rfloor$ is the greatest integer not larger that x. Does the Plotkin bound preclude the existence of

(a) (12, 52, 5) codes? **(b)** (12, 7, 7) codes?

(c) (13, 13, 7) codes? **(d)** (15, 2048, 3) codes?

(Justify your answers.)

10 Does the sphere-packing bound (Theorem 1.4.10) rule out the existence of a

(a) (12, 52, 5) code? **(b)** (12, 7, 7) code?

(c) (13, 13, 7) code? **(d)** (15, 2048, 3) code?

(Justify your answers.)

*Binary codes with specified minimum distances, *IEEE Trans. Info. Theory* 6 (1960), 445–450.

11 The purpose of this exercise is to prove the Plotkin bound from Exercise 9. Let $\mathscr{C} = \{c_1, c_2, \ldots, c_M\}$ be an (n, M, d) code where $n < 2d$. Define

$$D = \sum_{i,j=1}^{M} d(c_i, c_j).$$

(a) Prove that $D \geq M(M-1)d$.

(b) Let A be the $M \times n$ (0, 1)-matrix whose ith row consists of the bits of codeword c_i. If the kth column of A contains z_k 0's (and $M - z_k$ 1's), prove that

$$D = 2\sum_{k=1}^{n} z_k(M - z_k).$$

(c) If M is even, show that $f(z) = z(M-z)$ is maximized when $z = \frac{1}{2}M$.
(d) Prove the Plotkin bound in the case that M is even.
(e) If M is odd, show that $D \leq \frac{1}{2}n(M^2-1)$.
(f) Prove the Plotkin bound in the case that M is odd.
(g) Where is the hypothesis $n < 2d$ used in the proof?

12 The *parity* of binary word b is 0 if $\mathrm{wt}(b)$ is even and 1 if $\mathrm{wt}(b)$ is odd. (See Exercise 7.) If $b = xy\ldots z$ is a binary word of length n and parity p, denote by $b^+ = xy\ldots zp$ the binary word of length $n+1$ obtained from b by appending a new bit equal to its parity. For any binary code $\mathscr{C}$ of length n, let $\mathscr{C}^+ = \{c^+ : c \in \mathscr{C}\}$.

(a) Show that $\mathscr{C}_3 = \mathscr{C}_2^+$, where $\mathscr{C}_2$ and $\mathscr{C}_3$ are the codes from Exercises 3(b) and (c), respectively.
(b) If $\mathscr{C}$ is an (n, M, d) code, where d is odd, prove that $\mathscr{C}^+$ is an $(n+1, M, d+1)$ code.
(c) Prove that exactly half the words in F^n have parity $p = 0$.
(d) Prove or disprove that if $\mathscr{C}$ is a fixed but arbitrary binary code of length n, then exactly half the words in $\mathscr{C}$ have even weight.

13 Let $M(n, d)$ be the largest possible value of M in any (n, M, d) code. Prove that $M(n, 2r-1) = M(n+1, 2r)$.

14 If $\mathscr{C}$ is a code of length n, its "weight enumerator" is the two-variable polynomial defined by

$$W_{\mathscr{C}}(x, y) = \sum_{c \in \mathscr{C}} x^{\mathrm{wt}(c)} y^{n - \mathrm{wt}(c)},$$

where $\mathrm{wt}(c)$ is the weight of c defined in Exercise 7.

(a) Compute $W_{\mathscr{C}}(x, y)$ for each of the codes in Exercise 3.

(b) Show that $W_{\mathscr{C}}(x, y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7$ for the perfect Hamming code $\mathscr{C} = \mathscr{H}_3$ of Example 1.4.15.

(c) Two codes are *equivalent* if one can be obtained from the other by uniformly permuting (rearranging) the order of the bits in each codeword. Show that equivalent codes have the same parameters.

(d) Show that equivalent codes have the same weight enumerator.

(e) Exhibit two inequivalent codes with the same weight enumerator.

15 Exhibit the parameters for the perfect Hamming code $\mathscr{H}_4$ (corresponding to $m = 4$ in Lemma 1.4.14).

16 Show that the Plotkin bound (Exercise 9) is strong enough to preclude the existence of a (10, 3, 7) code (see Example 1.4.11).

17 Can the (11, 4, 7) code in Example 1.4.11 be extended to an (11, 5, 7) code?

18 Let u, v, and w be binary words of length n. Show that $d(u, w) = d(u, v) + d(v, w) - 2b$, where b is the number of places in which u and w both differ from v.

19 Following up on the discussion between Examples 1.4.11 and 1.4.12, show that two solid Euclidean spheres of radius 3 cannot be fit inside a cubical box of volume 1024 in such a way that both spheres touch the bottom of the box.

20 Show that the necessary condition for the existence of an r-error-correcting code given by the sphere-packing bound is not sufficient.

21 Let $M(n, d)$ be the largest possible value of M in any (n, M, d) code.

(a) If $n \geq 2$, prove that $M(n, d) \leq 2M(n - 1, d)$.

(b) Prove that $M(2d, d) \leq 4d$.

22 Show that a necessary condition for equality to hold in the Plotkin bound (Exercises 9 and 11) is $d(c_i, c_j) = d$, $i \neq j$.

23 The (7, 16, 3) code $\mathscr{H}_3$ in Example 1.4.15 is advertised as a perfect code. While it is easy to check that $\mathscr{H}_3$ is a binary code of length 7 containing 16 codewords, (given what we know now) it might take a minite or two to confirm that the minimum distance between any two codewords is 3. Assuming that has been done, how hard is it to confirm that $\mathscr{H}_3$ is a perfect code? (Justify your answer by providing the confirmation.)

24 Let $A = F^3 \backslash S_1(110)$ the (set-theoretic) complement of $S_1(110)$ in F^3.

(a) Show that A is a sphere in F^3.

(b) Do A and $S_1(110)$ exhibit both kinds of complementarity discussed in Exercise 6?

25 Prove that every (23, 4096, 7) code is perfect.

26 Construct a code with parameters (8, 16, 4).

27 Construct a code with parameters

(a) (6, 8, 3). **(b)** (7, 8, 4).

28 The purpose of this exercise is to justify nearest-neighbor decoding. We begin with some assumptions about the transmission channel. The simplest case is a so-called *symmetric* channel in which the probability of a 1 being changed to 0 is the same as that of a 0 being changed to 1. If we assume this common error probability, call it p, is the same for each bit of every word, then $q = 1 - p$ is the probability that any particular bit is transmitted correctly.

(a) Show that the probability of transmitting codeword c and receiving binary word w along such a channel is $p^r q^{n-r}$, where r is the number of places in which c and w differ.

(b) Under the assumption that $p < \frac{1}{2}$ (engineers work very hard to ensure that p is *much* less than $\frac{1}{2}$, show that the probability in part (a) is maximized when r is as small as possible.

29 Suppose the two-error-correcting code $\mathscr{C} = \{00000, 11111\}$ is used in a symmetric channel for which the probability of a transmission error in each bit is $p = 0.05$. (See exercise 28.)

(a) Show that the probability of more than two errors in the transmission of a single codeword is less than 0.0012.

(b) There may be cases in which a probability of failure as high as 0.0012 is unacceptable. What is the probability of more than three errors in the transmission of a single codeword using the same channel and the code $\{0000000, 1111111\}$?

1.5. COMBINATORIAL IDENTITIES

Poetry is the art of giving different names to the same thing.

— Anonymous

As we saw in Section1.2, $C(n, r) = \binom{n}{r}$ is the same as multinomial coefficient $\binom{n}{r, n-r}$. In fact, $C(n, r)$ is commonly called a *binomial* coefficient.* Given that binomial coefficients are special cases of multinomial coefficients, it is natural to wonder whether we still need a separate name and notation for n-choose-r. On the other hand, it turns out that multinomial coefficients can be expressed as products of binomial coefficients. Thus, one could just as well argue for discarding the multinomial coefficients!

1.5.1 Theorem. *If* $r_1 + r_2 + \cdots + r_k = n$, *then*

$$\binom{n}{r_1, r_2, \ldots, r_k} = \binom{n}{r_1}\binom{n - r_1}{r_2}\binom{n - r_1 - r_2}{r_3} \cdots \binom{n - r_1 - r_2 - \cdots - r_{k-1}}{r_k}.$$

*This name is thought to have been coined by Michael Stifel (ca. 1485–1567), among the most celebrated algebraists of the sixteenth century. Also known for numerological prophesy, Stifel predicted publicly that the world would end on October 3, 1533.

Proof. Multinomial coefficient $\binom{n}{r_1, r_2, \ldots, r_k}$ is the number of n-letter "words" that can be assembled using r_1 copies of one "letter", say A_1; r_2 copies of a second, A_2; and so on, finally using r_k copies of some kth character, A_k. The theorem is proved by counting these words another way and setting the two (different-looking) answers equal to each other.

Think of the process of writing one of the words as a sequence of k decisions. Decision 1 is which of n spaces to fill with A_1's. Because this amounts to selecting r_1 of the n available positions, it involves $C(n, r_1)$ choices. Decision 2 is which of the remaining $n - r_1$ spaces to fill with A_2's. Since there are r_2 of these characters, the second decision can be made in any one of $C(n - r_1, r_2)$ ways. Once the A_1's and A_2's have been placed, there are $n - r_1 - r_2$ positions remaining to be filled, and A_3's can be assigned to r_3 of them in $C(n - r_1 - r_2, r_3)$ ways, and so on. By the fundamental counting principle, the number of ways to make this sequence of decisions is the product

$$C(n, r_1) \times C(n - r_1, r_2) \times C(n - r_1 - r_2, r_3) \times \cdots \times C(n - r_1 - r_2 - \cdots - r_{k-1}, r_k).$$

(Because $r_1 + r_2 + \cdots + r_k = n$, the last factor in this product is $C(r_k, r_k) = 1$.) ■

It turns out that both binomial and multinomial coefficients have their unique qualities and uses. Keeping both is vastly more convenient than eliminating either.

Let's do some mathemagic. Pick a number, any number, just so long as it is an entry from Pascal's triangle. Suppose your pick happened to be $15 = C(6, 2)$. Starting with $C(2, 2)$, the first nonzero enry in column 2 (the third column of Fig. 1.5.1),

C(0,0)				
C(1,0)	C(1,1)			
C(2,0)	C(2,1)	**C(2,2)**		
		+		
C(3,0)	C(3,1)	**C(3,2)**	C(3,3)	
		+		
C(4,0)	C(4,1)	**C(4,2)**	C(4,3)	C(4,4)
		+		
C(5,0)	C(5,1)	**C(5,2)**	C(5,3)	C(5,4)
		+		
C(6,0)	C(6,1)	**C(6,2)**	C(6,3)	C(6,4)
C(7,0)	C(7,1)	C(7,2)	**C(7,3)**	C(7,4)

Figure 1.5.1

add the entries down to and including $C(6,2)$. The sum will be $C(7,3)$. Check it out:

$$\begin{aligned} C(2,2)+C(3,2)+C(4,2)+C(5,2)+C(6,2) &= 1+3+6+10+15 \\ &= 35 \\ &= C(7,3). \end{aligned}$$

The trick is an easy consequence of Pascal's relation and the fact that $C(2,2) = C(3,3)$. (See if you can reason it out before reading on.)

1.5.2 Chu's Theorem.* *If $n \geq r$, then*

$$\begin{aligned} \sum_{k=0}^{n} C(k,r) &= C(r,r)+C(r+1,r)+C(r+2,r)+\cdots+C(n,r) \\ &= C(n+1,r+1) \end{aligned}$$

(where $\sum_{k=0}^{n} C(k,r) = \sum_{k=r}^{n} C(k,r)$ because $C(k,r) = 0$, $k < r$).

Proof. Replace $C(r,r)$ with $C(r+1,r+1)$ and use Pascal's relation repeatedly to obtain

$$\begin{aligned} C(r+1,r+1)+C(r+1,r) &= C(r+2,r+1), \\ C(r+2,r+1)+C(r+2,r) &= C(r+3,r+1), \end{aligned}$$

and so on, ending with

$$C(n,r+1)+C(n,r) = C(n+1,r+1). \qquad \blacksquare$$

Chu's theorem has many interesting applications. To set the stage for one of them, we interrupt the mathematical discussion to relate a story about the young Carl Friedrich Gauss.† At the age of seven, Gauss entered St. Katharine's Volksschule in the duchy of Brunswick. One day his teacher, J. G. Büttner, assigned Gauss's class the problem of computing the sum

$$1+2+\cdots+100.$$

*Rediscovered many times, Theorem 1.5.2 can be found in Chu Shih-Chieh, *Precious Mirror of the Four Elements*, 1303.

†Gauss (1777–1855) is one of the half-dozen greatest mathematicians of the last millenium.

While his fellow pupils went right to work computing sums, Gauss merely stared at his slate and, after a few minutes, wrote

$$\frac{100 \times 101}{2} = 5050.$$

He seems to have reasoned that numbers can be added forwards or backwards,

$$\begin{aligned} 1 + \ \ 2 + \ \ 3 + \cdots + 98 + 99 + 100, \\ 100 + 99 + 98 + \cdots + \ \ 3 + \ \ 2 + \ \ \ 1, \end{aligned}$$

or even sidewards. Adding sidewards gives $1 + 100 = 101$, $2 + 99 = 101$, $3 + 98 = 101$, and so on. With each of the hundred columns adding to 101, the sum of the numbers in *both* rows, twice the total we're looking for, is 100×101.

Gauss's method can just as well be used to sum the first n positive integers:

$$\begin{aligned} 1 + 2 + \cdots + n &= \frac{n(n+1)}{2} \\ &= C(n+1, 2). \end{aligned} \tag{1.6}$$

Seeing the answer expressed as a binomial coefficient may seem a little contrived, but, with its left-hand side rewritten as $C(1,1) + C(2,1) + \cdots + C(n,1)$, Equation (1.6) is seen to be the $r = 1$ case of Chu's theorem!

There is a formula comparable to Equation (1.6) for the sum of the *squares* of the first n positive integers, namely,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}. \tag{1.7}$$

Once one has seen it (or guessed it), Equation (1.7) is easy enough to prove by induction. But, where did the formula come from in the first place? Chu's theorem! Summing both sides of

$$\begin{aligned} k^2 &= k + k(k-1) \\ &= C(k,1) + 2C(k,2), \end{aligned} \tag{1.8}$$

we obtain

$$\sum_{k=1}^{n} k^2 = \sum_{k=1}^{n} C(k,1) + 2\sum_{k=1}^{n} C(k,2).$$

Two applications of Chu's theorem (one with $r = 1$ and the other with $r = 2$) yield

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 &= C(n+1,2) + 2C(n+1,3) \\ &= \frac{(n+1)n}{2} + 2\frac{(n+1)n(n-1)}{6} \\ &= n(n+1)\left[\frac{3+2(n-1)}{6}\right] \\ &= \frac{n(n+1)(2n+1)}{6}, \end{aligned}$$

precisely Equation (1.7).

What about summing mth powers? If we just had an analog of Equation (1.8), i.e., an identity of the form

$$k^m = \sum_{r=1}^{m} a_{r,m} C(k,r) \tag{1.9}$$

(where $a_{r,m}$ is independent of k, $1 \le r \le m$), we could sum both sides and use Chu's theorem to obtain

$$\begin{aligned} \sum_{k=1}^{n} k^m &= \sum_{k=1}^{n} \sum_{r=1}^{m} a_{r,m} C(k,r) \\ &= \sum_{r=1}^{m} a_{r,m} \sum_{k=1}^{n} C(k,r) \\ &= \sum_{r=1}^{m} a_{r,m} C(n+1,r+1). \end{aligned} \tag{1.10}$$

To see what's involved when $m = 3$, consider the equation

$$\begin{aligned} k^3 &= xC(k,1) + yC(k,2) + zC(k,3) \\ &= xk + \frac{1}{2}yk(k-1) + \frac{1}{6}zk(k-1)(k-2), \end{aligned}$$

which is equivalent to

$$6k^3 = (6x - 3y + 2z)k + (3y - 3z)k^2 + zk^3.$$

(Check it.) Equating coefficients of like powers of the integer variable k yields the system of linear equations

$$\begin{aligned} 6x - 3y + 2z &= 0, \\ 3y - 3z &= 0, \\ z &= 6, \end{aligned}$$

which has the unique solution $y = z = 6$ and $x = 1$. (Confirm this too.) Therefore,

$$k^3 = C(k,1) + 6C(k,2) + 6C(k,3) \tag{1.11}$$

or, in the language of Equation (1.9), $a_{1,3} = x = 1$, $a_{2,3} = y = 6$, and $a_{3,3} = z = 6$. Together, Equations (1.9)–(1.11) yield

$$\begin{aligned} 1^3 + 2^3 + \cdots + n^3 &= C(n+1,2) + 6C(n+1,3) + 6C(n+1,4) \\ &= \frac{n^2(n+1)^2}{4}. \end{aligned}$$

(Confirm *these* computations.)

Now we know where formulas for sums of powers of positive integers come from. They are consequences of Chu's theorem as manifested in Equations (1.9)-(1.10). From a theoretical point of view, that is all very well. The disagreeable part is the prospect of having to solve a system of m equations in m unknowns in order to identify the mystery coefficients $a_{r,m}$. In fact, there is an elegant solution to this difficulty!

In the form

$$\sum_{r=1}^{m} C(k,r)a_{r,m} = k^m,$$

Equation (1.9) is reminiscent of matrix multiplication. To illustrate this perspective, let $m = 6$ and consider that portion of Pascal's triangle lying in rows and columns numbered 1–6, i.e.,

$$\begin{array}{cccccc} 1 & & & & & \\ 2 & 1 & & & & \\ 3 & 3 & 1 & & & \\ 4 & 6 & 4 & 1 & & \\ 5 & 10 & 10 & 5 & 1 & \\ 6 & 15 & 20 & 15 & 6 & 1 \end{array}$$

Filling in the zeros corresponding to $C(n,r)$, $n < r \leq 6$, we obtain the matrix

$$C_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 \\ 3 & 3 & 1 & 0 & 0 & 0 \\ 4 & 6 & 4 & 1 & 0 & 0 \\ 5 & 10 & 10 & 5 & 1 & 0 \\ 6 & 15 & 20 & 15 & 6 & 1 \end{pmatrix}.$$

Anyone familiar with determinants will see that this matrix has an inverse. It is one of the most remarkable properties of binomial coefficients that C_n^{-1} can be obtained from C_n, just by sprinkling in some minus signs, e.g.,

$$C_6^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 & 0 & 0 \\ 3 & -3 & 1 & 0 & 0 & 0 \\ -4 & 6 & -4 & 1 & 0 & 0 \\ 5 & -10 & 10 & -5 & 1 & 0 \\ -6 & 15 & -20 & 15 & -6 & 1 \end{pmatrix}.$$

(Before reading on, confirm that the product of these two matrices is the identity matrix, I_6.)

1.5.3 Definition. Let C_n be the $n \times n$ *Pascal matrix* whose (i,j)-entry is binomial coefficient $C(i,j)$, $1 \le i, j \le n$.

1.5.4 Alternating-Sign Theorem. *The Pascal matrix C_n is invertible; the (i,j)-entry of C_n^{-1} is $(-1)^{i+j}C(i,j)$.*

While it may seem a little like eating the dessert before the broccoli, let's defer the proof of the alternating-sign theorem to the end of the section and go directly to the application.

1.5.5 Theorem. *If m and r are positive integers, the coefficient of $C(k,r)$ in the equation $k^m = \sum_{r=1}^{m} a_{r,m}C(k,r)$ is given by*

$$a_{r,m} = \sum_{t=1}^{m} (-1)^{r+t} C(r,t) t^m.$$

This more-or-less explicit formula for $a_{r,m}$ eliminates the need to solve a system of equations. Put another way, Theorem 1.5.5 solves the corresponding system of m equations in m unknowns, once and for all, *for every* m.

Proof of Theorem 1.5.5. Suppose $n \ge m, r$. Let $A_n = (a_{i,j})$ be the $n \times n$ matrix of mystery coefficients (where $a_{r,m} = 0$ whenever $r > m$). Then, by Equation (1.9), the (k,m)-entry of C_nA_n is

$$\sum_{r=1}^{m} C(k,r)a_{r,m} = k^m,$$

$1 \le k, m \le n$. In other words, $C_nA_n = P_n$, where P_n is the $n \times n$ matrix whose (i,j)-entry is i^j. Thus, $A_n = C_n^{-1}P_n$, so the mystery coefficient $a_{r,m}$ is the (r,m)-entry of the matrix product $C_n^{-1}P_n$. ■

1.5.6 Example. Let's reconfirm Equation (1.11). By Theorem 1.5.5,

$$\begin{aligned} a_{1,3} &= (-1)^{1+1}C(1,1)1^3 = 1, \\ a_{2,3} &= (-1)^{2+1}C(2,1)1^3 + (-1)^{2+2}C(2,2)2^3 \\ &= -2 + 8 = 6, \\ a_{3,3} &= (-1)^{3+1}C(3,1)1^3 + (-1)^{3+2}C(3,2)2^3 + (-1)^{3+3}C(3,3)3^3 \\ &= 3 - 24 + 27 = 6; \end{aligned}$$

i.e., with $m = 3$, Equation (1.9) becomes $k^3 = C(k,1) + 6C(k,2) + 6C(k,3)$. □

In fact, it isn't necessary to compute $a_{r,m}$ for one value of r at a time, or even for one value of m at a time! Using matrices, we can calculate the numbers $a_{r,m}$, $1 \le r \le m$, $1 \le m \le n$, *all at once*!

1.5.7 Example. When $n = 4$,

$$P_4 = \begin{pmatrix} 1^1 & 1^2 & 1^3 & 1^4 \\ 2^1 & 2^2 & 2^3 & 2^4 \\ 3^1 & 3^2 & 3^3 & 3^4 \\ 4^1 & 4^2 & 4^3 & 4^4 \end{pmatrix}.$$

So,

$$\begin{aligned} C_4^{-1}P_4 &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 3 & -3 & 1 & 0 \\ -4 & 6 & -4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 4 & 8 & 16 \\ 3 & 9 & 27 & 81 \\ 4 & 16 & 64 & 256 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 2 & 6 & 14 \\ 0 & 0 & 6 & 36 \\ 0 & 0 & 0 & 24 \end{pmatrix} = A_4. \end{aligned}$$

(Check the substitutions and confirm the matrix multiplication.) Observe that column 3 of A_4 recaptures Equation (1.11), column 2 reconfirms Equation (1.8), and column 1 reflects the fact that $k^1 = k = C(k,1)$. Column 4 is new:

$$k^4 = C(k,1) + 14C(k,2) + 36C(k,3) + 24C(k,4). \tag{1.12}$$

□

So much for the desert. It's time for the broccoli.

Proof of the Alternating-Sign Theorem. Given an $n \times n$ matrix $C = (c_{ij})$, recall that the $n \times n$ matrix $B = (b_{ij})$ is its inverse if and only if $CB = I_n$ if and only if $BC = I_n$. Let $C = C_n$ be the $n \times n$ Pascal matrix, so that $c_{ij} = C(i,j)$. In the context

of Theorem 1.5.4, we have a candidate for C^{-1}, namely, the matrix B, whose (i,j)-entry is $b_{ij} = (-1)^{i+j}C(i,j)$. With these choices, $CB = I_n$ if and only if

$$\sum_{k=1}^{n} C(i,k)(-1)^{k+j}C(k,j) = \delta_{i,j}, \tag{1.13a}$$

$1 \le i, j \le n$, and $BC = I_n$ if and only if

$$\sum_{k=1}^{n} (-1)^{i+k}C(i,k)C(k,j) = \delta_{i,j}, \tag{1.13b}$$

$1 \le i, j \le n$, where

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise} \end{cases}$$

is the so-called *Knonecker delta*.

Let's prove Equation (1.13a). Because $C(i,k) = 0$, $k > i$, and $C(k,j) = 0$, $k < j$,

$$\sum_{k=1}^{n} C(i,k)(-1)^{k+j}C(k,j) = \sum_{k=j}^{i} (-1)^{k+j}C(i,k)C(k,j).$$

If $j > i$, the right-hand sum is empty, meaning that the left-hand sum is zero. (So far, so good.) If $i \ge k \ge j$, then (confirm it) $C(i,k)C(k,j) = C(i,j)C(i-j,k-j)$. Substituting this identity into the right-hand sum yields

$$\begin{aligned} \sum_{k=j}^{i} (-1)^{k+j}C(i,j)C(i-j,k-j) &= C(i,j)\sum_{k=j}^{i} (-1)^{j+k}C(i-j,k-j) \\ &= C(i,j)\sum_{r=0}^{i-j} (-1)^{r}C(i-j,r), \end{aligned}$$

where $r = k - j$. If $i = j$, this expression contains just one term, namely, $C(i,i)\times (-1)^0 C(0,0) = 1$. So, to complete the proof of Theorem 1.5.4, it remains to establish the following. ■

1.5.8 Lemma. *If $n > 0$, then $\sum_{r=0}^{n} (-1)^r C(n,r) = 0$.*

1.5.9 Example. With $n = 5$, Lemma 1.5.8 becomes

$$C(5,0) - C(5,1) + C(5,2) - C(5,3) + C(5,4) - C(5,5) = 0,$$

which is an immediate consequence of symmetry: $C(5,2) = C(5,3)$, $C(5,1) = C(5,4)$, and $C(5,0) = C(5,5)$. If $n = 4$, the identity

$$\begin{aligned} C(4,0) - C(4,1) + C(4,2) - C(4,3) + C(4,4) &= 1 - 4 + 6 - 4 + 1 \\ &= 0, \end{aligned}$$

while just as valid, is a little less obvious. □

Proof of Lemma 1.5.8. The lemma follows from the binomial theorem, which will be taken up in section 1.7. It is easy enough, however, to give a direct proof. Observe that the conclusion is equivalent to

$$\sum_{r \text{ even}} C(n,r) = \sum_{r \text{ odd}} C(n,r),$$

i.e., the number of subsets of $T = \{1, 2, \ldots, n\}$ having even cardinality is equal to the number of subsets of T with odd cardinality.

Temporarily denote the family of all 2^n subsets of T by $\mathscr{F}$. We will prove the result by exhibiting a one-to-one, onto function* $f : \mathscr{F} \to \mathscr{F}$ such that $A \in \mathscr{F}$ has an even (odd) number of elements if and only if $f(A)$ has an odd (even) number. If $n = o(T)$ is odd, the function defined by $f(A) = T \backslash A = \{x \in T : x \notin A\}$, the complement of A, meets our needs. (This is the easy case, illustrated for $n = 5$ in Example 1.5.9.) If n is even, the function defined by

$$f(A) = \begin{cases} A \cup \{n\} & \text{when } n \notin A, \\ A \backslash \{n\} & \text{when } n \in A \end{cases}$$

satisfies our requirements. ■

1.5.10 Example. Some values of the function

$$f(A) = \begin{cases} A \cup \{4\} & \text{when } 4 \notin A, \\ A \backslash \{4\} & \text{when } 4 \in A \end{cases}$$

(corresponding to $n = 4$) are given in Fig. 1.5.2. □

A	$f(A)$
ϕ	{4}
{1}	{1,4}
{2}	{2,4}
{3,4}	{3}
{1,3,4}	{1,3}
{1,2,3,4}	{1,2,3}

Figure 1.5.2

1.5. EXERCISES

1 Prove that

(a) The sum $2 + 4 + 6 + \cdots + 2n$ of the first n even integers is $n(n + 1)$.

(b) The sum $1 + 3 + 5 + \cdots + (2n - 1)$ of the first n odd integers is n^2.

* One-to-one, onto functions are also known as *bijections*.

2 Evaluate

(a) $\sum_{i=1}^{n} i(i-1)$. **(b)** $\sum_{i=1}^{n} i(i+1)$.

(c) $\sum_{i=3}^{n}(2i-1)$. **(d)** $\sum_{i=1}^{n} i(i-1)(i-2)$.

3 A sequence of numbers $a_1, a_2, \ldots$ is *arithmetic* if there is a fixed constant c such that $a_{i+1} - a_i = c$ for all $i \geq 1$. For such a sequence, show that

(a) $a_{n+1} = a_1 + nc$. **(b)** $\sum_{i=1}^{n} a_i = \frac{1}{2}n(a_1 + a_n)$.

4 The proof of Theorem 1.5.1 given in the text is the *combinatorial proof*. Sketch the *algebraic proof*, i.e., write each of the binomial coefficients in terms of factorials and do lots of cancelling to obtain the multinomial coefficient.

5 Show that

(a) $C(r_k, r_k) \times C(r_{k-1} + r_k, r_{k-1}) \times \cdots \times C(r_1 + r_2 + \cdots + r_k, r_1)$

$$= \binom{n}{r_1, r_2, \ldots, r_k}.$$

(b) $\binom{r}{0} + \binom{r+1}{1} + \binom{r+2}{2} + \cdots + \binom{r+k}{k} = \binom{r+k+1}{k}$.

6 Use mathematical induction to prove that $1^3 + 2^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$.

7 Confirm (by a brute-force computation) that

$$k^4 = C(k,1) + 14C(k,2) + 36C(k,3) + 24C(k,4).$$

8 Prove that $1^4 + 2^4 + \cdots + n^4 = \frac{1}{30}n(n+1)(2n+1)(3n^2+3n-1)$

(a) using Equations (1.9)–(1.10) and (1.12).

(b) using mathematical induction.

9 Solve for the coefficients $a_{r,5}$, $1 \leq r \leq 5$, in the equation $k^5 = \sum_{r=1}^{5} a_{r,5}C(k,r)$

(a) using the matrix equation $A_5 = C_5^{-1}P_5$.

(b) by solving a system of five equations in five unknowns *without* using the matrix equation.

10 What is the formula for the sum of the fifth powers of the first n positive integers? (*Hint:* Lots of computations afford lots of opportunities to make mistakes. Confirm your formula for three or four values of n.)

11 Suppose f and g are functions of the positive integer variable n. If $f(n) = \sum_{r=1}^{n} C(n,r)g(r)$ for all $n \geq 1$, prove that $g(n) = \sum_{r=1}^{n}(-1)^{n+r}C(n,r)f(r)$ for all $n \geq 1$.

12 If $m \geq n$, prove that

(a) $\sum_{r=1}^{n} C(m,r)C(n-1,r-1) = C(m+n-1,n)$.

(b) $\sum_{r=1}^{n} rC(m,r)C(n,r) = nC(m+n-1,n)$.

13 Prove that $1 \times 2 + 2 \times 3 + 3 \times 4 + \cdots + n \times (n+1) = \frac{1}{3}n(n+1)(n+2)$.

14 Prove that $1 \times 2 \times 3 + 2 \times 3 \times 4 + \cdots + n(n+1)(n+2) = \frac{1}{4}n(n+1) \times (n+2)(n+3)$.

15 Prove Vandermonde's identity*: If m and n are positive integers, then

$$C(m,0)C(n,r) + C(m,1)C(n,r-1) + \cdots + C(m,r)C(n,0) = C(m+n,r).$$

16 Prove that $\sum_{r=0}^{n} C(n,r)^2 = C(2n,n)$. (Compare with Exercise 11, Section 1.2.)

17 How many of the $C(52,5)$ different five-card poker hands contain

(a) a full house? **(b)** four of a kind?

18 How many of the $C(52,13)$ different 13-card bridge hands contain

(a) all four aces? **(b)** a 4–3–3–3 suit distribution?

19 Show that

(a) $\sum_{r=1}^{n+1}(-1)^{r-1}[C(n,r-1)/r] = 1/(n+1)$.

(b) $\sum_{r=0}^{n}(-1)^{r}[C(n,r)/(r+1)] = 1/(n+1)$.

(c) $\sum_{r=1}^{n}(-1)^{r-1}[C(n,r)/r] = \sum_{k=1}^{n} 1/k$.

(d) $C_m^{-1}v^{\mathrm{t}} = w^{\mathrm{t}}$, where $v = (1/2, 1/3, \ldots, 1/[m+1])$ and $w = (1/2, -2/3, 3/4, -4/5, \ldots, [(-1)^{m+1}m/(m+1)])$.

(e) $C_m w^{\mathrm{t}} = v^{\mathrm{t}}$, where v and w are the vectors from part (d).

(f) Confirm the $m = 6$ case of part (e); i.e., write down the 6×6 matrix C_6 and confirm that $C_6 w^{\mathrm{t}} = v^{\mathrm{t}}$.

20 Let n be fixed. Denote the rth-power sum of the first $n-1$ positive integers by $g(r) = 1^r + 2^r + \cdots + (n-1)^r$. Show that

(a) $g(0) = n - 1$. **(b)** $g(1) = \frac{1}{2}n^2 - \frac{1}{2}n$.

(c) $g(2) = \frac{1}{3}n^3 - \frac{1}{2}n^2 + \frac{1}{6}n$. **(d)** $g(3) = \frac{1}{4}n^4 - \frac{1}{2}n^3 + \frac{1}{4}n^2$.

(e) $g(4) = \frac{1}{5}n^5 - \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n$.

21 The nth *Bernoulli number*, b_r, is the coefficient of n in the function $g(r)$ of Exercise 20. The first few Bernoulli numbers are exhibited in Fig. 1.5.3. Jakob Bernoulli (1654–1705) showed that the remaining coefficients in $g(r)$, $r \geq 1$,

r	0	1	2	3	4
b_r	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$

Figure 1.5.3. Bernoulli numbers.

* Named for Abnit-Theophile Vandermonde (1735–1796), who published the result in 1772 (469 years *after* it appeared in Chu Shih-Chieh's book).

can be expressed in terms of the b_r's by means of the identity

$$g(r) = \sum_{k=0}^{r} \frac{1}{k+1} C(r,k) b_{r-k} n^{k+1}.$$

(a) use the $r = 4$ case of this identity, along with Fig. 1.5.3, to recapture the expression for $g(4)$ in Exercise 20(e).

(b) Show that your solution to part (a) is consistent with Exercise 8.

(c) Compute $g(5)$.

(d) Show that your solution to part (c) is consistent with your solution to Exercise 10.

22 The Bernoulli numbers (Exercise 21) satisfy the implicit recurrence $\sum_{k=0}^{r} C(r+1,k) b_k = 0$, $r \geq 1$. Use this relation (and Fig. 1.5.3) to show that

(a) $b_5 = 0$. **(b)** $b_6 = \frac{1}{42}$. **(c)** $b_7 = 0$.

(d) $b_8 = -\frac{1}{30}$. **(e)** $b_9 = 0$. **(f)** $b_{10} = \frac{5}{66}$.

23 Let n be fixed. Prove that the function $g(r) = 1^r + 2^r + \cdots + (n-1)^r$, from Exercise 20, can expressed in the form $\sum_{k=1}^{r+1} c_{r,k} n^k$, where the coefficients satisfy the recurrence $(k+1)c_{r,k+1} = r c_{r-1,k}$ for all r, $k \geq 1$.

24 Use Exercises 20(e) and 23 and the fact that $g(r) = 1$ when $n = 2$ to compute $g(5)$.

25 Let r and s be integers, $0 \leq r < s$, and let

$$C_{[r,s]} = \begin{pmatrix} C(r,r) & C(r,r+1) & \cdots & C(r,s) \\ C(r+1,r) & C(r+1,r+1) & \cdots & C(r+1,s) \\ \vdots & \vdots & \ddots & \vdots \\ C(s,r) & C(s,r+1) & \cdots & C(s,s) \end{pmatrix}.$$

(a) Show that $C_{[1,n]} = C_n$.

(b) Exhibit $C_{[2,6]}$.

(c) Show that $C_{[r,s]}$ is an $(s-r+1)$-square matrix.

(d) Show that the (i,j)-entry of $C_{[r,s]}$ is $C(r+i-1, r+j-1)$.

(e) Show that $C_{[r,s]}$ is invertible.

(f) Exhibit $C_{[2,6]}^{-1}$.

(g) Prove that the (i,j)-entry of the inverse of $C_{[r,s]}$ is $(-1)^{i+j} C(r+i-1, r+j-1)$, $1 \leq i, j \leq s-r+1$.

(h) Let t be a nonnegative integer. If f and g are functions that satisfy $f(n) = \sum_{k=t}^{n} C(n,k) g(k)$ for all $n \geq t$, prove that $g(n) = \sum_{k=t}^{n} (-1)^{n+k} C(n,k) f(k)$ for all $n \geq t$.

26 The Fibonacci sequence (Exercise 19, Section 1.2) may be defined by $F_0 = F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$, $n \geq 1$.

(a) Show that $F_4 = F_2 + 2F_1 + F_0$.

(b) Show that $F_5 = F_3 + 2F_2 + F_1$.

(c) Show that $F_6 = F_3 + 3F_2 + 3F_1 + F_0$.

(d) Show that $F_7 = F_4 + 3F_3 + 3F_2 + F_1$.

(e) Given that $F_{2n+1} = \sum_{r=0}^{n} C(n,r)F_{r+1}$, prove that $F_{2n} = \sum_{r=0}^{n} C(n,r)F_r$.

(f) Prove that $F_n = \sum_{r=0}^{n} (-1)^{n+r} C(n,r)F_{2r}$. (*Hint:* Use part (e) and the $t = 1$ case of Exercise 25(h).)

27 If $C = C_{[0,m]}$ is the matrix from Exercise 25, show that $CK = L$, where

$$L = \begin{pmatrix} C(0,0) & C(1,1) & C(2,2) & C(3,3) & \cdots & C(m,m) \\ C(1,0) & C(2,1) & C(3,2) & C(4,3) & \cdots & C(m+1,m) \\ C(2,0) & C(3,1) & C(4,2) & C(5,3) & \cdots & C(m+2,m) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ C(m,0) & C(m+1,1) & C(m+2,2) & C(m+3,3) & \cdots & C(m+m,m) \end{pmatrix},$$

$$K = \begin{pmatrix} C(0,0) & C(1,1) & C(2,2) & C(3,3) & \ldots & C(m,m) \\ 0 & C(1,0) & C(2,1) & C(3,2) & \cdots & C(m,m-1) \\ 0 & 0 & C(2,0) & C(3,1) & \cdots & C(m,m-2) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & C(m,0) \end{pmatrix}.$$

28 For a fixed but arbitrary positive integer m, prove that the coefficients $a_{r,m}$, $1 \leq r \leq m$, in Equation (1.9) exist and are independent of k. (*Hint:* Show that any polynomial $f(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ of degree at most m can be expressed (uniquely) as a linear combination of $p_0(x)$, $p_1(x), \ldots, p_m(x)$, where $p_0(x) = 1$ and $p_r(x) = (1/r!)x(x-1)\cdots(x-r+1)$, $r \geq 1$.)

1.6. FOUR WAYS TO CHOOSE

The prologues are over. ... It is time to choose.

— Wallace Stevens (*Asides on the Oboe*)

From its combinatorial definition, n-choose-r is the number of different r-element subsets of an n-element set. Because two subsets are equal if and only if they contain the same elements, $\binom{n}{r}$ depends on *what* elements are chosen, not when. In

computing $C(n, r)$, the *order* in which elements are chosen is irrelevant. The $C(5, 2) = 10$ two-element subsets of $\{\mathrm{L}, \mathrm{U}, \mathrm{C}, \mathrm{K}, \mathrm{Y}\}$ are

$$\{\mathrm{L}, \mathrm{U}\}, \{\mathrm{L}, \mathrm{C}\}, \{\mathrm{L}, \mathrm{K}\}, \{\mathrm{L}, \mathrm{Y}\}, \{\mathrm{U}, \mathrm{C}\}, \{\mathrm{U}, \mathrm{K}\}, \{\mathrm{U}, \mathrm{Y}\}, \{\mathrm{C}, \mathrm{K}\}, \{\mathrm{C}, \mathrm{Y}\}, \{\mathrm{K}, \mathrm{Y}\},$$

where, e.g., $\{\mathrm{L}, \mathrm{U}\} = \{\mathrm{U}, \mathrm{L}\}$. There are, of course, circumstances in which order is important.

1.6.1 Example. Consider all possible "words" that can be produced using two letters from the word LUCKY. By the fundamental counting principle, the number of such words is 5×4, twice $C(5, 2)$, reflecting the fact that order is important. The 20 possibilities are

$$\mathrm{LU}, \mathrm{LC}, \mathrm{LK}, \mathrm{LY}, \mathrm{UC}, \mathrm{UK}, \mathrm{UY}, \mathrm{CK}, \mathrm{CY}, \mathrm{KY},$$
$$\mathrm{UL}, \mathrm{CL}, \mathrm{KL}, \mathrm{YL}, \mathrm{CU}, \mathrm{KU}, \mathrm{YU}, \mathrm{KC}, \mathrm{YC}, \mathrm{YK}. \qquad \square$$

1.6.2 Definition. Denote by $P(n, r)$ the number of *ordered* selections of r elements chosen from an n-element set.

By the fundamental counting principle,

$$\begin{aligned} P(n, r) &= n(n-1)(n-2)\cdots(n-[r-1]) \\ &= n(n-1)(n-2)\cdots(n-r+1) \\ &= \frac{n!}{(n-r)!} \\ &= r!C(n, r). \end{aligned}$$

There is another way to arrive at this last identity: We may construe $P(n, r)$ as the number of ways to make a sequence of just two decisions. Decision 1 is which of the r elements to select, without regard to order, a decision having $C(n, r)$ choices. Decision 2 is how to order the r elements once they have been selected, and there are $r!$ ways to do that. By the fundamental counting principle, the number of ways to make the sequence of two decisions is $C(n, r) \times r! = P(n, r)$.

1.6.3 Example. Suppose nine members of the Alameda County School Boards Association meet to select a three-member delegation to represent the association at a statewide convention. There are $C(9, 3) = 84$ different ways to choose the delegation from those present. If the bylaws stipulate that each delegation be comprised of a delegate, a first alternate, and a second alternate, the nine members can comply from among themselves in any one of $P(9, 3) = 3!C(9, 3) = 504$ ways. $\square$

1.6.4 Example. Door prizes are a common feature of fundraising luncheons. Suppose each of 100 patrons is given a numbered ticket, while its duplicate is placed in a bowl from which prize-winning numbers will be drawn. If the prizes are \$10, \$50, and \$150, then (assuming winning tickets are not returned to the

bowl) a total of $P(100, 3) = 970,200$ different outcomes are possible. If, on the other hand, the three prizes are each \$70, then the order in which the numbers are drawn is immaterial. In this case, the number of different outcomes is $C(100, 3) = 161,700$. □

Both $C(n, r)$ and $P(n, r)$ involve situations in which an object can be chosen at most once. We have been choosing *without replacement*. What about choosing *with* replacement? What if we recycle the objects, putting them back so they can be chosen again? How many ways are there to choose r things from n things with replacement? The answer depends on whether order matters. If it does, the answer is easy. The number of ways to make a sequence of r decisions each of which has n choices is n^r.

1.6.5 Example. How many different two-letter "words" can be produced using the "alphabet" $\{L, U, C, K, Y\}$? If there are no restrictions on the number of times a letter can be used, then $5^2 = 25$ such words can be produced; i.e., there are 25 ways to choose 2 things from 5 with replacement if order matters. In addition to the 20 words from Example 1.6.1, there are five new ones, namely, LL, UU, CC, KK, and YY. □

This brings us to the fourth way to choose.

1.6.6 Example. In how many ways can $r = 10$ items be chosen from $\{A, B, C, D, E\}$ with replacement if order doesn't matter? As so often happens in combinatorics, the solution is most easily obtained by solving another problem that has the same answer. Suppose, e.g., A were chosen three times, B once, C twice, D not at all, and E four times. Associate with this selection the 14-letter "word"

$$|||-|-||--||||.$$

In this word, the "letter" | represents a tally mark. Since we are choosing 10 times, there are ten |'s. The dashes are used to separate tally marks corresponding to one letter from those that correspond to another. The first three |'s are for the three A's. The first dash separates the three A tallies from the single tally corresponding to the only B; the second dash separates the B tally from the two C tallies. There is no tally mark between the third and fourth dashes because there are no D's. Finally, the last four |'s represent the four E's. Since $\{A, B, C, D, E\}$ has $n = 5$ elements, we need 4 dashes to keep their respective tally marks separate. Conversely, any 14-letter word consisting of ten |'s and four —'s corresponds to a unique selection. The word |||||||--|-||-, e.g., correspons to seven A's, no B's, one C, two D's, and no E's.

Because the correspondence is one-to-one, the number of ways to select $r = 10$ things from $n = 5$ things with replacement where order doesn't matter is equal to the number of 14-letter words that can be made up from ten |'s and four —'s, i.e., to $C(14, 10) = 1001$. □

	Order matters	Order doesn't matter
Without replacement	$P(n,r)$	$C(n,r)$
With replacement	n^r	$C(r+n-1, r)$

Figure 1.6.1. The four ways to choose.

1.6.7 Theorem. *The number of different ways to choose r things from n things with replacement if order doesn't matter is* $C(r+n-1,r)$.

Proof. As in Example 1.6.6, there is a one-to-one correspondence between selections and $[r+(n-1)]$-letter words consisting of r tally marks and $n-1$ dashes. The number of such words is $C(r+n-1,r)$. ■

1.6.8 Example. Let's return to the door prizes of Example 1.6.4, but, this time, suppose that winning tickets are returned to the bowl so they have a chance to be drawn again. When the prizes are different, the $r=3$ winning tickets are chosen from the $n=100$ tickets in the bowl with replacement where order matters, and $100^3 = 1$ million different outcomes are possible. When the prizes are all the same (choosing with replacement when order doesn't matter), the number of different outcomes is only $C(3+100-1,3) = C(102,3) = 171,700$. □

The four ways to choose are summarized in Fig. 1.6.1. Because $C(r+n-1,r) = C(r+n-1,n-1) \neq C(r+n-1,n)$, it is important to remember that in the last column of the table each entry takes the form $C(*,r)$, where *r is the number of things chosen*, replacement or not. (Don't expect this second variable always to be labeled r.)

Choosing with replacement just means that elements may be chosen more than once. If order doesn't matter, then the only thing of interest is the multiplicity with which each element is chosen. As we saw in Example 1.6.6, $C(14,10) = 1001$ different outcomes are possible when choosing 10 times from $\{A,B,C,D,E\}$ with replacement when order doesn't matter. If, in one of these outcomes, A is chosen a times, B a total of b times, and so on, then

$$\mathrm{a}+\mathrm{b}+\mathrm{c}+\mathrm{d}+\mathrm{e} = 10. \tag{1.14}$$

Evidently, each of the 1001 outcomes gives rise to a different nonnegative integer solution to Equation (1.14), and every nonnegative integer solution of this equation corresponds to a different outcome. In particular, Equation (1.14) must have precisely 1001 nonnegative integer solutions! The obvious generalization is this.

1.6.9 Corollary. *The equation* $x_1+x_2+\cdots+x_n = r$ *has exactly* $C(r+n-1,r)$ *nonnegative integer solutions.*

What about positive integer solutions? That's easy! The number of positive integer solutions to Equation (1.14) is equal to the number of nonnegative integer solutions to the equation

$$(a-1)+(b-1)+(c-1)+(d-1)+(e-1)=10-5,$$

namely, to $C(5+5-1,5)=C(9,5)=126$. [Of the 1001 nonnegative integer solutions to Equation (1.14), at least one variable is zero in all but 126 of them.]

1.6.10 Definition. A *composition*[*] of n having m *parts* is a solution, in positive integers, to the equation

$$n=x_1+x_2+\cdots+x_m. \tag{1.15}$$

Notice the change in notation. This is not deliberately meant to be confusing. Notation varies with context, and we are now moving on to a new idea. It might be useful to think of the integer variables n, r, k, m, etc., as a traveling company of players whose roles depend upon the demands of the current drama production.

A composition expresses n as a sum of parts; $7=5+2$ is a two-part composition of 7, not to be confused with $7=2+5$. In the first case, $x_1=5$ and $x_2=2$; in the second, $x_1=2$ and $x_2=5$. Never mind that addition is commutative. A composition is an *ordered* or *labeled* solution of Equation (1.15). The six two-part compositions of $n=7$ are $6+1$, $5+2$, $4+3$, $3+4$, $2+5$, and $1+6$, corresponding, e.g., to the six ways to roll a 7 with two dice (one red and one green).

1.6.11 Theorem. *The number of m-part compositions of n is* $C(n-1,m-1)$.

Proof. The number of positive integer solutions to Equation (1.15) is equal to the number of nonnegative integer solutions to

$$(x_1-1)+(x_2-1)+\cdots+(x_m-1)=n-m.$$

By Corollary 1.6.9, this equation has $C([n-m]+m-1,n-m)=C(n-1,n-m)=C(n-1,m-1)$ nonnegative integer solutions. ■

1.6.12 Example. The $C(6-1,3-1)=C(5,2)=10$ three-part compositions of 6 are illustrated in Fig. 1.6.2. □

1.6.13 Corollary. *The (total) number of compositions of n is* 2^{n-1}.

[*] The term was coined by Major Percy A. MacMahon (1854–1929). *Decomposition* might be a more descriptive word.

x_1	x_2	x_3
4	1	1
1	4	1
1	1	4
3	2	1
3	1	2
2	3	1
2	1	3
1	3	2
1	2	3
2	2	2

Figure 1.6.2

Proof. The number of compositions of n is the sum, as m goes from 1 to n, of the number of m-part compositions of n. According to Theorem 1.6.11, that sum is equal to

$$C(n-1,0) + C(n-1,1) + \cdots + C(n-1,n-1),$$

the sum of the numbers in row $n-1$ of Pascal's triangle. ■

By Corollary 1.6.13, there are $2^5 = 32$ different compositions of 6. Ten of them are tabulated in Fig. 1.6.2. You will be asked to list the remaining 22 compositions in Exercise 11, but why not do it now, while the idea is still fresh?

1.6.14 Example. How many integer solutions of $x + y + z = 20$ satisfy $x \geq 1$, $y \geq 2$, and $z \geq 3$? Solution: $x + y + z = 20$ if and only if $(x-1) + (y-2) + (z-3) = 14$. Setting $a = x - 1$, $b = y - 2$, and $c = z - 3$ transforms the problem into one involving the number of nonnegative integer solutions of $a + b + c = 14$. By Corollary 1.6.9, the answer is $C(14 + 3 - 1, 14) = 120$. □

1.6.15 Example. Some people are suspicious when consecutive integers occur among winning lottery numbers. This reaction is probably due to the common misconception that truly random numbers would be "spread out". Consider a simple example. Of the $C(6,3) = 20$ three-element subsets of $\{1,2,3,4,5,6\}$, how many fail to contain at least one pair of consecutive integers? Here is the complete list: $\{1,3,5\}$, $\{1,3,6\}$, $\{1,4,6\}$, and $\{2,4,6\}$.

What about the general case? Of the $C(n,r)$ r-element subsets of $S = \{1,2,\ldots,n\}$, how many do not contain even a single pair of consecutive integers? Recall the correspondence between r-element subsets of S and n-letter "words" consisting of r Y's and $n-r$ N's. In any such word, w, there will be some number, x_0, of N's that come before the first Y, some number x_1 of N's

between the first and second Y, some number x_2 of N's between the second and third Y, and so on, with some number x_r or N's coming after the last (rth) Y. Since w must contain a total of $n - r$ N's, it must be the case that

$$x_0 + x_1 + \cdots + x_r = n - r.$$

Every r-element subset of S corresponds to a unique solution of this equation, in nonnegative integers, and every nonnegative integer solution of this equation corresponds to a unique r-element subset of S. (Confirm that $C([n-r] + [r+1] - 1, [n-r]) = C(n, r)$.)

In this correspondence between subsets and words, a subset contains no consecutive integers if and only if $x_i > 0$, $1 \leq i \leq r-1$. If we substitute $y_0 = x_0$, $y_r = x_r$, and $y_i = x_i - 1$, $1 \leq i \leq r-1$, then, as in Example 1.6.14, the answer to our problem is equal to the number of nonnegative integer solutions of

$$\begin{aligned} y_0 + y_1 + \cdots + y_r &= (n-r) - (r-1) \\ &= n - 2r + 1, \end{aligned}$$

i.e., to

$$\begin{aligned} C([n-2r+1] + [r+1] - 1, [n-2r+1]) &= C(n-r+1, n-2r+1) \\ &= C(n-r+1, r). \end{aligned}$$

(Be careful, $C(n-r+1, r) \neq C(r+n-1, r)$.)

When $n = 6$ and $r = 3$, $C(6-3+1, 3) = C(4, 3) = 4$, confirming the result of the brute-force list in the first paragraph of this example. □

1.6. EXERCISES

1 Compute

(a) $P(5, 3)$. **(b)** $C(5, 3)$. **(c)** $C(5, 2)$.

(d) $P(5, 2)$. **(e)** $C(10, 4)$. **(f)** $P(10, 4)$.

(g) 7!.

2 Show that

(a) $nP(n-1, r) = P(n, r+1)$.

(b) $P(n+1, r) = rP(n, r-1) + P(n, r)$.

3 In how many ways can four elements be chosen from a seven-element set

(a) with replacement if order doesn't matter?

(b) without replacement if order does matter?

(c) without replacement if order doesn't matter?

(d) with replacement if order matters?

4 In how many ways can seven elements be chosen from a four-element set

(a) with replacement if order matters?

(b) with replacement if order doesn't matter?

(c) without replacement if order matters?

(d) without replacement if order doesn't matter?

5 In how many ways can four elements be chosen from a ten-element set

(a) with replacement if order matters?

(b) with replacement if order doesn't matter?

(c) without replacement if order doesn't matter?

(d) without replacement if order matters?

6 In how many ways can seven elements be chosen from a ten-element set

(a) without replacement if order matters?

(b) with replacement if order doesn't matter?

(c) without replacement if order doesn't matter?

(d) with replacement if order matters?

7 Show that multinomial coefficient $\binom{n}{n-r,1,1,\cdots,1} = P(n,r)$.

8 Compute the number of nonnegative integer solutions to

(a) $a+b=9$. **(b)** $a+b+c=9$.

(c) $a+b+c=30$. **(d)** $a+b+c+d=30$.

9 How many integer solutions of $a+b+c+d=30$ satisfy

(a) $d \geq 3$, $c \geq 2$, $b \geq 1$, $a \geq 0$?

(b) $a \geq 3$, $b \geq 2$, $c \geq 1$, $d \geq 0$?

(c) $a \geq 7$, $b \geq 2$, $c \geq 5$, $d \geq 6$?

(d) $a \geq -3$, $b \geq 20$, $c \geq 0$, $d \geq -2$?

10 Write down all 16 compositions of 5.

11 Ten of the 32 compositions of 6 appear in Fig. 1.6.2. Write down the remaining 22 compositions of 6.

12 How many compositions of 8 have

(a) 4 parts? **(b)** 4 or fewer parts?

(c) 6 parts? **(d)** 6 or fewer parts?

13 Prove that the inequality $x+y+z \leq 14$ has a total of 680 nonnegative integer solutions.

14 Prove that the inequality $x_1 + x_2 + \cdots + x_m \leq n$ has a total of $C(n+m, m)$ nonnegative integer solutions.

15 Starting with $F_0 = F_1 = 1$, the Fibonacci numbers satisfy the recurrence $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$. Prove that

(a) $F_{k+n} = F_k F_n + F_{k-1} F_{n-1}$, $k, n \geq 1$.

(b) F_{2k+1} is a multiple of F_k, $k \geq 1$.

(c) F_{3k+2} is a multiple of F_k, $k \geq 1$.

16 Let F_n, $n \geq 0$, be the nth Fibonacci number. (See Exercise 15.) Prove that

(a) $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1} = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}, n \geq 1.$

(b) $F_{n+1} F_{n-1} = F_n^2 + (-1)^{n+1}$.

(c) F_n and F_{n+1} are relatively prime.

17 Let n be a positive integer. Prove that there is a composition of n each of whose parts is a different Fibonacci number. (See Exercise 15.)

18 Let ρ_n be the number of compositions of n each of whose parts is greater than 1.

(a) Show that $\rho_6 = 5$ by writing down the compositions of 6 each of whose parts is at least 2.

(b) Show that $\rho_7 = 8$.

(c) If $n \geq 2$, prove that ρ_n is a Fibonacci number. (*Hint:* Exercise 19, Section 1.2.)

19 Let l_n be the number of compositions of n each of whose parts is at most 2. If $n \geq 1$, prove that $l_n = F_n$, the nth Fibonacci number.

20 The first "diagonal" of Pascal's triangle consists entirely of 1's. The second is comprised of the numbers 1, 2, 3, 4, 5, ... The fourth is illustrated in **boldface** in Fig. 1.6.3. Explain the relationship between the kth entry of the mth diagonal and choosing, with replacement, from $\{1, 2, \ldots, k\}$ where order doesn't matter.

1						
1	1					
1	2	1				
1	3	3	1			
1	**4**	6	4	1		
1	5	**10**	10	5	1	
1	6	15	**20**	15	6	1
			...			

Figure 1.6.3

21 Suppose five different door prizes are distributed among three patrons, Betty, Joan, and Marge. In how many different outcomes does

(a) Betty get three prizes while Joan and Marge each get one?

(b) Betty get one prize while Joan and Marge each get two?

22 Let A be the collection of all 32 compositions of 6. Let B be the 32-element family consisting of all subsets of $\{1, 2, 3, 4, 5\}$. Because $o(A) = o(B)$, there is a one-to-one correspondence between A and B.

(a) Prove that there are a total of 32! different one-to-one correspondences between A and B.

(b) Of the more than 2.6×10^{35} one-to-one correspondences between A and B, can any be described by an algorithm, or recipe, that transforms compositions into subsets?

23 What about choosing with *limited* replacement? Maybe the fundraising patrons in Examples 1.6.4 and 1.6.8 should be limited to at most two prizes. How many different outcomes are possible, under these terms of limited replacement, if there are 100 patrons and

(a) three different prizes? **(b)** three equal prizes?

(c) four different prizes? **(d)** four equal prizes?

24 Revisiting the "birthday paradox" (Exercises 20–21, Section 1.3), suppose each of k people independently chooses an integer between 1 and m (inclusive). Let p be the probability that some two of them choose the same number.

(a) Show that $p = 1 - P(m, k)/m^k$.

(b) M. Sayrafiezadeh showed that $p \doteq 1 - [1 - (k/2m)]^{k-1}$ as long as $k \leq m$, where "$\doteq$" means "about equal". Find the error in Sayrafiezadeh's estimate when $k = 23$ and $m = 365$.

25 Show that the number of compositions of n having k *or fewer* parts is $N(n-1, k-1) = C(n-1, 0) + C(n-1, 1) + \cdots + C(n-1, k-1)$ (a number involved in the sphere-packing bound of Section 1.4).

26 There is evidence in tomb paintings that ancient Egyptians used astragali (ankle bones of animals) to determine moves in simple board games. In later Greek and Roman times it was common to gamble on the outcome of throwing several astragali at once. When an astragalus is thrown, it can land in one of four ways. Compute the number of different outcomes when five astragali are thrown simultaneously.

27 Suppose you have four boxes, labeled A, B, C, and D. How many ways are there to distribute

(a) ten identical marbles among the four boxes?

(b) the numbers 0–9 among the four boxes?

28 Suppose, to win a share of the grand prize in the weekly lottery, you must match five numbers chosen at random from 1 to 49.

(a) Of the $C(49,5) = 1,906,884$ five-element subsets of $\{1,2,\ldots,49\}$, how many contain no consecutive integers? (*Hint*: Example 1.6.15.)

(b) Show that the probability of at least one pair of consecutive integers occurring in the weekly drawing is greater than $\frac{1}{3}$.

29 Prove that the (total!) number of subsets of $\{1,2,\ldots,n\}$ that contain no two consecutive integers is F_{n+1}, the $(n+1)$st Fibonacci number. (See Exercises 15–19.)

1.7. THE BINOMIAL AND MULTINOMIAL THEOREMS

> Two roads diverged in a wood, and I—
> I took the one less traveled by,
> And that has made all the difference.
>
> — Robert Frost (*The Road Not Taken*)

Among the most widely known applications of binomial coefficients is the following.

1.7.1 Binomial Theorem. *If n is a nonnegative integer, then*

$$(x+y)^n = \sum_{r=0}^{n} C(n,r)x^r y^{n-r}.$$

Three applications of distributivity produce the identity

$$\begin{aligned}(x+y)^2 &= (x+y)(x+y)\\ &= x(x+y)+y(x+y)\\ &= xx+xy+yx+yy.\end{aligned} \tag{1.16}$$

The familiar next step would be to replace xx with x^2, $xy+yx$ with $2xy$, and so on, but let's freeze the action with Equation (1.16). As it stands, the right-hand side of this identity looks as if it could be a sum of two-letter "words". There is an alternative way to think about this word sum.

Starting with the expression $(x+y)(x+y)$, choose a letter, x or y, from the first set of parentheses, and one letter from the second set. Juxtapose the choices, in order, so as to produce what looks like a two-letter word. Do this in all possible ways, and sum the results. From this perspective, the right-hand side of

Equation (1.16) is a kind of *inventory*[*] of the four ways to make a sequence of two decisions. The term yx, e.g., records the sequence in which y is the choice for decision 1, namely, which letter to take from the first set of parentheses, and x is the choice for decision 2.

Applied to the expression

$$\begin{aligned}(x+y)^3 &= (x+y)^2(x+y)\\ &= (xx+xy+yx+yy)(x+y),\end{aligned}$$

this alternative view of distributivity suggests the following process: Select a two-letter word from $(xx+xy+yx+yy)$ and a letter from $(x+y)$. Juxtapose these selections (in order), so as to produce a three-letter word. Do this in all $(4\times 2=8)$ possible ways and sum, obtaining the following analog of Equation (1.16):

$$xxx+xyx+yxx+yyx+xxy+xyy+yxy+yyy. \tag{1.17}$$

A *variation* on this alternative view of distributivity would be to picture $(x+y)^3=(x+y)(x+y)(x+y)$ in terms, not of two decisions, but of three. Choose one of x or y from the first set of parentheses, one of x or y from the second set, and one of x or y from the third. String the three letters together (in order) to produce a three-letter word. Doing this in all $(2\times 2\times 2=8)$ possible ways and summing the results leads to Expression (1.17). However one arrives at that expression, replacing words like xyx with monomials like x^2y, and then combining like terms, produces the identity

$$(x+y)^3 = x^3+3x^2y+3xy^2+y^3. \tag{1.18}$$

The two variations on our alternative view of distributivity afford two different routes to a proof of the binomial theorem. One is inductive: Given the binomial *expansion* of $(x+y)^{n-1}$, the computation of $(x+y)^n$ is viewed in terms of two decisions, as in $(x+y)^n=(x+y)^{n-1}(x+y)$, and the proof is completed using Pascal's relation. In the second route, the expansion of $(x+y)^n$ is viewed in terms of n decisions.

Proof of Theorem 1.7.1. Taking the route "less traveled by", we evaluate the right-hand side of the equation

$$(x+y)^n=(x+y)(x+y)\cdots(x+y)$$

[*] Using distributivity to inventory the ways to make a sequence of decisions is an idea of fundamental importance in Pólya's enumeration theory (Chapter 3) and the theory of generating functions (Chapter 4).

in a series of steps. Begin by choosing one of x or y from the first set of parentheses, one from the second set, and so on, finally choosing one of x or y from the nth set. String the n choices together in order. Do this in all possible ways and sum the corresponding n-letter words. The resulting analog of expressions (1.16)–(1.17) is both an inventory of the 2^n ways to make a sequence of decisions and a vocabulary of all possible n-letter words that can be produced using the alphabet $\{x, y\}$. From this sum of words, the analog of Equation (1.18) is reached in two steps. Viewing x and y not as letters in an alphabet but as commuting variables, replace each n-letter word with a monomial of the form $x^r y^{n-r}$. Then combine like terms. In the resulting two-variable polynomial, the coefficient of $x^r y^{n-r}$ is the number of n-letter words in which r of the letters are x's and $n - r$ or them are y's. That number is known to us as $C(n, r)$. ■

Substituting $x = y = 1$ in the binomial theorem results in a new proof that

$$2^n = \sum_{r=0}^{n} C(n, r).$$

Setting $x = -1$ and $y = 1$ leads to another proof of Lemma 1.5.8, i.e.,

$$\sum_{r=0}^{n} (-1)^r C(n, r) = 0$$

for all $n \geq 1$. New results can be derived by making other substitutions, e.g., $x = 2$ and $y = 1$ yields an identity expressing 3^n in terms of powers of 2, namely,

$$3^n = \sum_{r=0}^{n} C(n, r) 2^r. \tag{1.19}$$

What happens if there are three variables? This is where the road less traveled by makes all the difference. Just as $(x + y)(x + y) \cdots (x + y)$ inventories the ways to make a sequence of n decisions each having two choices, $(x + y + z) \times (x + y + z) \cdots (x + y + z)$ inventories the ways to make a comparable sequence of decisions each having three choices. From this perspective, the process of expanding $(x_1 + x_2 + \cdots + x_k)^n$ is the same whether $k = 2$ or $k = 100$. Choose one of $x_1, x_2, \ldots, x_k$ from each of n sets of brackets. String the choices together, in order, obtaining an n-letter word. Do this in all k^n possible ways and sum. The resulting inventory is then simplified in two steps. First, each word is replaced with a monomial of (total) degree n, and then like terms are combined. At the end of this process, the coefficient of $x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k}$, is the number of n-letter words that can be produced using r_1 copies of x_1, r_2 copies of $x_2, \ldots,$ and r_k copies of x_k. This proves the following generalization of the binomial theorem.

1.7.2 Multinomial Theorem. *If n is a nonnegative integer, then*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum \binom{n}{r_1, r_2, \ldots, r_k} x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k}, \tag{1.20}$$

where the sum is over all nonnegative integer solutions to the equation $r_1 + r_2 + \cdots + r_k = n$, *and*

$$\binom{n}{r_1, r_2, \ldots, r_k} = \frac{n!}{r_1! r_2! \cdots r_k!}.$$

Because some of the r's in Equation (1.20) may be zero, the sum is *not* over the k-part compositions of n. (Since $0! = 1$, the definition of multinomial coefficient is easily modified so as to permit zeros among its entries.)

1.7.3 Example. It isn't necessary to compute all $5^{10} = 9,765,625$ products in the expansion of $(a + b + c + d + e)^{10}$ just to determine the coefficient of $a^4 d^6$! From the multinomial theorem,

$$\binom{10}{4, 0, 0, 6, 0} = \frac{10!}{4!0!0!6!0!} = \frac{10!}{4!6!} = 210.$$

Observe that $210 = C(10, 4)$ is also the coefficient of $a^4 d^6$ in $(a + d)^{10}$, just as it should be. Setting $b = c = e = 0$ in $(a + b + c + d + e)^{10}$ has no effect on the coefficient of $a^4 d^6$. Also, observe that $\binom{10}{4,0,0,6,0} = \binom{10}{0,0,6,0,4}$. The coefficient of $c^6 e^4$ is also 210, reflecting the symmetry of $(a + b + c + d + e)^{10}$. We will return to this point momentarily. □

The usefulness of the multinomial theorem is not limited to picking off single coefficients. The expansion of all $3^4 = 81$ terms of $(x + y + z)^4$, e.g., looks like this:

$$\binom{4}{1, 2, 1} = 12 \qquad \binom{4}{1, 0, 3} = 4$$
$$x^4 + \cdots + \underset{\downarrow}{\text{——}}\, xy^2z + \cdots + \underset{\downarrow}{\text{——}}\, xz^3 + \cdots + z^4.$$

1.7.4 Example. What is the coefficient of xy in the expansion of $(1 + x + y)^5$? Solution: Because $xy = 1^3 xy$, the multinomial theorem can be applied directly. The answer is $\binom{5}{3,1,1} = 20$. Computing the coefficient of xy in $(2 + x + y)^5$ requires two steps. From the multinomial theorem, the coefficient of $2^3 xy$ is $\binom{5}{3,1,1} = 20$. So, the xy-term in the expansion of $(2 + x + y)^5$ is $20 \times 2^3 \times xy$, and the coefficient we're looking for is $20 \times 8 = 160$.

What about the coefficient of $x^3y^5z^2$ in $(2x-3y+4z)^{10}$? Since the coefficient of $(2x)^3(-3y)^5(4z)^2$ is $\binom{10}{3,5,2} = 2520$, the coefficient of $x^3y^5z^2$ must be $2520\times 2^3\times(-3)^5\times 4^2 = -78,382,080$. □

As with the binomial theorem, numerous identities can be obtained by making various substitutions for the variables in the multinomial theorem. Setting $x = y = z = 1$ in $(x+y+z)^n$, e.g., yields

$$3^n = \sum_{r+s+t=n} \binom{n}{r,s,t}. \tag{1.21}$$

Together with Equation (1.19), this produces the curious identity

$$\sum_{r=0}^{n} C(n,r)2^r = \sum_{r+s+t=n} \binom{n}{r,s,t}.$$

The multinomial theorem tells us that $x_1^{r_1}x_2^{r_2}\cdots x_k^{r_k}$ occurs among the k^n products in the expansion of $(x_1+x_2+\cdots+x_k)^n$ with multiplicity $\binom{n}{r_1,r_2,\ldots,r_k}$, but it does not tell us how many different monomial terms of the form $\binom{n}{r_1,r_2,\ldots,r_k}x_1^{r_1}x_2^{r_2}\cdots x_k^{r_k}$ occur in the expansion.

1.7.5 Theorem. *The number of different monomials of degree n in the k variables $x_1, x_2, \ldots, x_k$ is $C(n+k-1,n)$.*

Proof. From Corollary 1.6.9, the equation $r_1+r_2+\cdots+r_k = n$ has exactly $C(n+k-1,n)$ nonnegative integer solutions. ■

It makes perfect sense, of course, that the multinomial expansion of $(x_1+x_2+\cdots+x_k)^n$ should consist of $C(n+k-1,n)$ different monomial terms! In the first stage of computing

$$(x_1+x_2+\cdots+x_k)(x_1+x_2+\cdots+x_k)\cdots(x_1+x_2+\cdots+x_k),$$

each n-letter word identifies one of the k^n different ways to choose n times from $\{x_1, x_2, \ldots, x_k\}$ with replacement *where order matters*. After simplifying, each term in the resulting sum represents one of the $C(n+k-1,n)$ different ways to choose n times from $\{x_1, x_2, \ldots, x_k\}$ with replacement *where order doesn't matter*.

The multinomial expansion of $(x+y+z)^4$ is a *homogeneous* polynomial* comprised of $C(4+3-1,4)=15$ monomial terms, one of which is

$$\binom{4}{1,2,1}xy^2z = 12xy^2z.$$

Because $(x+y+z)^4$ is *symmetric*†, its multinomial expansion must be symmetric as well. Because switching x and y would interchange, e.g., xy^2z and x^2yz, these two monomials must have the same coefficient in the expansion of $(x+y+z)^4$. Indeed, $\binom{4}{1,2,1} = \binom{4}{2,1,1}$; the value of a multinomial coefficient does not change when two numbers in its bottom row are switched! Form either perspective, it is clear that

$$12x^2yz + 12xy^2z + 12xyz^2 = 12(x^2yz + xy^2z + xyz^2)$$

is a summand in the expansion of $(x+y+z)^4$, and it is natural to group these terms together. Organizing the remaining 12 terms in a similar fashion yields

$$\begin{aligned}(x+y+z)^4 = (x^4+y^4+z^4) + 4(x^3y+x^3z+xy^3+xz^3+y^3z+yz^3)\\ + 6(x^2y^2+x^2z^2+y^2z^2) + 12(x^2yz+xy^2z+xyz^2).\end{aligned} \tag{1.22}$$

The *minimal symmetric polynomials*‡ on the right-hand side of this equation have the symbolic names

$$\begin{aligned}M_{[4]}(x,y,z) &= x^4+y^4+z^4,\\ M_{[3,1]}(x,y,z) &= x^3y+x^3z+xy^3+xz^3+y^3z+yz^3,\\ M_{[2,2]}(x,y,z) &= x^2y^2+x^2z^2+y^2z^2,\\ M_{[2,1,1]}(x,y,z) &= x^2yz+xy^2z+xyz^2.\end{aligned}$$

Using this terminology, Equation (1.22) can be expressed as

$$\begin{aligned}(x+y+z)^4 = M_{[4]}(x,y,z) + \binom{4}{3,1}M_{[3,1]}(x,y,z) + \binom{4}{2,2}M_{[2,2]}(x,y,z)\\ + \binom{4}{2,1,1}M_{[2,1,1]}(x,y,z).\end{aligned} \tag{1.23}$$

*Each term has the same (total) degree, in this case four.

†Switching (any) two variables does not change the polynomial.

‡ "Minimal symmetric polynomial" is a descriptive name. these polynomials are known to experts as *monomial symmetric functions*.

1.7.6 Example. If $37y^3z$ is among the monomial terms of a symmetric polynomial $p(x, y, z)$, then

$$37(x^3y + x^3z + xy^3 + xz^3 + y^3z + yz^3) = 37M_{[3,1]}(x, y, z)$$

must be a summand of $p(x, y, z)$. □

There is nothing quite like a mountain of superscripts and subscripts to dull one's enthusiasm. So, there must be very good reasons for tolerating them in an introductory text. With a little getting used to, Equation (1.23) offers the best way to get a handle on the multinomial theorem, and a whole lot more! Let's see some more examples.

1.7.7 Example. By the multinomial theorem,

$$(x + y + z)^5 = \sum \binom{5}{a, b, c} x^a y^b z^c, \tag{1.24}$$

where the sum is over the nonnegative integer solutions to $a + b + c = 5$. The analog of Equation (1.23) is

$$\begin{aligned}(x + y + z)^5 = M_{[5]}(x, y, z) &+ \binom{5}{4, 1} M_{[4,1]}(x, y, z) + \binom{5}{3, 2} M_{[3,2]}(x, y, z) \\ &+ \binom{5}{3, 1, 1} M_{[3,1,1]}(x, y, z) + \binom{5}{2, 2, 1} M_{[2,2,1]}(x, y, z),\end{aligned} \tag{1.25}$$

where the $C(5 + 3 - 1, 5) = 21$ monomials of degree 5 have been organized into the minimal symmetric polynomials*

$$\begin{aligned}M_{[5]}(x, y, z) &= x^5 + y^5 + z^5, \\ M_{[4,1]}(x, y, z) &= x^4y + x^4z + xy^4 + xz^4 + y^4z + yz^4, \\ M_{[3,2]}(x, y, z) &= x^3y^2 + x^3z^2 + x^2y^3 + x^2z^3 + y^3z^2 + y^2z^3, \\ M_{[3,1,1]}(x, y, z) &= x^3yz + xy^3z + xyz^3, \\ M_{[2,2,1]}(x, y, z) &= x^2y^2z + x^2yz^2 + xy^2z^2.\end{aligned}$$

□

1.7.8 Example. The fifth power of a three-term sum was expanded in Example 1.7.7. Applying the multinomial theorem to the third power of a five-term sum produces

$$\begin{aligned}(a + b + c + d + e)^3 = M_{[3]}(a, b, c, d, e) &+ 3M_{[2,1]}(a, b, c, d, e) \\ &+ 6M_{[1,1,1]}(a, b, c, d, e),\end{aligned} \tag{1.26}$$

*It is just a coincidence that the 4*th* and 5*th* powers of $x + y + z$ involve four and five minimal symmetric polynomials, respectively. The 6*th* power involves seven.

where

$$\begin{aligned} M_{[3]}(a,b,c,d,e) &= a^3+b^3+c^3+d^3+e^3, \\ M_{[2,1]}(a,b,c,d,e) &= (a^2b+a^2c+a^2d+a^2e) \\ &\quad +(ab^2+b^2c+b^2d+b^2e)+\cdots+(ae^2+be^2+ce^2+de^2), \end{aligned} \tag{1.27}$$

and

$$\begin{aligned} M_{[1,1,1]}(a,b,c,d,e) &= abc+abd+abe+acd+ace+ade \\ &\quad +bcd+bce+bde+cde. \end{aligned} \tag{1.28}$$

□

1.7. EXERCISES

1 What is the coefficient of x^5 in the binomial expansion of

(a) $(x+y)^5$? **(b)** $(1+x)^7$? **(c)** $(1+x)^9$?

(d) $(2+x)^7$? **(e)** $(1+2x)^7$? **(f)** $(1-x)^9$?

(g) $(2-x)^4$? **(h)** $(2x+y)^4$? **(i)** $(2x-3y)^8$?

2 What is the coefficient of x^2y^3 in the multinomial expansion of

(a) $(x+y)^5$? **(b)** $(1+x+y)^5$?

(c) $(1+x+y)^8$? **(d)** $(2x-y)^5$?

(e) $(2+x+y)^5$? **(f)** $(3+2x-y)^8$?

(g) $(x-y+z)^5$? **(h)** $(-3+x-2y+z)^8$?

(i) $(1-2x+3y-4z)^7$? **(j)** $(1-2x+3y-4z)^4$?

3 Confirm Equation (1.21) in the case

(a) $n=4$ by setting $x=y=z=1$ in Equation (1.22).

(b) $n=5$ by setting $x=y=z=1$ in Equation (1.25).

4 Prove that $k^n = \sum \binom{n}{r_1,r_2,\ldots,r_k}$, where the sum is over all nonnegative integer sequences $(r_1,r_2,\ldots,r_k)$ that sum to n.

5 Consider the multinomial expansion of $(a+b+c+d+e)^3$ from Example 1.7.8.

(a) Explain why 3 and 6 are the correct coefficients of $M_{[2,1]}(a,b,c,d,e)$ and $M_{[1,1,1]}(a,b,c,d,e)$, respectively.

(b) Explain why $M_{[2,1]}(a,b,c,d,e)$ is a sum, not of $C(5,2)=10$ monomials, but of $P(5,2)=20$.

(c) Explain why $M_{[1,1,1]}(a,b,c,d,e)$ is a sum, not of $P(5,3)=60$ monomials, but of $C(5,3)=10$.

(d) Explain why the equation $5+P(5,2)+C(5,3)=C(7,3)$ is a confirming instance of Theorem 1.7.5.

(e) Without doing any arithmetic, explain why $5+3P(5,2)+6C(5,3)=5^3$.

6 Prove the following special case of Exercise 10(c), Section 1.2, by differentiating $(1+x)^n$ and setting $x=1$:

$$\binom{n}{1}+2\binom{n}{2}+3\binom{n}{3}+\cdots+r\binom{n}{r}+\cdots+n\binom{n}{n}=n2^{n-1}.$$

7 Of the 66 terms in the multinomial expansion of $(x+y+z)^{10}$, how many involve

(a) just one variable?

(b) exactly two variables?

(c) all three variables?

8 Show how Vandermonde's identity,

$$C(m,0)C(n,r)+C(m,1)C(n,r-1)+\cdots+C(m,r)C(n,0)=C(m+n,r),$$

follows from the equation $(x+1)^m(x+1)^n=(x+1)^{m+n}$.

9 Let n be a fixed but arbitrary positive integer. Multiply each multinomial coefficient of the form $\binom{n}{a,b,c,d}$ by $(-1)^{b+d}$ and add the results. Prove that the sum is zero.

10 Compute the coefficient of

(a) x^8 in $(x^2+1)^7$.

(b) x^8 in $(x^2+x)^7$.

(c) x^8 in $(x^2+x+1)^7$.

(d) x^5 in $(1+x+x^2)^7$.

(e) x^2y^2 in $(3+xy+xz+yz)^4$.

(f) $x^2y^2z^2$ in $(3+xy+xz+yz)^4$.

11 Let n be a positive integer and p a positive prime.

(a) Suppose $0\le r_i<p$, $1\le i\le n$. Prove that $\binom{p}{r_1,r_2,\ldots,r_n}$ is a multiple of p.

(b) Prove Fermat's "little theorem"*, i.e., that n^p-n is an integer multiple of p.

*After Pierre de Fermat (1601–1665).

12 Give the (two-decision) inductive proof of the binomial theorem.

13 Write out all the terms of the minimal symmetric polynomial

(a) $M_{[6,4]}(x, y, z)$ **(b)** $M_{[5,5]}(x, y, z)$

14 Denote the coefficient of x^r in $(1 + x + x^2 + \cdots + x^{k-1})^n$ by $C_k(n, r)$.

(a) Show that $C_2(n, r) = C(n, r)$.

(b) Compute $C_3(3, 3)$.

(c) If $n > 1$, show that $C_k(n, r) = \sum_{i=0}^{k-1} C_k(n-1, r-i)$.

15 The multinomial expansion of $(x + y + z)^4$ can be expressed as a linear combination of four minimal symmetric polynomials and the expansion of $(x + y + z)^5$ as a linear combination of five. How many minimal symmetric polynomials are involved in the multinomial expansion of $(x + y + z)^{10}$? (Two of them appear in Exercise 13.)

16 It follows from Theorem 1.6.11 that the number of compositions of n having k or fewer parts is $N(n-1, k-1) = C(n-1, 0) + C(n-1, 1) + \cdots + C(n-1, k-1)$. By Theorem 1.7.5, there are $C([n-1]+k, k-1)$ different monomials in the multinomial expansion of $(x_1 + x_2 + \cdots + x_k)^n$. It does not seem to follow, however, that $N(n-1, k-1) = C([n-1]+k, k-1)$. With $n = 6$ and $k = 3$, $N(5, 2) = 16$ while $C([6-1]+3, 3-1) = C(8, 2) = 28$. Write out enough terms in the expansion of $(x + y + z)^6$ to explain where the numbers 16 and 28 come from.

17 Use Theorem 1.5.1 and the binomial theorem to give another proof of the multinomial theorem.

18 Exercise 14, Section 1.1, asks for an explicit listing of the 24 (exact) positive integer divisors of $360 = 2^3 3^2 5$. *Without* doing any arithmetic, explain why the *sum* of these 24 divisors is given by the product $(1 + 2 + 2^2 + 2^3) \times (1 + 3 + 3^2)(1 + 5)$.

19 Suppose the prime factorization of $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. Prove that the sum of the divisors of n is the product

$$\prod_{t=1}^{k} \left(\sum_{s=0}^{r_t} p_t^s \right).$$

20 Explain how the binomial theorem can be used to prove that $\sum_{r=0}^{n} P(r) = 1$, where $P(r) = C(n, r) p^r q^{n-r}$ is the binomial probability distribution of Section 1.3, Equation (1.5).

21 For a fixed but arbitrary integer $n \geq 2$, define $g(r) = M_{[r]}(1, 2, \ldots, n-1) = 1^r + 2^r + \cdots + (n-1)^r$.

(a) Prove that $\sum_{r=0}^{k} C(k+1, r) g(r) = n^{k+1} - 1$.

(b) Given $g(0), g(1), \ldots, g(r)$, the equation in part (a) can be used to solve for $g(r+1)$. Starting from $g(0) = n - 1$, use this method to compute $g(1)$, $g(2)$, $g(3)$, and $g(4)$.

(c) Compare and contrast with the approach suggested by Section 1.5, Exercise 11.

(d) Explain the connection with Bernoulli numbers (Section 1.5, Exercises 20–22).

22 Show that $\sum_{r=0}^{25} C(50, r)C(50 - r, 25 - r) = 2^{25}C(50, 25)$.

23 Compute

(a) $\sum_{r=25}^{50} C(50, r)C(r, 25)$.

(b) $\sum_{r=0}^{25} (-1)^r C(50, r)C(50 - r, 25)$.

24 Prove that the alternative view of distributivity used to prove the binomial and multinomial theorems is valid, i.e., suppose $S_1, S_2, \ldots, S_n$ are sums of algebraic terms. Prove that $S_1 \times S_2 \times \cdots \times S_n$ is the sum of all products that can be obtained by choosing one term from each sum, multiplying the choices together, doing this in all $o(S_1) \times o(S_2) \times \cdots \times o(S_n)$ possible ways, and adding the resulting products. (*Hint:* Induction on n.)

1.8. PARTITIONS

Something there is that doesn't love a wall.

— Robert Frost (*Mending Wall*)

In the last section, we grouped the $C(n + k - 1, n)$ different monomials from the multinomial expansion of $(x_1 + x_2 + \cdots + x_k)^n$ into certain minimal symmetric polynomials with symbolic names like $M_{[4,1]}$ and $M_{[2,2,1]}$.

1.8.1 Definition. A *partition* of n having m *parts* is an unordered collection of m positive integers that sum to n.

1.8.2 Example. The number 6 is said to be *perfect*[*] because it is the sum of its proper divisors: $6 = 1 + 2 + 3$. Since addition is commutative, this sum could just as well have been written $2 + 3 + 1$. In this context, $1 + 2 + 3$ is the same as

[*]A Christian theologian once argued that God, who could have created the universe in an instant, chose instead to labor for 6 days in order to emphasize the perfection of His creation. (It is just an accident that this book has 6 chapters.)

$2 + 3 + 1$ but different from $4 + 2$. In expressing the prefection of 6, what interests us is the unordered collection of its proper divisors, the partition whose parts are 3, 2, and 1. □

Two partitions of n are equal if and only if they have the same parts with the same multiplicities. By way of contrast, a *composition* of n (Definition 1.6.10) is an *ordered* collection of positive integers that sum to n. Compositions are sometimes called *ordered partitions*. Two compositions are equal if and only if they have the same parts with the same multiplicities, *in the same order.*

Our discussion of partitions will be simplified by the adoption of some notation.

1.8.3 Definition. An m-part partition of n is represented by a sequence $\pi = [\pi_1, \pi_2, \ldots, \pi_m]$ in which the parts are arranged so that $\pi_1 \geq \pi_2 \geq \cdots \geq \pi_m > 0$. The number of parts is the *length* of π, denoted $\ell(\pi) = m$. The shorthand expression $\pi \vdash n$ signifies that "π is a partition of n".

In ordinary English usage, arranging the parts of a partition from largest to smallest would typically be called "orderning" the parts. This semantic difficulty is the source of more than a little confusion. It is precisely because a partition is unordered that we are free to arrange its parts any way we like. The 5 cards comprising a poker hand can be arranged in any one of $5! = 120$ different ways. But, no matter how the cards are arranged or rearranged, the poker hand is the same. So it is with partitions. A composition, on the other hand, is some specified arrangement of the parts of a partition. By convention (Definition 1.8.3), we uniformly choose one such composition to represent each partition.

1.8.4 Example. The three-part partitions of 6 are [4, 1, 1], [3, 2, 1], and [2, 2, 2]. There are 3 ways to arrange the parts of [4, 1, 1], 6 ways to arrange the parts of [3, 2, 1], but only one way to arrange the parts of [2, 2, 2]. Taken together, these 10 arrangements comprise the compositions of 6 having 3 parts (as illustrated in Fig. 1.6.2). □

Already it seems convenient to introduce some additional shorthand notation. Rather than [4, 1, 1] and [2, 2, 2], we will write $[4, 1^2]$ and $[2^3]$, respectively. Similarly, the partition [5, 5, 3, 3, 3, 3, 2, 2, 2, 1] is abbreviated $[5^2, 3^4, 2^3, 1]$. In this notation superscripts denote, not exponents, but multiplicities. In the 10-part partition $[5^2, 3^4, 2^3, 1]$, the piece 3^4 contributes, not $3 \times 3 \times 3 \times 3 = 81$, but $3 + 3 + 3 + 3 = 12$ to the sum

$$5 + 5 + 3 + 3 + 3 + 3 + 2 + 2 + 2 + 1 = 29.$$

The m-part compositions of n were counted in Theorem 1.6.11. (They number $C(n-1, m-1)$.) Counting the m-part partitions of n is not so easy. Let's begin by giving this number a name.

n \ m	1	2	3	4	5	6	7
1	1						
2	1	1					
3	1	1	1				
4	1	$p_2(4)$	1	1			
5	1	2	2	1	1		
6	1	$p_2(6)$	3	$p_4(6)$	1	1	
7	1	$p_2(7)$	$p_3(7)$	$p_4(7)$	$p_5(7)$	1	1
				...			

Figure 1.8.1. The partition triangle.

1.8.5 Definition. The number of m-part partitions of n is denoted $p_m(n)$.

1.8.6 Example. From Example 1.8.4, $p_3(6) = 3$. The seven partitions of 5 are $[5]$, $[4,1]$, $[3,2]$, $[3,1^2] = [3,1,1]$, $[2^2,1] = [2,2,1]$, $[2,1^3] = [2,1,1,1]$, and $[1^5] = [1,1,1,1,1]$, having lengths 1, 2, 2, 3, 3, 4, and 5, respectively. Hence, $p_1(5) = 1$, $p_2(5) = 2$, $p_3(5) = 2$, $p_4(5) = 1$, and $p_5(5) = 1$. □

Because $[n]$ is the only partition of n having just one part and, at the other extreme, $[1^n]$ is the only partition of n having n parts, $p_1(n) = 1 = p_n(n)$ for all n. If $n \geq 2$, then $[2,1^{n-2}]$ is the only partition of n having length $n-1$, so $p_{n-1}(n) = 1$ as well.

The numbers $p_m(n)$ are displayed in the Pascal-like *partition triangle* of Fig. 1.8.1, where it is understood that $p_m(n) = 0$ when $m > n$. What is needed is a Pascal-like relation that would allow the entries of this triangle to be filled in a row at a time.

1.8.7 Theorem. *The number of m-part partitions of n is* $p_m(n) = p_{m-1}(n-1) + p_m(n-m)$, $1 < m < n$.

Proof. If π is an m-part partition of n, then $\pi_m = 1$ or it doesn't. There are $p_{m-1}(n-1)$ partitions of the first kind. Because $\pi \leftrightarrow [\pi_1 - 1, \pi_2 - 1, \ldots, \pi_m - 1]$ is a one-to-one correspondence between the m-part partitions of n satisfying $\pi_m > 1$ and the m-part partitions of $n-m$, there must be $p_m(n-m)$ partitions of the second kind. ■

From Theorem 1.8.7, $p_2(4) = p_1(3) + p_2(4-2) = p_1(3) + p_2(2) = 1 + 1 = 2$. (The two-part partitions of 4 are [3, 1] and $[2^2]$.) Similarly, $p_2(6) = p_1(6) + p_2(4) = 1 + 2 = 3$, and $p_4(6) = p_3(5) + p_4(2) = 2 + 0 = 2$. This completes Fig. 1.8.1 through row 6. Rows 7–10 are completed in Fig. 1.8.2.

1.8.8 Definition. Denote the number of partitions of n by $p(n) = p_1(n) + p_2(n) + \cdots + p_n(n)$.

n \ m	1	2	3	4	5	6	7	8	9	10
1	1									
2	1	1								
3	1	1	1							
4	1	2	1	1						
5	1	2	2	1	1					
6	1	3	3	2	1	1				
7	1	3	4	3	2	1	1			
8	1	4	5	5	3	2	1	1		
9	1	4	7	6	5	3	2	1	1	
10	1	5	8	9	7	5	3	2	1	1
					⋯					

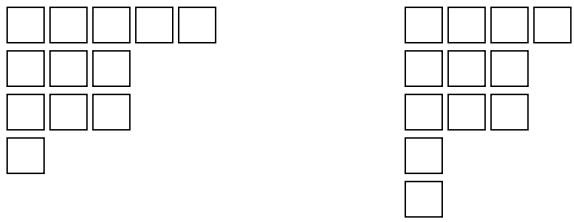
Figure 1.8.2. The partition numbers $p_m(n)$.

Just as the nth row sum of Pascal's triangle is 2^n, the total number of subsets of an n-element set, the nth row sum of the partition triangle is $p(n)$, the total number of partitions of n. Summing, rows 9 and 10 of Fig. 1.8.2, e.g., yields the partition numbers $p(9) = 30$ and $p(10) = 42$.*

If π is an m-part partition of n, its *Ferrers diagram*,† $F(\pi)$, consists of n "boxes" arrayed in m left-justified rows, where the number of boxes in row i is π_i. The diagrams for $[5, 3^2, 1]$ and $[4, 3^2, 1^2]$, e.g., appear in Fig. 1.8.3.

1.8.9 Definition. The *conjugate* of $\pi \vdash n$ is the partition $\pi^* \vdash n$ whose jth part is the number of boxes in the jth column of $F(\pi)$.

Because the number of boxes in row j of $F(\pi^*)$ is equal to the number of boxes in column j of $F(\pi)$ for all j, the two diagrams are *transposes* of each other. In



$F([5, 3^2, 1])$ $F([4, 3^2, 1^2])$

Figure 1.8.3. Two Ferrers diagrams.

*The partition numbers grow rapidly with n. MacMahon showed, e.g., that $p(200) = 3,972,999,029,388$.

†Named for Norman Macleod Ferrers (1829–1903) but possibly used earlier by J. J. Sylvester (1814–1897).

particular, partition $\alpha = \pi^*$ if and only if $\alpha^* = \pi$. This situation is illustrated in Fig. 1.8.3 for the conjugate pair $[5, 3^2, 1]$ and $[4, 3^2, 1^2]$.

The number of boxes in the jth column of $F(\pi)$ is equal to the number of rows of $F(\pi)$ that contain at least j boxes, i.e., π_j^* is equal to the number of parts of π that are not less than j. Said another way, the jth part of π^* is

$$\pi_j^* = o(\{i : \pi_i \geq j\}). \tag{1.29}$$

1.8.10 Theorem. *The number of m-part partitions of n is equal to the number of partitions of n whose largest part is m.*

Proof. If π is an m-part partition of n, then m is the number of boxes in the first column of $F(\pi)$, i.e., $m = \pi_1^*$, the largest part of π^*. Hence, in the one-to-one correspondence between partitions and their conjugates, the set of m-part partitions corresponds to the set of partitions whose largest part is m. ■

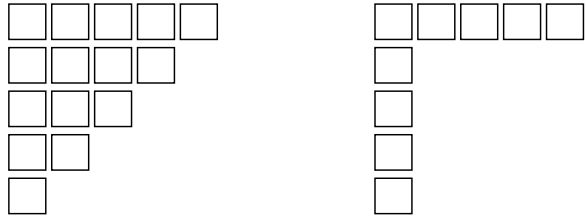
1.8.11 Definition. Partition π is *self-conjugate* if $\pi^* = \pi$.

1.8.12 Example. Because $\pi = \pi^*$ if and only if $F(\pi) = F(\pi^*) = F(\pi)^t$, the transpose of $F(\pi)$, π is self-conjugate if and only if its Ferrers diagram is symmetric about the "main diagonal". Thus, merely by glancing at Fig. 1.8.4, one sees that $[5, 4, 3, 2, 1]$ and $[5, 1^4]$ are self-conjugate partitions. On the other hand, without a Ferrers diagram to look at, it is much less obvious that $[5^2, 4, 3, 2]$ is self-conjugate. □

Knowing something about partitions, we can now give a formal definition of "minimal symmetric polynomial".

1.8.13 Definition. Let k and n be positive integers. Suppose π is an m-part partition of n. If $k \geq m$, the *minimal symmetric polynomial*

$$M_\pi(x_1, x_2, \ldots, x_k) = \sum x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k},$$



F ([5, 4, 3, 2, 1]) F ([5, 1^4])

Figure 1.8.4. Two self-conjugate partitions.

where the sum is over all different rearrangements $(r_1, r_2, \ldots, r_k)$ of the k-tuple $(\pi_1, \pi_2, \ldots, \pi_m, 0, \ldots, 0)$ that is obtained by appending $k - m$ zeros to the end of π. If $k < m$, then $M_\pi(x_1, x_2, \ldots, x_k) = 0$.

If, e.g., $\pi = [\pi_1, \pi_2] = [2, 2]$ and $k = 3$, the *different rearrangements* of $(\pi_1, \pi_2, 0)$ are (2, 2, 0), (2, 0, 2), and (0, 2, 2), and *not* the six different-*looking* ways to rearrange the symbols π_1, π_2, and 0. In particular,

$$M_{[2,2]}(x, y, z) = x^2y^2 + x^2z^2 + y^2z^2.$$

If $\pi \vdash n$ and $m = \ell(\pi) \leq k$, then each monomial $x_1^{r_1}x_2^{r_2}\cdots x_k^{r_k}$ in Definition 1.8.13 has (total) degree $r_1 + r_2 + \cdots + r_k = \pi_1 + \pi_2 + \cdots + \pi_m = n$, i.e., $M_\pi(x_1, x_2, \ldots, x_k)$ is homogeneous of degree n.

1.8.14 Example. From Fig. 1.8.2, there are $p_1(6) + p_2(6) + p_3(6) = 1 + 3 + 3 = 7$ different partitions of 6 having at most three parts. Hence, there are 7 different minimal symmetric polynomials of degree 6 in the variables x, y, and z, namely,

$$\begin{aligned}
M_{[6]}(x, y, z) &= x^6 + y^6 + z^6,\\
M_{[5,1]}(x, y, z) &= x^5y + x^5z + xy^5 + xz^5 + y^5z + yz^5,\\
M_{[4,2]}(x, y, z) &= x^4y^2 + x^4z^2 + x^2y^4 + x^2z^4 + y^4z^2 + y^2z^4,\\
M_{[3^2]}(x, y, z) &= x^3y^3 + x^3z^3 + y^3z^3,\\
M_{[4,1^2]}(x, y, z) &= x^4yz + xy^4z + xyz^4,\\
M_{[3,2,1]}(x, y, z) &= x^3y^2z + x^3yz^2 + x^2y^3z + x^2yz^3 + xy^3z^2 + xy^2z^3,
\end{aligned}$$

and

$$M_{[2^3]}(x, y, z) = x^2y^2z^2. \qquad \square$$

Minimal symmetric polynomials are to symmetric polynomials what atoms are to molecules. they are the basic building blocks.

1.8.15 Theorem. *The polynomial $f = f(x_1, x_2, \ldots, x_k)$ is symmetric in $x_1, x_2, \ldots, x_k$ if and only if it is a linear combination of minimal symmetric polynomials.*

Proof. Because minimal symmetric polynomials are symmetric, any linear combination of minimal symmetric polynomials in $x_1, x_2, \ldots, x_k$ is symmetric.

Conversely, suppose $cx_1^{s_1}x_2^{s_2}\cdots x_k^{s_k}$ is among the nonzero terms of $f(x_1, x_2, \ldots, x_k)$. Then $(s_1, s_2, \ldots, s_k)$ is a rearrangement of $(\alpha_1, \alpha_2, \ldots, \alpha_m, 0, \ldots, 0)$ for some partition α. Because f is symmetric, $cx_1^{r_1}x_2^{r_2}\cdots x_k^{r_k}$ must occur among its terms for *every* rearrangement $(r_1, r_2, \ldots, r_k)$ of $(\alpha_1, \alpha_2, \ldots, \alpha_m, 0, \ldots, 0)$, i.e.,

$cM_\alpha(x_1, x_2, \ldots, x_k)$ is a summand of f. Therefore, $f(x_1, x_2, \ldots, x_k) - cM_\alpha(x_1, x_2, \ldots, x_k)$ is a symmetric polynomial with fewer terms than f, and the result follows by induction. ■

1.8.16 Example. Let

$$\begin{aligned} f(a,b,c,d) = {} & 2a^3 - a^2b - a^2c - a^2d - ab^2 + abc + abd - ac^2 + acd - ad^2 \\ & + 2b^3 - b^2c - b^2d - bc^2 + bcd - bd^2 + 2c^3 - c^2d - cd^2 + 2d^3. \end{aligned}$$

Probably the easiest way to confirm that this polynomial is symmetric is to express it as

$$f(a,b,c,d) = 2M_{[3]}(a,b,c,d) - M_{[2,1]}(a,b,c,d) + M_{[1^3]}(a,b,c,d). \qquad \square$$

There are, of course, easier ways to verify that the polynomial $f(x_1, x_2, \ldots, x_k) = (x_1 + x_2 + \cdots + x_k)^n$ is symmetric than by expressing it as a linear combination of minimal symmetric polynomials. On the other hand, because it *is* symmetric, $f(x_1, x_2, \ldots, x_k)$ *is* a linear combination of minimal symmetric polynomials. What combination? The answer to that question is what the multinomial theorem is all about:

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\pi \vdash n} \binom{n}{\pi} M_\pi(x_1, x_2, \ldots, x_k), \tag{1.30}$$

where the coefficient $\binom{n}{\pi}$ is an abbreviation for the multinomial coefficient whose bottom row consists of the $\ell(\pi)$ parts of π. (Recall that $M_\pi(x_1, x_2, \ldots, x_k) = 0$ whenever $k < \ell(\pi)$.)

1.8.17 Example. Together with Example 1.8.14, Equation (1.30) yields

$$\begin{aligned} (x+y+z)^6 = {} & M_{[6]}(x,y,z) + 6M_{[5,1]}(x,y,z) + 15M_{[4,2]}(x,y,z) \\ & + 20M_{[3^2]}(x,y,z) + 30M_{[4,1^2]}(x,y,z) \\ & + 60M_{[3,2,1]}(x,y,z) + 90M_{[2^3]}(x,y,z). \end{aligned} \qquad \square$$

1.8. EXERCISES

1 Explicitly write down

(a) all 11 partitions of 6.

(b) all 8 partitions of 7 having at most three parts.

(c) all 8 partitions of 7 whose largest part is at most three.

2 Show that

(a) $p_{n-2}(n) = 2, \quad n \geq 4.$

(b) $p_{n-3}(n) = 3, \quad n \geq 6.$

(c) for all $n \geq 6$, the last four (nonzero) numbers in row n of the partition triangle are 3, 2, 1, 1.

(d) $p_2(n) = \lfloor n/2 \rfloor$, the greatest integer not exceeding $\frac{1}{2}n$.

3 Compute rows 11–15 of the partition triangle.

4 Evaluate

(a) $p(11)$. **(b)** $p(12)$.

(c) $p(13)$. **(d)** $p(14)$.

5 The number of partitions of n into three or fewer parts turns out to be the nearest integer to $\frac{1}{12}(n+3)^2$.

(a) Confirm this fact for $1 \leq n \leq 6$.

(b) Confirm this fact for $7 \leq n \leq 10$.

(c) Determine the number of different minimal symmetric polynomials, in three variables, of degee $n = 27$.

6 How many different eight-part compositions can be produced by rearranging the parts of the partition

(a) $[5^3, 4, 2^4]$? **(b)** $[2^5, 1^3]$?

(c) $[8, 7, 6, 5, 4, 3, 2, 1]$?

(*Hint*: Don't try to write them all down.)

7 Confirm, by writing them all down, that there are $p_3(9)$ four-part partitions $\pi \vdash 10$ that satisfy $\pi_4 = 1$.

8 Confirm Theorem 1.8.10 for the pair

(a) $n = 5$ and $m = 2$. **(b)** $n = 6$ and $m = 3$.

(c) $n = 10$ and $m = 3$. **(d)** $n = 10$ and $m = 5$.

9 Prove that the partition number $p(n) \geq 2^{\lfloor \sqrt{n} \rfloor}$ for all sufficiently large n.

10 Exhibit Ferrers diagrams for all the self-conjugate partitions of

(a) 6. **(b)** 10. **(c)** 17.

11 Let $p_{\text{odd}}(n)$ be the number of partitions of n each of whose parts is odd and $p_{\text{dist}}(n)$ be the number of partitions of n having distinct parts. It is proved in Section 4.3 that $p_{\text{odd}}(n) = p_{\text{dist}}(n)$ for all n. Confirm this result now for the case

(a) $n = 5$. **(b)** $n = 6$. **(c)** $n = 7$. **(d)** $n = 8$.

12 The first odd "abundant" number is 945.

(a) How many positive integer divisors does 945 have?

(b) Sum up the "proper" divisors of 945 (those divisors less than 945).

(c) What do you suppose an "abundant" number is?

13 Prove that the number of partitions of n with at most m parts is equal to the number of partitions of $n + m$ with exactly m parts, i.e., prove that

$$\sum_{k=1}^{m} p_k(n) = p_m(n+m)$$

(a) by induction on m.

(b) by means of Ferrers diagrams.

14 Prove that

(a) $p_m(n) = p_m(n-m) + p_{m-1}(n-m) + \cdots + p_1(n-m), \quad m < n.$

(b) $p(n) = p_n(2n).$

(c) $p(n) = p_{n+m}(2n+m), \quad m \geq 0.$

(d) For all $n \geq 8$, the last five (nonzero) numbers in row n of the partition triangle are 5, 3, 2, 1, 1.

(e) What is the generalization of Exercises 2(c) and 14(d)?

15 Suppose $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_m]$ and $\beta = [\beta_1, \beta_2, \ldots, \beta_k]$ are two partitions of n. Then α *majorizes* β if $m \leq k$ and

$$\sum_{i=1}^{r} \alpha_i \geq \sum_{i=1}^{r} \beta_i, \qquad 1 \leq r \leq m.$$

(a) Show that [6, 4] majorizes [4, 3, 2, 1].

(b) Show that [4, 3, 2, 1] majorizes $[3^2, 2^2]$.

(c) If α majorizes β and β majorizes γ, prove that α majorizes γ.

(d) Prove that α majorizes β if and only if β^* majorizes α^*.

16 Confirm that the coefficients 1, 6, 15, 20, 30, 60, and 90 in Example 1.8.17 are all correct.

17 Prove that the number of self-conjugate partitions of n is equal to the number of partitions of n that have distinct parts each of which is odd.

18 The great Indian mathematician Srinivasa Ramanujan (1887–1920) proved a number of theorems about partition numbers. Among them is the fact that $p(5n+4)$ is always a multiple of 5. Confirm this fact for $n = 0$, 1, and 2.

19 We saw in Section 1.6 that the equation $a+b+c+d+e=10$ has a total of $C(9,4)=126$ different positive integer solutions. Of these, how many satisfy $a \geq b \geq c \geq d \geq e$?

20 Denote by $t(n)$ the number of partitions of n each of whose parts is a power of 2 (including $2^0=1$).

(a) Compute $t(n), \quad 1 \leq n \leq 6$.

(b) Prove that $t(2n+1)=t(2n), \quad n \geq 1$.

(c) Prove that $t(2n)=t(n)+t(2n-2), \quad n \geq 2$.

(d) Prove that $t(n)$ is even, $n \geq 2$.

21 When $p(a,b,c,d)=(a+b+c+d)^{10}$ is expressed as a linear combination of minimal symmetric polynomials, compute the coefficient of

(a) $M_{[8,1^2]}(a,b,c,d)$. **(b)** $M_{[10]}(a,b,c,d)$.

(c) $M_{[3^2,2^2]}(a,b,c,d)$. **(d)** $M_{[3^2,2,1^2]}(a,b,c,d)$.

22 Compute the coefficient of

(a) $M_{[2,1^3]}(x_1,x_2,x_3,x_4,x_5,x_6)$ in $(x_1+x_2+x_3+x_4+x_5+x_6)^5$.

(b) $M_{[2,1^3]}(x_1,x_2,x_3,x_4,x_5)$ in $(x_1+x_2+x_3+x_4+x_5)^5$.

23 Express $p(x,y,z)$ as a linear combination of minimal symmetric polynomials, where

(a) $p(x,y,z)=5x^2+5y^2+5z^2-xy-xz-yz$.

(b) $p(x,y,z)=2x(1+2yz)-3x^2+2y-3y^2+2z-3z^2$.

24 Write out, in full,

(a) $M_{[5]}(w,x,y,z)$. **(b)** $M_{[4,1]}(w,x,y,z)$.

(c) $M_{[1^3]}(w,x,y,z)$. **(d)** $M_{[8,1]}(x,y,z)$.

(e) $M_{[3,2,1]}(x,y,z)$. **(f)** $M_{[3,1^2]}(x,y,z)$.

25 Theorem 1.8.15 can be use to custom design symmetric polynomials. The *homogeneous symmetric function* of degree n is defined by $H_0(x_1,x_2,\ldots,x_k)=1$ and

$$H_n(x_1,x_2,\ldots,x_k)=\sum_{\pi\vdash n} M_\pi(x_1,x_2,\ldots,x_k), \qquad n \geq 1,$$

where, recall, $M_\pi(x_1,x_2,\ldots,x_k)=0$ whenever $\ell(\pi)>k$. Explicitly write out all the terms in

(a) $H_2(x,y)$. **(b)** $H_3(x,y)$.

(c) $H_2(a,b,c)$. **(d)** $H_3(a,b,c)$.

26 Let $H_n(x_1,x_2,\ldots,x_k)$ be the homogeneous symmetric function defined in Exercise 25.

(a) Compare and contrast $H_n(x_1, x_2, \ldots, x_k)$ with $(x_1 + x_2 + \cdots + x_k)^n$. (*Hint:* See Equation (1.30).)

(b) Show that $H_n(x_1, x_2, \ldots, x_k)$ is the sum of $p_1(n) + p_2(n) + \cdots + p_k(n)$ different minimal symmetric polynomials.

(c) Prove that $H_n(x_1, x_2, \ldots, x_k)$ is the sum of $C(n + k - 1, n)$ different terms. (*Hint:* Theorem 1.7.5.)

(d) Prove that $H_n(x_1, x_2, \ldots, x_k) = H_n(x_1, x_2, \ldots, x_{k-1}) + x_k H_{n-1}(x_1, x_2, \ldots, x_k)$.

(e) Prove that $H_s(x_1, x_2, \ldots, x_n) - H_s(x_2, \ldots, x_n, x_{n+1}) = (x_1 - x_{n+1}) H_{s-1}(x_1, x_2, \ldots, x_{n+1})$.

27 Suppose m is a nonnegative integer. A *lattice path* of length m in the cartesian plane begins at the origin and consists of m unit "steps" each of which is either up or to the right. If s of the steps are up and $r = m - s$ of them are to the right, the path terminates at the point (r, s). "Directions" for the lattice path illustrated in Fig. 1.8.5 might go something like this: Beginning from (0, 0) (the lower left-hand corner), take two steps up, two to the right, one up, three right, one up, one right, and one up. If this grid were a street map and one were in the business of delivering packages, lattice paths would probably the called "routes", and these directions might be given in shorthand as UURRURRRURU. Suppose r and s are fixed but arbitrary nonnegative integers, with $r + s > 0$.

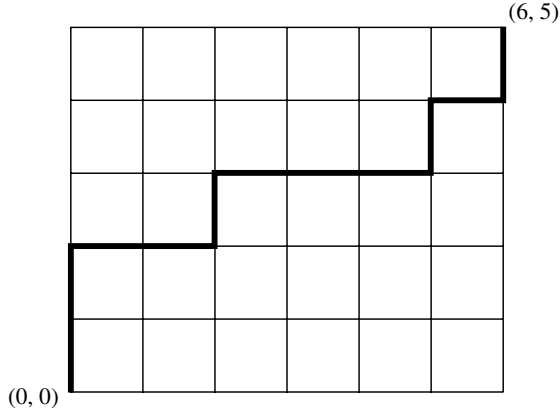


Figure 1.8.5

(a) Compute the number of different lattice paths from $(0, 0)$ to (r, s).

(b) The lattice path in Figure 1.8.5 "partitions" the 5×6 grid into two pieces. In this case, the piece above the path might easily be mistaken for the Ferrers diagram of partition $\pi = [6, 5, 2]$. Use this observation to compute the number of partitions that have at most s parts each of which is at most r.

(c) As an alternative to the alphabet $\{R, U\}$, one could just as well encode lattice paths using, say, the horizontal displacement of each step. In this scheme, each vertical step would correspond to a 0 and each horizontal step to a 1. For example, the lattice path in Fig. 1.8.5 would be encoded as the binary word 00110111010, a word of length 11 and "weight" 6. Compute the number of different binary words of length $r + s$ and weight r.

(d) Consider a binary word $w = b_1 b_2 \dots b_m$ of length m consisting of the letters (bits) $b_1, b_2, \dots, b_m$. The *inversion number* $\text{inv}(b_i) = 0$ if $b_i = 1$; if $b_i = 0$, it is the number of 1's to the left of b_i. If, e.g., $u = 00110111010$ (corresponding to Fig 1.8.5), the inversion numbers of its bits are 0, 0, 0, 0, 2, 0, 0, 0, 5, 0, and 6, respectively. In this case, the nonzero inversion numbers of u are precisely the parts of the corresponding partition π from part (b). Show that, in general, the nonzero inversion numbers of the bits of w are the parts of the partition to which w corresponds.

28 Galileo Galilei (1564–1642) once wondered about the frequency of throwing totals of 9 and 10 with three dice.

(a) Show that 9 and 10 have the same number of 3-part partitions each of whose parts is at most 6.

(b) Explain why it does not follow that 9 and 10 occur with equal frequency when three dice are rolled (repeatedly).

29 Suppose π is an m-part partition of n. Show that the number of different compositions of n that can be obtained by rearranging the parts of π is multinomial coefficient $\binom{n}{\pi}$.

1.9. ELEMENTARY SYMMETRIC FUNCTIONS

What immortal hand or eye could frame thy fearful symmetry?

— William Blake (*Songs of Experience*)

Let's begin by exploring the relationship between the coefficients of a monic polynomial

$$p(x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_n \tag{1.31a}$$

and its roots $a_1, a_2, \dots, a_n$. Writing $p(x)$ in the form

$$p(x) = (x - a_1)(x - a_2) \cdots (x - a_n) \tag{1.31b}$$

suggests mimicking the alternative view of distributivity used to prove the binomial theorem, i.e., select one of x or $-a_1$ from the first set of parentheses, one of x or $-a_2$ from the second set, and so on. Finally, choose one of x or $-a_n$ from the nth set. String these selections together, in order, so as to create an n-letter "word", something like

$$(-a_1)xxx(-a_5)x\ldots xx.$$

If the total number of x's in this word is $n-r$, then the remaining "letters" are of the form $(-a_i)$ for r different values of i.

The sum of all such words is an inventory of the 2^n ways to make the sequence of decisions. Replacing each word with a monomial of the form

$$(-1)^r(a_1a_5\cdots)x^{n-r}$$

and combining terms of the same degree (in x) should yield Equation (1.31a). So, the coefficient of x^{n-r} in Equation (1.31a) must be the sum of all possible terms of the form

$$(-1)^r a_{i_1}a_{i_2}\cdots a_{i_r},$$

where $1 \le i_1 < i_2 < \cdots < i_r \le n$. In other words, c_r is $(-1)^r$ times the sum of the products of the roots taken r at a time. Let's give that sum a name.

1.9.1 Definition. The rth *elementary symmetric function*

$$E_r(x_1, x_2, \ldots, x_n)$$

is the sum of all possible products of r elements chosen from $\{x_1, x_2, \ldots, x_n\}$ without replacement where order doesn't matter.

Evidently, $E_r(x_1, x_2, \ldots, x_n)$ is the sum of all $C(n, r)$ "square-free" monomials of (total) degree r in the variables $x_1, x_2, \ldots, x_n$. Our conclusions about the relationship between roots and coefficients can now be stated as follows.

1.9.2 Theorem. *Let $a_1, a_2, \ldots, a_n$ be the roots of a monic polynomial $p(x) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n$. Then*

$$c_r = (-1)^r E_r(a_1, a_2, \ldots, a_n), \qquad 1 \le r \le n. \tag{1.32}$$

1.9.3 Example. Suppose $f(x) = x^4 - x^2 + 2x + 2$. Then, counting multiplicities, $f(x)$ has four (complex) roots; call them a_1, a_2, a_3, and a_4. Setting $E_r = E_r(a_1, a_2, a_3, a_4)$ and comparing the actual coefficients of $f(x)$ with the generic

formula $f(x) = x^4 - E_1x^3 + E_2x^2 - E_3x + E_4$, we find that

$$\begin{aligned}
0 &= E_1(a_1, a_2, a_3, a_4) = a_1 + a_2 + a_3 + a_4,\\
-1 &= E_2(a_1, a_2, a_3, a_4) = a_1a_2 + a_1a_3 + a_1a_4 + a_2a_3 + a_2a_4 + a_3a_4,\\
-2 &= E_3(a_1, a_2, a_3, a_4) = a_1a_2a_3 + a_1a_2a_4 + a_1a_3a_4 + a_2a_3a_4,\\
2 &= E_4(a_1, a_2, a_3, a_4) = a_1a_2a_3a_4.
\end{aligned}$$

So, just from its coefficients, we can tell, e.g., that the sum of the roots of $f(x)$ is 0 and that their product is 2. □

1.9.4 Example. Suppose $a_i = 1$, $1 \le i \le n$, so that

$$\begin{aligned}
p(x) &= (x-1)^n\\
&= C(n,0)x^n - C(n,1)x^{n-1} + C(n,2)x^{n-2} - \cdots + (-1)^n C(n,n).
\end{aligned}$$

In this case, $E_r(1, 1, \ldots, 1) = C(n, r)$, $1 \le r \le n$, which makes perfect sense. After all, $E_r(a_1, a_2, \ldots, a_n)$ is the sum of all $C(n, r)$ products of the a_i's taken r at a time. If $a_i = 1$ for all i, then every one of these products is 1, and their sum is $E_r(1, 1, \ldots, 1) = C(n, r)$. □

Consistent with the fact that the leading coefficient of a monic polynomial is 1, we *define* $E_0(x_1, x_2, \ldots, x_n) = 1$.

1.9.5 Example. If $a_i = i$, $1 \le i \le 4$, then

$$\begin{aligned}
&E_0(1,2,3,4) = 1,\\
&E_1(1,2,3,4) = 1 + 2 + 3 + 4 = 10,\\
&E_2(1,2,3,4) = 1\times 2 + 1\times 3 + 1\times 4 + 2\times 3 + 2\times 4 + 3\times 4 = 35,\\
&E_3(1,2,3,4) = 1\times 2\times 3 + 1\times 2\times 4 + 1\times 3\times 4 + 2\times 3\times 4 = 50,\\
&E_4(1,2,3,4) = 1\times 2\times 3\times 4 = 24.
\end{aligned}$$

If $p(x) = (x-1)(x-2)(x-3)(x-4)$, then, with the abbreviation $E_r = E_r(1,2,3,4)$, $0 \le r \le 4$, Theorem 1.9.2 yields

$$\begin{aligned}
p(x) &= E_0x^4 - E_1x^3 + E_2x^2 - E_3x + E_4\\
&= x^4 - 10x^3 + 35x^2 - 50x + 24.
\end{aligned}$$

Let's confirm this directly:

$$\begin{aligned}
p(x) &= (x-1)(x-2)(x-3)(x-4)\\
&= (x^2 - 3x + 2)(x^2 - 7x + 12)\\
&= x^4 - (7+3)x^3 + (12 + 21 + 2)x^2 - (36 + 14)x + 24.
\end{aligned}$$ □

Apart from their intrinsic significance, elementary symmetric functions have important (and, in some cases, unexpected) connections with other combinatorial

objects. Recall, e.g., that the number of ways to choose $n+1$ items from an m-element set without replacement where order matters is

$$P(m, n+1) = m(m-1)(m-2)\cdots(m-n).$$

1.9.6 Definition. The *falling factorial function* is defined by $x^{(0)} = 1$ and

$$x^{(n+1)} = x(x-1)(x-2)\cdots(x-n), \qquad n \geq 0.$$

Since $x^{(n+1)}$ is a polynomial of degree $n+1$, whose roots are $0, 1, \ldots, n$, and because $E_r(0, 1, \ldots, n) = E_r(1, 2, \ldots, n)$, $0 \leq r \leq n$, it follows that

$$\begin{aligned} x^{(n+1)} = {} & x^{n+1} - E_1(1, 2, \ldots, n)x^n + E_2(1, 2, \ldots, n)x^{n-1} - \cdots \\ & + (-1)^n E_n(1, 2, \ldots, n)x. \end{aligned}$$

In particular,

$$\begin{aligned} P(m, n+1) = m\big[& m^n - E_1(1, 2, \ldots, n)m^{n-1} + E_2(1, 2, \ldots, n)m^{n-2} - \cdots \\ & + (-1)^n E_n(1, 2, \ldots, n)\big]. \end{aligned}$$

Let's take a brief excursion* and investigate the numbers $E_t(1, 2, \ldots, n)$.

1.9.7 Definition. The *elementary number*

$$e(n, t) = \begin{cases} 0, & t < 0 \quad \text{or} \quad t > n, \\ E_t(1, 2, \ldots, n), & 0 \leq t \leq n. \end{cases}$$

Apart from Example 1.9.5, where we computed

$$\begin{aligned} (x-1)(x-2)(x-3)(x-4) &= x^4 - 10x^3 + 35x^2 - 50x + 24 \\ &= x^4 - e(4,1)x^3 + e(4,2)x^2 - e(4,3)x + e(4,4), \end{aligned}$$

we know that

$$\begin{aligned} e(n, 0) &= E_0(1, 2, \ldots, n) \\ &= 1, \\ e(n, 1) &= E_1(1, 2, \ldots, n) \\ &= 1 + 2 + \cdots + n \\ &= \frac{1}{2}n(n+1), \\ e(n, n) &= E_n(1, 2, \ldots, n) \\ &= 1 \times 2 \times \cdots \times n \\ &= n!. \end{aligned}$$

*There is a serious side to this excursion. In Chapter 2, we will discover that $s(n, r) = E_{n-r}(1, 2, \ldots, n-1)$ is a *Stirling number of the first kind*.

n \ t	0	1	2	3	4	5	6	7
1	1	1						
2	1	3	2					
3	1	6	$e(3,2)$	6				
4	1	10	35	50	24			
5	1	15	$e(5,2)$	$e(5,3)$	$e(5,4)$	120		
6	1	21	$e(6,2)$	$e(6,3)$	$e(6,4)$	$e(6,5)$	720	
7	1	28	$e(7,2)$	$e(7,3)$	$e(7,4)$	$e(7,5)$	$e(7,6)$	5040
				⋯				

Figure 1.9.1. Elementary triangle.

This gives us a start at filling in some entries of the *elementary triangle* exhibited in Fig. 1.9.1. What is (momentarily) missing is a recurrence for the elementary numbers analogous to Pascal's relation for binomial coefficients and/or to Theorem 1.8.7 for partition numbers.

1.9.8 Lemma. *If* $n > t > 1$, *then*

$$e(n,t) = e(n-1,t) + ne(n-1,t-1).$$

Proof: $E_t(1,2,\ldots,n) = e(n,t)$ is the sum of all $C(n,t)$ products of the numbers $1,2,\ldots,n$ taken t at a time. Some of these products involve n, and some do not. The sum of the products that do not involve n is $E_t(1,2,\ldots,n-1) = e(n-1,t)$. When n is factored out of the remaining terms, the other factor is $E_{t-1}(1,2,\ldots,n-1) = e(n-1,t-1)$. ■

From Fig. 1.9.1 and Lemma 1.9.8 we see, e.g., that

$$\begin{aligned} e(3,2) &= e(2,2) + 3e(2,1) \\ &= 2 + 3 \times 3 \\ &= 11. \end{aligned}$$

Similarly,

$$\begin{aligned} e(5,2) &= e(4,2) + 5e(4,1) \\ &= 35 + 5 \times 10 \\ &= 85, \end{aligned}$$

and

$$\begin{aligned} e(5,3) &= e(4,3) + 5 \times e(4,2) \\ &= 50 + 5 \times 35 \\ &= 225. \end{aligned}$$

Continuing in this way, a row at a time, one obtains Fig. 1.9.2.

n \ t	0	1	2	3	4	5	6	7
1	1	1						
2	1	3	2					
3	1	6	11	6				
4	1	10	35	50	24			
5	1	15	85	225	274	120		
6	1	21	175	735	1624	1764	720	
7	1	28	322	1960	6769	13132	13068	5040
				⋯				

Figure 1.9.2. The elementary numbers $e(n,t)$.

As their name implies, elementary symmetric functions are symmetric. Because multiplication is commutative, the coefficients of

$$p(x) = (x-1)(x-2)(x-3)(x-4)$$

are identical to the coefficients of

$$p(x) = (x-3)(x-1)(x-4)(x-2);$$

the sum of the products of $x_1, x_2, \ldots, x_n$ taken t at a time is equal to the sum of the products of any rearrangement of the x's, taken t at a time. In fact, elementary symmetric functions are minimal symmetric polynomials!

1.9.9 Theorem. *The tth elementary symmetric function is identical to the minimal symmetric polynomial corresponding to the partition* $[1^t]$*, i.e.,*

$$M_{[1^t]}(x_1, x_2, \ldots, x_n) = E_t(x_1, x_2, \ldots, x_n).$$

Proof. If $(r_1, r_2, \ldots, r_n)$ is some rearrangement of the sequene $(1, 1, \ldots, 1, 0, 0, \ldots, 0)$ consisting of t 1's followed by $n-t$ 0's, then

$$x_1^{r_1} x_2^{r_2} \cdots x_n^{r_n} = x_{i_1} x_{i_2} \cdots x_{i_t},$$

where $1 \le i_1 < i_2 < \cdots < i_t \le n$, $r_{i_1} = r_{i_2} = \cdots = r_{i_t} = 1$, and the rest of the r's are zero. Adding the monomials corresponding to all possible rearrangements of $(1, 1, \ldots, 1, 0, 0, \ldots, 0)$ yields

$$M_{[1^t]}(x_1, x_2, \ldots, x_n) = \sum x_{i_1} x_{i_2} \cdots x_{i_t}, \tag{1.33}$$

where the sum is over $1 \le i_1 < i_2 < \cdots < i_t \le n$. In other words, the right-hand side of Equation (1.33) is the sum of all $C(n,t)$ products of the x's taken t and a time, which is the definition of $E_t(x_1, x_2, \ldots, x_n)$. ■

Conjugate to $[1^t]$ is the partition $[t]$.

1.9.10 Definition. The minimal symmetric polynomial corresponding to $[t]$ is the tth *power sum*, abbreviated

$$\begin{aligned} M_t(x_1, x_2, \ldots, x_n) &= M_{[t]}(x_1, x_2, \ldots, x_n) \\ &= x_1^t + x_2^t + \cdots + x_n^t. \end{aligned}$$

If $t = 1$, then

$$\begin{aligned} M_1(x_1, x_2, \ldots, x_n) &= x_1 + x_2 + \cdots + x_n \\ &= E_1(x_1, x_2, \ldots, x_n). \end{aligned} \tag{1.34}$$

Our interest in power sums goes back to Section 1.5, where it was discovered, e.g., that

$$\begin{aligned} M_1(1, 2, \ldots, n) &= 1 + 2 + \cdots + n \\ &= \tfrac{1}{2} n(n+1), \end{aligned}$$

$$\begin{aligned} M_2(1, 2, \ldots, n) &= 1^2 + 2^2 + \cdots + n^2 \\ &= \tfrac{1}{6} n(n+1)(2n+1), \end{aligned} \tag{1.35}$$

$$\begin{aligned} M_3(1, 2, \ldots, n) &= 1^3 + 2^3 + \cdots + n^3 \\ &= \tfrac{1}{4} n^2 (n+1)^2, \end{aligned} \tag{1.36}$$

and so on.

Recall (Theorem 1.8.15) that a polynomial in n variables is symmetric if and only if it is a linear combination of minimal symmetric polynomials. In this sense, the minimal symmetric polynomials are building blocks from which all symmetric polynomials can be constructed. The power sums are also building blocks, but in a different sense. The following result is proved in Appendix A1.

1.9.11 Theorem.[*] *Any polynomial symmetric in the variables $x_1, x_2, \ldots, x_n$ is a polynomial in the power sums $M_t = M_t(x_1, x_2, \ldots, x_n)$, $1 \le t \le n$.*

[*]To be encountered in Section 3.6, the symmetric "pattern inventory" is a polynomial in the power sums. A description of that polynomial is the substance of Pólya's theorem.

1.9.12 Example. We do not need Theorem 1.9.11 to tell us that $p(x,y,z) = (x+y+z)^3$ as a polynomial in the power sums. By definition, $p(x,y,z) = M_1(x,y,z)^3$. What about something more interesting, like $M_{[2,1]}(x,y,z) = x^2y + x^2z + xy^2 + xz^2 + y^2z + yz^2$? Observe that the product

$$\begin{aligned} M_2(x,y,z)M_1(x,y,z) &= (x^2+y^2+z^2)(x+y+z) \\ &= x^3+y^3+z^3+x^2y+x^2z+xy^2+xz^2+y^2z+yz^2 \\ &= M_3(x,y,z) + M_{[2,1]}(x,y,z). \end{aligned}$$

So, $M_{[2,1]}(x,y,z) = M_2(x,y,z)M_1(x,y,z) - M_3(x,y,z)$. Similarly,

$$\begin{aligned} M_2(x,y,z)^2 &= (x^2+y^2+z^2)^2 \\ &= x^4+y^4+z^4+2x^2y^2+2x^2z^2+2y^2z^2 \\ &= M_4(x,y,z) + 2M_{[2,2]}(x,y,z), \end{aligned}$$

so that $M_{[2,2]}(x,y,z) = \frac{1}{2}[M_2(x,y,z)^2 - M_4(x,y,z)]$. □

1.9.13 Example. Let's see how to express elementary symmetric functions as polynomials in the power sums. Already having observed that $E_1(x,y,z) = M_1(x,y,z)$, consider $E_2(x,y,z) = xy + xz + yz$. Rearranging terms in

$$\begin{aligned} M_1(x,y,z)^2 &= (x+y+z)^2 \\ &= (x^2+y^2+z^2) + (2xy+2xz+2yz) \\ &= M_2(x,y,z) + 2E_2(x,y,z) \end{aligned}$$

yields

$$E_2(x,y,z) = \tfrac{1}{2}[M_1(x,y,z)^2 - M_2(x,y,z)]. \tag{1.37}$$

Similar computations starting from $M_1(x,y,z)^3 = (x+y+z)^3$ lead to the identity

$$E_3(x,y,z) = \tfrac{1}{6}[M_1(x,y,z)^3 - 3M_1(x,y,z)M_2(x,y,z) + 2M_3(x,y,z)]. \tag{1.38}$$

(Confirm it.) □

Surely, Equations (1.37) and (1.38) are examples of some more general relationship between power sums and elementary symmetric functions. To discover what that pattern is, let's return to the source. Suppose, e.g., that

$$\begin{aligned} p(x) &= (x-a_1)(x-a_2)\cdots(x-a_n) \\ &= x^n - E_1x^{n-1} + E_2x^{n-2} - \cdots + (-1)^nE_n, \end{aligned}$$

where $E_r = E_r(a_1, a_2, \ldots, a_n)$. Substituting $x = a_i$ in this equation yields

$$\begin{aligned} 0 &= p(a_i) \\ &= a_i^n - E_1a_i^{n-1} + E_2a_i^{n-2} - \cdots + (-1)^nE_n. \end{aligned}$$

Summing on i and setting $M_t = M_t(a_1, a_2, \ldots, a_n) = a_1^t + a_2^t + \cdots + a_n^t$, we obtain

$$0 = M_n - E_1M_{n-1} + E_2M_{n-2} - \cdots + (-1)^nnE_n,$$

the $t = n$ case of the following.

1.9.14 Newton's Identities. [*] For a fixed but arbitrary positive integer n, let $M_r = M_r(x_1, x_2, \ldots, x_n)$ and $E_r = E_r(x_1, x_2, \ldots, x_n)$. Then, for all $t \geq 1$,

$$M_t - M_{t-1}E_1 + M_{t-2}E_2 - \cdots + (-1)^{t-1}M_1E_{t-1} + (-1)^ttE_t = 0. \tag{1.39}$$

1.9.15 Example. The first four of Newton's identities are equivalent to

$$\begin{aligned} M_1 &= E_1, \\ M_2 - M_1E_1 &= -2E_2, \\ M_3 - M_2E_1 + M_1E_2 &= 3E_3, \\ M_4 - M_3E_1 + M_2E_2 - M_1E_3 &= -4E_4. \end{aligned}$$

The first identity, $M_1 = E_1$, is the same as Equation (1.34). Substituting M_1 for E_1 in the second identity yields

$$E_2 = \frac{1}{2}[M_1^2 - M_2], \tag{1.40}$$

extending to n variables and confirming Equation (1.37). Eliminating E_1 and E_2 from the third identity recaptures the following extension of Equation (1.38):

$$E_3 = \frac{1}{6}[M_1^3 - 3M_1M_2 + 2M_3]. \tag{1.41}$$

[*]Named for Isaac Newton (1642–1727).

Eliminating E_1, E_2, and E_3 from the fourth identity produces something new, namely,

$$E_4 = \frac{1}{24}[M_1^4 - 6M_1^2M_2 + 8M_1M_3 + 3M_2^2 - 6M_4]. \tag{1.42}$$

Evidently, Newton's identities can be used to express any elementary symmetric function as a polynomial in the power sums. □

Because $E_3(x_1, x_2) = 0$, the right-hand side of Equation (1.41) had better be zero when $n = 2$. Let's confirm that it is:

$$\begin{aligned} M_1^3 + 2M_3 &= (x_1 + x_2)^3 + 2(x_1^3 + x_2^3) \\ &= 3x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + 3x_2^3 \\ &= 3(x_1 + x_2)(x_1^2 + x_2^2) \\ &= 3M_1M_2. \end{aligned}$$

So, as predicted, $M_1^3 - 3M_1M_2 + 2M_3 = 0$. More generally, because $E_{n+r}(x_1, x_2, \ldots, x_n) = 0$, $r \geq 1$, Equation (1.39) has a simpler form when $t > n$, namely,

$$M_t - M_{t-1}E_1 + M_{t-2}E_2 - \cdots + (-1)^n M_{t-n}E_n = 0. \tag{1.43}$$

A proof of Newton's identities for all $t \geq 1$ can be found in Appendix A1.

1.9. EXERCISES

1 Without computing the roots of $f(x) = x^4 - x^2 + 2x + 2$, it was argued in Example 1.9.3 that their elementary symmetric functions are $E_1 = 0$, $E_2 = -1$, $E_3 = -2$, and $E_4 = 2$. Confirm this result by finding the four roots and then computing their elementary symmetric functions directly from the definition.

2 Show that $(a^2 + b^2) - (a + b)(a + b) + 2ab = 0$ (thus confirming the $n = t = 2$ case of Newton's identities).

3 Find the elementary symmetric functions of the roots of

(a) $x^4 - 5x^3 + 6x^2 - 2x + 1$. **(b)** $x^4 + 5x^3 + 6x^2 + 2x + 1$.

(c) $x^4 + 5x^3 - 6x^2 + 2x - 1$. **(d)** $2x^4 + 10x^3 - 12x^2 + 4x - 2$.

(e) $x^5 - x^3 + 3x^2 + 4x - 8$. **(f)** $x^5 + x^4 - 2x$.

4 Compute

(a) $E_t(1, 2, 3, 4, 5)$, $1 \leq t \leq 5$, directly from Definition 1.9.1 (*Hint:* Use row 5 of Fig. 1.9.2 to check your answers.)

(b) $E_5(1,2,3,4,5,6,7)$.

5 Find the missing coefficients in

(a) $x^{(5)} = x^5 - 10x^4 + 35x^3 - \_\_\_x^2 + \_\_\_x - \_\_\_$.

(b) $x^{(6)} = x^6 - \_\_\_x^5 + \_\_\_x^4 - 225x^3 + \_\_\_x^2 - \_\_\_x$.

6 Compute

(a) $E_3(1,2,3,4,5,6,7,8)$. **(b)** $E_4(1,2,3,4,5,6,7,8)$.

(c) $E_6(1,2,3,4,5,6,7,8)$. **(d)** $E_7(1,2,3,4,5,6,7,8)$.

7 Let $f(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n$ be a polynomial of degree n whose roots are $a_1, a_2, \ldots, a_n$. Prove that $E_t(a_1, a_2, \ldots, a_n) = (-1)^t b_t/b_0$.

8 Confirm that $6(abc + abd + acd + bcd) = M_1^3 - 3M_1M_2 + 2M_3$, where $M_t = a^t + b^t + c^t + d^t$, $1 \le t \le 3$.

9 Newton's identities were used in Equations (1.40)–(1.42) to express $E_t = E_t(x_1, x_2, \ldots, x_n)$ as a polynomial in the power sums $M_t = M_t(x_1, x_2, \ldots, x_n)$, $2 \le t \le 4$.

(a) Confirm by a direct computation that

$$a^2 + b^2 + c^2 + d^2 = E_1(a,b,c,d)^2 - 2E_2(a,b,c,d).$$

(b) Show that $M_2 = E_1^2 - 2E_2$ for arbitrary n.

(c) Express M_3 as a polynomial in elementary symmetric functions.

(d) Show that $M_4 = E_1^4 - 4E_1^2E_2 + 4E_1E_3 + 2E_2^2 - 4E_4$.

(e) Prove that any polynomial symmetric in the variables $x_1, x_2, \ldots, x_n$ is a polynomial in the elementary symmetric functions $E_t(x_1, x_2, \ldots, x_n)$, $1 \le t \le n$.*

10 Express the symmetric function $f(a,b,c,d)$ from Example 1.8.16 as a polynomial in power sums.

11 Express $x^3y + xy^3$ as a polynomial in

(a) $M_1(x,y)$ and $M_2(x,y)$. **(b)** $E_1(x,y)$ and $E_2(x,y)$.

12 Because equations like those in Exercises 9(b)–(d) are polynomial identities, any numbers can be substituted for the variables $x_1, x_2, \ldots, x_n$.

(a) Use this idea to show that $1^2 + 2^2 + \cdots + n^2 = e(n,1)^2 - 2e(n,2)$.

(b) Use Fig. 1.9.2 and the result of part (a) to evaluate $1^2 + 2^2 + 3^2 + 4^2 + 5^2$. (Confirm that your answer is consistent with Equation (1.35).)

(c) Find a formula for $1^3 + 2^3 + \cdots + n^3$ in terms of $e(n,t)$, $t \le n$. (*Hint:* Use your solution to Exercise 9(c).)

*This is the so-called *Fundamental Theorem of Symmetric Polynomials*.

(d) Use Fig. 1.9.2 and the result of part (c) to evaluate $1^3 + 2^3 + 3^3 + 4^3 + 5^3$. (Confirm that your answer is consistent with Equation (1.36).)

13 Let $E_t = E_t(a_1, a_2, \ldots, a_n)$, $0 \le t \le n$. Show that

(a) $(a_1 - 1)(a_2 - 1)\cdots(a_n - 1) = E_n - E_{n-1} + E_{n-2} - \cdots + (-1)^n E_0$.

(b) $(1 - a_1x)(1 - a_2x)\cdots(1 - a_nx) = E_0 - E_1x + E_2x^2 - \cdots + (-1)^n E_n x^n$.

14 If $n \ge t \ge 2$, prove that

$$E_t(a_1, a_2, \ldots, a_n) = E_t(a_1, a_2, \ldots, a_{n-1}) + a_n E_{t-1}(a_1, a_2, \ldots, a_{n-1}).$$

(*Hint:* See the proof of Lemma 1.9.8.)

15 Give the inductive proof that

$$\prod_{i=1}^{n}(x - a_i) = \sum_{t=0}^{n}(-1)^t E_t(a_1, a_2, \ldots, a_n)x^{n-t}.$$

16 If $f(x) = x^{(n+1)}$, show that $f'(0) = \pm n!$.

17 Show that

(a) $x^{(m+n)} = x^{(m)}(x - m)^{(n)}$.

(b) $(x + y)^{(n)} = \sum_{r=0}^{n} C(n, r)x^{(r)}y^{(n-r)}$.

18 Recall (Section 1.8, Exercise 15) that if $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_m]$ and $\beta = [\beta_1, \beta_2, \ldots, \beta_k]$ are two partitions of n, then α *majorizes* β if $m \le k$, and

$$\sum_{i=1}^{r}\alpha_i \ge \sum_{i=1}^{r}\beta_i, \qquad 1 \le r \le m.$$

(a) Show that majorization imposes a linear order on the $p_3(8) = 5$ partitions of 8 having three parts.

(b) Among the many properties of elementary symmetric functions is *Schur concavity*, meaning that $E_t(\alpha) \le E_t(\beta)$ whenever α majorizes β. Confirm this property for $2 \le t \le 3$ using the three-part partitions of 8.

(c) If you were to compute $E_3(\alpha)$ for each four-part partition α of 24, which partition would produce the maximum? (The minimum?)

19 Let $H_t = H_t(x_1, x_2, \ldots, x_n)$ be the homogeneous symmetric function of Section 1.8, Exercise 25. Then H_t is *Schur convex*, meaning that $H_t(\alpha) \ge H_t(\beta)$, whenever α majorizes β.

(a) Confirm this result for H_2 and the three-part partitions of 8.

(b) If you were to compute $H_4(\alpha)$ for each three-part partition α of 24, which partition would produce the maximum? (The minimum?)

20 Show that the general formula for E_t as a polynomial in the power sums M_t is $t!E_t = \det(L_t)$, where

$$L_t = \begin{pmatrix} M_1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ M_2 & M_1 & 2 & 0 & \cdots & 0 & 0 \\ M_3 & M_2 & M_1 & 3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ M_{t-1} & M_{t-2} & M_{t-3} & M_{t-4} & \cdots & M_1 & t-1 \\ M_t & M_{t-1} & M_{t-2} & M_{t-3} & \cdots & M_2 & M_1 \end{pmatrix}.$$

(*Hint:* Use Cramer's rule on the following matrix version of Newton's identities:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots \\ M_1 & -2 & 0 & 0 & \cdots \\ M_2 & -M_1 & 3 & 0 & \cdots \\ M_3 & -M_2 & M_1 & -4 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \\ E_3 \\ E_4 \\ \vdots \end{pmatrix} = \begin{pmatrix} M_1 \\ M_2 \\ M_3 \\ M_4 \\ \vdots \end{pmatrix}.$$

21 Confirm that the result in Exercise 20, i.e., $t!E_t = \det(L_t)$, agrees with

(a) Equation (1.40) when $t = 2$.

(b) Equation (1.41) when $t = 3$.

(c) Equation (1.42) when $t = 4$.

22 Bertrand Russell* once wrote, "I used, when excited, to calm myself by reciting the three factors of $a^3 + b^3 + c^3 - 3abc$."

(a) Express $a^3 + b^3 + c^3 - 3abc$ as a product of *two* nontrivial polynomials that are symmetric in a, b, and c. (*Hint:* Example 1.9.15 and $M_1(a, b, c) = E_1(a, b, c)$.)

(b) Show that $(a + b + c)(a + \theta b + \theta^2 c)(a + \theta^2 b + \theta c) = a^3 + b^3 + c^3 - 3abc$, where $\theta = \frac{1}{2}(-1 + i\sqrt{3})$ is a *primitive cube root of unity.*

(c) Show that if $a^3 + b^3 + c^3 - 3abc$ is a product of three polynomials, each of which is symmetric in a, b, and c, then one (at least) of them is a constant polynomial.

23 Prove that

(a) $e(n, 2) = C(n + 1, 2)$.

(b) $e(n, 3) = \frac{1}{48}(n - 2)(n - 1)n^2(n + 1)^2$.

*In 1914, having completed *Principia Mathematica* with Alfred North Whitehead, Bertrand Russell (1872–1970), Third Earl Russell, abandoned mathematics in favor of philosophy, social activism, and writing. He was awarded the Nobel Prize for Literature in 1950.

24 Show that $\{x^{(n)} : 0 \le n \le m\} = \{1, x, x^{(2)}, x^{(3)}, \ldots, x^{(m)}\}$ is a basis for the vector space of polynomials of degree at most m. (*Hint:* Show that any polynomial $f(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$ of degree at most m can be expressed (uniquely) as a linear combination of $1, x, x^{(2)}, x^{(3)}, \ldots, x^{(m)}$.)

25 Let A be a real, symmetric, $n \times n$ matrix with characteristic polynomial

$$\det(xI_n - A) = x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots + (-1)^n c_n.$$

Show that

(a) $c_1 = \sum_{i=1}^{n} a_{ii} = tr(A)$, the *trace* of A.

(b) $c_2 = \frac{1}{2}[\text{tr}(A)^2 - \text{tr}(A^2)]$

(c) $c_3 = \frac{1}{6}[\text{tr}(A)^3 - 3\ \text{tr}(A)\ \text{tr}(A^2) + 2\ \text{tr}(A^3)]$

(d) $\text{tr}(A^t) - c_1\,\text{tr}(A^{t-1}) + c_2\,\text{tr}(A^{t-2}) - \cdots + (-1)^t t c_t = 0,\ t \ge 1.$

26 Recall that $[k, 1^m]$ is shorthand for the partition of $m + k$ consisting of a single k followed by m 1's.

(a) Show that $M_s(x_1, x_2, \ldots, x_n)E_t(x_1, x_2, \ldots, x_n) = M_{[s+1,1^{t-1}]}(x_1, x_2, \ldots, x_n) + M_{[s,1^t]}(x_1, x_2, \ldots, x_n)$, $s > 1$.

(b) Show that $M_1(x_1, x_2, \ldots, x_n)E_t(x_1, x_2, \ldots, x_n) = M_{[2,1^t]}(x_1, x_2, \ldots, x_n) + (t+1)E_{t+1}(x_1, x_2, \ldots, x_n)$.

(c) Base a proof of Newton's identities on parts (a) and (b).

*1.10. COMBINATORIAL ALGORITHMS

> In a few generations you can bread a racehorse. The recipe for making a man like Delacroix is less well known.
>
> — Jean Renoir

Algos is the Greek word for "pain"; *algor* is Latin for "to be cold"; and Al Gore is a former Vice President of the United States. Having no relation to any of these, *algorithm* derives from the ninth-century Arab mathematician Mohammed ben Musa al-Khowârizmi.* Translated into Latin in the twelfth century, his book *Algorithmi de numero Indorum* consists of step-by-step procedures, or recipes, for solving arithmetic problems.

As an illustration of the role of algorithms in mathematics, consider the following example: one version of the *well-ordering principle* is that any nonempty set of

*Mohammed, son of Moses, of Khowârizm. Al-Khowârizmi also wrote *Hisâb al-jabr wa'1 muqâbalah*; from which the word *algebra* is derived. It was largely through the influence of his books that the Hindu-Arabic numeration system reached medieval Europe.

positive intergers contains a least element. Given two positive integers a and b, well ordering implies the existence of a least element d of the set

$$\{sa + tb : s \text{ and } t \text{ are integers and } sa + tb > 0\}.$$

This least element has a name; it is the greatest common divisor (GCD) of a and b. Well ordering establishes the existence of d but furnishes little information about its value. For that we must look elsewhere.

Among the algorithms for computing GCDs is one attributed to Euclid, based on the fact that if r is the remainder when a is divided by b, then the GCD of a and b is equal to the GCD of b and r. A different algorithm is based on the unique prime factorizations of a and b. Either algorithm works just fine for small numbers, where the second approach may even have a conceptual advantage. For actual computations with large numbers, however, the Euclidean algorithm is much easier and much *much* faster.

Not until digital computers began to implement algorithms in calculations involving astronomically large numbers did the mathematical community, *as a whole*, pay much attention to these kinds of computational considerations. Courses in the analysis of algorithms are relatively new to the undergraduate curriculum.

This section is devoted to a naive introduction to a few of the ideas associated with combinatorial algorithms. Let's begin with the multinomial coefficient

$$M = \binom{n}{r_1, r_2, \ldots, r_k}$$

$$= \frac{n!}{r_1! r_2! \cdots r_k!},$$

where, e.g.,

$$n! = 1 \times 2 \times \cdots \times n.$$

Observe that $n!$ is not so much a number as an algorithm for computing a number. To compute $n!$, multiply 1 by 2, multiply their product by 3, multiply that product by 4, and so on, stopping only when the previous product has been multiplied by n.

The following is a subalgorithm, or *subroutine*, to compute the factorial F of an arbitrary integer X:

```
1. Input X.
2. F = 1 and I = 0.
3. I = I + 1.
4. F = F × I.
5. If I < X, then go to step 3.
6. Return F.
```

These lines should be interpreted as a step-by-step recipe that, absent directions to the contrary (like "go to step 3"), is to be executed in numerical order. In step 6, the value *returned* is $F = X!$.

This subroutine is written in the form of a primitive computer program. To a hypothetical computer, symbols like X, F, and I are names for memory locations. Step 1 should be interpreted as an instruction to wait for a number to be entered, then to store the number in some ("random"*) memory location and, so as not to forget the location, flag it with the symbol X. In step 2, the numbers 1 and 0 are stored in memory locations labeled F and I, respectively. In step 3, the number in memory location I is replaced with the next larger integer.† In step 4, the number in memory location F is replaced with the product of the number found there, and the number currently residing in memory location I. If, in step 5, memory location I contains X, operation moves on to step 6, where the subroutine terminates by returning $F = X!$. Otherwise, the action loops back to step 3 for another iteration.

The *loop* in steps 3–5 can be expressed more compactly using the equivalent "For ... Next" construction foud in steps 3–5 of the following:

1.10.1 (Factorial Subroutine) Algorithm

1. Input X.
2. $F = 1$.
3. For $I = 1$ to X.
4. $F = F \times I$.
5. Next I.
6. Return F. □

The factorial subroutine affords the means to compute $n!$, $r_1!$, $r_2!$, and so on, from which the multinomial coefficient $M = \binom{n}{r_1, r_2, \ldots, r_k}$ can be obtained, either as the quotient of $n!$ and the product of the factorials of the r's or, upon dividing $n!$ by $r_1!$, dividing the quotient by $r_2!$, dividing that quotient by $r_3!$, and so on. While these two approaches may be arithmetically equivalent, they represent *different* algorithms.

1.10.2 (Multinomial Coefficient) Algorithm

1. Input $n, k, r_1, r_2, \ldots, r_k$.
2. $X = n$.
3. Call Algorithm 1.10.1.
4. $M = F$.
5. For $j = 1$ to k.
6. $X = r_j$

*Hence the name random-access memory, or RAM.

†Notations such as "$I \leftarrow I + 1$" or "$I := I + 1$" are sometimes used in place of "$I = I + 1$".

```
 7. Call Algorithm 1.10.1.
 8. M = M/F.
 9. Next j.
10. Return M.
```

□

Having let $X = n$ in step 2, the factorial subroutine is called upon in step 3 to return $F = n!$. Thus, in step 4, the number entered into memory location M is $n!$. On the first trip through the loop in steps 5–9, $j = 1$ and $X = r_1$. When the factorial subroutine is called in step 7, the number it returns is $F = r_1!$ so, in step 8, the number in memory location M is replaced by $n!/r_1!$. Assuming $j < k$ in step 9, action is directed back to step 5, and the value of j is increased by 1. The second time step 8 is encountered, the number currently being stored in memory location M, namely, $n!/r_1!$, is replaced with $(n!/r_1!)/r_2! = n!/(r_1!r_2!)$. And so on. Finally, the kth and last time step 8 is encountered, the number in memory location M is replaced with $\binom{n}{r_1, r_2, \ldots, r_k}$.

It might be valuable to pause here and give this algorithm a try, either by writing a computer program to implement it or by following the steps of Algorithm 1.10.2 yourself as if you were a (*virtual*) computer. Test some small problem, the answer to which you already know, e.g., $\binom{11}{4,4,2,1} = 34,650$ from the original MISSISSIPPI problem. After convincing yourself that the algorithm works properly, try it on $C(100, 2)$.

Whether your computer is virtual or real, using Algorithm 1.10.2 to compute $C(100, 2)$ may cause it to choke. If this happens, the problem most likely involves the magnitude of 100!. The size of this number can be estimated by means of an approximation known as *Stirling's formula*[*]:

$$n! \doteq \sqrt{2\pi n}\left(\frac{n}{e}\right)^n. \tag{1.44}$$

Using common logarithms, $100/e = 36.8 \doteq 10^{1.57}$, so $(100/e)^{100} \doteq 10^{157}$. Since $\sqrt{2\pi} \times 10 \doteq 25$, Equation (1.44) yields $100! \doteq 2.5 \times 10^{158}$. (Current estimates put the age of the universe at something less than 5×10^{26} nanoseconds.)

Without a calculator or computer, one would not be likely even to consider evaluating $C(100, 2)$ by first computing 100!, because something along the following lines is so much easier:

$$\begin{aligned} C(100, 2) &= \frac{98! \times 99 \times 100}{98! \times 1 \times 2} \\ &= 99 \times 50 \\ &= (100 - 1) \times 50 \\ &= 4950. \end{aligned}$$

[*]Stirling's formula should not be confused with *Stirling's identity*, soon to be encountered in Chapter 2.

The key to converting this easier approach into an algorithm is best illustrated with a slightly less trivial example, e.g., (see Theorem 1.5.1)

$$\binom{n}{r,s,t} = \frac{P(n,r)}{r!} \times \frac{P(n-r,s)}{s!} \times \frac{P(n-r-s,t)}{t!}. \tag{1.45}$$

Viewing $P(n,r)/r!$ as

$$\frac{n \times (n-1) \times \cdots \times (n-r+1)}{1 \times 2 \times \cdots \times r} = \frac{n}{1} \times \frac{n-1}{2} \times \cdots \times \frac{n-r+1}{r},$$

$P(n-r,s)/s!$ as

$$\frac{n-r}{1} \times \frac{n-r-1}{2} \times \cdots \times \frac{n-r-s+1}{s},$$

and so on, suggests another subroutine:

```
1. M=1.
2. For J=1 to r.
3. M=M × N/J.
4. N=N-1.
5. Next J.
```

Setting $N = n$ and $r = r_I$ and *nesting* this subroutine inside a "For $I = 1$ to k" loop yields another algorithm.

Can we do better? Almost surely. Because $n = r + s + t$, the last factor in Equation (1.45) is $P(t,t)/t! = t!/t! = 1$. Evidently, "For $I = 1$ to $k - 1$" suffices in the "outside loop". On the other hand, since $\binom{n}{r_1,r_2,\ldots,r_k} = \binom{n}{r_2,\ldots,r_k,r_1}$, the outside loop could just as well be "For $I = 2$ to k".

1.10.3 (Improved Multinomial Coefficient) Algorithm

```
1. Input n, k, r1, r2, ..., rk.
2. M=1 and N=n.
3. For I=2 to k.
4. For J=1 to rI.
5. M=M × N/J.
6. N=N-1.
7. Next J.
8. Next I.
9. Return M.
```

□

LUCK	LUKC	LCUK	LCKU	LKUC	LKCU
ULCK	ULKC	UCLK	UCKL	UKLC	UKCL
CLUK	CLKU	CULK	CUKL	CKLU	CKUL
KLUC	KLCU	KULC	KUCL	KCLU	KCUL

Figure 1.10.1. Rearrangements of LUCK.

It is clear from our experience so far that different algorithms can achieve the same outcome, *some better than others*! Algorithm 1.10.3 is superior to Algorithm 1.10.2 because it is more widely applicable. (Check to see that calculating $C(100, 2)$ is no trouble for Algorithm 1.10.3.) In general, however, it is not always clear which of two (or more) algorithms is best. It may not even be clear how to interpret "best"!

This book began with a discussion of the four-letter words that can be produced by rearranging the letters in LUCK. An initial (brute-force) approach resulted in a systematic list, reproduced in Fig. 1.10.1 for easy reference. In subsequent discussions, it was often useful to *imagine* constructing a list, with the implied understanding that list making is mildly distasteful. And, so it is, as long as the only reason to make a list is to count the words on it! Such peremptory judgments do not apply when the list serves other purposes. There are, in fact, many good reasons to make a list.

Suppose one had a reason for wanting a list of the $4! = 24$ rearrangements of LUCK, e.g., to use in constructing a master list of encryption keys upon which to base monthly corporate passwords for the next two years. In order to be most useful, such a list should be organized so that specific words are easy to locate. Figure 1.10.1 gives one possibility, based on the order in which the letters appear in LUCK. A more common approach is based on the order in which letters appear in the alphabet.

1.10.4 Definition. Let $X = x_1x_2 \ldots x_p$ and $Y = y_1y_2 \ldots y_q$ be words containing p and q letters, respectively. Then X comes before Y, in *dictionary order*,* if x_1 comes before y_1 in alphabetical order; or if there is a positive integer $r \leq p$ such that $x_i = y_i$, $1 \leq i < r$, and x_r precedes y_r in alphabetical order; or if $p < q$ and $x_i = y_i$, $1 \leq i \leq p$.

A list of words in dictionary order is often called an *alphabetized list*, and dictionary order is sometimes referred to as "alphabetical order." Whatever such lists are called, algorithms to generate them are surprisingly difficult to design. Our approach takes advantage of the numerical order that is already hard-wired into computers.

* Dictionary order is also known as *lexicographic order*, *lexicon* being another word for "dictionary".

1.10.5 Example. Consider "*words*" assembled from the *alphabet* $\{0, 1, 2, \ldots, 9\}$. Suppose *alphabetical order* for these ten "*letters*" is interpreted as numerical order. Would it surprise you to learn that, in this context, dictionary order does not coincide with the usual extension of numerical order? While 9 comes before 10 in numerical order, 9 comes after 10 in dictionary order! (Confirm that, upon restriction to number/words of the same length, the two orderings *do* coincide.) □

1.10.6 Example. In the spirit of Example 1.10.5, consider the $4! = 24$ four-letter words that can be assembled by rearranging the letters/digits in 3142. Among the challenges that stand between us and an algorithm to generate and list these words in dictionary order is familiarity! We do chores like this all the time without thinking about *how* we do them.

Let's start at the beginning, focusing on process: Since 1 comes first in alphabetical order, any word that begins with 1 will precede, in dictionary order, all words that begin with something else. Similarly, among the words whose first letter is 1, any whose second letter is 2 will precede all those whose second letter is not. Continuing in this way, it is easy to see that the list must begin with 1234, the unique rearrangement of 3142 in which the letters occur in increasing alphabetical order. Reversing the argument shows that the last word on the list is 4321, the unique word in which the letters decrease, in alphabetical order (when read from left to right).

Because only two rearrangements of 3142 have initial fragment 12, the word following 1234 on the list can only be 1243. Indeed, any two words with the same initial fragment have tailing fragments consisting of the same (complementary) letters. Moreover, all words with the same initial fragment must appear consecutively on the list, starting with the word in which the tailing letters are arranged in increasing order and ending with the word in which the tailing letters are in decreasing order.

After 1243 come the words with initial fragment 13. In the first of these, the tail is 24, and in the second it is 42. The observation that 42 is the reverse of 24 suggests a two-step procedure for finding the next word after 1342 on the list.

In the first step, 1342 is transformed into the intermediate word 1432 by switching the positions of 3 and 4. Observe that, while the switch changes the tail from 42 to 32, the new tail is (still) in decreasing order. In the second step, this intermediate word is transformed from last to first among the words with initial fragment 14 by reversing its tail. The result, 1423, is the next rearrangement of 3142 after 1342.

What comes after 1423? Well, 1432, of course! But, how does 1432 emerge from the two-step process outlined in the previous paragraph? Because 1423 is the only word on the list that begins with 142, it is the last word on the list with initial fragment 142. (This time, the tail is 3.) Switching 2 and 3 results in the intermediate word 1432 (whose tail is 2). Because a tail of length one reverses to itself, the output of the two-step process is 1432.

What comes after 1432? Because 432 is in decreasing order, 1432 is the last word on the list with initial fragment 1. Switching 1 with 2 produces the intermediate word 2431. Reversing the tail, 431, yields the next word on the list, namely, 2134.

Imagine yourself somewhere in the middle of the list, having just written the word $d_1d_2d_3d_4$. Using the two-step process to find the next word depends on being able to recognize the letter to be switched. The key to doing that is the tail. Assuming $d_1d_2d_3d_4 \neq 4321$, the only way it can be the last word on the list with initial fragment $d_1 \ldots d_j$ is if letters $d_{j+1}, \ldots, d_4$ are in decreasing order. For d_j to be the letter that gets switched, there must be some letter in the tail with which to switch it, i.e., some $d_k \in \{d_{j+1}, \ldots, d_4\}$ that comes after d_j in alphabetical (numerical) order. If $d_j, d_{j+1}, \ldots, d_4$ were in decreasing order, there could be no such d_k.

In the two-step process, the tail is the longest fragment (starting from the right-hand end of $d_1d_2d_3d_4$) whose letters decrease (when read from left to right). Put another way, the letter to be switched is d_j, where j is the largest value of i such that $d_i < d_{i+1}$. Once j has been identified, step 1 is accomplished by switching d_j with d_k, where d_k is the smallest letter in the tail that is larger than d_j, i.e.,

$$d_k = \min\{d_i : i > j \text{ and } d_i > d_j\}. \tag{1.46}$$

(Because $d_{j+1} > d_j$ and because d_{j+1} belongs to the tail, d_k always exists.)

When d_j and d_k are switched, a new tail is produced in which d_k (from the old tail) has been replaced by d_j. Because of the way j and d_k have been chosen, the letters in the new tail are (still) decreasing. Reversing the new tail in step 2 is equivalent to rearranging its letters into increasing order. □

The discussion in Example 1.10.6 leads to an algorithm for listing, in dictionary order, all rearrangements of 3142.

1.10.7 Algorithm

1. Set $d_i = i$, $1 \leq i \leq 4$.
2. Write $d_1\ d_2\ d_3\ d_4$.
3. If $d_i > d_{i+1}$, $1 \leq i \leq 3$, then stop.
4. Let j be the largest i such that $d_i < d_{i+1}$.
5. Let k be chosen to satisfy Equation (1.46).
6. Switch d_j and d_k.*
7. Reverse $d_{j+1}, \ldots, d_4$.
8. Go to step 2.

□

It would not be a bad idea to pause and implement Algorithm 1.10.7 on a computer (real or virtual) and check to see that the output is something closely resembling Fig. 1.10.2.

What about the master list of encryption keys upon which to base monthly corporate passwords for the next two years? An algorithm to generate a list, in

*So that the new d_j is the old d_k, and vice versa.

1234	1243	1324	1342	1423	1432
2134	2143	2314	2341	2413	2431
3124	3142	3214	3241	3412	3421
4123	4132	4213	4231	4312	4321

Figure 1.10.2. The 24 rearrangements of 1234.

dictionary order, of all 24 rearrangements of LUCK, is only a step or two from Algorithm 1.10.7. The missing steps involve explaining to a computer that C, K, L, U is an alphabetical listing of the letters in LUCK.* This is most easily accomplished using "string variables".

Like a word, a text *string* is a sequence (ordered concatenation) of symbols. Like numbers, strings of text can be stored in memory locations and labeled with symbols. But, it is often necessary to choose labels that distinguish string memory locations from those used to store numbers. We will use a dollar sign to indicate a string variable. The notation $A\$(4) =$ "FOOD", e.g., indicates that the string FOOD should be stored in the fourth cell of an *array* of string variable memory locations labeled $A\$$.

1.10.8 Example. To convert Algorithm 1.10.7 to an algorithm for generating, in dictionary order, the rearrangements of LUCK, add step

`0. L$(1) = "C", L$(2) = "K", L$(3) = "L", L$ (4) = "U"`

and modify step 2 so that it reads

`2. Write L$(d1)L$(d2)L$(d3) L$(d4).` □

Why not pause, modify Algorithm 1.10.7 now, and confirm that its output resembles Fig. 1.10.3. (Compare with Fig. 1.10.1.)

1.10.9 Example. The conversion of Algorithm 1.10.7 in Example 1.10.8 was relatively easy because the letters L, U, C, and K are all different. How much harder would it be to design an algorithm to generate, in dictionary order, all $4!/2 = 12$ four-letter rearrangements of LOOK?

CKLU	CKUL	CLKU	CLUK	CUKL	CULK
KCLU	KCUL	KLCU	KLUC	KUCL	KULC
LCKU	LCUK	LKCU	LKUC	LUCK	LUKC
UCKL	UCLK	UKCL	UKLC	ULCK	ULKC

Figure 1.10.3. Rearrangements of LUCK in dictionary order.

*As the name *digital computer* suggests, these machines were conceived and designed to crunch numbers. Numerical order is programmed into their genes, so to speak. Tasks related to word processing, on the other hand, have to be "learned", or "memorized" (which is why word processing software takes up so much space on a hard drive).

Let's begin with an algorithm to produce, in dictionary order, all twelve rearrangements of 1233. This is surprisingly easy! It can be done by replacing step 1 in Algorithm 1.10.7 with

$$\texttt{1. Set } d_1 = 1\texttt{, } d_2 = 2\texttt{, } d_3 = 3\texttt{, and } d_4 = 3$$

and replacing "$<$" in step 4 with "$\leq$".

To generate an ordered list of the rearrangements of LOOK, it suffices to modify this modified algorithm in the same way that Algorithm 1.10.7 was modified to obtain Example 1.10.8, namely, by adding step

$$\texttt{0. } L\$(1) = \text{“K”}\texttt{, } L\$(2) = \text{“L”}\texttt{, } L\$(3) = \text{“O”}$$

and changing step 2 to

$$\texttt{2. Write } L\$\ (d_1)\ L\$\ (d_2)\ L\$\ (d_3)\ L\$\ (d_4)\texttt{.}$$

At this point, how hard can it be to write an algorithm for listing, in dictionary order, all 11-letter words that can be produced by rearranging the letters in MISSISSIPPI? □

It is one thing to generate and list, in dictionary order, all possible rearrangements of the letters in some arbitrary word. It is something else to rearrange some arbitrary list of words into dictionary order. The latter is a so-called *sorting problem*. The comparison of various sorting algorithms affords a natural introduction to some applications of combinatorics in the analysis of algorithms. Those interested in pursuing such a discussion are referred to Appendix A2.

1.10.10 Example. A systematic listing of the seven partitions of 5 might be expected to look like this:

$$[5], [4, 1], [3, 2], [3, 1, 1], [2, 2, 1], [2, 1, 1, 1], [1, 1, 1, 1, 1].$$

In *reverse* dictionary order, $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_\ell] \vdash n$ comes before $\beta = [\beta_1, \beta_2, \ldots, \beta_s] \vdash n$ if (and only if) $\alpha_1 > \beta_1$ or there is an integer $t < \ell$ such that $\alpha_i = \beta_i$, $1 \leq i \leq t$, and $\alpha_{t+1} > \beta_{t+1}$. Let's see if we can devise an algorithm to generate and list, in reverse dictionary order, all $p(n)$ partitions of n.

Because the list begins with $[n]$, all that's required is a step-by-step procedure to find the next partition, in reverse dictionary order, after a fixed but arbitrary $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_\ell] \neq [1^n]$ (the last partition on the list). There are two cases.

Case 1: If $\alpha_\ell = 1$, then $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_k, 1, \ldots, 1]$, where 1 occurs with multiplicity m, $\alpha_k > 1$, and $\ell = k + m$. If μ is the next partition after α, then μ is the first partition, in reverse dictionary order, that satisfies the conditions $\mu_i = \alpha_i$, $1 \leq i < k$,

and $\mu_k = \alpha_k - 1$. To find μ, let $S = \alpha_k + m$, the sum of the parts of α coming after α_{k-1}. If q is the quotient and r the remainder, when S is divided by $d = \alpha_k - 1$, then

$$\mu = [\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_k - 1, \ldots, \alpha_k - 1, r],$$

where $\alpha_k - 1$ occurs with multiplicity q and it is understood that r does not appear if it is zero.

Case 2: If $\alpha_\ell > 1$, the next partition after α is

$$\mu = [\alpha_1, \alpha_2, \ldots, \alpha_{\ell-1}, \alpha_\ell - 1, 1]. \qquad \square$$

Let's design an algorithm to implement the ideas of Example 1.10.10. Suppose

$$\alpha = [n^{m(n)}, \ldots, 2^{m(2)}, 1^{m(1)}],$$

where $i^{m(i)}$ is understood not to appear when $m(i) = 0$. If $m(1) = n$, then $\alpha = [1^n]$ and the list is complete. Otherwise, let j be the smallest integer larger than 1 such that $m(j) > 0$. The steps used in Example 1.10.10 to produce μ, the next partition after α, are these. Replace $m(j)$ with $m(j) - 1$. In case 1 (the case in which $m(1) > 0$), let q and r be the quotient and remainder when $S = j + m(1)$ is divided by $d = j - 1$. Set $m(1) = 0$; then set $m(j-1) = q$ and, if $r > 0$, set $m(r) = 1$. In case 2, if $j = 2$, set $m(1) = 2$; otherwise, set $m(j-1) = 1$ and $m(1) = 1$. A formal algorithm might look like this:

1.10.11 (Partition Generating) Algorithm

1. Input n.
2. Set $m(i) = 0$, $1 \le i < n$, and $m(n) = 1$.
3. Write $[n^{m(n)}, \ldots, 2^{m(2)}, 1^{m(1)}]$.
4. If $m(1) = n$, then stop.
5. $S = m(1)$.
6. $m(1) = 0$.
7. $j = 1$.
8. $j = j + 1$.
9. If $m(j) = 0$, then go to step 8.
10. $D = j - 1$.
11. $m(j) = m(j) - 1$.
12. If $S = 0$, then go to step 19.
13. $S = S + j$.
14. $Q = \lfloor S/D \rfloor$.
15. $R = S - D \times Q$.
16. $m(D) = Q$.
17. If $R > 0$, then $m(R) = 1$.

```
18. Go to step 3.
19. If j = 2, then go to step 23.
20. m(D) = 1.
21. m(1) = 1.
22. Go to step 3.
23. m(1) = 2.
24. Go to step 3.
```
□

Note that case 1 is addressed in steps 13–18 of Algorithm 1.10.11, while case 2 is handled in steps 19–24.

Having endured the development of Algorithm 1.10.11, why not convert it to a computer program and have the satisfaction of seeing the partitions of n appear on a computer screen?

1.10. EXERCISES

1 Write an algorithm to list the integers 1–100 in numerical order.

2 Write an algorithm to input two numbers and output

(a) their product.

(b) their sum.

(c) their difference.

3 Assuming that $r_1, r_2, \ldots, r_k$ vary in size, which of them should be chosen to play the role of r_1 in Algorithm 1.10.3?

4 Without actually running any programs, describe the output that would be produced if step 0 in Example 1.10.8 were replaced with

```
0. L$(1) = "K", L$(2) = "L", L$(3) = "O", L$(4) = "O".
```

5 Write an algorithm to generate and list, in dictionary order,

(a) all $5! = 120$ rearrangements of LUCKY.

(b) all $4!/2 = 12$ rearrangements of COOL.

6 Write an algorithm to compute and output the first ten rows (as n goes from 0 to 9) of Pascal's triangle. Base your algorithm on

(a) the algebraic formula $C(n, r) = n!/[r!(n-r)!]$.

(b) Pascal's relation.

7 Write an algorithm to generate and list, in dictionary order, all rearrangements of

(a) BANANA. **(b)** MISSISSIPPI. **(c)** MATHEMATICS.

8 Write an algorithm to generate and output the first ten rows of the partition triangle (i.e., the array whose (n, m)-entry is $p_m(n)$, the number of m-part partitions of n).

9 Write an algorithm to input n and output $p(n)$, the number of partitions of n. Base your algorithm on

(a) your solution to Exercise 8.

(b) Algorithm 1.10.11.

10 Write an algorithm to input a_0–a_4 and b_0–b_3 and to output the coefficient of x^k, $7 \geq k \geq 0$, in the product

$$(a_0x^4 + a_1x^3 + \cdots + a_4)(b_0x^3 + b_1x^2 + \cdots + b_3).$$

11 Write an algorithm to input x_1–x_6 and to output

(a) the third elementary symmetric function, $E_3(x_1, x_2, \ldots, x_6)$.

(b) all C(6,3) three-element subsets of $\{1, 2, 3, 4, 5, 6\}$.

(c) all $C(6, 3)$ three-element subsets of $\{x_1, x_2, \ldots, x_6\}$.

12 Write an algorithm to input x_1–x_6 and to output

(a) $E_2(x_1, x_2, \ldots, x_6)$.

(b) all $C(6, 2)$ two-element subsets of $\{x_1, x_2, \ldots, x_6\}$.

(c) the complements of the subsets in part (b).

(d) $E_4(x_1, x_2, \ldots, x_6)$.

13 Write an algorithm to input six *positive* numbers x_1–x_6 and to output $E_5(x_1, x_2, \ldots, x_6)$.

14 Write an algorithm to input the parts of a partition and output the parts of its conjugate.

15 Assuming 0 comes before 1 in alphabetical order, write an algorithm to generate and output, in dictionary order,

(a) all binary words of length 4 (i.e., all four-letter words that can be assembled using the alphabet $\{0, 1\}$).

(b) all binary words of length 8 and weight 4, where the weight of a binary word is the number of 1's among its bits.

16 Write an algorithm to input n and output, in dictionary order, all binary words of length n. (*Hint:* Exercise 15(a).)

17 The problem in Exercise 16 is to generate and list binary words in dictionary order. Here, the problem is to generate and list binary words in a different

order, one in which adjacent words differ in a single bit.* Because the kth word differs from its immediate predecessor in a single bit, to solve this problem it suffices to identify that bit. Here is a procedure for doing that: Every bit of the first word is zero. For $1 < k \leq 2^n$, the kth word is obtained from its predecessor by changing the dth bit, where $d - 1$ is the highest power of 2 that exactly divides $k - 1$.

(a) List the 16 binary words of length 4 in the order prescribed by this procedure. (*Hint:* As you go along, check to be sure that each newly listed word is different from all of its predecessors, and that it differs from its immediate predecessor in a single bit.)

(b) Show that word k differs from word $2^n - k + 1$ in a single bit, $1 \leq k \leq 2^n$.

(c) Show that the procedure described in this exercise generates 2^n different binary words of length n.

(d) Write an algorithm to implement the procedure described in the introduction to this exercise.

(e) Write an algorithm to list the 2^n subsets of $\{1, 2, \ldots, n\}$ in such a way that any two adjacent subsets on the list differ by just one element.

18 Assuming the keyword RND returns a pseudorandom† number from the interval (0, 1), the following subroutine will generate 1000 pseudorandom integers from the interval [0, 9]:

```
1. For I = 1 to 1000.
2. R(I) = ⌊10 × RND⌋.
3. Next I.
```

To the extent that RND simulates a true random-number generator, each integer in [0, 9] ought to occur with equal likelihood. Each time the subroutine is implemented, one would expect the number 9, e.g., to occur about 100 times.

(a) Write a computer program based on (an appropriate modification of) the subroutine to generate and output 50 pseudorandom integers between 0 and 9 (inclusive).

(b) Run your program from part (a) ten times (using ten different randomizing "seeds") and record the number of 9's that are produced in each run.

(c) Modify your program from part (a) to generate and print out 500 pseudorandom integers between 0 and 9 (inclusive) and, at the end, to output the number of 9's that were printed.

*A list in which each entry differs as little as possible from its predecessor is commonly called a "Gray code". Because such lists have nothing to do with binary codes, "Gray list" might be a better name for them.

†An algorithm to generate random numbers is something of an oxymoron. Truly random numbers are surprisingly difficult to obtain.

19 Assuming keyword RND returns a pseudorandom number, here is an algorithm to simulate the flipping of a single fair coin:

```
1. X = RND.
2. If X < 1/2, then write "H".
3. If X ≥ 1/2, then write "T".
```

(a) Write an algorithm to output 100 simulated flips of a fair coin.

(b) If you were to run a computer program that implements your algorithm from part (a), how many *H*'s would you expect to see?

(c) Write a computer program to implement your algorithm from part (a), run it ten times (with ten different randomizing "seeds"), and record the total number of *H*'s produced on each run.

(d) Write an algorithm to output 100 simulated flips of a fair coin and, at the end, output the total numbers of heads and tails.

(e) Write an algorithm to output 100 simulated flips of a fair coin and, at the end, output the (empirical) probability of heads.

20 If a fair coin is flipped 100 times, it would not be unusual to see a string of four or five heads in a row.

(a) Run your program from Exercise 19(c) ten times (using ten different randomizing "seeds") and record the longest string of consecutive *H*'s and the longest string of consecutive *T*'s for each run.

(b) Modify your algorithm/program from Exercise 19(a)/(c) so that it outputs the length of a longest string of consecutive *H*'s and of a longest string of consecutive *T*'s.

21 Suppose 12 fair coins are tossed into the air at once.

(a) Compute the probability of six heads and six tails.

(b) Write an algorithm to simulate 100 trials of tossing a dozen coins and to output the empirical probability that half the coins come up heads and half tails. (See the discussion of the keyword RND in the introduction to Exercise 18.)

22 Write an algorithm to simulate 100 flips of a biased coin, one in which heads occurs a third of the time. (*Hint:* See the introduction to Exercise 19.)

23 Write an algorithm to simulate 100 rolls of a fair die. (See the introduction to Exercise 18 for an explanation of the keyword RND.)

24 Assuming keyword RND returns a pseudorandom number, write an algorithm to simulate 1200 trials of rolling two (fair) dice

(a) and output the results.

(b) and output the empirical probability of rolling a (total of) 7.

25 Assuming keyword RND returns a pseudorandom number, write an algorithm to simulate 1200 trials of rolling a single (fair) dodecahedral die, and to output the results and the empirical probability of rolling a 7. (*Hint:* A dodecahedral die has twelve faces numbered 1–12.)

26 Assuming keyword RND returns a pseudorandom number, write an algorithm to simulate 1200 trials of rolling five (fair) dodecahedral dice and output the empirical probability of rolling a (sum of) 30.

2

The Combinatorics of Finite Functions

Choose if you dare.

— Pierre Corneille (*Héraclius*, Act IV, Scene iv)

In Chapter 2, we enter the second stratum of combinatorics. The material here is deeper, in the sense that the objects of study are functions. Functions of finite sets have a very different flavor from the kinds of functions one sees, e.g., in calculus or linear algebra. Ironically, it is probably the simplicity of these functions that make them feel so unfamiliar. On the other hand, there is a good deal of back-and-forth interplay with the material of Chapter 1. Stirling's triangles, for example, have much in common with the better known triangle of Pascal.

Partitions of positive integers were introduced in Section 1.8. The different notion of partitions of finite sets arises in Section 2.1 in the context of counting onto functions. Properties and applications of Stirling numbers of the second kind are the theme of Section 2.2, where an unexpected connection with sums of powers of positive integers is revealed. Together with the tools of Chapter 1, Stirling numbers give us the means to solve a class of problems historically stated in terms of balls and urns.

Introduced in the context of fixed points, the famous principle of inclusion and exclusion is the topic of Section 2.3, and Section 2.4 involves cycle structure and Stirling numbers of the first kind. In the final section, Stirling numbers of the first kind are expressed in terms of the elementary numbers (elementary symmetric functions) of Section 1.9. Section 2.5 concludes with a remarkable connection between the two kinds of Stirling numbers.

2.1. STIRLING NUMBERS OF THE SECOND KIND

It is easy for any former calculus student to come up with lots of examples of functions, e.g., $f(x) = x^2$, $f(x) = \sin(x)$, or $f(x) = \ln(x)$. In Chapter 1, we discussed

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

some functions that could easily have come from a course in multivariable calculus, e.g., $E_2(x, y, z) = xy + xz + yz$.

Strictly speaking, a function is comprised of three parts, a *domain* D, a *range*[*] R, and a "rule of assignment" f that associates to each $x \in D$ a unique of element $f(x) \in R$. In single variable calculus, R is typically the set of real numbers and D is the largest of its subsets for which the rule of assignment makes sense. If $f(x) = \ln(x)$, then $D = (0, \infty)$. If $f(x) = 1/x$, D is the set of nonzero real numbers.

In these familiar examples, both D and R are infinite sets. The most practical way to describe a rule of assignment in these circumstances is by means of a formula. Implicit in the formula $f(x) = x^2$ is an algorithm for evaluating $f(x)$. Computing $f(3)$ is trivial. On the other hand, no comparable algorithm is implicit in $f(x) = \ln(x)$. Because it is no more than a name for the mysterious power of e that it takes to produce 3, computing ln(3) is anything but trivial.

The good news about functions of *finite* sets is that, at least in principle, there is no need for formulas or algorithms. Rules of assignment can be given by means of lists or sequences. Suppose, e.g., that $D = \{1, 2, 3, 4\}$ and $R = \{1, 2, 3, 4, 5\}$. Then

$$f(1) = 2, \qquad f(2) = 1, \qquad f(3) = 2, \qquad f(4) = 5 \tag{2.1}$$

completes the description of a unique function. Instead of a formula like $f(x) = x^2 - 4x + 5$, this function can be expressed as $f = (2, 1, 2, 5)$.

2.1.1 Example. Suppose $D = \{1, 2, 3, 4\}$ and $R = \{1, 2, 3, 4, 5\}$. What function is given by the rule $g = (5, 3, 1, 3)$? In sequence notation, $g(i)$ is listed in the ith place. So,

$$g(1) = 5, \qquad g(2) = 3, \qquad g(3) = 1, \qquad g(4) = 3.$$

What about (4, 1, 5, 3, 3)? This sequence does not correspond to any function of $D = \{1, 2, 3, 4\}$. Its length is wrong. The functions on $D = \{1, 2, 3, 4\}$ are represented by sequences of length 4. Similarly, $h = (6, 2, 3, 1)$ could not possibly be a function from D into $R = \{1, 2, 3, 4, 5\}$ because $h(1) = 6$ is not an element of R. □

2.1.2 Definition. Denote by $F_{m,n}$ the set of all functions from $D = \{1, 2, \ldots, m\}$ into $R = \{1, 2, \ldots, n\}$. The notation for $f \in F_{m,n}$ is

$$f = (f(1), f(2), \ldots, f(m)).$$

2.1.3 Example. The set of all possible functions from $\{1, 2, 3\}$ into $\{1, 2\}$ is

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

[*] The *image* of f, $\{f(x) : x \in D\}$, is a subset of R.

Similarly,

$$F_{2,3} = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}. \quad \square$$

In Example 2.1.3, the elements of $F_{3,2}$ and $F_{2,3}$ were listed in so-called dictionary order.

2.1.4 Definition. Suppose $f, g \in F_{m,n}$, $f \neq g$. Let i be the smallest positive integer such that $f(i) \neq g(i)$. If $f(i) < g(i)$, then f comes before g in *dictionary order*,* and we write $f < g$.

2.1.5 Example. If $f = (2,2,1)$ and $g = (2,1,2)$, then $f(1) = 2 = g(1)$, but $f(2) = 2 > 1 = g(2)$. So, f comes after g in dictionary order, i.e., $f > g$. [In Example 2.1.3, $f = (2,2,1)$ comes *immediately* after $g = (2,1,2)$.]

The *smallest* positive integer i such that $f(i) \neq g(i)$ corresponds to the *first* place in their respective sequences that f and g differ. In this case, $i = 2$. In particular, it is irrelevant which of $f(3)$ and $g(3)$ is larger. $\square$

Thinking of $F_{3,2}$ as the set of all functions from $\{1, 2, 3\}$ into $\{1,2\}$ may take some getting used to. For one thing, $F_{3,2}$ is finite. To count the function in $F_{m,n}$, observe that there are n choices for each of $f(1), f(2), \ldots, f(m)$. Therefore, $o(F_{m,n}) = n^m$.

2.1.6 Example. Is $o(F_{2,3})$ equal to 8 or 9? Note that m and n are read first m then n in $F_{m,n}$ but first n then m in n^m. In particular, $o(F_{2,3}) = 3^2$. (Is it obvious, just by glancing at $F_{2,3}$ and $F_{3,2}$ in Example 2.1.3, that $F_{2,3}$ is the larger set?) $\square$

Recall that f is one-to-one if and only if $f(x_1) = f(x_2)$ implies $x_1 = x_2$. Represented by sequences without repetitions, the one-to-one functions in $F_{m,n}$ are easy to count. There are n choices for $f(1)$, $n-1$ choices for $f(2), \ldots$, and $n - (m-1) = n - m + 1$ choices for $f(m)$. The product of these numbers is $P(n,m) = n(n-1)\cdots(n-m+1)$. Again, there is a reversal of m and n. In "the one-to-one functions in $F_{m,n}$", m is read before n. In "$P(n,m)$", it's the other way around.

Among the $3^2 = 9$ functions in $F_{2,3}$, $P(3,2) = 3 \times 2 = 6$ are one-to-one. [The three remaining functions are (1, 1), (2, 2), and (3, 3).] No function in $F_{3,2}$ is one-to-one. If $m > n$, then $P(n,m) = 0$.

Among the one-to-one functions are the increasing functions.

2.1.7 Definition. Denote by $Q_{m,n} \subset F_{m,n}$ the set of (strictly) increasing functions, i.e., $f \in Q_{m,n}$ if (and only if) $1 \leq f(1) < f(2) < \cdots < f(m) \leq n$.

* Dictionary order is also known as *lexicographic order.*

2.1.8 Example. In dictionary order, $Q_{2,3} = \{(1,2),(1,3),(2,3)\}$, $Q_{3,3} = \{(1,2,3)\}$, and $Q_{3,5} = \{(1,2,3),(1,2,4),(1,2,5),(1,3,4),(1,3,5),(1,4,5),(2,3,4),(2,3,5),(2,4,5),(3,4,5)\}$. □

To count the functions in $Q_{m,n}$, observe that an increasing sequence is uniquely determined by the integers that it contains. Once they have been chosen, there is just one way to arrange them into increasing order. Therefore, $o(Q_{m,n}) = C(n,m)$. (Note the "reversal" of m and n.) That $o(Q_{2,3}) = C(3,2) = 3, o(Q_{3,3}) = C(3,3) = 1$, and $o(Q_{3,5}) = C(5,3) = 10$ can be confirmed by glancing at Example 2.1.8.

There is a curious irony about the identity $o(Q_{m,n}) = C(n,m)$. While the elements of $Q_{m,n}$ are ordered sequences, order *doesn't* matter in their enumeration. (Recall the similar semantic difficulty in connection with arranging the parts of a partition from largest to smallest.)

One application of $Q_{m,n}$ is an explicit formula for elementary symmetric functions.

2.1.9 Theorem. *If n is a fixed positive integer, then*

$$E_m(x_1, x_2, \ldots, x_n) = \sum_{f \in Q_{m,n}} \prod_{i=1}^{m} x_{f(i)}, \qquad 1 \le m \le n. \tag{2.2}$$

Proof. Recall that $E_m(x_1, x_2, \ldots, x_n)$ is the sum of all products of the x's taken m at a time. Equation (2.2) is obtained by observing that each selection of m variables corresponds to a unique function $f \in Q_{m,n}$. ■

2.1.10 Example. Let's use Equation (2.2) to evaluate $E_2(x_1, x_2, x_3)$. From Example 2.1.8, $Q_{2,3} = \{(1,2),(1,3),(2,3)\}$. If $f = (1,2)$, then $\prod x_{f(i)} = x_1x_2$; if $f = (1,3)$, then $\prod x_{f(i)} = x_1x_3$; and if $f = (2,3)$, then $\prod x_{f(i)} = x_2x_3$. The sum of these products is $x_1x_2 + x_1x_3 + x_2x_3 = E_2(x_1, x_2, x_3)$. □

One interesting thing about Equation (2.2) is the way it blends two very different species of function. Elementary symmetric functions are fairly sophisticated polynomials in several variables. It makes sense, e.g., to say things like "the partial derivative of $E_m(x_1, x_2, \ldots, x_n)$ with respect to the variable x_n is $E_{m-1}(x_1, x_2, \ldots, x_{n-1})$." On the other hand, it makes no sense at all to talk about the derivative of some finite function $f \in Q_{m,n}$.

Recall that $f : D \to R$ is *onto* if and only if $\{f(x) : x \in D\} = R$. If $m < n$, then a sequence of length m cannot contain all the integers in $\{1, 2, \ldots, n\}$. So, $m \ge n$ is a necessary condition for there to exist *any* onto functions in $F_{m,n}$. Okay, assuming $m \ge n$, how many of the n^m functions in $F_{m,n}$ are onto? This problem is not so easily solved as its one-to-one counterpart. The solution begins with the following.

2.1.11 Definition. If $y \in \{1, 2, \ldots, n\}$ and $f \in F_{m,n}$, then $f^{-1}(y) = \{x : f(x) = y\}$.

A potentially troublesome feature of Definition 2.1.11 is its abuse of the usual language. Recall that $f : D \to R$ has an inverse, $f^{-1} : R \to D$, if and only if f is

one-to-one and onto, in which case $f^{-1}(y)$ is the *unique* $x \in D$ such that $f(x) = y$. If f is not one-to-one, there may be more than one such x, and that is what Definition 2.1.11 seeks to capture: $f^{-1}(y)$ is the set of *all* such x's. (Note that f is onto if and only if $f^{-1}(y)$ is nonempty for all $y \in R$.)

If f is one-to-one and onto, and if $f(x) = y$, then the notation of Definition 2.1.11 yields $f^{-1}(y) = \{x\}$ rather than $f^{-1}(y) = x$, which may cause some confusion. If f is not one-to-one and onto, there should be no confusion. When the ordinary inverse does not exist, f^{-1} can be interpreted in only one way, namely, the one given by Definition 2.1.11.

Finally, the variables needn't be called x or y. Integer variables commonly have names like i, j, and k. If $f \in F_{m,n}$, then, e.g., $f^{-1}(j)$ is the subset of $\{1, 2, \ldots, m\}$ consisting of all those integers i such that $f(i) = j$.

2.1.12 Example. If $f = (2, 1, 2, 5) \in F_{4,5}$, then $f^{-1}(1) = \{2\}$, $f^{-1}(2) = \{1, 3\}$, $f^{-1}(3) = \varnothing = f^{-1}(4)$, and $f^{-1}(5) = \{4\}$. If $g = (7, 4, 2, 8, 3) \in F_{m,n}$, then $m = 5$ and $n \geq 8$. Because g is one-to-one, $o(g^{-1}(j)) \leq 1$, $1 \leq j \leq n$. Since, e.g., $o(g^{-1}(5)) = 0$, g is not onto. □

2.1.13 Lemma. *Suppose $f \in F_{m,n}$. Then f is one-to-one if and only if $o(f^{-1}(j)) \leq 1$, $1 \leq j \leq n$, and f is onto if and only if $o(f^{-1}(j)) \geq 1$, $1 \leq j \leq n$.*

Proof. Immediate from the definitions. ■

Among the topics discussed in Chapter 1 are partitions of the positive integer n. We are about to abuse the language again by using the word "partition" in a different way.

2.1.14 Definition. Let S be a set. A *partition* of S is an unordered collection of pairwise disjoint, nonempty subsets of S whose union is all of S. The subsets of a partition are called *blocks*.

For $S = A_1 \cup A_2 \cup \cdots \cup A_k$ to be a partition of S, two things are required: (1) $A_i \cap A_j = \varnothing$ whenever $i \neq j$ and (2) $A_j \neq \varnothing$, $1 \leq j \leq k$.

2.1.15 Example. Two partitions are equal if and only if they have the same blocks. So. e.g., $\{1\} \cup \{2, 3\}$, $\{1\} \cup \{3, 2\}$, and $\{2, 3\} \cup \{1\}$ are three different-*looking* ways to write the same two-block partition of $S = \{1, 2, 3\}$. The other partitions of S are $\{1\} \cup \{2\} \cup \{3\}$, having three blocks; $\{1, 2\} \cup \{3\}$ and $\{1, 3\} \cup \{2\}$, each having two blocks; and $\{1, 2, 3\}$, having just one block. In particular, S has a total of five different partitions. □

What do partitions and onto functions have in common? Suppose $f \in F_{m,n}$. Let $D = \{1, 2, \ldots, m\}$. Because it is the domain of f,

$$D = \bigcup_{j=1}^{n} f^{-1}(j). \tag{2.3}$$

If $i \in f^{-1}(j_1) \cap f^{-1}(j_2)$, then $j_1 = f(i) = j_2$, and so, because f is a function, $j_1 = j_2$. Therefore, $f^{-1}(j_1)$ and $f^{-1}(j_2)$ are disjoint whenever $j_1 \neq j_2$. Moreover, f is onto if and only if $f^{-1}(j) \neq \varnothing$ for all $j \in \{1, 2, \ldots, n\}$. Let's summarize.

2.1.16 Lemma. *The function $f \in F_{m,n}$ is onto if and only if Equation (2.3) is a partition of $D = \{1, 2, \ldots, m\}$.*

2.1.17 Definition. The number partitions of $\{1, 2, \ldots, m\}$ into n blocks is denoted $S(m, n)$ and called a *Stirling number of the second kind.*[*]

Evidently, $S(m, n) = 0$ if $n < 1$ or $n > m$. Because there is just one way to partition $\{1, 2, \ldots, m\}$ into a single block and $\{1\} \cup \{2\} \cup \cdots \cup \{m\}$ is the unique (unordered) way to express it as the disjoint union of m nonempty subsets, $S(m, 1) = 1 = S(m, m)$.

2.1.18 Example. In Example 2.1.15 we saw, e.g., that $S(3, 2) = 3$. the two-block partitions of $\{1, 2, 3, 4\}$ are

$$\{1\} \cup \{2, 3, 4\}, \quad \{2\} \cup \{1, 3, 4\}, \quad \{3\} \cup \{1, 2, 4\}, \quad \{4\} \cup \{1, 2, 3\},$$
$$\{1, 2\} \cup \{3, 4\}, \quad \{1, 3\} \cup \{2, 4\}, \quad \text{and} \quad \{1, 4\} \cup \{2, 3\},$$

so $S(4, 2) = 7$. The three-block partitions of $\{1, 2, 3, 4\}$ are

$$\{1\} \cup \{2\} \cup \{3, 4\}, \quad \{1\} \cup \{3\} \cup \{2, 4\}, \quad \{1\} \cup \{4\} \cup \{2, 3\},$$
$$\{2\} \cup \{3\} \cup \{1, 4\}, \quad \{2\} \cup \{4\} \cup \{1, 3\}, \quad \text{and} \quad \{3\} \cup \{4\} \cup \{1, 2\}.$$

So, $S(4, 3) = 6$. □

Onto functions and Stirling numbers come together in the next result.

2.1.19 Theorem. *The number of onto functions in $F_{m,n}$ is $n!S(m, n)$.*

Proof. If $n > m$, there are no n-part partitions of $\{1, 2, \ldots, m\}$ and no onto functions in $F_{m,n}$. When $n \leq m$, the theorem is proved by establishing a many-to-one correspondence between onto functions and n-block partitions.

By Lemma 2.1.16, each onto function $f \in F_{m,n}$ affords a unique partition, namely, $f^{-1}(1) \cup f^{-1}(2) \cup \cdots \cup f^{-1}(n)$. Indeed, from the perspective of f, this is an *ordered* partition. For onto function $f \in F_{m,n}$ to afford partition $A_1 \cup A_2 \cup \cdots \cup A_n$, it isn't necessary for A_1 to be $f^{-1}(1)$. Since partitions are unordered, the block A_1 could just as well be $f^{-1}(j)$ for any $j \in \{1, 2, \ldots, n\}$. There are n ways to choose an integer j_1 to satisfy $A_1 = f^{-1}(j_1)$, $n - 1$ ways to choose j_2 so that $A_2 = f^{-1}(j_2)$, $n - 2$ ways to choose j_3, and so on. Evidently, each of the $S(m, n)$ n-block partitions of $\{1, 2, \ldots, m\}$ can be arranged in $n!$ ways, corresponding to the ordered partitions afforded by $n!$ different onto functions $f \in F_{m,n}$. ■

[*] Named for James Stirling (1692–1770). The terminology suggests the existence, at the very least, of Stirling numbers of the first kind.

m \ n	1	2	3	4	5	6	7
1	1						
2	1	1					
3	1	3	1				
4	1	7	6	1			
5	1	$S(5,2)$	$S(5,3)$	$S(5,4)$	1		
6	1	$S(6,2)$	$S(6,3)$	$S(6,4)$	$S(6,5)$	1	
7	1	$S(7,2)$	$S(7,3)$	$S(7,4)$	$S(7,5)$	$S(7,6)$	1
				⋯			

Figure 2.1.1. Stirling's triangle.

From Example 2.1.18, $S(3,2) = 3$, $S(4,2) = 7$, and $S(4,3) = 6$. Together with $S(m,1) = 1 = S(m,m), m \geq 1$, this gives us a start at filling in some of the entries of *Stirling's triangle* (Fig. 2.1.1).

2.1.20 Theorem. *If $m \geq n \geq 2$, then $S(m+1,n) = S(m,n-1) + nS(m,n)$.*

Theorem 2.1.20 allows us to fill in as many rows of Fig. 2.1.1 as we like, e.g.,

$$\begin{aligned} S(5,2) &= S(4,1) + 2S(4,2) \\ &= 1 + 2 \times 7 \\ &= 15 \\ S(5,3) &= S(4,2) + 3S(4,3) \\ &= 7 + 3 \times 6 \\ &= 25, \\ S(5,4) &= S(4,3) + 4S(4,4) \\ &= 6 + 4 \times 1 \\ &= 10. \end{aligned}$$

Thus, we obtain Fig. 2.1.2.

Proof of Theorem 2.1.20. The n-block partitions of $T = \{1,2,\ldots,m,m+1\}$ can be divided into two types, those for which $m+1$ is alone is its block and those for which it isn't. Counting partitions of the first type is easy: If $\{m+1\}$ is a block of the partition, then the remaining m elements of T can be partitioned into $n-1$ blocks in $S(m,n-1)$ ways.

If $m+1$ is not isolated, then removing $m+1$ from its block produces an n-part partition of $\{1,2,\ldots,m\}$, say, $A_1 \cup A_2 \cup \cdots \cup A_n$. Now, this same partition would

m \ n	1	2	3	4	5	6	7
1	1						
2	1	1					
3	1	3	1				
4	1	7	6	1			
5	1	15	25	10	1		
6	1	31	90	65	15	1	
7	1	63	301	350	140	21	1
				⋯			

Figure 2.1.2. Stirling numbers of the second Kind, $S(m,n)$.

arise if $m+1$ had been removed from any one of the blocks A_i, $1 \le i \le n$. In other words, to each n-part partition of $\{1,2,\ldots,m\}$ there correspond n different n-part partitions of T of the second type, i.e., there are (exactly) $nS(m,n)$ partitions of T in which $m+1$ shares its block with at least one other integer. ■

2.1.21 Example. Observe that

$$\begin{aligned} 2+1 &= 3 && \text{is prime,}\\ 2\times 3+1 &= 7 && \text{is prime,}\\ 2\times 3\times 5+1 &= 31 && \text{is prime,}\\ 2\times 3\times 5\times 7+1 &= 211 && \text{is prime,}\\ 2\times 3\times 5\times 7\times 11+1 &= 2311 && \text{is prime,} \end{aligned}$$

but (maybe 13 is unlucky)

$$\begin{aligned} 2\times 3\times 5\times 7\times 11\times 13+1 &= 30,031\\ &= 59\times 509 \end{aligned}$$

is not. However, because 59 and 509 are primes, this is the only nontrivial factorization of 30,031. By way of comparison, if its immediate predecessor

$$\begin{aligned} 30,031-1 &= 30,030\\ &= 2\times 3\times 5\times 7\times 11\times 13\\ &= dq, \end{aligned}$$

where $1<d<q$, then the prime factors of d and q correspond to the blocks of a two-part partition of $\{2,3,5,7,11,13\}$. Moreover, because partitions are unordered, this correspondence is one-to-one, i.e., 30,030 has (exactly) $S(6,2)=31$ different factorizations as a product of two integers each greater than 1. □

2.1. EXERCISES

1 Find $f(3)$ and $f^{-1}(4)$ if

(a) $f = (4, 1, 5)$. **(b)** $f = (9, 4, 5, 4, 2)$.

(c) $f = (3, 3, 4, 4)$. **(d)** $f = (4, 3, 2, 1)$.

(e) $f = (8, 2)$. **(f)** $f = (4, 4, 4, 4, 4)$.

2 Compute

(a) $o(F_{5,3})$. **(b)** $o(F_{3,5})$. **(c)** $o(F_{4,4})$.

(d) $o(Q_{5,3})$. **(e)** $o(Q_{3,5})$. **(f)** $o(Q_{4,4})$.

3 Write down all the one-to-one functions in

(a) $F_{2,3}$. **(b)** $F_{3,3}$. **(c)** $F_{4,3}$.

(d) $Q_{2,3}$. **(e)** $Q_{3,3}$. **(f)** $Q_{3,4}$.

4 Write down all the onto functions in

(a) $F_{3,2}$. **(b)** $F_{3,3}$. **(c)** $F_{3,4}$.

(d) $Q_{2,3}$. **(e)** $Q_{3,3}$. **(f)** $Q_{4,4}$.

5 Compute $S(m, n)$, $1 \leq n \leq m$, $8 \leq m \leq 9$.

6 Show that

(a) $S(n+1, n) = C(n+1, 2)$.

(b) $S(n+2, n) = C(n+2, 3) + 3C(n+2, 4)$.

(c) $S(n+1, 2) = 2^n - 1$.

7 Suppose $n = p_1 p_2 \cdots p_r$, where $p_1, p_2, \ldots, p_r$ are distinct primes and $r \geq 2$. Prove that n can be factored as $n = dq$, where $1 < d < q$, in exactly $S(r, 2)$ different ways.

8 Prove that

$$(x_1 + x_2 + \cdots + x_n)^m = \sum_{f \in F_{m,n}} \prod_{i=1}^{m} x_{f(i)}.$$

9 Between $Q_{m,n}$ and $F_{m,n}$ is $G_{m,n}$, the set of nondecreasing functions, i.e., $f \in G_{m,n}$ if and only if $1 \leq f(1) \leq f(2) \leq \cdots \leq f(m) \leq n$.

(a) List the elements of $G_{2,3}$.

(b) List the elements of $G_{3,3}$.

(c) Prove that $o(G_{m,n}) = C(m+n-1, m)$.

10 The homogeneous symmetric function $H_m(x_1, x_2, \ldots, x_n)$ was introduced in Exercise 25, Section 1.8. It is the sum of all $C(m+n-1, m)$ different monomials of degree m in the variables $x_1, x_2, \ldots, x_n$.

(a) Show that

$$H_m(x_1, x_2, \ldots, x_n) = \sum_{f \in G_{m,n}} \prod_{i=1}^{m} x_{f(i)},$$

where $G_{m,n}$ is the set of nondecreasing functions (sequences) defined in Exercise 9.

(b) Use part (a) to compute $H_2(1, 2, 3)$.

(c) Show that $H_3(1, 2, 3) = 90$.

(d) Without evaluating any of the three terms, show that $H_3(1, 2, 3, 4) = H_3(1, 2, 3) + 4H_2$ (1, 2, 3, 4).

11 Let $H_m(x_1, x_2, \ldots, x_n)$ be the homogeneous symmetric function from Exercise 10.

(a) Prove that $H_{m+1}(x_1, x_2, \ldots, x_n) = H_{m+1}(x_1, x_2, \ldots, x_{n-1}) + x_n H_m(x_1, x_2, \ldots, x_n), n \geq 2$.

(b) Define $h(m, m) = 1$ and $h(m, n) = H_{m-n}(1, 2, \ldots, n)$, $m > n$. Prove that $h(m + 1, n) = h(m, n - 1) + nh(m, n)$, $m \geq n \geq 2$.

(c) Prove that $S(m, n) = H_{m-n}(1, 2, \ldots, n)$, $m \geq n \geq 1$.

(d) Prove that

$$S(n + r, n) = \sum_{f \in G_{r,n}} \prod_{i=1}^{r} f(i).$$

12 The *image* of $f \in F_{m,n}$ is

$$\text{image } (f) = \{f(x) : x \in \{1, 2, \ldots, m\}\},$$

i.e., image (f) is the set of numbers that occur in the sequence $(f(1), f(2), \ldots, f(m))$. Prove that the number of functions $f \in F_{m,n}$ that satisfy $o(\text{image}(f)) = t$ is $n!S(m, t)/(n - t)!$.

13 Prove the following analog of Chu's theorem:

$$S(m + 1, n + 1) = \sum_{k=n}^{m} C(m, k)S(k, n).$$

14 In how many ways can 30,030 be factored as a product of three integers, $a \times b \times c$, where $1 < a < b < c$?

15 Organize the set of area codes (4, 1, 5), (2, 1, 3), (2, 1, 2), (2, 0, 5), (2, 0, 2), (7, 0, 7), (4, 0, 5), (8, 0, 5), and (8, 1, 8) into dictionary order.

16 A *substitution code* encrypts ordinary text messages by uniformly replacing each letter with a substitute. Among the simplest of these are the *Caesar cypher's*, in which each letter is replaced by the one coming n places after it (or before it if n is negative) in alphabetical order. In the Stanley Kubrick film

2001: A Space Odyssey, the computer's name, HAL, is a Caesar cypher for IBM, corresponding to $n = -1$. (It has been said that an early Roman emperor amused himself by handing the following note to a messenger and ordering him to carry it to the local military commander: "JHKK SGD ADZQDQ NE SGHR MNSD.")

Code breaking frequently involves the notion of a word *pattern*. The pattern WXYZXW, for example, is common to several English words, e.g., EVOLVE, LARVAL, READER, RENTER, SERIES, and TIDBIT. (Note that REGRET exhibits a different pattern, namely, WXYWXZ.) There are no English words with pattern WWWWWW (the same as pattern XXXXXX) nor, for that matter, with pattern WWXYY (the same as QQALL).*

Denote by $T(m, n)$ the number of different m-letter word patterns that use a total of n different letters. (Then, e.g., $T(3, 1) = 1$, $T(3, 2) = 3$, and $T(3, 3) = 1$.)

(a) Compute $T(4, n)$, $1 \leq n \leq 4$.

(b) There are two four-letter English words having word pattern XYXX. Find one of them.

(c) Show that $T(m, 1) = 1 = T(m, m)$.

(d) Prove that the array of word pattern numbers is identical to the array of Stirling numbers of the second kind, i.e., for all positive integers, m, $T(m, n) = S(m, n)$, $1 \leq n \leq m$.

17 Let $S = \{1, 2, 3, 4, 5\}$. In how many partitions of S will

(a) 1 and 2 be in the same block of S?

(b) 1 and 2 be in different blocks of S?

18 Write an algorithm/program to generate and list, in dictionary order,

(a) all the one-to-one functions in $F_{4,4}$. (*Hint*: How is this different from listing all 4! rearrangements of 1234?)

(b) all 4^4 functions in $F_{4,4}$. (*Hint*: Start from scratch.)

(c) all five functions in $Q_{4,5}$.

(d) all C(6, 4) functions in $Q_{4,6}$.

(e) all C(6, 4) four-element subsets of $\{1, 2, 3, 4, 5, 6\}$.

19 Write an algorithm/program to input x_i, $1 \leq i \leq 6$, and output $E_4(x_1, x_2, \ldots, x_6)$.

20 Denote by $S_k(m, n)$ the number of partitions of $\{1, 2, \ldots, m\}$ into n blocks each of which contains *at least* k elements. Show that

(a) $S(m, n) = S_1(m, n)$.

(b) $S_k(m + 1, n) = C(m, k - 1)S_k(m - k + 1, n - 1) + nS_k(m, n)$.

* See, e.g., S. W. Golomb, On the enumeration of cryptograms, *Math. Mag.* 53 (1980), 219–221.

21 Let $G_{m,n} \subset F_{m,n}$ be the set of nondecreasing functions from Exercise 9. Compute $o(\{f \in G_{m,n} : o(\{j : o(f^{-1}(j)) \geq 2\}) = 1\})$.

22 There is an analog of the fundamental theorem of symmetric polynomials (Appendix A1) for the homogeneous symmetric functions of Exercise 10: Any polynomial symmetric in the variables $x_1, x_2, \ldots, x_n$ is a polynomial in the homogeneous symmetric functions $H_m(x_1, x_2, \ldots, x_n)$, $1 \leq m \leq n$.

(a) Show that the elementary symmetric function $E_2(x, y, z) = H_1(x, y, z)^2 - H_2(x, y, z)$.

(b) Show that the second power sum $M_2(x, y, z) = 2H_2(x, y, z) - H_1(x, y, z)^2$.

(c) Express $E_3(x, y, z)$ as a polynomial in $H_m(x, y, z)$, $1 \leq m \leq 3$.

(d) Express $M_3(x, y, z)$ as a polynomial in $H_m(x, y, z)$, $1 \leq m \leq 3$.

(e) Express $M_4(x, y, z)$ as a polynomial in $H_m(x, y, z)$, $1 \leq m \leq 3$.

23 Let $H_m = H_m(x, y, z)$ be the homogeneous symmetric function of Exercise 10. For each partition $\pi \vdash 4$, let $M_\pi = M_\pi(x, y, z)$. Show that

(a) $H_1^4 = M_{[4]} + 4M_{[3,1]} + 6M_{[2^2]} + 12M_{[2,1^2]}$.

(b) $H_1^2 H_2 = M_{[4]} + 3M_{[3,1]} + 4M_{[2^2]} + 7M_{[2,1^2]}$.

(c) $H_2^2 = M_{[4]} + 2M_{[3,1]} + 3M_{[2^2]} + 4M_{[2,1^2]}$.

(d) $H_1 H_3 = M_{[4]} + 2M_{[3,1]} + 2M_{[2^2]} + 3M_{[2,1^2]}$.

24 An equivalence relation on $S = \{1, 2, 3, 4, 5, 6, 7\}$ partitions the set into the disjoint union of equivalence classes.

(a) Show that every partition of S corresponds to the family of equivalence classes for some equivalence relation.

(b) How many different equivalence relations on S are there?

25 Write an algorithm/program to compute $S(m, n)$, $1 \leq m \leq 12$, $1 \leq n \leq m$.

2.2. BELLS, BALLS, AND URNS

Heard melodies are sweet, but those unheard are sweeter.

— John Keats (*Ode on a Grecian Urn*)

Recall that the falling factorial function is defined by $x^{(0)} = 1$ and

$$x^{(n+1)} = x(x-1)(x-2)\cdots(x-n), \qquad n \geq 0.$$

If $m \geq 1$, then $x^{(m)}$ is a polynomial of degree m whose roots are $0, 1, 2, \ldots, m-1$. Thus,

$$x^{(m)} = x^m - e(m-1,1)x^{m-1} + e(m-1,2)x^{m-2} - \cdots + (-1)^{m-1}e(m-1,m-1)x, \tag{2.4}$$

where the elementary number $e(m-1,r) = E_r(1,2,\ldots,m-1) = E_r(0,1,2,\ldots,m-1)$, $1 \leq r < m$.

2.2.1 Example. Let's confirm Equation (2.4). From Fig. 1.9.2,

$$\begin{aligned} x^{(3)} &= x^3 - e(2,1)x^2 + e(2,2)x \\ &= x^3 - 3x^2 + 2x \end{aligned}$$

when $m = 3$ and

$$\begin{aligned} x^{(4)} &= x^4 - e(3,1)x^3 + e(3,2)x^2 - e(3,3)x \\ &= x^4 - 6x^3 + 11x^2 - 6x \end{aligned}$$

when $m = 4$. On the other hand, from the definition,

$$\begin{aligned} x^{(3)} &= x(x-1)(x-2) \\ &= x(x^2 - 3x + 2), \end{aligned}$$

and

$$\begin{aligned} x^{(4)} &= x(x-1)(x-2)(x-3) \\ &= (x^2 - x)(x^2 - 5x + 6) \\ &= x^4 - (1+5)x^3 + (5+6)x^2 - 6x. \end{aligned}$$ □

Equation (2.4) is an explicit expression of the (obvious) fact that $x^{(m)}$ is *some* linear combination of $x, x^2, x^3, \ldots, x^m$. On the other hand, because $x^{(r)}$ has degree r, it must also be the case that x^m is some (unique*) linear combination of $x^{(1)}, x^{(2)}, x^{(3)}, \ldots, x^{(m)}$. More remarkable is the fact that the coefficients in this inverse expression are Stirling numbers of the second kind!

2.2.2 Theorem. *For any positive integer m,*

$$x^m = \sum_{r=1}^{m} S(m,r)x^{(r)}.$$

* See, e.g., Exercise 28, Section 1.5, or Exercise 24, Section 1.9.

Let's confirm this identity when $m = 4$. Together with the fourth row of Fig. 2.1.2 (read backward!), Theorem 2.2.2 yields

$$\begin{aligned} x^4 &= S(4,4)x^{(4)} + S(4,3)x^{(3)} + S(4,2)x^{(2)} + S(4,1)x^{(1)} \\ &= (x^4 - 6x^3 + 11x^2 - 6x) + 6(x^3 - 3x^2 + 2x) + 7(x^2 - x) + x \\ &= x^4 + (-6+6)x^3 + (11 - 18 + 7)x^2 + (-6 + 12 - 7 + 1)x. \end{aligned}$$

Proof of Theorem 2.2.2. Because $S(1,1) = 1$ and $x = x^{(1)}$, the $m = 1$ case is trivial. If $m > 1$, then, by induction,

$$\begin{aligned} x^m &= x^{m-1} \cdot x \\ &= \left(\sum_{r=1}^{m-1} S(m-1,r)x^{(r)} \right) x \\ &= \sum_{r=1}^{m-1} S(m-1,r)[x^{(r)}x]. \end{aligned} \tag{2.5}$$

Because $x = (x - r) + r$,

$$\begin{aligned} x^{(r)}x &= x^{(r)}(x-r) + x^{(r)}r \\ &= x^{(r+1)} + rx^{(r)}. \end{aligned}$$

Substituting this identity into Equation (2.5) and reorganizing, we obtain

$$x^m = \sum_{r=1}^{m-1} S(m-1,r)x^{(r+1)} + \sum_{r=1}^{m-1} rS(m-1,r)x^{(r)}.$$

Changing the variable in the first summation yields

$$\begin{aligned} x^m &= \sum_{r=2}^{m} S(m-1,r-1)x^{(r)} + \sum_{r=1}^{m-1} rS(m-1,r)x^{(r)} \\ &= x^{(m)} + \sum_{r=2}^{m-1} S(m-1,r-1)x^{(r)} + \sum_{r=2}^{m-1} rS(m-1,r)x^{(r)} + x^{(1)} \\ &= x^{(m)} + \sum_{r=2}^{m-1} [S(m-1,r-1) + rS(m-1,r)]x^{(r)} + x^{(1)} \\ &= \sum_{r=1}^{m} S(m,r)x^{(r)} \end{aligned}$$

because $S(m,r) = S(m-1,r-1) + rS(m-1,r)$, $2 \le r \le m-1$. ■

2.2.3 Corollary. *For all positive integers k and m,*

$$k^m = \sum_{r=1}^{m} r!S(m,r)C(k,r). \tag{2.6}$$

Proof. Because Theorem 2.2.2 is a polynomial identity, we can substitute any number we like for x. Setting $x = k$ gives

$$\begin{aligned} k^m &= \sum_{r=1}^{m} S(m,r)P(k,r) \\ &= \sum_{r=1}^{m} r!S(m,r)P(k,r)/r! \\ &= \sum_{r=1}^{m} r!S(m,r)C(k,r). \end{aligned}$$

■

Recall the approach that was used in Section 1.5 to obtain a formula for the sum of the mth powers of the first n positive integers. If

$$k^m = \sum_{r=1}^{m} a_{r,m}C(k,r), \tag{2.7}$$

then, by Equation (1.10),

$$1^m + 2^m + \cdots + n^m = \sum_{r=1}^{m} a_{r,m}C(n+1, r+1).$$

Inverting the $n \times n$ Pascal matrix C_n whose (i,j)-entry is $C(i,j)$, we obtained (Theorem 1.5.5) the *unique* solution

$$a_{r,m} = \sum_{t=1}^{m} (-1)^{r+t} C(r,t)t^m. \tag{2.8a}$$

It follows from Equations (2.6) and (2.7) that

$$a_{r,m} = r!S(m,r). \tag{2.8b}$$

Two conclusions can be drawn from these observations. The first is a new formula for the sum of the mth powers of the first n positive integers, namely,

$$1^m + 2^m + \cdots + n^m = \sum_{r=1}^{m} r!S(m,r)C(n+1, r+1). \tag{2.9}$$

The second is a new formula for the number of onto functions in $F_{m,r}$.

2.2.4 Corollary (Stirling's Identity*). *For any two positive integers m and r,*

$$r!S(m,r) = \sum_{t=1}^{r} (-1)^{r+t} C(r,t) t^m.$$

Proof. Equations (2.8a) and (2.8b). ■

2.2.5 Example. For $1 \le r \le m = 4$, Stirling's identity produces

$$\begin{aligned}
S(4,1) &= C(1,1)1^4 \\
&= 1, \\
S(4,2) &= \tfrac{1}{2}[-C(2,1)1^4 + C(2,2)2^4] \\
&= \tfrac{1}{2}[-2 + 16] = 7, \\
S(4,3) &= \tfrac{1}{6}[C(3,1)1^4 - C(3,2)2^4 + C(3,3)3^4] \\
&= \tfrac{1}{6}[3 - 48 + 81] = 6, \\
S(4,4) &= \tfrac{1}{24}[-C(4,1)1^4 + C(4,2)2^4 - C(4,3)3^4 + C(4,4)4^4] \\
&= \tfrac{1}{24}[-4 + 96 - 324 + 256] = 1.
\end{aligned}$$

While its usefulness to computing $S(m,r)$ may be restricted to $r \le m$, Stirling's identity remains valid when $r > m$. If $r = 4$ and $m = 3$, e.g.,

$$\begin{aligned}
4!S(3,4) &= -C(4,1)1^3 + C(4,2)2^3 - C(4,3)3^3 + C(4,4)4^3 \\
&= -4 \times 1 + 6 \times 8 - 4 \times 27 + 1 \times 64 \\
&= -4 + 48 - 108 + 64 \\
&= 0.
\end{aligned}$$

Indeed, Stirling's identity implies that

$$C(r,r)r^m - C(r,r-1)(r-1)^m + \cdots + (-1)^{r+1} C(r,1)1^m = 0$$

for all $r > m$. □

Recall that the nth-row sum of the partition triangle is $\sum_{r=1}^{n} p_r(n) = p(n)$, the total number of partitions of n. Similarly, $\sum_{r=1}^{n} S(n,r)$ is the total number of partitions of $\{1, 2, \ldots, n\}$.

2.2.6 Definition. The *Bell numbers*† are defined by $B_0 = 1$ and

$$B_n = \sum_{r=1}^{n} S(n,r), \qquad n \ge 1.$$

* Not to be confused with Stirling's formula: $n!/n^n \doteq \sqrt{2\pi n}/e^n$.
† After Eric Temple Bell (1883–1960).

From Figure 2.1.2, the Bell sequence (starting with B_0) is 1, 1, 2, 5, 15, 52, 203, 877, ...

2.2.7 Theorem. *The Bell numbers satisfy the recurrence*

$$B_{n+1} = \sum_{r=o}^{n} C(n,r)B_r. \tag{2.10}$$

Equation (2.10) is reminiscent of the binomial theorem. Changing each subscript to a superscript gives a (nonsensical) way to remember Equation (2.10) :

$$B^{n+1} = \sum_{r=0}^{n} C(n,r)B^r = (B+1)^n.$$

Proof of Theorem 2.2.7. In any partition of $\{1, 2, \ldots, n, n+1\}$, the number $n+1$ belongs to a unique block. Apart from $n+1$ itself, this block contains some k other elements, where $0 \le k \le n$. Because the k companions of $n+1$ can be chosen from $\{1, 2, \ldots, n\}$ in $C(n,k)$ ways and the remaining $n-k$ elements can be partitioned into blocks in B_{n-k} ways, the number of partitions in which $n+1$ belongs to a block with k other elements is $C(n,k)B_{n-k}$. Summing over $r = n-k$ yields

$$B_{n+1} = \sum_{r=o}^{n} C(n,n-r)B_r = \sum_{r=0}^{n} C(n,r)B_r.$$

■

Among other things, the Bell numbers enumerate equivalence relations.

2.2.8 Definition. Let S be a set. A binary relation $\sim$ on S is an *equivalence relation* if it satisfies three properties:

1. $x \sim x$ for all $x \in S$;
2. if $x \sim y$, then $y \sim x$;
3. if $x \sim y$, and $y \sim z$, then $x \sim z$.

2.2.9 Theorem. *If $o(S) = n$, then the number of different equivalence relations on S is the nth Bell Number B_n.*

Proof. If $s \in S$, the *equivalence class* to which s belongs is $\{x \in S : s \sim x\}$. Two equivalence classes are either disjoint or identical. In paticular, the different equivalence classes comprise a partition of S. Conversely, any partition of S is the family of equivalence classes for some equivalence relation. Thus, the number of equivalence relations is equal to the number of partitions of S. ■

Turning to other applications, there is a family of problems (somewhat analogous to the four "choosing" problems of Section 1.6) that are traditionally stated

in terms of balls and urns. The general problem involves the question, "In how many different ways can m balls be distributed among n urns?" The answer depends upon how the word "different" is interpreted. It may be, for example, that among the balls are Ping-Pong balls, golf balls, baseballs, and volleyballs. The urns might come in red, white, or blue versions. More formally, we would like to be able to allow for the possibility of equivalence relations on the sets of balls and urns.

For now, we adopt an "all-or-nothing" attitude. Either the balls are all equivalent or all inequivalent and, independently, the urns are all identical or all different. In this context, the words *labeled* and *unlabeled* are useful. If we can't tell the balls apart, we'll say they are unlabeled; if the urns are all different from each other, we'll say they are labeled. (In all cases, we presume that balls and urns can be distinguished from each other!) Another consideration is whether to allow some of the urns to wind up empty. So, at this stage, there are eight variations of the problem.*

Let's begin with the two cases in which the balls are labeled but the urns are not. It really doesn't matter how the balls are labeled as long as the labels suffice to distinguish one ball from another. So, we may as well suppose the balls are labeled with the numbers $1, 2, \ldots, m$.

Variation 1. In how may ways can m labeled balls be distributed among n unlabeled urns if no urn is left empty? Stripping away the colorful terminology of balls and urns, this is just asking in how many ways the set $\{1, 2, \ldots, m\}$ can be partitioned into n blocks. The answer is $S(m, n)$.

2.2.10 Example. In how many ways can four labeled balls be distributed among two unlabeled urns if no urn is left empty? According to Variation 1, the answer the $S(4, 2) = 7$. If the balls are labeled 1, 2, 3, and 4, then the seven possibilities are

$$\{1\}\ \&\ \{2,3,4\};\quad \{2\}\ \&\ \{1,3,4\};\quad \{3\}\ \&\ \{1,2,4\};\quad \{4\}\ \&\ \{1,2,3\};$$
$$\{1,2\}\ \&\ \{3,4\};\quad \{1,3\}\ \&\ \{2,4\}\quad \text{and}\quad \{1,4\}\ \&\ \{2,3\}.$$

(Because the urns are unlabeled, $\{1\}\ \&\ \{2,3,4\}$ is the same as $\{2,3,4\}\ \&\ \{1\}$. Since it is a set, $\{2,3,4\} = \{3,4,2\}$.) □

Variation 2. In how many ways can m labeled balls be distributed among n unlabeled urns? Since it is no longer a requirement that no urn be left empty, this is the same as asking for the number of ways in which $\{1, 2, \ldots, m\}$ can be partitioned into *n or fewer* blocks. The answer is

$$S(m, 1) + S(m, 2) + \cdots + S(m, n).$$

(When $m \leq n$, this sum is the mth Bell number B_m.)

* Since the balls are free to roll around in the urns, the order in which the balls are distributed among the urns doesn't matter.

2.2.11 Example. The number of ways to distribute four labeled balls among two unlabeled urns is $S(4,1) + S(4,2) = 1 + 7 = 8$. In addition to the 7 possibilities listed in Example 2.2.10, we have $\{1,2,3,4\}$ & $\{\}$, the case in which one of the urns winds up empty. (Because the urns are indistinguishable, the question of which urn is left empty does not arise.) □

Turning to the cases in which the balls are labeled 1, 2, . . . , m and the urns are labeled $1, 2, \ldots, n$, each distribution of balls among urns is uniquely described by a function $f \in F_{m,n}$, where $f(i) = j$ is interpreted to mean that the ith ball is assigned to the jth urn.

Variation 3. In how many ways can m labeled balls be distributed among n labeled urns? The answer is just $o(F_{m,n}) = n^m$.

2.2.12 Example. Four labeled balls can be distributed among two labeled urns in $2^4 = 16$ ways. Indeed, now that the urns can be distinguished (maybe one of them is chipped), why not just double the answer from Example 2.2.11? What if there were three labeled balls and three unlabeled urns? Then, by Variation 2, there would be $B_3 = 5$ ways to distribute the balls and $3! \times 5 = 30$, whereas the correct answer for the number of ways to distribute three labeled balls among three labeled urns is $3^3 = 27$. In this case, the four unlabeled solutions

$$\{1\} \text{ \& } \{2,3\} \text{ \& } \{\}; \quad \{2\} \text{ \& } \{1,3\} \text{ \& } \{\}; \quad \{3\} \text{ \& } \{1,2\} \text{ \& } \{\} : \\ \text{and} \quad \{1\} \text{ \& } \{2\} \text{ \& } \{3\}$$

each have six labeled counterparts, while $\{1,2,3\}$ & $\{\}$ & $\{\}$ has only three. □

Variation 4. In how many ways can m labeled balls be distributed among n labeled urns if no urn is left empty? The answer is $n!S(m,n)$, the number of onto functions in $F_{m,n}$.

This time, the obvious shortcut *is* valid. By Variation 1, there are $S(m,n)$ ways to distribute m labeled balls among n unlabeled urns. Once the balls have been distributed, there are $n!$ ways to label the urns. By the fundamental counting principle, the answer we seek is $n!S(m,n)$.

In fact, there is a third approach to Variation 4. While it could not be called a shortcut, it is useful in another way. Let's begin with an example.

2.2.13 Example. In how many ways can five labeled balls be distributed among three labeled urns if no urn is left empty? As an example of Variation 4, the answer is $3!S(5,3)$. But, consider the following alternate approach: Label the balls 1, 2, 3, 4, 5 and the urns 1, 2, 3. As before, we describe a distribution of balls among urns

by means of a function $f \in F_{5,3}$, but this time concentrate on the sequence

$$f = (f(1), f(2), f(3), f(4), f(5)).$$

For our present purposes, it is useful to abbreviate the sequence, writing it in the form

$$f = f(1)f(2)f(3)f(4)f(5).$$

Thus, e.g., $f = 31121$ is the assignment of ball 1 to urn 3, ball 4 to urn 2, and balls 2, 3, and 5 to urn 1. While 31121 may look like a number, we are going to view it as a word. There is a one-to-one correspondence between assignments of balls to urns and five-letter words produced from the alphabet $\{1, 2, 3\}$. Moreover, assignments leaving no urn empty correspond to words that use all three "letters".

Let's examine some possibilities. If all three letters are used, the maximum multiplicity any one letter can have is three, and then only when each of the other two letters occurs exactly once. Just to get warmed up, how many five-letter words use 1 three times and each of 2 and 3 just once? The answer is multinomial coefficient $\binom{5}{3,1,1}$. Similarly, the number of five-letter words that use three 2's, one 1, and one 3 is $\binom{5}{1,3,1}$; and $\binom{5}{1,1,3}$ is the number that use three 3's, one 1, and one 2.

If no "letter" occurs as often as three times, then the only possibility is that one of the letters occurs once and the other two occur twice. Since the letter used only once can be any one of 1, 2, or 3, the number of possibilities of this type is $\binom{5}{1,2,2} + \binom{5}{2,1,2} + \binom{5}{2,2,1}$.

Putting it all together, we obtain the identity

$$\begin{aligned} 3!S(5,3) = &\left[\binom{5}{3,1,1} + \binom{5}{1,3,1} + \binom{5}{1,1,3}\right] \\ &+ \left[\binom{5}{1,2,2} + \binom{5}{2,1,2} + \binom{5}{2,2,1}\right]. \end{aligned}$$

While the two sides of this equation may *look* different, they had better not *be* different. Indeed, $6 \times 25 = 3 \times 20 + 3 \times 30$. □

Example 2.2.13 can be generalized as follows.

2.2.14 Theorem. *If $m \geq n$, then the number of onto functions in $F_{m,n}$ is*

$$n!S(m,n) = \sum \binom{m}{r_1, r_2, \ldots, r_n},$$

where the summation is over all n-part compositions of m, i.e., over those multinomial coefficients having exactly n positive integers in the bottom row.

2.2.15 Example. Apart from (1,1,1,1) and (2,2,2,2), the remaining $2^4 - 2 = 14$ functions in $F_{4,2}$ are onto. To confirm Theorem 2.1.19, observe that $2!S(4,2) = 2 \times 7 = 14$. To confirm Theorem 2.2.14, observe that $\binom{4}{3,1} + \binom{4}{2,2} + \binom{4}{1,3} = 4 + 6 + 4 = 14$. □

The number of ways to distribute m unlabeled balls among n labeled urns $U_1, U_2, \ldots, U_n$ is the number of solutions to the equation

$$u_1 + u_2 + \cdots + u_n = m$$

in positive integers (no empty urns) or nonnegatve integers (empty urns allowed). The number of ways to distribute m unlabeled balls among n unlabeled urns is the number of n-part partitions of m (no empty urns) or the number of partitions of m into at most n parts (empty urns allowed). Details are left to the exercises.

2.2. EXERCISES

1 Confirm

(a) Equation (2.4) when $m = 5$.

(b) Theorem 2.2.2 when $m = 5$.

(c) Corollary 2.2.4 when $m = 5$ and $1 \leq r \leq 5$.

(d) Theorem 2.2.14 when $m = 5$ and $1 \leq n \leq 5$.

2 Confirm that the $m = 4$ case of Corollary 2.2.3 is identical to Equation (1.12). (*Hint*: Fig. 2.1.2.)

3 In the spirit of Exercise 2, explicitly compute the numbers

(a) $a_{r,5} = r!S(5,r)$, $\quad 1 \leq r \leq 5$. **(b)** $a_{r,6}$, $\quad 1 \leq r \leq 6$.

4 Use Stirling's identity (Corollary 2.2.4) to

(a) confirm that $S(6,2) = 31$.

(b) confirm that $S(7,2) = 63$.

(c) compute $S(8,2)$.

(d) prove that $S(m,2) = 2^{m-1} - 1$.

5 Compare and contrast Stirling's identity (Corollary 2.2.4) with

$$(t-1)^m = \sum_{r=0}^{m} (-1)^{m-r} C(m,r) t^r.$$

6 Show that $B_n = \sum_{r=1}^{n} \sum_{t=1}^{r} (-1)^{r+t} C(r,t) t^n / r!$. (*Hint*: B_n is a sum of Stirling numbers.)

7 From Figure 2.1.2, the first eight Bell numbers (starting with B_0) are 1, 1, 2, 5, 15, 52, 203, and 877. Use these data to confirm that $B_7 = C(6,0)B_0 + C(6,1)B_1 + \cdots + C(6,6)B_6$.

8 Denoting the nth Bell number by B_n,

(a) compute B_8. **(b)** show that $B_9 = 21,147$.

9 Explain how the identification of the word pattern number $T(m,n)$ with the Stirling number $S(m,n)$ in Exercise 16(d), Section 2.1, follows from Theorem 2.2.14.

10 How many of the equivalence relations on $\{1,2,\ldots,n\}$ afford exactly k equivalence classes?

11 Confirm Theorem 2.2.14 when

(a) $m = 6$ and $n = 2$. **(b)** $m = 6$ and $n = 3$.

12 Use Exercise 12, Section 2.1, as the basis of a new proof of Corollary 2.2.3.

13 In how many ways can five identical black ceramic Maltese falcons be distributed among the Turnage brothers Bill, Jim, and Robert?

14 Prove that m unlabeled balls can be distributed among n labeled urns in exactly $C(m+n-1,m)$ different ways. (*Hint*: Label the urns $U_1, U_2, \ldots, U_n$. Let u_i be the number of balls that wind up in urn U_i.)

15 Prove that m unlabeled balls can be distributed among n labeled urns, leaving no urn empty, in exactly $C(m-1,n-1)$ different ways.

16 In how many ways can five identical balls be distributed among three unlabeled urns? (*Hint*: Some urn, since they are not labeled it doesn't matter which one, getting all five balls is one way. One urn getting four balls and another getting one is a second way.)

17. In how many ways can five identical grapefruits be distributed among three unlabeled boxes if no box is left empty?

18 Prove that m unlabeled balls can be distributed among n unlabeled urns in $p_1(m) + p_2(m) + \cdots + p_n(m)$ ways, where $p_k(m)$ is the number of k-part partitions of m.

19 If $m \leq n$, show that m unlabeled balls can be distributed among n unlabeled urns in $p(m)$ ways, where $p(m)$ is the number of partitions of m.

20 In how many ways can six balls be distributed among four urns if

(a) the urns are labeled but the balls are not?

(b) the balls are labeled but the urns are not?

(c) both balls and urns are labeled?

(d) neither balls nor urns are labeled?

21 Rework Exercise 20 under the condition that no urn is left empty.

22 In how many ways can 10 theatre tickets be distributed among the Turnage brothers Robert, Jim, and Bill if the tickets

(a) are for specific seats in the auditorium?

(b) are for admission to the auditorium where seating is on a first-come, first-served basis?

23 Given ten unlabeled balls and four unlabeled urns, in how many ways can the balls be distributed among the urns if no urn is left empty?

24 In how many ways can nine balls be distributed among five urns if no urn is left empty and

(a) the balls are labeled but the urns are not.

(b) neither the balls nor the urns are labeled.

(c) the urns are labeled but the balls are not.

(d) both the balls and the urns are labeled.

25 Rework Exercise 24 when empty urns are permitted.

26 Fill in the blanks (with actual numbers, as opposed to names for numbers).

(a) $x^5 = x^{(5)} + \_\_\, x^{(4)} + \_\_\, x^{(3)} + \_\_\, x^{(2)} + \_\_\, x + \_\_$.

(b) $n^5 = P(n,5) + \_\_\, P(n,4) + \_\_\, P(n,3) + \_\_\, P(n,2) + \_\_\, P(n,1)$.

(c) $n^5 = \_\_\, C(n,5) + \_\_\, C(n,4) + \_\_\, C(n,3) + \_\_\, C(n,2) + \_\_\, C(n,1)$.

27 Suppose m houses are to be painted. Assume that x colors are available but that each house is to be uniformly painted just one color. The houses are labeled (by their street addresses) and the colors can be distinguished from each other (so they are labeled too).

(a) Show that the number of ways to paint the m houses using exactly r of the x colors is $S(m,r)x^{(r)}$.

(b) In how many ways can the m houses be painted using m or fewer of the x colors?

(c) Give a combinatorial proof of Theorem 2.2.2.

28 In the Bose–Einstein model of statistical mechanics, each of r identical particles can have any one of k different energy levels.

(a) How many energy *states* can such a system exhibit?

(b) Suppose there are six particles and four energy levels. Assuming all the states are equally likely, what is the probability that all six particles will have the same energy?

29 Suppose $U_1, U_2, \ldots, U_n$ are (labeled) urns and $r_1 + r_2 + \cdots + r_n = m$ is an n-part composition of m. In how many ways can m labeled balls be distributed among the urns so that urn U_k receives exactly r_k balls, $1 \le k \le n$?

30 The number of different (unordered) ways to express 30 as a *sum* of (one or more) integers greater than zero is $p(30) = 5604$.

(a) List the $B_3 = 5$ different (unordered) ways to express 30 as a *product* of (one or more) integers each of which is greater than 1.

(b) Show that there are 203 (unordered) ways to write 30,030 as a product of (one or more) integers greater than 1.

31 Suppose $n = p_1 p_2 \ldots p_r$, where $p_1, p_2, \ldots, p_r$ are r different primes (so n is "square free"). Let $\prod(n)$ be the number of different (unordered) ways to write n as a product of (one or more) integers greater than 1. Prove that $\prod(n) = B_r$, the rth Bell number.

32 Rephrase the astragali problem from Exercise 26, Section 1.6, in terms of balls and urns.

33 Let n be a positive integer and p a (positive) prime that is not a factor of n. Those having some acquaintance with congruences will recognize that $n^{p-1} \equiv 1 \pmod{p}$ is a consequence of Fermat's little theorem (Section 1.7, Exercise 11 (b)). Use this result, along with Stirling's identity, to prove Wilson's theorem: $(p-1)! \equiv -1 \pmod{p}$.

34 In how many ways can 24 students be evenly divided into six "teams"

(a) if the teams are "labeled".

(b) if the teams are "unlabeled".

35 In how many ways can 10 students be divided into three "teams" if each team has at least three students and

(a) the teams are "labeled".

(b) the teams are "unlabeled".

36 Suppose balls 1, 2, 3, 4, and 5 are distributed randomly among three urns. Compute the probability that no urn is left empty if

(a) the urns are unlabeled.

(b) the urns are labeled.

2.3. THE PRINCIPLE OF INCLUSION AND EXCLUSION

A cow has 12 legs, 2 in front, 2 in back, 2 on each side, and 1 in each corner.

— N. J. Rose

Suppose $f : A \to A$ is a function from a set A to itself, i.e., suppose the domain and range of f are equal. If A is the set of real numbers, it is not difficult to find functions like $f(x) = e^x$ that are one-to-one but not onto and functions like

$f(x) = x^3 - x$ that are onto but not one-to-one. This kind of thing cannot, happen if A is finite. Specifically, $f \in F_{n,n}$ is one-to-one if and only if it is onto. (The same thing cannot be said about functions in $F_{m,n}$ when $m \neq n$. There are $P(5,3) = 60$ one-to-one functions in $F_{3,5}$, but $F_{3,5}$ contains no onto functions at all; there are $3!S(5,3) = 150$ onto functions in $F_{5,3}$, but $F_{5,3}$ does not contain a single one-to-one function.)

2.3.1 Definition. A one-to-one function in $F_{n,n}$ is called a *permutation*. The subset of $F_{n,n}$ consisting of the one-to-one (onto) functions is denoted S_n.

Of the n^n functions in $F_{n,n}$, $P(n,n) = n!$ are one-to-one, so $o(S_n) = n!$. (The same conclusion follows by counting the $n!S(n,n) = n!$ onto functions in $F_{n,n}$.) Recognizing the permutations in $F_{n,n}$ is easy. They are the sequences in which no integer occurs twice.

2.3.2 Example. $F_{2,2} = \{(1,1),(1,2),(2,1),(2,2)\}$ and $S_2 = \{(1,2),(2,1)\}$. Of the $3^3 = 27$ functions in $F_{3,3}$, only $3! = 6$ are permutations: $S_3 = \{(1,2,3), (1,3,2),(2,1,3),(2,3,1),(3,1,2),(3,2,1)\}$. □

A *fixed point* of $f \in F_{n,n}$ is an element $i \in \{1,2,\ldots,n\}$ such that $f(i) = i$. Some of the deepest theorems in mathematics involve fixed points. Fixed points of permutations comprise the foundation of Pólya's theory of enumeration (discussed in Chapter 3). For the present, we will focus on permutations that have no fixed points.

2.3.3 Definition. A permutation with no fixed points is called a *derangement*. The number of derangements in S_n is denoted $D(n)$.

There is only one permutation $p \in S_1$, and it is completely defined by $p(1) = 1$. Because 1 is a fixed point of p, there are no derangements in S_1, i.e., $D(1) = 0$. There is one derangement in S_2, namely (2, 1), so $D(2) = 1$. In S_3 (see Example 2.3.2), the derangements are (2, 3, 1) and (3, 1, 2), so $D(3) = 2$. While one can tell at a glance whether a sequence represents a permutation, it usually takes more than a glance to recognize a derangement. Identification of functions with sequences has many advantages, but picking out derangements is not one of them.

The easiest (and most illuminating) way to evaluate $D(n)$ involves a new idea. Let's begin by recalling our discussion of the second counting principle: If A and B are disjoint, then $o(A \cup B) = o(A) + o(B)$. If A and B are not disjoint, then $o(A \cup B) < o(A) + o(B)$, because $o(A) + o(B)$ counts every element of $A \cap B$ twice. (See Fig. 2.3.1.) Compensating for this double counting yields the formula

$$o(A \cup B) = o(A) + o(B) - o(A \cap B). \tag{2.11}$$

What if there are three sets? Then

$$\begin{aligned} o(A \cup B \cup C) &= o(A \cup [B \cup C]) \\ &= o(A) + o(B \cup C) - o(A \cap [B \cup C]). \end{aligned}$$

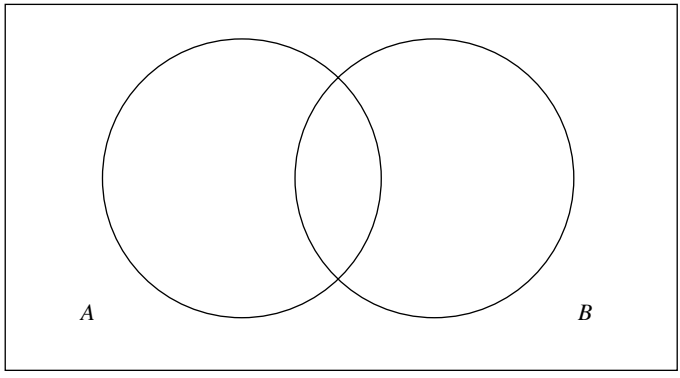


Figure 2.3.1

Applying Equation (2.11) to $o(B \cup C)$ gives

$$o(A \cup B \cup C) = o(A) + [o(B) + o(C) - o(B \cap C)] - o(A \cap [B \cup C]). \tag{2.12}$$

Because $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, we can apply Equation (2.11) again to obtain

$$o(A \cap [B \cup C]) = o(A \cap B) + o(A \cap C) - o(A \cap B \cap C). \tag{2.13}$$

Finally, a combination of Equations (2.12) and (2.13) produces

$$\begin{aligned} o(A \cup B \cup C) = {} & [o(A) + o(B) + o(C)] - [o(A \cap B) + o(A \cap C) + o(B \cap C)] \\ & + o(A \cap B \cap C). \end{aligned} \tag{2.14}$$

Adding back $o(A \cap B \cap C)$ is, perhaps, the most interesting part of Equation (2.14). It seems the subtracted term *over* compensates for elements that belong to all three sets. An element of $A \cap B \cap C$ is counted seven times in Equation (2.14), the first three times with a plus sign, then three time with a minus sign, and then once more with a plus. (See Fig 2.3.2.)

2.3.4 Example. If $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$, and $C = \{2, 4, 6, 7\}$, then $A \cup B \cup C = \{1, 2, 3, 4, 5, 6, 7\}$, a set of seven elements. Let's see what Equation (2.14) produces. Because $o(A) = o(B) = o(C) = 4$,

$$o(A) + o(B) + o(C) = 12.$$

In this case, it just so happens that $o(A \cap B) = o(A \cap C) = o(B \cap C) = 2$, so

$$o(A \cap B) + o(A \cap C) + o(B \cap C) = 6.$$

Finally, $A \cap B \cap C = \{4\}$, so $o(A \cap B \cap C) = 1$. Substituting these values into Equation (2.14) yields $o(A \cup B \cup C) = 12 - 6 + 1 = 7$.

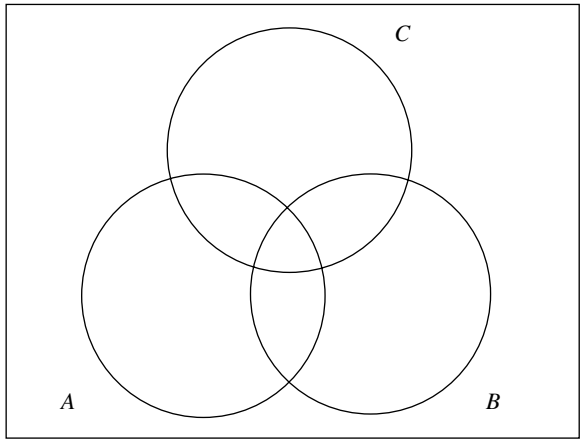


Figure 2.3.2

Don't misunderstand. No one is suggesting that Equation (2.14) is the easiest way to solve *this* problem. The point of the example is merely to confirm that Equation (2.14) generates the correct solution! □

Let's skip over four sets and go directly to the general case.

2.3.5 Principle of Inclusion and Exclusion (PIE). If $A_1, A_2 \ldots, A_n$ are finite sets, the cardinality of their union is

$$o\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{r=1}^{n} (-1)^{r+1} N_r, \tag{2.15}$$

where

$$N_r = \sum_{f \in Q_{r,n}} o\left(\bigcap_{i=1}^{r} A_{f(i)}\right). \tag{2.16}$$

Because $f \in Q_{r,n}$ if and only if f is a strictly increasing function, N_r is the sum of the cardinalities of the intersections of the sets taken r at a time. That is,

$$N_1 = \sum_{i=1}^{n} o(A_i), \qquad N_2 = \sum_{\substack{i,j=1 \\ i<j}}^{n} o(A_i \cap A_j), \qquad N_3 = \sum_{\substack{i,j,k=1 \\ i<j<k}}^{n} o(A_i \cap A_j \cap A_k),$$

and so on. Written out, Equations (2.15)–(2.16) look like this:

$$o(A_1 \cup \cdots \cup A_n) = \sum_{i} o(A_i) - \sum_{i<j} o(A_i \cap A_j) + \sum_{i<j<k} o(A_i \cap A_j \cap A_k) - \cdots.$$

Proof. Let x be a fixed but arbitrary element of $A_i \cup A_2 \cup \cdots \cup A_n$. Then x belongs to some k of the n sets. Without loss of generality, we may assume that x belongs to the *first* k sets, i.e., $x \in A_i$, $1 \le i \le k$, and $x \notin A_i$, $k < i \le n$. Let's compute the contribution of x to N_r. For any $f \in Q_{r,n}$, $x \in \cap_{i=1}^{r} A_{f(i)}$ if and only if $f(r) \le k$ if and only if $f \in Q_{r,k}$. Hence, the contribution of x to N_r is $o(Q_{r,k}) = C(k,r)$, $1 \le r \le k$. So, the contribution of x to the right-hand side of Equation (2.15) is

$$\begin{aligned}\sum_{r=1}^{k}(-1)^{r+1}C(k,r) &= 1 - \sum_{r=0}^{k}(-1)^{r}C(k,r)\\ &= 1\end{aligned}$$

(because $\sum_{r=0}^{k}(-1)^{r}C(k,r) = [-1+1]^{k} = 0$). In other words, the right-hand side of Equation (2.15) counts every element of the union exactly once. ■

It may seem hard to believe that PIE could ever be *useful*. In fact, it is exactly the right tool for counting problems like the one in Example 2.3.4, where, for $1 \le r \le n$, "it just so happens" that

$$o\left(\bigcap_{i=1}^{r} A_{f(i)}\right)$$

is the same for all $f \in Q_{r,n}$. Let's illustrate with the derangement numbers. If $A_i = \{p \in S_n : p(i) = i\}$, $1 \le i \le n$, then $A_1 \cup A_2 \cup \cdots \cup A_n$ is the set of permutations having at least one fixed print, so

$$D(n) = n! - o(A_1 \cup A_2 \cup \cdots \cup A_n).$$

Using the Principle of Inclusion and Exclusion,

$$D(n) = n! - \sum_{r=1}^{n}(-1)^{r+1}N_r. \tag{2.17}$$

To evaluate N_r on the right-hand side of Equation (2.17), let $f \in Q_{r,n}$. Then $p \in A_{f(1)} \cap A_{f(2)} \cap \cdots \cap A_{f(r)}$ if and only if the numbers $f(1), f(2) \ldots, f(r)$ are all fixed points of p. Because there are no restrictions on how p might permute the remaining $n - r$ numbers among themselves, there are exactly $(n-r)!$ permutations $p \in S_n$ that fix $f(i)$, $1 \le i \le r$, i.e.,

$$o(A_{f(1)} \cap A_{f(2)} \cap \cdots \cap A_{f(r)}) = (n-r)!,$$

for all $f \in Q_{r,n}$. It follows that $N_r = (n-r)!C(n,r) = n!/r!$. Thus, from Equation (2.17),

$$\begin{aligned} D(n) &= n! - \sum_{r=1}^{n} \frac{(-1)^{r+1} n!}{r!} \\ &= n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \cdots + \frac{(-1)^n n!}{n!} \\ &= n!\left[\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right]. \end{aligned} \tag{2.18}$$

Recall that the power series expansion

$$e^x = \sum_{n \geq 0} \frac{x^n}{n!}$$

is absolutely convergent for all x. Setting $x = -1$, we obtain the alternating series

$$\frac{1}{e} = \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots.$$

By the alternating-series test, the error in the estimate

$$\frac{1}{e} \doteq \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}$$

is at most $1/(n+1)!$. (The notation "$\doteq$" means "approximately equal".) It follows that the error in the estimate

$$D(n) \doteq \frac{n!}{e} \tag{2.19}$$

is at most $1/(n+1)$, which is enough to prove the following.

2.3.6 Theorem. *The nth derangement number, $D(n)$, is the integer closest to $n!/e$.*

2.3.7 Example. From Equation (2.18),

$$\begin{aligned} D(4) &= 4!\left(1 - 1 + \tfrac{1}{2} - \tfrac{1}{6} + \tfrac{1}{24}\right) \\ &= 24 - 24 + 12 - 4 + 1 \\ &= 9, \end{aligned}$$

whereas $4!/e \doteq 8.8291$. Similarly,

$$\begin{aligned} D(5) &= 5!\left(1 - 1 + \tfrac{1}{2} - \tfrac{1}{6} + \tfrac{1}{24} - \tfrac{1}{120}\right) \\ &= 120 - 120 + 60 - 20 + 5 - 1 \\ &= 44, \end{aligned}$$

while $5!/e \doteq 44.1455$. (It turns out that $D(n) > n!/e$ if n is even and $D(n) < n!/e$ if n is odd.) □

How many permutations $p \in S_n$ have exactly k fixed points? This is a job for the fundamental counting principle. There are $C(n,k)$ ways to choose the numbers to be fixed and $D(n-k)$ ways to derange the remaining $n-k$ "points". So, among the $n!$ permutations of S_n, $C(n,k) \times D(n-k)$ have exactly k fixed points.

Denote by $P(k)$ the fraction of permutations in S_n that have exactly k fixed points.* If we assume that n is enough larger than k for the estimate $D(n-k) \doteq (n-k)!/e$ to be valid, then

$$P(k) = \frac{C(n,k)D(n-k)}{n!} \doteq \frac{1}{k!e}. \tag{2.20}$$

It is proved in Section 3.3 that the *average* of the numbers of fixed points of the permutations in S_n is 1. Setting $k = 1$ in Equation (2.20) shows that the fraction of permutations in S_n that have exactly 1 fixed point is $P(1) \doteq 1/e$.

2.3.8 Example. Let $F(p)$ be the number of fixed points of $p \in S_3 = \{(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)\}$. Then $F(1,2,3) = 3$, $F(1,3,2) = F(2,1,3) = F(3,2,1) = 1$, and $F(2,3,1) = F(3,1,2) = 0$. From these data, it is easy to see that the average number of fixed points is $[3+1+1+1+0+0]/6 = 1$, and easy to confirm that the fraction of permutations in S_3 having exactly one fixed point is $C(3,1)D(2)/6 = \frac{3}{6} = 0.5$. (The estimate $0.5 \doteq 1/e = 0.3678794\ldots$ afforded by Equation (2.20) when $n = 3$ and $k = 1$ is evidently not very good.)

It follows from Theorem 2.3.6 that $D(9) = 133,496$. From Equation (2.20), the fraction of permutations in S_{10} having exactly one fixed point is $C(10,1)D(9)/10! = D(9)/9! \doteq 0.3678792$, which compares more favorably with $1/e$. □

Let's see how the Principle of Inclusion and Exclusion might be used to produce new information about Stirling numbers of the second kind. Let $A_s = \{f \in F_{m,n} : f^{-1}(s) = \varnothing\}$, $1 \le s \le n$. Observe that no $f \in A_s$ can be onto. In fact, $g \in F_{m,n}$ is onto if and only if

$$g \notin A_1 \cup A_2 \cup \cdots \cup A_n.$$

* Then $P(k)$ is the probability that a randomly chosen permutation in S_n has exactly k fixed points.

Therefore,

$$\begin{aligned} n!S(m,n) &= n^m - o(A_1 \cup A_2 \cup \cdots \cup A_n) \\ &= n^m - \sum_i o(A_i) + \sum_{i<j} o(A_i \cap A_j) \\ &\quad - \sum_{i<j<k} o(A_i \cap A_j \cap A_k) + \cdots . \end{aligned} \tag{2.21}$$

Now, A_n is the set of functions in $F_{m,n}$ that do not map anything to n. In fact, it would be very easy to confuse A_n with $F_{m,n-1}$. Certainly, $o(A_n) = (n-1)^m$. But, the number of functions in $F_{m,n}$ that map nothing to n is the same as the number of functions that map nothing to 1 or nothing to 2. In other words, $o(A_i) = (n-1)^m$, $1 \le i \le n$. Similarly, there is a one-to-one correspondence between the functions in $A_n \cap A_{n-1}$ and $F_{m,n-2}$. Thus, $o(A_n \cap A_{n-1}) = (n-2)^m$. Hence, $o(A_i \cap A_j) = (n-2)^m$, $1 \le i < j \le n$. Similarly, $o(A_i \cap A_j \cap A_k) = (n-3)^m$, $1 \le i < j < k \le n$, and so on. Substituting these values into Equation (2.21) yields

$$\begin{aligned} n!S(m,n) &= n^m - n(n-1)^m + C(n,2)(n-2)^m - C(n,3)(n-3)^m + \cdots \\ &= \sum_{s=0}^{n-1} (-1)^s C(n,s)(n-s)^m . \end{aligned} \tag{2.22}$$

Because $C(n, n-t) = C(n,t)$, replacing s with $n-t$ in Equation (2.22) yields

$$n!S(m,n) = \sum_{t=1}^{n} (-1)^{n-t} C(n,t) t^m .$$

It seems we have done nothing more than rediscover Stirling's identity (Corollary 2.2.4)!

Let's try something else, maybe an example from the intersection of combinatorics and number theory.

2.3.9 Definition. Let n be a positive integer. The *Euler totient function* $\varphi(n)$ is the number of positive integers $m \le n$ such that m and n are relatively prime.

2.3.10 Example. The positive integers less than 9 and relatively prime to 9 are 1, 2, 4, 5, 7, and 8, so $\varphi(9) = 6$. The first few values of $\varphi(n)$ appear in Fig. 2.3.3. □

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Figure 2.3.3. The Euler totient function.

2.3.11 Theorem. *Suppose* $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, *where* $r_i > 0$, $1 \le i \le k$, *and* $p_1, p_2, \ldots, p_k$ *are distinct primes. Then*

$$\varphi(n) = n \prod_{i=1}^{k} \frac{p_i - 1}{p_i}.$$

Proof. Let $S = \{1, 2, \ldots, n\}$. Define

$$A_i = \left\{ p_i, 2p_i, 3p_i, \ldots, \left(\frac{n}{p_i}\right) p_i \right\}, \qquad 1 \le i \le k.$$

Then A_i is the subset of S consisting of the multiples of p_i. Moreover (just count its elements), $o(A_i) = n/p_i$. If $i \ne j$, then $A_i \cap A_j$ consists of those elements of S that are multiples of p_i and p_j and, therefore, of $p_i p_j$. So,

$$A_i \cap A_j = \{p_i p_j, 2p_i p_j, 3p_i p_j, \ldots, \left(\frac{n}{p_i p_j}\right) p_i p_j\}.$$

In particular, for $i < j$, $o(A_i \cap A_j) = n/(p_i p_j)$. If $i < j < k$, then $o(A_i \cap A_j \cap A_k) = n/(p_i p_j p_k)$, and so on.

If $1 \le m \le n$ (i.e., if $m \in S$), then the greatest common divisor of m and n is greater than 1 if and only if m and n have a common prime divisor if and only if $m \in A_1 \cup A_2 \cup \cdots \cup A_k$. So,

$$\begin{aligned}
\varphi(n) &= n - o(A_1 \cup A_2 \cup \cdots \cup A_k) \\
&= n - \sum_i o(A_i) + \sum_{i<j} o(A_i \cap A_j) - \sum_{i<j<k} o(A_i \cap A_j \cap A_k) + \cdots \\
&= n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \cdots\right) + \left(\frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \cdots\right) - \left(\frac{n}{p_1 p_2 p_3} + \cdots\right) + \cdots \\
&= \frac{n}{p_1 p_2 \cdots p_k} (E_k - E_{k-1} + E_{k-2} - \cdots + [-1]^k E_0),
\end{aligned}$$

where $E_t = E_t(p_1, p_2, \ldots, p_k)$ is the tth elementary symmetric function, $1 \le t \le k$. Because $(p_1 - 1)(p_2 - 1) \cdots (p_k - 1) = E_k - E_{k-1} + E_{k-2} - \cdots + [-1]^k E_0$,

$$\varphi(n) = \frac{n}{p_1 p_2 \cdots p_k} (p_1 - 1)(p_2 - 1) \cdots (p_k - 1). \qquad \blacksquare$$

2.3.12 Example. A favorite number of the Babylonians was $60 = 2^2 \times 3 \times 5$. By Theorem 2.3.11,

$$\begin{aligned}
\varphi(60) &= 60 \left(\frac{2-1}{2}\right)\left(\frac{3-1}{3}\right)\left(\frac{5-1}{5}\right) \\
&= 16.
\end{aligned}$$

The 16 numbers less than 60 and relatively prime to 60 are 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, and 59. $\square$

2.3. EXERCISES

1 List all 24 elements of S_4 and underline the nine derangements.

2 Tabulate the numbers of permutations in S_5 that have exactly k fixed points, $0 \leq k \leq 5$. (*Hint*: Be sure the numbers add up to 5!.)

3 How many elements of S_6 have exactly

(a) two fixed points? **(b)** three fixed points?

(c) four fixed points? **(d)** five fixed points?

4 If $p \in S_n$, then $p^{-1} \in S_n$ is the unique permutation satisfying $p(p^{-1}(x)) = x = p^{-1}(p(x))$ for all $x \in \{1, 2, \ldots, n\}$. Prove that p and p^{-1} have the same number of fixed points.

5 It would seem to follow from Exercise 4 that derangements come in pairs, so that $D(n)$ should always be even. Find the fallacy in this argument.

6 Show that $D(10) = 1,334,961$.

7 Compute the number of permutations in S_{15} that have exactly five fixed points and compare it to the approximation $15!/5!e$ obtained by multiplying both sides of Equation (2.20) by $n!$.

8 Use $A \cup B \cup C \cup D = A \cup (B \cup C \cup D)$ along with Equations (2.11) and (2.14) to give an independent proof of the $n = 4$ case of the Principle of Inclusion and Exclusion.

9 Among the math courses offered by Sunrise High School are algebra, geometry, and trigonometry. To be in the Math Club, a student must have completed (at least) one of these three courses. The Math Club has 56 student members, altogether. Of these, 28 have taken algebra and 28 have taken geometry, 11 have taken both algebra and geometry, 12 have taken both algebra and trig, and 13 have taken both geometry and trig. If 5 of the students have taken all three courses, how many have taken trigonometry?

(a) Solve the problem using Venn diagrams.

(b) Solve the problem using the Principle of Inclusion and Exclusion.

(c) Which is easier?

10 Use Stirling's identity (circa Equation (2.22)) to

(a) compute $S(12, 3)$.

(b) prove that $2S(m + 1, 3) = 3^m - 2^{m+1} + 1$, $m \geq 0$.

(c) prove that $2S(m + 1, 3) = \det \begin{pmatrix} 1^0 & 1^1 & 1^m \\ 2^0 & 2^1 & 2^m \\ 3^0 & 3^1 & 3^m \end{pmatrix}$.

(d) prove or disprove that $3!S(m+1,4) = \det \begin{pmatrix} 1^0 & 1^1 & 1^2 & 1^m \\ 2^0 & 2^1 & 2^2 & 2^m \\ 3^0 & 3^1 & 3^2 & 3^m \\ 4^0 & 4^1 & 4^2 & 4^m \end{pmatrix}$

11 Show that exactly 24,024 of the 40,320 permutations in S_8 derange the even integers 2, 4, 6, and 8.

12 Prove that $n! = 1 + \sum_{k=2}^{n} C(n,k)D(k)$.

13 Prove that

(a) $D(n) = (n-1)[D(n-1) + D(n-2)]$, $n \geq 3$.

(b) $D(n) = nD(n-1) + (-1)^n$, $n \geq 2$.

(c) $D(n+1)$ is even if and only if $D(n)$ is odd.

14 Starting with $D(1)$, the sequence of derangement numbers is 0, 1, 2, 9, 44, ... Continue the sequence through $D(10)$ using

(a) the recurrence from Exercise 13(a).

(b) the recurrence from Exercise 13(b).

(c) Theorem 2.3.6.

[*Hint*: Be mindful of Exercise 13(c).]

15 How many integer solutions of $a+b+c+d = 30$ satisfy the *boundary* condition that

(a) a, b, c, and d are nonnegative?

(b) a, b, c, and d are not less than 4.

(c) a, b, and c are nonnegative and $d \geq 11$.

(d) $0 \leq a, b, c, d \leq 10$.

16 In Exercise 9(b), Section 1.6, one finds that there are 2925 integer solutions to $a+b+c+d = 30$ that satisfy $3 \leq a$, $2 \leq b$, $1 \leq c$, and $0 \leq d$. Use the Principle of Inclusion and Exclusion to find the number of integer solutions of $a+b+c+d = 30$ that satisfy $3 \leq a \leq 5$, $2 \leq b \leq 6$, $1 \leq c \leq 7$, and $0 \leq d \leq 8$. (*Hint*: Among the 2925 solutions from Section 1.6, let A_1 be the set consisting of those that satisfy, not $a \geq 3$, but $a \geq 6$; A_2 the solutions that satisfy $b \geq 7$; A_3 the solutions that satisfy $c \geq 8$; and A_4 the solutions that satisfy $d \geq 9$.)

17 Find the number of compositions of 12 that have three parts none of which is larger than 5

(a) by listing them.

(b) using the ideas suggested in Exercise 16. (Show your work!)

(c) by computing the coefficient of x^{12} in $(x + x^2 + x^3 + x^4 + x^5)^3$. (Show your work!)

18 There are four primes in the range $1 < p < 10$. How many are there in the range $10 < p < 100$? To find out, let $S = \{n : 10 < n < 100\}$. If $n \in S$ is composite, then n has a prime divisor less than $\sqrt{100} = 10$. So, $n \in A_2 \cup A_3 \cup A_5 \cup A_7$, where $A_p = \{n \in S : p \text{ is a factor of } n\}$. Thus, the number of primes p satisfying $10 < p < 100$ is $o(S) - o(A_2 \cup A_3 \cup A_5 \cup A_7)$. Use the Principle of Inclusion and Exclusion to evaluate this difference.

19 The positive integer n is "square free" if it is not (exactly) divisible by the square of any prime. Show that there are (exactly) 61 square-free positive integers less than 100.

20 Suppose the positive integer divisors of n (all of them, including 1 and n) are $d_1, d_2, \ldots, d_r$. It is shown in Section 4.4 (Exercise 21) that $n = \varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_r)$. Confirm this fact when

(a) $n = 6$. **(b)** $n = 12$.

(c) $n = 15$. **(d)** $n = 60$.

21 Show that

(a) $\varphi(p) = p - 1$ if p is a prime.

(b) $\varphi(2^n) = 2^{n-1}$.

(c) $\varphi(60) = \varphi(3)\varphi(20)$, $\varphi(60) = \varphi(5)\varphi(12)$, and $\varphi(60) = \varphi(4)\varphi(15)$, but $\varphi(60) \neq \varphi(6)\varphi(10)$.

(d) $\varphi(mn) = \varphi(m)\varphi(n)$ whenever m and n are relatively prime.

22 Euler proved that $n^{\varphi(m)} - 1$ is an integer multiple of m whenever m and n are relatively prime. Confirm Euler's theorem when

(a) $n = 4$ and $m = 3$.

(b) $n = 3$ and $m = 4$.

(c) $n = 35$ and $m = 6$.

23 Explain why Euler's theorem (Exercise 22) is a generalization of Fermat's "little theorem" (Exercise 11, Section 1.7).

24 An *inversion* of the permutation $p \in S_n$ is an ordered pair (i, j) such that $i < j$ but $p(i) > p(j)$. If $q = (4, 3, 1, 2, 5)$, then $q(1) = 4 > 3 = q(2)$, so (1,2) is an inversion of q; its other inversions of q are (1,3), (1,4), (2,3), and (2,4), so $\text{inv}(q) = 5$, where $\text{inv}(p)$ denotes the *number of inversions* of p.

(a) If $p = (i_1, i_2, \ldots, i_n) \in S_n$, define $p^{\#} = (i_n, i_{n-1}, \ldots, i_1)$. Show that $\text{inv}(p) + \text{inv}(p^{\#}) = C(n, 2)$.

(b) Prove that the average number of inversions over $p \in S_n$ is $\frac{1}{2}C(n, 2)$.

25 Let $r(n,k)$ be the number of permutations in S_n that have exactly k inversions (see Exercise 24). Prove that

(a) $r(n,k) = r(n, C(n,2) - k)$.

(b) $r(n+1,k) = r(n,k) + r(n,k-1) + \cdots + r(n,k-n)$.

26 Let F_n be the number of permutations $p \in S_n$ that satisfy $|i - p(i)| \leq 1$, $1 \leq i \leq n$. Prove that F_n is the nth Fibonacci number, $n \geq 1$. (The Fibonacci sequence is defined by $F_0 = F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$, $n \geq 1$.)

27 Imagine 15 numbered pool balls tumbled, one at a time, onto a pool table in some random order while a score keeper records an "event" every time the *ordinal* number of a ball equals its *nominal* number (i.e., whenever the kth ball to hit the table happens to be the one decorated with number k). The total (*cardinal*) number of events is the score, something between 0 and 15, inclusive. Compute the probability that the score is

(a) 0. **(b)** 1. **(c)** 2.

(d) 3. **(e)** more than 3.

28 Of the 635 billion bridge hands (Example 1.2.5), how many contain at least one void? (*Hint*: A void is a missing suit. Let A_1 be the set of 13-card bridge hands that contain no spades, A_2 the hands with a heart void, etc.)

29 Write an algorithm/program to generate and list, in dictionary order, all $m!$ permutations in S_m.

30 Suppose $n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$, where $r_i > 0$, $1 \leq i \leq k$, and $p_1, p_2, \ldots, p_k$ are distinct primes. Prove that

$$\varphi(n) = \prod_{i=1}^{k} p_i^{r_1 - 1}(p_i - 1).$$

2.4. DISJOINT CYCLES

One picture is worth a thousand words.

— Fred R. Barnard

Of the many differences between the kinds of functions one studies in calculus (e.g., continuous functions, differentiable functions, etc.) and the kinds we have been looking at here (e.g., derangements), one of the most striking concerns pictures. There haven't been any pictures of these *finite functions*.

The *graph* of function f is a picture of the set $G(f) = \{(x, f(x)) : x \in D\}$. The value of a calculus-type graph lies in the qualitative information that it reveals at a

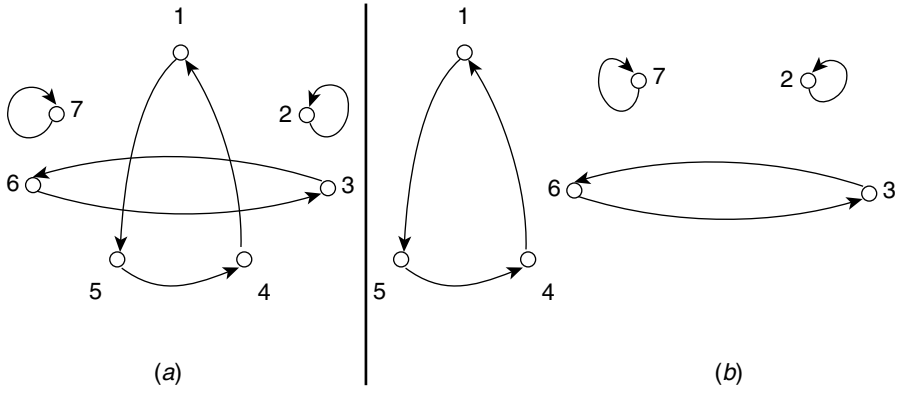


Figure 2.4.1. "X-ray images" of $p_1 = (5, 2, 6, 1, 4, 3, 7)$.

glance. But, consider the permutation $p_1 = (5, 2, 6, 1, 4, 3, 7) \in S_7$. A picture of $G(p_1) = \{(1, 5), (2, 2), (3, 6), (4, 1), (5, 4), (6, 3), (7, 7)\}$ would consist of seven points scattered in the first quadrant of the xy-plane. Such a graph is not without value. It would, e.g., make it easy to identify the fixed points of p_1 lying, as they do, on the line $y = x$. But, such a graph just does not have the same impact, say, as a sweeping parabolic illustration of $f(x) = x^2$. On the other hand, why should it? Calculus-type pictures are crafted to illustrate calculus-type notions. If we are going to draw pictures, they should be designed to reveal combinatorial notions.

One possibility is the geometric diagram in Fig. 2.4.1*a*, where the numbers from the domain/range of p_1 are represented by dots and the assignment $p_1(i) = j$ is illustrated by a directed arc. Reminiscent of an X-ray image, this diagram reveals some unexpected internal structure. The seven numbers are clearly arranged in four disjoint *cycles*, perhaps better illustrated in Fig. 2.4.1*b*. The *lengths* of these cycles are 3, 2, 1 and 1. The cycles of length 1 have a clear interpretation. They represent the fixed points of p_1. The significance of the larger cycles will become more apparent as we proceed.

Let $p_2 = (6, 5, 1, 3, 7, 4, 2) \in S_7$. As a sequence, p_2 looks, qualitatively at least, just like p_1. However (see Fig. 2.4.2), its cycle structure is quite different. (Before going on, check to be sure that you understand how the picture in Fig. 2.4.2 arises from the permutation p_2.)

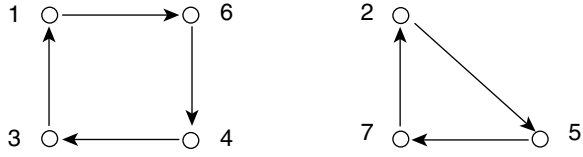


Figure 2.4.2. Diagram of $p_2 = (6, 5, 1, 3, 7, 4, 2)$.

Cycle structure turns out to be as important to the theory of permutations as the *fundamental theorem of arithmetic*[*] is to the theory of numbers. When a permutation is expressed as a sequence, however, this structure is completely hidden. What's needed is a notation, specific to permutations, that *illuminates* cycle structure.

Consider the "4-cycle" of p_2 (Fig. 2.4.2), the one that cycles from 1 to 6 to 4 to 3 and back to 1. One way to represent it is "(1643)", where the numbers 1, 6, 4, and 3 occur in the same order that they appear in the cycle but with the understanding that, when 3 is encountered at the end, the thing to do is cycle back to 1 at the beginning. This strategy of *cycling back* compensates for the fact that while the cycle has no beginning and no end, (1643) has both.

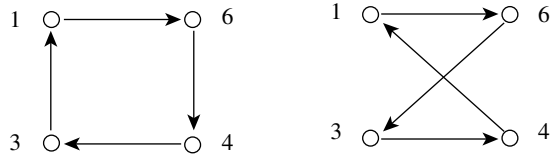
Because each of them represents the same cycle of p_2, let's agree to regard (1643), (6431), (4316), and (3164) as *equivalent*. Observe that, while they contain the same four integers, (1643) and (1634) are *not* equivalent. They do not "cycle" the numbers in the same order. (See Fig. 2.4.3.) Similarly, the other cycle of p_2 can be written in any one of the three equivalent ways (257), (572), or (725), but not as (275).

Once we have our hands on the inequivalent cycles, it only remains to put them together—literally. The *disjoint cycle notation* for p_2 is obtained by juxtaposing its cycles in either order. So, e.g., we may write $p_2 = (1643)(257)$ or $p_2 = (725)(3164)$. Notice that there are many different-*looking* ways to express p_2 in this new notation. How many? Since there are four (equivalent) ways to write the 4-cycle and three ways to write the 3-cycle, and since either cycle can be written first, there must be $4 \times 3 \times 2 = 24$ ways to express p_2 in disjoint cycle notation.

If $q = (16)(45)(237) \in S_7$, then $q(1) = 6$, $q(2) = 3$, $q(3) = 7$, $q(4) = 5$, $q(5) = 4$, $q(6) = 1$, and $q(7) = 2$. In sequence notation, $q = (6, 3, 7, 5, 4, 1, 2)$. (Disregarding sequence notation, it would surely be easier to organize this information as $q(1) = 6$ & $q(6) = 1$; $q(4) = 5$ & $q(5) = 4$; and $q(2) = 3$, $q(3) = 7$, & $q(7) = 2$.)

A formal definition of cycle structure depends on the following technical result.

2.4.1 Lemma. *Let $p \in S_m$ and $x \in \{1, 2, \ldots, m\}$. Consider the sequence defined recursively by $x_1 = x$ and $x_{n+1} = p(x_n)$, $n \geq 1$. If k is the smallest positive integer such that $x_{k+1} \in \{x_1, x_2, \ldots, x_k\}$, then $x_{k+1} = p(x_k) = x_1$.*



(1643) (1634)

Figure 2.4.3

[*] Every integer greater than 1 can be factored uniquely as a product of primes.

Proof. If $k = 1$, then x_1 is a fixed point of p, and the proof is complete. If $p(x_k) = x_i$, where $k \geq i > 1$, then $p(x_k) = p(x_{i-1})$ and, because p is one-to-one, $x_k = x_{i-1}$, contradicting the minimality of k. ■

Because $x_{k+1} = x_1$, $x_{k+2} = p(x_{k+1}) = p(x_1) = x_2$. Similarly, $x_{k+3} = x_3$, $x_{k+4} = x_4$, and so on. The sequence $x_1, x_2, \ldots$ is cyclic with period k. The numbers in the sequence just cycle through $x_1, x_2, \ldots, x_k$ over and over again. If $p = p_2$ and $x = 7$, then (see Fig. 2.4.2) the sequence is

$$7, 2, 5, 7, 2, 5, 7, 2, 5, 7, \ldots$$

If $p = p_2$ and $x = 4$, the sequence is

$$4, 3, 1, 6, 4, 3, 1, 6, 4, \ldots$$

2.4.2 Definition. Suppose $p, q \in S_m$ and $x \in \{1, 2, \ldots, m\}$. Let $x_1 = x$ and $x_{n+1} = p(x_n)$, $n \geq 1$. If k is the smallest positive integer such that $x_{k+1} = x_1$, then the *cycle* of p containing x is

$$C_p(x) = (x_1 x_2 \cdots x_k). \tag{2.23}$$

The *length* of $C_p(x)$ is k, and $C_p(x)$ is sometimes called a *k-cycle*. If $i + 1 = j$, or if $i = k$ and $j = 1$, the number x_j *follows* x_i in $C_p(x)$. If v follows u in $C_p(x)$, if and only if v follows u in $C_q(y)$, $1 \leq u, v \leq m$, then the cycles $C_p(x)$ and $C_q(y)$ are *equivalent*.

Evidently, $C_p(x)$ and $C_q(y)$ are equivalent if and only if they have the same length and contain the same integers in the same (cyclical) order.

2.4.3 Example. Suppose $p = (16)(24)(357)$ and $q = (124)(357)(6)$. Then $C_p(3) = (357)$ is equivalent to $C_p(7) = (735)$. While $C_p(7)$ is also equivalent to $C_q(3) = (357)$, neither is equivalent to (375) nor to $C_q(4) = (412)$. □

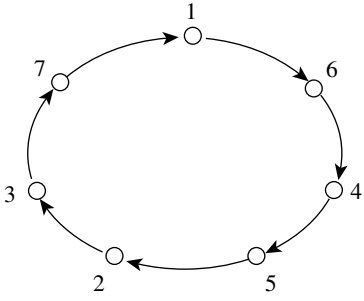
Let $p \in S_m$ and $x \in \{1, 2, \ldots, m\}$. Suppose $y \in C_p(x) = (x_1 x_2 \cdots x_k)$, i.e., $y = x_i$ for some $i \leq k$. Then

$$C_p(y) = (x_i x_{i+1} \cdots x_k x_1 x_2 \cdots x_{i-1}) \tag{2.24}$$

is equivalent to $C_p(x)$. Indeed, $C_p(x_1)$, $C_p(x_2), \ldots,$ and $C_p(x_k)$ are all equivalent to each other and they are the only cycles that are equivalent to $C_p(x)$. Two conclusions follow from this observation.

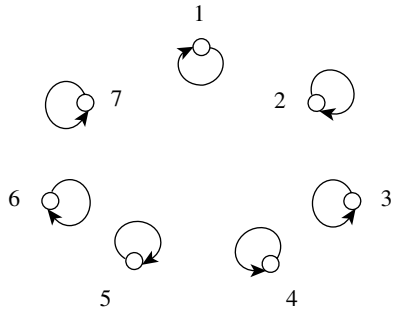
2.4.4 Lemma. *Suppose p and q are permutations in S_m. If $x, y \in \{1, 2, \ldots, m\}$, then*

(a) *either $C_p(x)$ and $C_p(y)$ are disjoint or they are equivalent;*
(b) *either $C_p(x)$ and $C_q(x)$ are identical or they are inequivalent.*



$p_3 = (1645237)$

Figure 2.4.4



$p_4 = (1)\,(2)\,(3)\,(4)\,(5)\,(6)\,(7)$

Figure 2.4.5

2.4.5 Definition. Suppose $p \in S_m$. If $C_p(x)$, $C_p(y), \ldots,$ and $C_p(z)$ are the inequivalent cycles of p, then its *disjoint cycle factorization* is $p = C_p(x)C_p(y)\cdots C_p(z)$.

2.4.6 Example. The disjoint cycle factorization of

$$\begin{aligned} p_1 &= (5,2,6,1,4,3,7) \quad \text{is} \quad (154)(2)(36)(7);\\ p_2 &= (6,5,1,3,7,4,2) \quad \text{is} \quad (1643)(257);\\ p_3 &= (6,3,7,5,2,4,1) \quad \text{is} \quad (1645237);\\ p_3^{-1} &= (7,5,2,6,4,1,3) \quad \text{is} \quad (1732546);\\ p_4 &= (1,2,3,4,5,6,7) \quad \text{is} \quad (1)(2)(3)(4)(5)(6)(7). \end{aligned}$$

Diagrams illustrating p_3 and p_4 can be found in Fig.s 2.4.4 and 2.4.5, respectively. A picture for p_3^{-1} can be obtained from the diagram for p_3 just by reversing the direction of each arc. □

2.4.7 Example. Using disjoint cycle notation, $S_3 = \{(1)(2)(3), (1)(23), (12)(3), (123), (132), (13)(2)\}$. (Compare with Example 2.3.2.) □

Apart from equivalence and the order in which the cycles are written, the disjoint cycle factorization of p is unique. Without loss of generality, we can always choose, if we wish, to write $C_p(1)$ first, to begin the second cycle (if there is one) with the smallest integer that does not appear in $C_p(1)$, to begin the third with the smallest integer that does not appear in either of the first two cycles, etc. This convention was used in Examples 2.4.6 and 2.4.7. However, we will not use it all the time because that would unnecessarily complicate future counting arguments. Another informal convention is to treat equivalent cycles as if they were the same, reflecting the fact that they represent the same geometric cycle.

Let's take stock of where we are. Illustrating permutations by means of dots and arcs led to the intuitive notion of a cycle, a simple notion that was, nevertheless, surprisingly awkward to define formally. Think of that as the price of admission.

Having paid the price, let's amuse ourselves by exploring the *cycle structure* of permutations.

Observe that the lengths of the cycles in the disjoint cycle factorization of (any) $p \in S_m$ comprise the parts of a partition of m. In Example 2.4.6, the partition of 7 afforded by p_1 is $[3, 2, 1^2]$. The partitions coming from p_2, p_3, and p_4 are $[4, 3]$, $[7]$, and $[1^7]$, respectively.

2.4.8 Definition. Suppose $p \in S_m$. The partition of m whose parts are the lengths of the cycles in the disjoint cycle factorization of p is the *cycle type* of p. Two permutations of the same cycle type are said to have the same *cycle structure*.

This definition suggests two questions: (1) How many different cycle types are there? (2) How many different permutations share a specified cycle type? The first question is easy to answer. The set S_m contains $p(m)$ different cycle types, one for each partition* of m. The second question is more interesting.

2.4.9 Example. Consider the permutation $p_2 = (1643)(257) \in S_7$ having cycle type $[4, 3]$. We have already observed that (1643) (257) is just one of 24 different-*looking* ways to express p_2 in disjoint cycle notation. We now want to consider a different question, namely, how many different permutations in S_7 have cycle type $[4, 3]$?

Any such permutation can be expressed in the form $p = (abcd)(xyz)$. There are 7 choices for a, 6 for b, 5 for c, and 4 for d. While $P(7, 4) = 840$ may give the number of ways to *fill* the 4-cycle, it is not the number of ways to *choose* the 4-cycle. It is too large. It does not take equivalence into account. Since $(abcd) = (bcda) = (cdab) = (dabc)$, the number of different 4-cycles that can be produced using seven numbers is $P(7, 4)/4 = 210$. (Don't confuse $P(7, 4)/4$ with $P(7, 4)/4! = C(7, 4)$.)

Once a 4-cycle is chosen, three numbers remain to play the roles of x, y, and z. These can be arranged in a 3-cycle in $P(3, 3)/3 = 2$ inequivalent ways, e.g., (xyz) or (xzy). By the fundamental counting principle, S_7 must contain $210 \times 2 = 420$ permutations of cycle type $[4, 3]$. □

Note that the 420 permutations enumerated in Example 2.4.9 have the same cycle structure as $(abc)(wxyz)$. Indeed,

$$\frac{7 \times 6 \times 5 \times 4}{4} \times \frac{3 \times 2 \times 1}{3} = \frac{7 \times 6 \times 5}{3} \times \frac{4 \times 3 \times 2 \times 1}{4}.$$

2.4.10 Example. How many permutations in S_{12} have cycle type $[3^2, 2^3] = [3, 3, 2, 2, 2]$? Solution: The generic permutation of this type is

$$p = (abc)(xyz)(ij)(uv)(rs).$$

*Lowercase "p" has been used (so far!) for primes, probabilities, polynomials, partitions, and permutations. Here $p(m)$ is the number of partitions of m. (Is it any wonder that mathematicians frequently resort to other alphabets?)

There are $P(12,3)/3 = 440$ ways to choose the first 3-cycle. Once it is chosen, there are $P(9,3)/3 = 168$ ways to choose the second. So, $440 \times 168 = 73,920$ is the number of ways to choose an *ordered* sequence of two 3-cycles. Because the cycles of a permutation can be arranged in any order, this number double counts the pair of 3-cycles, once in the form $(abc)(xyz)$ and again as $(xyz)(abc)$. Compensating for this double counting, we see that there are $73,920/2 = 36,960$ different ways to choose the *pair* of 3-cycles.

This issue of double counting did not arise in Example 2.4.9 because cycle type $[4,3]$ does not admit two (or more!) cycles of the same length. (Check to see, e.g., that (1643) (257) and (257) (1643) did not get counted as different permutations in Example 2.4.9.)

No matter which six numbers occur in the two 3-cycles, six numbers remain to be distributed among the three 2-cycles: (ij) can be chosen in $P(6,2)/2 = 15$ ways*; (uv) in $P(4,2)/2 = 6$ ways; and (rs) in $P(2,2)/2 = 1$ way. So, six numbers will produce $15 \times 6 = 90$ ordered sequences of three 2-cycles. Because an unordered collection of three 2-cycles can be arranged in $3! = 6$ ways, the same six numbers will produce $\frac{90}{6} = 15$ unordered sequences of three 2-cycles. Hence, the number of permutations in S_{12} of cycle type $[3^2, 2^3]$ is $36,960 \times 15 = 554,400$.

Each of the $12! = 479,001,600$ permutations in S_{12} has one of $p(12) = 77$ cycle types. Our calculations show that a little over 0.11% of the permutations in S_{12} have cycle type $[3^2, 2^3]$. □

2.4.11 Example. Of the permutations in S_7, how many have disjoint cycle factorizations consisting of exactly three cycles? Solution: The $p_3(7) = 4$ three-part partitions of 7 are $[5,1^2]$, $[4,2,1]$, $[3^2,1]$, and $[3,2^2]$. Given the tools presently at our disposal, answering the question evidently requires four computations of the type just completed in Example 2.4.10. That's the bad news. The good news is that, while S_{12} contains nearly 500 million permutations, S_7 contains only $7! = 5040$.

Let's start with cycle type $[5,1^2]$, corresponding to a permutation of the form $(abcde)(x)(y)$. There are $P(7,5)/5 = 504$ ways to choose the 5-cycle. Once that is done, there is only one way to fix the remaining two points. So, exactly 10% of the permutations in S_7 have cycle type $[5,1^2]$.

Alternatively, because there are 7 ways to choose the fixed point x, and then 6 ways to choose y, there are 7×6 ways to choose an ordered pair of 1-cycles. Adjusting for the fact that this counts $(x)(y)$ as different from $(y)(x)$ yields $[7 \times 6]/2 = C(7,2) = 21$ ways to choose an unordered pair of 1-cycles. After the 1-cycles have been chosen, there are $P(5,5)/5 = 5!/5 = 24$ ways to choose the 5-cycle. This alternative computation leads, of course, to the same answer, i.e., $21 \times 24 = 504$ of the permutations in S_7 have cycle type $[5,1^2]$.

*Because (ij) and (ji) are equivalent, one could just as well argue that there are $C(6,2)$ ways to choose this 2-cycle. Of course, $C(6,2) = \frac{1}{2}P(6,2)$.

Among the various ways to count the permutations of cycle type $[4, 2, 1]$, having the generic form $(abcd)(ij)(z)$, are

$$[P(7,4)/4] \times [P(3,2)/2] = 210 \times 3 = 630,$$
$$[P(7,2)/2] \times [P(5,4)/4] = 21 \times 30 = 630,$$

and/or

$$7 \times [P(6,4)/4] = 7 \times 90 = 630.$$

In the first and second alternatives, after the 4-cycle and 2-cycle have been chosen, there is only one way to choose the 1-cycle. In the third case, after the fixed point and the 4-cycle are chosen, there is just one way to choose the 2-cycle (because (xy) and (yx) are equivalent).

Next, consider the generic permutation $(abc)(xyz)(w)$ of cycle type $[3^2, 1]$. Once the 3-cycles have been chosen, there is just one choice for w. So, because an unordered pair of 3-cycles can be chosen in

$$([P(7,3)/3] \times [P(4,3)/3])/2 = (70 \times 8)/2$$

ways, there are 280 permutations in S_7 of cycle type $[3^2, 1]$.

The fourth three-part partition of 7 is $[3, 2^2]$. There are $P(7,3)/3 = 70$ ways to choose the 3-cycle. Once it has been chosen, there are $([P(4,2)/2] \times [P(2,2)/2])/2 = 6/2 = 3$ ways to choose an unordered pair of 2-cycles from the remaining four numbers. So, the number of permutations having this cycle type is $70 \times 3 = 210$. Alternatively, we could just as well choose the unordered pair of 2-cycles in

$$([P(7,2)/2] \times [P(5,2)/2])/2 = (21 \times 10)/2$$
$$= 105$$

ways, and a 3-cycle from the remaining three numbers in $P(3,3)/3 = 2$ ways, for a total of $105 \times 2 = 210$.

Adding the numbers of each cycle type produces a total of

$$504 + 630 + 280 + 210 = 1624 \tag{2.25}$$

permutations in S_7 having disjoint cycle factorizations consisting of exactly three cycles. □

Example 2.4.11 involved a lot of work. If it is going to be important to know how many permutations in S_m have disjoint cycle factorizations consisting of (exactly) n cycles, i.e., faced with the prospect of having to do many problems like the one in Example 2.4.11, it would surely be worth the effort to look for an easier way of going about it. Such efforts often begin by giving the desired quantity a name.

2.4.12 Definition. The number of permutations in S_m whose disjoint cycle factorizations consist of (exactly) n cycles is the *Stirling number of the first kind*, $s(m, n)$.

From Equation (2.25), $s(7,3) = 1624$. From Example 2.4.7, $s(3,1) = 2$, $s(3,2) = 3$, and $s(3,3) = 1$. Stirling numbers of the first kind, $s(m,n)$, and their relationship to Stirling numbers of the second kind, $S(m,n)$, are the subject of the next section. (Be aware that s and S are easily confused, especially when they are not printed side by side.)

2.4. EXERCISES

1 Draw the "X-ray image" and then write down the disjoint cycle factorization of

(a) $p = (2,6,4,5,3,1,7)$. **(b)** $p = (7,6,5,4,3,2,1)$.

(c) $p = (7,6,4,5,3,2,1)$. **(d)** $p = (4,7,6,1,3,2,5)$.

(e) $p = (6,1,4,9,8,2,5,7,3)$. **(f)** $p = (3,4,5,2,7,8,9,6,1)$.

2 By the reasoning of Example 2.4.10, exactly 15 permutations in S_6 have cycle type $[2^3]$. Write them all down (using disjoint cycle notation).

3 Convert from disjoint cycle to sequence notation:

(a) (123) (45) (67). **(b)** (135) (246).

(c) (13) (5) (246). **(d)** (12) (3) (4) (5).

(e) (1) (2) (345). **(f)** (15432).

4 If $p \in S_m$, then $p^{-1} \in S_m$ is the unique permutation that satisfies $p(p^{-1}(x)) = x = p^{-1}(p(x))$, $1 \leq x \leq m$. Find the disjoint cycle factorization of p^{-1} when

(a) $p = (1234)$. **(b)** $p = (12345)$.

(c) $p = (123456)$. **(d)** $p = (15432)$.

(e) $p = (15)(23)(4)$. **(f)** $p = (184)(2756)(3)$.

(g) $p = (1357)(8642)$. **(h)** $p = (1742)(3586)$.

5 Suppose $(x_1 x_2 \cdots x_{k-1} x_k)$ is a cycle in the disjoint cycle factorization of permutation p. Show that $(x_k x_{k-1} \cdots x_2 x_1)$ is a cycle in the disjoint cycle factorization of p^{-1} (treating equivalent cycles as if they were equal).

6 Suppose $p \in S_m$. Prove that p and p^{-1} have the same cycle type. (*Hint*: Exercise 5.)

7 Express all 24 permutation of S_4 in disjoint cycle notation.

8 Write down the seven cycle types that occur among the permutations of S_5. (*Hint*: Example 1.8.6.)

9 Compute the number of permutations in S_5 of each cycle type.

10 Compute the Stirling numbers of the first kind, $s(5,n)$, $1 \leq n \leq 5$. (*Hint*: Exercise 9.)

11 Show that the number of permutations in S_{12} of cycle type

(a) $[3^4]$ is $246,400$. **(b)** $[4^3]$ is $1,247,400$.

(c) $[6^2]$ is $6,652,800$. **(d)** $[2^6]$ is $10,395$.

12 How many permutations in S_{12} have cycle type

(a) $[4, 2^4]$? **(b)** $[4^2, 2, 1^2]$?

(c) $[1^{12}]$? **(d)** $[12]$?

13 A *transposition* is a permutation of cycle type $[2, 1^{m-2}]$. How many permutations in S_m are transpositions.

14 Show that there are $P(m, k)/k$ permutations in S_m of cycle type $[k, 1^{m-k}]$.

15 Compute $s(7, 2)$. (*Hint*: Begin with $p_2(7)$.)

16 Exhibit the cycle types of the derangements in S_m for

(a) $m = 4$. **(b)** $m = 5$. **(c)** $m = 6$.

17 Prove that the total number of different cycle types afforded by derangements in S_m is

$$\sum_{n=1}^{\lfloor m/2 \rfloor} p_n(m-n),$$

where $\lfloor m/2 \rfloor$ is the greatest integer not larger than $m/2$.

18 Recall that $C_p(1)$ is the cycle of the permutation p that contains the number 1. If k is a fixed but arbitrary integer satisfying $1 \leq k \leq m$, prove that the length of $C_p(1)$ is k in exactly $(m-1)!$ of the permutations of S_m.

19 Denote by $c_t(p)$ (not to be confused with $C_p(t)$) the number of cycles of length t in the disjoint cycle factorization of $p \in S_m$.

(a) Prove that $c_1(p) + 2c_2(p) + 3c_3(p) + \cdots + mc_m(p) = m$.

(b) Let $(k_1, k_2, \ldots, k_m)$ be a sequence of nonnegative integers that satisfies $k_1 + 2k_2 + 3k_3 + \cdots + mk_m = m$. Prove that the number of permutations $p \in S_m$ that satisfy $c_t(p) = k_t$, $1 \leq t \leq m$, is $m!/K$, where $K = 1^{k_1}k_1!2^{k_2}k_2!3^{k_3}k_3! \cdots m^{k_m}k_m!$.

2.5. STIRLING NUMBERS OF THE FIRST KIND

The wind had dropped, and the snow, tired of rushing round in circles trying to catch itself up, now fluttered gently down until it found a place on which to rest, and sometimes that place was Pooh's nose and sometimes it wasn't.

— A. A. Milne

How many permutations $p \in S_m$ have disjoint cycle factorizations that consist of a single cycle? The name of the answer is $s(m, 1)$, a Stirling number of the first kind.* In this case, the number itself is easy enough to compute. In the generic m-cycle, $p = (x_1 x_2 \cdots x_m)$, there are m choices for x_1, $m - 1$ choices for $x_2, \ldots,$ and 1 choice for x_m. So, there are $m!$ ways to fill the m-cycle. Taking equivalence into account, we obtain

$$s(m, 1) = \frac{m!}{m} = (m - 1)!. \tag{2.26}$$

Strictly speaking, $(m - 1)!$ is just another name for the answer. However, associated with *this* name is an algorithm for producing an actual number. It would be useful to have simple algorithms for producing the remaining Stirling numbers, $s(m, n)$, $2 \leq n \leq m$.

The only partition of m having m parts is $[1^m]$, and the only permutation in S_m of this cycle type is the one having m fixed points. So,

$$s(m, m) = 1. \tag{2.27}$$

From Equation (2.26), $s(3, 1) = (3 - 1)! = 2$ and, from Equation (2.27), $s(3, 3) = 1$. Because

$$s(3, 1) + s(3, 2) + s(3, 3) = o(S_3) = 6,$$

$s(3, 2) = 3$, confirming the values found in the last section using Example 2.4.7.

From Equation (2.25), $s(7, 3) = 1624$, and $s(7, 2) = 1764$ is the answer to Exercise 15, Section 2.4. So, we are well on our way to filling in the entries of Fig. 2.5.1, a *second* Stirling triangle, one comprised of Stirling numbers of the first, kind.

m \ n	1	2	3	4	5	6	7
1	1						
2	1	1					
3	2	3	1				
4	6	s (4,2)	s (4,3)	1			
5	24	s (5,2)	s (5,3)	s (5,4)	1		
6	120	s (6,2)	s (6,3)	s (6,4)	s (6,5)	1	
7	720	1764	1624	s (7,4)	s (7,5)	s (7,6)	1
			...				

Figure 2.5.1

*Sometimes called a "signless" Stirling number of the first kind.

Having been in similar places before, it is easy to anticipate that the next result will be a recurrence for Stirling numbers of the first kind.

2.5.1 Theorem. *If* $1 < n \leq m$, *then*

$$s(m+1,n) = s(m,n-1) + ms(m,n).$$

Compare and contrast Theorem 2.5.1 with $S(m+1,n) = S(m,n-1) + nS(m,n)$, the recurrence for Stirling numbers of the second kind (Theorem 2.1.20).

Proof of Theorem 2.5.1. Let K be the set of permutations in S_{m+1} whose disjoint cycle factorizations consist of n cycles. By definition, $o(K) = s(m+1,n)$. The theorem is proved by showing that $o(K_1) = s(m,n-1)$ and $o(K_2) = ms(m,n)$, where $K_1 = \{p \in K : p(m+1) = m+1\}$ and $K_2 = K \backslash K_1 = \{p \in K : p(m+1) \neq m+1\}$.

Observe that $p \in K_1$ if and only if $m+1$ is a fixed point of p if and only if $(m+1)$ is a cycle of p. Deleting this 1-cycle from p leaves a permutation $p' \in S_m$. Since p is the unique permutation in S_{m+1} that can be obtained by juxtaposing p' and the 1-cycle $(m+1)$, $p \leftrightarrow p'$ is a one-to-one correspondence between K_1 and the permutations in S_m whose disjoint cycle factorizations consist of $n-1$ cycles, i.e., $o(K_1) = s(m,n-1)$.

The evaluation of $o(K_2)$ is similar, except that the correspondence is m-to-one. If $p \in K_2$, then $m+1$ must lie in a cycle of p of length greater than 1, i.e., $p(m+1) = i$ for some $i \neq m+1$. Deleting $m+1$ from this cycle produces $p^{\#}$, a permutation in S_m with n cycles in its disjoint cycle factorization. Conversely, for any such $f \in S_m$, there is a $p \in K_2 \subset S_{m+1}$ such that $p^{\#} = f$: Simply insert $m+1$ just before i in the disjoint cycle factorization of f. Because there are m possible choices for i, there must be (exactly) m permutations $p \in K_2$ such that $p^{\#} = f$, i.e., $o(K_2) = ms(m,n)$. ■

Theorem 2.5.1 makes it easy to fill in the entries of Fig. 2.5.1, a row at a time, e.g.,

$$\begin{aligned} s(4,2) &= s(3,1) + 3s(3,2) \\ &= 2 + 3 \times 3 = 11, \\ s(4,3) &= s(3,2) + 3s(3,3) \\ &= 3 + 3 \times 1 = 6, \end{aligned}$$

and so on, resulting eventually in Fig. 2.5.2.

Stirling numbers of the first kind pop up in a variety of places that are not obviously related to the cycle structure of permutations. Recall, e.g., our discussion of formulas for the mth-power sum, $1^m + 2^m + \cdots + n^m$, $m \geq 0$. We are now able to address the case in which $m = -1$.

m \ n	1	2	3	4	5	6	7
1	1						
2	1	1					
3	2	3	1				
4	6	11	6	1			
5	24	50	35	10	1		
6	120	274	225	85	15	1	
7	720	1764	1624	735	175	21	1
			...				

Figure 2.5.2. Stirling numbers of the first kind, $s(m,n)$.

2.5.2 Theorem. *If n is a positive integer, then the harmonic number*

$$\sum_{k=1}^{n} k^{-1} = \frac{s(n+1,2)}{n!}. \tag{2.28}$$

Proof. The proof is by induction on n. When $n = 1$, Equation (2.28) becomes $1 = s(2,2)/1$, and we are off to a good start. Using the induction hypothesis,

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{1}{k} &= \sum_{k=1}^{n} \frac{1}{k} + \frac{1}{n+1} \\
&= \frac{s(n+1,2)}{n!} + \frac{1}{n+1} \\
&= \frac{(n+1)s(n+1,2) + n!}{(n+1)!} \\
&= \frac{s(n+1,1) + (n+1)s(n+1,2)}{(n+1)!} \\
&= \frac{s(n+2,2)}{(n+1)!},
\end{aligned}$$

by Equation (2.26) and Theorem 2.5.1. ■

2.5.3 Example. From Fig. 2.5.2, $s(6,2) = 274$. By Equation (2.28), $s(6,2)$ is equal to

$$\begin{aligned}
5!\left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5}\right) &= 120 + \frac{120}{2} + \frac{120}{3} + \frac{120}{4} + \frac{120}{5} \\
&= 120 + 60 + 40 + 30 + 24 \\
&= 274.
\end{aligned}$$

□

From Equations (2.26) and (2.28),

$$\frac{s(n,2)}{s(n,1)} = \sum_{k=1}^{n-1} \frac{1}{k}.$$

Because the harmonic series diverges, taking limits of both sides yields

$$\lim_{n\to\infty} \frac{s(n,2)}{s(n,1)} = \infty.$$

Hence, despite the rapid growth of $s(n,1) = (n-1)!$, the ratio $s(n,2)/s(n,1)$ is still unbounded.

We now have three ways to evaluate, say, $s(21,2)$. The original brute-force approach is to count the permutations in S_{21} whose disjoint cycle factorizations consist of two cycles. As illustrated in Example 2.4.11, this might be done by summing the numbers of permutations having cycle types $[20,1]$, $[19,2]$, $[18,3]$, ..., $[11,10]$. A second option is to use Equation (2.28) and compute

$$s(21,2) = 20!\left(1 + \tfrac{1}{2} + \tfrac{1}{3} + \cdots + \tfrac{1}{20}\right).$$

A third is to use Theorem 2.5.1, a method that requires us first to compute $s(20,2)$ (not to mention $s(20,1) = 19!$). None of these methods seems particularly easy.

Let's try another approach. Define

$$\begin{aligned} g_m(x) &= \sum_{n=1}^{m} s(m,n)x^n \\ &= s(m,1)x + s(m,2)x^2 + \cdots + s(m,m)x^m. \end{aligned} \tag{2.29}$$

Superficially, the *generating function* $g_m(x)$ is just a fancy way to display the numbers $s(m,n)$, $1 \le n \le m$. On the other hand, this perspective hints at the possibility of using facts about polynomials to shed some light on the coefficients of $g_m(x)$. Let's have a look at the first few of these polynomials. From Fig. 2.5.2,

$$\begin{aligned} g_1(x) &= x \\ g_2(x) &= x + x^2 = x(1+x) = x(x+1) \\ g_3(x) &= 2x + 3x^2 + x^3 = x(2 + 3x + x^2) = x(x+1)(x+2). \end{aligned}$$

Already, a pattern seems to be emerging. Observe that

$$\begin{aligned} x(x+1)(x+2)(x+3) &= g_3(x)(x+3) \\ &= (2x + 3x^2 + x^3)(3 + x) \\ &= 6x + 11x^2 + 6x^3 + x^4, \end{aligned}$$

which, by Fig. 2.5.2, is precisely $g_4(x)$.

2.5.4 Theorem. *If* $g_m(x) = \sum_{n=1}^{m} s(m,n)x^n$, *then, for all* $m \geq 1$,

$$g_m(x) = x(x+1)(x+2)\cdots(x+m-1). \tag{2.30}$$

Proof. The examples preceding the statement of Theorem 2.5.4 suffice to start an induction on m. From

$$g_m(x) = s(m,1)x + s(m,2)x^2 + \cdots + s(m,m)x^m,$$

we obtain

$$\begin{aligned} xg_m(x) &= s(m,1)x^2 + \cdots + s(m,n-1)x^n + \cdots + s(m,m-1)x^m + s(m,m)x^{m+1}, \\ mg_m(x) &= ms(m,1)x + \cdots + ms(m,n)x^n + \cdots + ms(m,m)x^m. \end{aligned}$$

Adding these two equations produces the identity

$$\begin{aligned} (x+m)g_m(x) = ms(m,1)x + \cdots &+ [s(m,n-1) + ms(m,n)]x^n + \cdots \\ &+ [s(m,m-1) + ms(m,m)]x^m + s(m,m)x^{m+1}. \end{aligned}$$

From Equation (2.26), $ms(m,1) = m(m-1)! = m! = s(m+1,1)$; from Theorem 2.5.1, $s(m,n-1) + ms(m,n) = s(m+1,n)$, $2 \leq n \leq m$; and from Equation (2.27), $s(m,m) = 1 = s(m+1,m+1)$. Hence, this last identity is equivalent to $(x+m)g_m(x) = g_{m+1}(x)$. ■

2.5.5 Corollary. *Stirling numbers of the first kind are given in terms of elementary symmetric functions by means of the identity*

$$s(m,n) = E_{m-n}(1,2,\ldots,m-1), \qquad m > n \geq 1. \tag{2.31}$$

Proof. Recall that

$$(x-a_1)(x-a_2)\cdots(x-a_m) = x^m - E_1x^{m-1} + E_2x^{m-2} - \cdots + (-1)^m E_m, \tag{2.32}$$

where $E_r = E_r(a_1, a_2, \ldots, a_m)$ is the rth elementary symmetric function. Substituting $a_i = 1 - i$, $1 \leq i \leq m$, in Equation (2.32) yields

$$x(x+1)(x+2)\cdots(x+m-1) = \sum_{r=0}^{m} (-1)^r E_r(0,-1,-2,\ldots,1-m)x^{m-r}.$$

Together with Theorem 2.5.4 and the fact that

$$\begin{aligned} (-1)^r E_r(0,-1,-2,\ldots,1-m) &= (-1)^r E_r(-1,-2,\ldots,1-m) \\ &= E_r(1,2,\ldots,m-1), \end{aligned}$$

we see from this identity that

$$\begin{aligned} g_m(x) &= s(m,m)x^m + s(m,m-1)x^{m-1} + \cdots + s(m,1)x \\ &= E_0x^m + E_1x^{m-1} + \cdots + E_{m-1}x + E_m, \end{aligned}$$

where, this time, $E_r = E_r(1, 2, \ldots, m-1)$. To complete the proof, it remains to compare $s(m,n)$, the coefficient to x^n in the first of these expressions, with $E_{m-n}(1, 2, \ldots, m-1)$, the coefficient of x^n in the second (and to observe that $E_m(1, 2, \ldots, m-1) = 0$). ■

The elementary numbers $e(n,r) = E_r(1, 2, \ldots, n)$ appeared in Section 1.9. By Corollary 2.5.5, $s(m,n) = e(m-1, m-n)$. (Confirm this identity by comparing Fig. 2.5.2 with Fig. 1.9.2.)

2.5.6 Example. Because $1 \times 2 \times \cdots \times (k-1)(k+1) \times \cdots \times m = m!/k$, it follows from Corollary 2.5.5 that

$$\begin{aligned} s(m+1, 2) &= E_{m-1}(1, 2, \ldots, m) \\ &= \sum_{k=1}^{m} \frac{m!}{k} \\ &= m! \sum_{k=1}^{m} \frac{1}{k}, \end{aligned}$$

giving another proof of Theorem 2.5.2. □

Let

$$\begin{aligned} f_m(x) = x^m &- s(m, m-1)x^{m-1} + s(m, m-2)x^{m-2} - \cdots \\ &+ (-1)^{m-1} s(m, 1)x. \end{aligned} \tag{2.33}$$

Then $f_m(x)$ can be obtained from $g_m(x)$ by alternating the signs of its coefficients. Hence, from Equations (2.29) and (2.30) (or Equation (2.32)),

$$\begin{aligned} f_m(x) &= x(x-1)(x-2)\cdots(x-m+1) \\ &= x^{(m)}, \end{aligned} \tag{2.34}$$

the falling factorial function. As will be seen in Theorem 2.5.8 (below), this observation has some surprising consequences.

2.5.7 Example. Consider the 5×5 matrix F_5 whose (i,j)-entry is the Stirling number of the first Kind, $s(i,j)$, $1 \le i, j \le 5$, where $s(i,j) = 0$ if $i < j$. From Fig. 2.5.2,

$$F_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 \\ 6 & 11 & 6 & 1 & 0 \\ 24 & 50 & 35 & 10 & 1 \end{pmatrix}.$$

This is another example of a matrix that is clearly invertible. (Its determinant is 1.) The last time we found ourselves in such a situation we were looking at the Pascal matrix $C_n = (C(i,j))$. In that context, C_n^{-1} was found by sprinkling minus signs among the entries of C_n. Might the same trick work again? Could

$$Y = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 2 & -3 & 1 & 0 & 0 \\ -6 & 11 & -6 & 1 & 0 \\ 24 & -50 & 35 & -10 & 1 \end{pmatrix},$$

be the inverse of F_5? Check it out. Before reading on, convince yourself that $F_5 Y \neq I_5$, the 5×5 identity matrix.

Okay, inverting F_5 is not as easy as alternating minus signs among its entries. Matrix Y is not the inverse of F_5; it is the inverse of $T_5 = (S(i,j))$, the 5×5 matrix whose (i,j)-entry is a Stirling number of the *second* kind! From Fig. 2.1.2,

$$T_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 1 & 7 & 6 & 1 & 0 \\ 1 & 15 & 25 & 10 & 1 \end{pmatrix},$$

and

$$\begin{aligned} T_5 Y &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 1 & 7 & 6 & 1 & 0 \\ 1 & 15 & 25 & 10 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 2 & -3 & 1 & 0 & 0 \\ -6 & 11 & -6 & 1 & 0 \\ 24 & -50 & 35 & -10 & 1 \end{pmatrix} \\ &= I_5. \end{aligned} \tag{2.35}$$

□

Recall that elementary row operations can be achieved via multiplication on the left by an elementary matrix. Thus, e.g., the effect of premultiplying an $n \times n$ matrix $A = (a_{ij})$ by the diagonal matrix diag $(-1, 1, 1, 1, \ldots, 1)$ is to change the sign of every entry in its first row. The result of premultiplying A by the diagonal matrix

$$D_n = \text{diag}(-1, 1, -1, 1, -1, \ldots, (-1)^n),$$

in which the n diagonal entries alternate between -1 and $+1$, is to change the signs of the entries of A that lie in odd-numbered rows. Similarly, the (i,j)-entry of AD_n is

$$(-1)^j a_{ij} = \begin{cases} a_{ij} & \text{if } j \text{ is even,} \\ -a_{ij} & \text{if } j \text{ is odd.} \end{cases}$$

Pre- *and* postmultiplying A by D_n sprinkles a checkerboard pattern of alternating minus signs among its entries—precisely the way $Y = T_5^{-1}$ is obtained from F_5, i.e., $Y = D_5F_5D_5$. Moreover, because $D_n^2 = I_n$, D_n is its own inverse. Thus, $D_nF_nD_n = T_n^{-1}$ if and only if $D_nF_n^{-1}D_n = T_n$ if and only if $F_n^{-1} = D_nT_nD_n$.

Let's illustrate this last point for $n = 5$. From Equation (2.35),

$$\begin{aligned} I_5 &= T_5Y \\ &= T_5(D_5F_5D_5), \end{aligned}$$

proving that $D_5F_5D_5 = T_5^{-1}$. Observe that

$$\begin{aligned} F_5(D_5T_5D_5) &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 \\ 6 & 11 & 6 & 1 & 0 \\ 24 & 50 & 35 & 10 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 \\ 1 & -3 & 1 & 0 & 0 \\ -1 & 7 & -6 & 1 & 0 \\ 1 & -15 & 25 & -10 & 1 \end{pmatrix} \\ &= I_5, \end{aligned}$$

confirming that $D_5T_5D_5 = F_5^{-1}$.

2.5.8 Theorem. *Let $F_n = (s(i,j))$ and $T_n = (S(i,j))$ be $n \times n$ matrices of Stirling numbers of the first and second kinds, respectively. Let D_n be the $n \times n$ diagonal matrix whose (i,i)-entry is $(-1)^i$, $1 \le i \le n$. Then $T_n^{-1} = D_nF_nD_n$ and $F_n^{-1} = D_nT_nD_n$.*

Proof. From the remarks preceding the statement of Theorem 2.5.8, its two conclusions are equivalent. So, it will suffice to prove the first, namely, that $T_nY_n = I_n$, where $Y_n = D_nF_nD_n$. This, in turn, is equivalent to proving that

$$\sum_{k=1}^{n} (-1)^{k+j} S(i,k)s(k,j) = \delta_{i,j}, \qquad 1 \le i,j \le n. \tag{2.36}$$

Because $s(i,n) = 0$, $1 \le i < n$, the only nonzero entry in the last column of Y_n is $s(n,n) = 1$. Similarly, because $S(i,n) = 0$, $1 \le i < n$, the only nonzero entry in the last column of T_n is $S(n,n) = 1$. From these observations, we draw two conclusions. First, the last column of T_nY_n is equal to the last column of I_n, which establishes the $j = n$ case of Equation (2.36). Second, the leading $(n-1) \times (n-1)$ principal submatrix of T_nY_n is $T_{n-1}Y_{n-1}$.

If follows from the second of these conclusions that Equation (2.35) establishes the theorem, not only for $n = 5$, but for $n = 1, 2, 3$, and 4 as well. It is a consequence of both conclusions that, to complete a proof by induction on n, all one

needs do is prove that the entries in the first $n-1$ columns of the nth row of T_nY_n are all zero. In other words, it suffices to prove that

$$\sum_{k=1}^{n}(-1)^{k+j}S(n,k)s(k,j)=0, \qquad 1\le j<n. \tag{2.37}$$

Replacing m with k in Equations (2.33) and (2.34) gives

$$x^{(k)}=\cdots+(-1)^{k+j}s(k,j)x^j+\cdots\ . \tag{2.38}$$

Multiplying both sides of Equation (2.38) by $S(n,k)$ and summing on k, we obtain

$$\sum_{k=1}^{n}S(n,k)x^{(k)}=\cdots+\left(\sum_{k=1}^{n}(-1)^{k+j}S(n,k)s(k,j)\right)x^j+\cdots \tag{2.39}$$

$$=x^n, \tag{2.40}$$

by Theorem 2.2.2. Comparing coefficients of x^j on the right-hand sides of Equations (2.39) and (2.40) produces

$$\sum_{k=1}^{n}(-1)^{k+j}S(n,k)s(k,j)=0, \tag{2.41}$$

$1\le j<n$. ■

2.5.9 Example. Let's confirm Equation (2.41) when $n=6$ and $j=2$. From row 6 of Fig. 2.1.2, the Stirling numbers of the second kind, $S(6,k)$, $1\le k\le 6$, are 1, 31, 90, 65, 15, and 1. From the second column of Fig. 2.5.2, the Stirling numbers of the first kind, $s(k,2)$, $1\le k\le 6$, are 0, 1, 3, 11, 50, and 274. Substituting these values into Equation (2.41) gives

$$\begin{aligned}&-S(6,1)s(1,2)+S(6,2)s(2,2)-S(6,3)s(3,2)+\cdots+S(6,6)s(6,2)\\&\quad=-1\times 0+31\times 1-90\times 3+65\times 11-15\times 50+1\times 274\\&\quad=0.\end{aligned}$$

□

2.5. EXERCISES

1 From Fig. 2.5.2, $s(4,2)=11$. Exhibit the 11 permutations in S_4 whose disjoint cycle factorizations consist of exactly two cycles.

2 Compute $s(7,2)$ using Equation (2.28). (*Hint*: Example 2.5.3.)

3 Confirm that $s(6,3)=225$ by showing

(a) that $p_3(6)=3$.

(b) that the three-part partitions of 6 are the cycle types of 15, 90, and 120 permutations in S_6.

4 Using the approach outlined in Exercise 3, confirm

(a) that $s(7,4) = 735$. **(b)** that $s(8,3) = 13,132$.

5 Using a method of your choice, compute

(a) $s(8,n)$, $1 \le n \le 8$. **(b)** $s(9,n)$, $1 \le n \le 9$.

6 Show that $E_r(1,2,\ldots,k) = s(k+1, k+1-r)$.

7 Prove that $s(m,m-1) = C(m,2)$.

8 Fill in the blanks (using actual numbers):

(a) $x^{(5)} = x^5 - \_\_\_\, x^4 + \_\_\_\, x^3 - \_\_\_\, x^2 + \_\_\_\, x - \_\_\_$.

(b) $x^5 = x^{(5)} + \_\_\_\, x^{(4)} + \_\_\_\, x^{(3)} + \_\_\_\, x^{(2)} + \_\_\_\, x + \_\_\_$.

9 Compute

(a) $E_{5-r}(1,2,3,4)$ and confirm that the answer is $s(5,r)$, $1 \le r \le 5$.

(b) $E_{6-n}(1,2,3,4,5)$ and confirm that the answer is $s(6,n)$, $1 \le n \le 6$.

10 Show that $\sum_{k=1}^{n} (-1)^{i+k} S(i,k)s(k,j) = \delta_{i,j}$, $1 \le i,j \le n$.

11 Prove that

(a) $m! = s(m,1) + s(m,2) + \cdots + s(m,m)$.

(b) $n! = s(n,n)n^n - s(n,n-1)n^{n-1} + s(n,n-2)n^{n-2} - \cdots + (-1)^{n-1} s(n,1)n$.

12 Prove that $s(m,1) - s(m,2) + s(m,3) - s(m,4) + \cdots - (-1)^m s(m,m) = 0$, $m > 1$. (Compare with Lemma 1.5.8.)

13 Base a new proof of Corollary 2.5.5 on Lemma 1.9.8 and Theorem 2.5.1.

14 Prove that $s(m+1, n+1) = \sum_{k=n}^{m} (m-k)!C(m,k)s(k,n)$.

15 Prove the following analog of Exercise 13, Section 2.1:

$$s(m+1, n+1) = \sum_{k=n}^{m} s(m,k)C(k,n).$$

16 Prove that

$$\sum_{k=j}^{i} (-1)^{k+j} S(i+1, k+1)s(k,j) = C(i,j).$$

(*Hint*: Exercise 13, Section 2.1.)

17 Let $g(n)$ (not to be confused with $g_m(x)$) be some function of n. Suppose f is another function, defined in terms of g by

(a) $f(m) = \sum_{n=1}^{m} S(m,n)g(n)$, with a big S. Prove that $g(m) = \sum_{n=1}^{m} (-1)^{m+n} s(m,n)f(n)$, with a small s.

(b) $f(m) = \sum_{n=1}^{m} s(m,n)g(n)$, with a small s. Prove that $g(m) = \sum_{n=1}^{m} (-1)^{m+n} S(m,n)f(n)$, with a big S.

18 Equation (2.9) in Section 2.2 suggests a role for Stirling numbers of the second kind in evaluating the sum of the mth powers of the first n positive integers. Explain how Stirling numbers of the first kind might be used to evaluate this same mth-power sum. (*Hint*: Exercise 12, Section 1.9.)

19 Prove that $\sum_{n=1}^{m}(-1)^{m+n}s(m,n)B_n = 1$, where B_n is the nth Bell number.

20 Confirm the identity in Exercise 19 when

(a) $m = 4$. **(b)** $m = 5$.

21 If p is an odd prime, then p is a factor of $s(p,r)$, $1 < r < p$.

(a) Confirm this result when $p = 7$.

(b) Show that this result need not remain true if "prime" is replaced with "composite integer".

22 Suppose $1 < n \leq m$. Generalize Theorem 2.5.2 by showing that

$$s(m,n) = (m-1)! \sum_{f \in Q_{n-1,m-1}} \prod_{i=1}^{n-1} f(t)^{-1}.$$

(*Hint*: Corollary 2.5.5.)

23 Use the formula from Exercise 22 to evaluate

(a) $s(4,2)$. **(b)** $s(4,3)$.

(c) $s(5,2)$. **(d)** $s(5,3)$.

24 It can be shown that

$$s(m,n) = \frac{m!}{n!} \sum \prod_{t=1}^{n} r_t^{-1},$$

where the summation is over all compositions $r_1 + r_2 + \cdots + r_n = m$ having n parts. Use this formula to evaluate

(a) $s(4,2)$. **(b)** $s(4,3)$.

(c) $s(5,2)$. **(d)** $s(5,3)$.

25 Confirm the equation

$$\sum_{t=1}^{m} \frac{1}{t^2} = \left(\frac{s(m+1,2)}{m!}\right)^2 - 2\frac{s(m+1,3)}{m!}$$

(a) for $m = 1$. **(b)** for $m = 2$.

(c) for $m = 3$. **(d)** for $m = 4$.

26 Show that $s(m+1,m-2) = \frac{1}{18}m(m+1)[3s(m+1,m-1) - m^3 + m]$. (*Hint*: Exercise 23, Section 1.9.)

27 Write an algorithm/program to compute $s(m,n)$, $1 \leq m \leq 10$, $1 \leq n \leq m$.

28 Suppose n and k are positive integers. Let A be the $k \times k$ matrix whose (i,j)-entry is $s(n+i,j)$. Prove that $\det(A) = (n!)^k$. (*Hint*: Using appropriate elementary row operations, show that $\det(A) = \det(U)$, where U is a $k \times k$ upper triangular matrix each of whose diagonal entries is $n!$.)

29 If A and B are $r \times r$ and $s \times s$ matrices, respectively, their *direct sum* $A \oplus B$ is the $(r+s) \times (r+s)$ matrix

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

(a) Show that the $(n+1) \times (n+1)$ matrix of Stirling numbers of the first kind,

$$F_{n+1} = (I_1 \oplus F_n) C_{[0,n]},$$

where

$$C_{[0,n]} = \begin{pmatrix} C(0,0) & C(0,1) & \cdots & C(0,n) \\ C(1,0) & C(1,1) & \cdots & C(1,n) \\ \vdots & \vdots & \ddots & \vdots \\ C(n,0) & C(n,1) & \ldots & C(n,n) \end{pmatrix},$$

is the $(n+1) \times (n+1)$ generalized Pascal matrix of Exercise 25, Section 1.5, and I_1 is the 1×1 identity matrix.

(b) Confirm part (a) when $n = 4$.

(c) Show that $F_4 = (I_2 \oplus C_{[0,1]}) \times (I_1 \oplus C_{[0,2]}) \times C_{[0,3]}$.

(d) Suggest a factorization for F_n in terms of direct sums of identity matrices and matrices of binomial coefficients.

(e) Prove or disprove your suggested generalization.

30 Confirm Theorem 2.5.8 when $n = 6$, i.e., show that

(a) $T_6 D_6 F_6 D_6 = I_6$.

(b) $D_6 T_6 D_6 F_6 = I_6$.

31 Using the notation from Exercise 29,

(a) Show that the $(n+1) \times (n+1)$ matrix of Stirling numbers of the second kind

$$T_{n+1} = C_{[0,n]} (I_1 \oplus T_n).$$

(b) Confirm part (a) when $n = 4$.

(c) Show that $T_4 = C_{[0,3]} \times (I_1 \oplus C_{[0,2]}) \times (I_2 \oplus C_{[0,1]})$.

(d) Suggest a factorization for T_n in terms of direct sums of identity matrices and matrices of binomial coefficients.

(e) Prove or disprove your suggested generalization.

3

Pólya's Theory of Enumeration

Man is but a reed, the most feeble thing in nature; but he is a thinking reed.

— Blaise Pascal (*Pensées*)

Chapter 3–6 are completely independent of each other. Following Chapters 1 and 2, *the final four* can be read in any order.

The topics of Chapter 3 are deeper than the second stratum, in part because they involve compositions of functions. Basic definitions of permutation groups are introduced in Sections 3.1 and 3.2. While there may be some overlap of this material with abstract algebra, the perspective is different. Section 3.3, e.g., contains a lovely characterization of *multiple transitivity* in terms of Bell numbers. Because transitivity is not an invariant of abstract groups, themes like this are unlikely to receive the same emphasis in an algebra course.

Burnside's lemma from Section 3.3 and symmetry groups from Section 3.4 are used in Section 3.5 to count *color patterns*. The finer enumeration of color patterns by *weight* using Pólya's *pattern inventory* is found in Section 3.6. Because it is a symmetric polynomial, the pattern inventory is a polynomial in the power sums (Theorem 1.9.11). This *cycle index polynomial* is the subject of Section 3.7.

There are many natural places to exit from Chapter 3, e.g., at the ends of Sections 3.3, 3.5, or 3.6, or immediately after the statement of Theorem 3.6.5.

3.1. FUNCTION COMPOSITION

Let $f : D \to R$ be a function. While there is general agreement that D should be called the *domain* of f, not everyone concurs that *range* is the proper name for R; some authors use "range" to denote the set $\{f(x) : x \in D\}$.

3.1.1 Definition. Let $f : D \to R$ be a function. The *image* of f is the set $f(D) = \{f(x) : x \in D\}$, sometimes denoted image(f).

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

Note that $\text{image}(f) = f(D) \subset R$, with equality if and only if f is onto. If $f \in F_{m,n}$, then $f(D)$ is the set of numbers that appear in the sequence $(f(1), f(2), \ldots, f(m))$.

Suppose $f : D \to R$ and $g : A \to B$ are functions. If $f(D) \subset A$, then the *composition* of g and f is the function $g \circ f : D \to B$ defined by $g \circ f(x) = g(f(x))$. (In calculus, the derivative of a composition of functions is described by the *chain rule*.)

There is an awkward "backwardness" about the standard notation for function composition. It is occasioned by the fact that we read from left to right but evaluate a composition from right to left: The rule of assignment $g \circ f$ is determined by first applying f and then applying g. The French school has eliminated the difficulty by putting the function on the right, i.e., writing xf rather than $f(x)$. In the French scheme, cumbersome expressions like $g \circ f(x)$ and $g(f(x))$ become xfg. Because this right-handed notation has not been widely accepted in the United States, we will stick with the familiar $f(x)$.

3.1.2 Example. If $f \in F_{2,5}$ and $g \in F_{5,3}$, where might $g \circ f$ be found? Because f is applied first, $g \circ f$ shares the domain of f. Because g is applied second, $\text{image}(g \circ f) \subset \text{image}(g)$; so $g \circ f$ shares the range of g. Therefore, $g \circ f \in F_{2,3}$. To take a specific example, let $f = (3, 4) \in F_{2,5}$ and $g = (3, 3, 2, 1, 3) \in F_{5,3}$. Then

$$g \circ f(1) = g(f(1)) = g(3) = 2,$$
$$g \circ f(2) = g(f(2)) = g(4) = 1,$$

so $g \circ f = (2, 1)$.

What about $f \circ g$? Because that little circle looks like multiplication, one might be tempted to conclude that $g \circ f = f \circ g$. Let's check it out. Observe that $f \circ g(1) = f(g(1)) = f(3)$. Given that $f = (3, 4)$, what is $f(3)$? (Don't say $f(3) = 4$. This is no time to confuse sequences with cycles. The cycle idea is valid only in the context of permutations. While $f \in F_{2,5}$ may be one-to-one, it most certainly is *not* onto.) Because $3 \notin \{1, 2\}$, the domain of f, "$f(3)$" is nonsense; there is no third component in the sequence $(3, 4) = (f(1), f(2))$. Since $f(3)$ doesn't exist, $f \circ g$ doesn't exist either. In other words, it doesn't make sense even to write $f \circ g$, much less expect that it should equal $g \circ f = (2, 1)$. □

3.1.3 Example. Suppose $f = (3, 2, 1, 1, 2) \in F_{5,3}$ and $g = (2, 1, 1) \in F_{3,2}$. Then $\text{image}(f) = \text{range}(f) = \{1, 2, 3\} = \text{domain}(g)$, so there is a function $g \circ f \in F_{5,2}$. To determine which function it is requires a little work:

$$g \circ f(1) = g(f(1)) = g(3) = 1,$$
$$g \circ f(2) = g(f(2)) = g(2) = 1,$$
$$g \circ f(3) = g(f(3)) = g(1) = 2,$$
$$g \circ f(4) = g(f(4)) = g(1) = 2,$$
$$g \circ f(5) = g(f(5)) = g(2) = 1,$$

so $g \circ f = (1,1,2,2,1)$. What about $f \circ g$? This time $\text{image}(g) = \{1,2\} \subset \{1,2,3,4,5\} = \text{domain}(f)$, so $f \circ g$ is a legitimate function. Maybe now $f \circ g = g \circ f$? Let's see. The domain of $f \circ g$ is $\text{domain}(g) = \{1,2,3\}$;

$$\begin{aligned} f \circ g(1) &= f(g(1)) = f(2) = 2, \\ f \circ g(2) &= f(g(2)) = f(1) = 3, \\ f \circ g(3) &= f(g(3)) = f(1) = 3, \end{aligned}$$

so $f \circ g = (2,3,3) \in F_{3,3}$, which is not hard to distinguish from $g \circ f = (1,1,2,2,1) \in F_{5,2}$. □

What is the easy way to compute function compositions? Unfortunately, there are no shortcuts. With a little experience, one can find $g \circ f$ without taking up so much space, but only by keeping track of all the steps in one's head. Give it a try. Let $f, g \in F_{4,4}$ be defined by $f = (1,1,2,2)$ and $g = (4,3,1,1)$. If you can, confirm in your head that $g \circ f = (4,4,3,3)$ and $f \circ g = (2,2,1,1)$. If you can't manage to do it in your head, that's not a problem, *provided* you work it out with pencil and paper!

What about composing three functions? The only really good news here is that function composition is *associative*. If the domains and images match up so that $f \circ (g \circ h)$ makes sense, then $(f \circ g) \circ h$ also makes sense, and

$$f \circ (g \circ h) = (f \circ g) \circ h. \tag{3.1}$$

This is useful for two reasons. It means $f \circ g \circ h$ is unambiguous, and it means that $f \circ g \circ h$ can be evaluated, one composition at a time.

Suppose $f \in F_{m,m}$ is a permutation. Then $f \in S_m$ is one-to-one (and onto). So, f has an inverse. It might be helpful at this point to recall the definition of "inverse".

3.1.4. Definition. Suppose $f : D \to R$ and $g : R \to D$ are functions. Then g is the *inverse* of f if

$$g \circ f(d) = d \quad \text{for every } d \in D, \tag{3.2}$$

and

$$f \circ g(r) = r \quad \text{for every } r \in R. \tag{3.3}$$

If f has an inverse, then its rule of assignment is uniquely determined by Equation (3.2). In other words, if f has an inverse, it is unique. The inverse of f is typically written, not g, but f^{-1}. Two things about this notation deserve comment. The first is that f^{-1} is just a name for the unique function g that, along with f, satisfies Equations (3.2) and (3.3). The second is that Equations (3.2) and (3.3) are symmetric, i.e., $f^{-1} = g$ if and only if $g^{-1} = f$. (In particular, $[f^{-1}]^{-1} = f$.)

From this point on, our primary interest will be in the composition of *permutations*.

3.1.5 Example. Focusing on permutations does not affect function composition, but disjoint cycle notation changes the way it looks! If $p_1 = (1473)(2)(56)$ and $p_2 = (167)(24)(35)$, then

$$\begin{aligned} p_1 \circ p_2 &= (1473)(2)(56) \circ (167)(24)(35) \quad (3.4) \\ &= (15)(274)(36), \quad (3.5) \end{aligned}$$

and

$$\begin{aligned} p_2 \circ p_1 &= (167)(24)(35) \circ (1473)(2)(56) \\ &= (124)(36)(57). \end{aligned}$$

There is a purely mechanical way to produce the disjoint cycle factorization of $p_1 \circ p_2$. Write "(1". Then place your finger at the *right-hand* end of Equation (3.4) and start moving it to the left, searching for the number 1. When your finger comes to 1, stop. The number immediately to the right of 1 is $p_2(1) = 6$. (So far, so good: $p_1 \circ p_2(1) = p_1(p_2(1)) = p_1(6)$. It remains to find $p_1(6)$.) Resume the leftward motion of your finger, but with a new objective. Instead of searching for 1, look for (another occurrence of) 6. When you come to 6, stop. (Having already determined that $p_2(1) = 6$, we are about to find $p_1(6)$.) Because 6 is the last number in its cycle, move your finger leftward to the first number of that same cycle. In this case, that number is 5. Write 5 next to 1 in "(1", obtaining "(15".

Now, return your finger to the far right-hand end of Equation (3.4) and repeat the process, this time beginning your search with 5. Because 5 is the first number encountered, the search is brief. As 5 is at the end of its cycle, move your finger to the 3 at the beginning of the (same) cycle. (You have just determined that $p_2(5) = 3$. The next step is to determine $p_1(3)$.) Without writing anything down, resume your leftward movement, looking for the next occurrence of 3. Since it is found at the end of its cycle, move your finger to the front of that same cycle, bringing it to rest on 1. Evidently, $1 = p_1(3) = p_1(p_2(5))$. In the disjoint cycle factorization of $p_1 \circ p_2$, 1 follows 5. Since we opened the cycle with 1, it is time to close the cycle, i.e., change "(15" to "(15)".

Next, find the smallest number that has not yet been used. In this case it is 2. Replace "(15)" with "(15) (2". Place your finger at the far right-hand end of Equation (3.4) and repeat the process, searching for 2. Continue in this way until you've obtained Equation (3.5). □

3.1.6 Definition. Let $e_m \in S_m$ be the function defined by $e_m(i) = i, 1 \leq i \leq m$. The permutation e_m is called the *identity* of S_m. In disjoint cycle notation, $e_m = (1)(2)\cdots(m)$.

Before reading on, convince yourself that

$$f \circ e_m = f = e_m \circ f \tag{3.6}$$

for every $f \in S_m$. A more significant application of Definition 3.1.6 is the following useful alternative to the definition of inverse, one that is special to permutations.

3.1.7 Theorem. *Suppose $f, g \in S_m$. Then $g = f^{-1}$ if and only if $g \circ f = e_m$ and $f \circ g = e_m$.*

Proof. This is just a restatement of Definition 3.1.4 using e_m. ■

We now come to an important technical observation.

3.1.8 Lemma. *If $p, q \in S_m$, then, while they may not be equal, both $p \circ q$ and $q \circ p$ exist, and both are permutations in S_m.*

Proof. Because $S_m \subset F_{m,m}$, both $p \circ q$ and $q \circ p$ exist as functions in $F_{m,m}$. It remains to prove that they are permutations. By definition, S_m consists of those functions $f \in F_{m,m}$ that are one-to-one (and onto), i.e., S_m consists (precisely) of the invertible functions in $F_{m,m}$. It follows from $[f^{-1}]^{-1} = f$ that the inverse of an invertible function is invertible, so $p^{-1}, q^{-1} \in S_m$. To see that $q \circ p$ is invertible, observe that

$$\begin{aligned}(q \circ p) \circ (p^{-1} \circ q^{-1}) &= q \circ (p \circ p^{-1}) \circ q^{-1} \\ &= q \circ e_m \circ q^{-1} \\ &= q \circ q^{-1} \\ &= e_m\end{aligned}$$

by associativity, Theorem, 3.1.7, and Equation (3.6). The identity $(p^{-1} \circ q^{-1}) \circ (q \circ p) = e_m$ can be proved similarly. Thus, by Theorem 3.1.7,

$$p^{-1} \circ q^{-1} = (q \circ p)^{-1}, \tag{3.7}$$

the inverse of $q \circ p$. In particular, $q \circ p$ *has* an inverse, which is the criterion that must be met to guarantee that $q \circ p \in S_m$. Interchanging p and q in Equation (3.7) yields $(p \circ q)^{-1} = q^{-1} \circ p^{-1}$, proving that $p \circ q \in S_m$. ■

3.1.9 Example. Let $p = (1524)(3)$ and $q = (143)(25)$. Then $p^{-1} = (4251)(3) = (1425)(3)$ and $q^{-1} = (341)(52) = (134)(25)$. Let's confirm Equation (3.7) by comparing $p^{-1} \circ q^{-1}$ with $(q \circ p)^{-1}$. Observe that

$$\begin{aligned}p^{-1} \circ q^{-1} &= (1425)(3) \circ (134)(25) \\ &= (132)(4)(5).\end{aligned}$$

Next, compute

$$\begin{aligned} q \circ p &= (143)(25) \circ (1524)(3) \\ &= (123)(4)(5), \end{aligned}$$

from which it follows that $(q \circ p)^{-1} = (321)(4)(5) = (132)(4)(5)$. □

One interpretation of Lemma 3.1.8 is that function composition is a *binary operation* on the set S_m. In a calculus course, one must contend with a variety of operations. There, it is important to distinguish the composition of two functions from their product (e.g., the chain rule from the product rule) and the inverse from the reciprocal (i.e., f^{-1} from $1/f$). In the context of S_m, however, composition is the *only* binary operation that we will be discussing. This leads to several more "abuses of the language." For one thing, it can do no harm to drop the little circle from the notation for function composition.

3.1.10 Convention. If $f, g \in S_m$, then $gf = g \circ f$, i.e., the composition of g and f may be expressed as gf, without the little circle.

So far, so good. But, the next abuse may be a little harder to swallow. The language and notation normally used with generic binary operations is borrowed from multiplication. We have already spoken, e.g., of disjoint cycle *factorizations*. We will occasionally go even further and describe gf as a *product*.

3.1.11 Convention. If $f, g \in S_m$, then the composition $g \circ f = gf$ is also known as the *product* of g and f.

While $o(S_m) = m!$ may be large, it is finite. In principle, at least, all $(m!)^2$ products of its elements can be tabulated explicitly in a so-called *Cayley table*.* A Cayley table for S_3 can be found in Fig. 3.1.1.

	e_3	(12) (3)	(13) (2)	(1) (23)	(123)	(132)
e_3	e_3	(12) (3)	(13) (2)	(1) (23)	(123)	(132)
(12) (3)	(12) (3)	e_3	(132)	(123)	(1) (23)	(13) (2)
(13) (2)	(13) (2)	(123)	e_3	(132)	(12) (3)	(1) (23)
(1) (23)	(1) (23)	(132)	(123)	e_3	(13) (2)	(12) (3)
(123)	(123)	(13) (2)	(1) (23)	(12) (3)	(132)	e_3
(132)	(132)	(1) (23)	(12) (3)	(13) (2)	e_3	(123)

Figure 3.1.1. Cayley Table for S_3.

*After Sir Arthur Cayley (1821–1895).

Because function composition is not commutative, care must be exercised when reading Cayley tables.

3.1.12 Convention. In Cayley tables associated with this book, fg is found in row f and column g.

Lemma 3.1.8 guarantees that, in a Cayley table for S_m, there are no missing entries, and there are no entries that do not come from S_m. Any two elements of S_m may be composed, and the result is another permutation in S_m. It turns out that some subsets of S_m also exhibit this *closure* property.

3.1.13 Definition. A nonempty subset G of S_m is *closed* if $fg \in G$ for all $f, g \in G$.

We have already proved that $f, g \in G$ implies $fg \in S_m$. That's not the point. The issue is whether the composition is an element of the subset G.

3.1.14 Example. Of the 63 nonempty subsets of S_3, only six are closed. Apart from S_3, itself, the other five are $\{e_3\}, \{e_3, (12)(3)\}, \{e_3, (13)(2)\}, \{e_3, (1)(23)\}$, and $\{e_3, (123), (132)\}$. If S is one of the remaining 57 nonempty subsets of S_3, there exist permutations $f, g \in S$ such that $fg \notin S$.

From our perspective, there is a kind of aristocracy among the subsets of S_m. The closed sub*sets* are called sub*groups*. □

3.1.15 Definition. Let G be a (nonempty) closed subset of S_m. Then G is a *subgroup* of S_m, or a *permutation group* of *degree m*.

In biology, a *riparian habitat* is found at the boundary of water and land. Life occurs in its richest diversity in the vicinity of such natural boundaries. A similar richness may frequently be found near the boundaries of mathematical disciplines. That is where we are now, at the boundary between combinatorics and algebra. Because every finite group is *isomorphic* to a permutation group, the case is sometimes made that combinatorial group theory embraces all finite group theory. At best, that viewpoint is misleading. Two permutation groups that are isomorphic as abstract groups may have very different combinatorial properties. It is the combinatorial properties of permutation groups that are of interest in this chapter.

One final pedagogical issue needs to be discussed. The group S_m has been defined in terms of the permutations of $V = \{1, 2, \ldots, m\}$. The fact that V is a set of *numbers* is beside the point. We have used V because it is convenient. We might just as well have discussed the set of permutations of $Y = \{y_1, y_2, \ldots, y_m\}$, denoting it S_Y. (In that notation, S_m becomes S_V.) Strictly speaking, elements of S_Y permute the $y's$, whereas elements of S_m permute their subscripts. But, the "action" is the same. For our purposes, S_m and S_Y are clones. When the time comes to talk about permutations of Y, we will talk about S_m *acting* on Y.

3.1. EXERCISES

Each problem that I solved became a rule which served afterwards to solve other problems.

—René Descartes (*Discourse on Method*)

1 Let $f, g, h \in F_{5,5}$ be defined by $f = (1,2,1,3,5)$, $g = (4,1,5,2,2)$, and $h = (1,3,1,3,3)$. Compute

(a) $f \circ g$. **(b)** $g \circ f$. **(c)** $f \circ h$. **(d)** $h \circ f$.

(e) $g \circ h$. **(f)** $h \circ g$. **(g)** $f \circ g \circ h$. **(h)** $f \circ h \circ g$.

(i) $g \circ f \circ h$. **(j)** $g \circ h \circ f$. **(k)** $h \circ f \circ g$. **(l)** $h \circ g \circ f$.

(m) $f \circ f$. **(n)** $g \circ g$. **(o)** $h \circ h$. **(p)** $h \circ g \circ h$.

2 Find the images of f, g, and h in Exercise 1.

3 Let $f, g, h \in S_5$ be defined by $f = (1)(253)(4)$, $g = (13425)$, and $h = (14)(25)(3)$. Find the disjoint cycle factorization of

(a) fg. **(b)** gf. **(c)** fh. **(d)** hf.

(e) gh. **(f)** hg. **(g)** fgh. **(h)** fhg.

(i) gfh. **(j)** ghf. **(k)** hfg. **(l)** hgf.

(m) ff. **(n)** fff. **(o)** hh. **(p)** ggg.

(q) f^{-1}. **(r)** g^{-1}. **(s)** h^{-1}. **(t)** $f^{-1}gf$.

4 Let $f, g \in F_{6,6}$ be defined by $f = (1,3,6,4,2,5)$ and $g = (2,3,1,5,6,4)$.

(a) Express $f \circ g$ as a sequence.

(b) Express $g \circ f$ as a sequence.

(c) Express f^{-1} as a sequence.

(d) Find the disjoint cycle factorization of f.

(e) Find the disjoint cycle factorization of g.

(f) Use your answer to part (a) to express $f \circ g$ in disjoint cycle notation.

(g) Use your answers to parts (d) and (e) to find the disjoint cycle factorization of $f \circ g$.

5 Find an appropriate expression for the unique function $f : D \to R$ that satisfies $f(1) = 3$, $f(2) = 1$, and $f(3) = 2$

(a) when $D = R$ is the set of real numbers and $f(x)$ is a polynomial of degree 2.

(b) when $D = R = \{1,2,3\}$ and $f \in F_{3,3}$ is interpreted as a sequence.

(c) when $f \in S_3$ is expressed in disjoint cycle notation.

6 Exhibit the Cayley table for S_2.

7 Let $p \in S_3$. Show that $\{p\}$ is a subgroup of S_3 if and only if $p = e_3$.

8 Explain, in words, how the Cayley table in Fig. 3.1.1 can be used to find p^{-1} for any permutation $p \in S_3$.

9 A curious fact about the Cayley table in Fig. 3.1.1 is that, apart from the headings, no element of S_3 occurs twice in any row or column. Prove that this property is valid in the Cayley table for S_m for all $m \geq 2$.

10 Let $A_3 = \{e_3, (123), (132)\}$.

(a) Exhibit the 3×3 Cayley table for A_3.

(b) Prove that A_3 is a permutation group. (*Hint*: Were you able to find an element of the set A_3 to fill every place in the table?)

(c) In what sense is the Cayley table you constructed for A_3 "symmetric"? Explain the implications of symmetry for this binary operation on A_3.

11 Prove that

(a) $G = \{e_4, (12)(3)(4), (1)(2)(34), (12)(34)\}$ is a permutation group of degree 4.

(b) $G = \{e_4, (12)(34), (13)(24), (14)(23)\}$ is a subgroup of S_4.

(c) $G = \{e_4, (1234), (13)(24), (1432)\}$ is a permutation group of degree 4.

12 Prove that

(a) $S = \{(123), (132)\}$ is not a subgroup of S_3.

(b) $S = \{(12), (3)\}$ is not a permutation group.

(c) $S = \{(123)(4), (1)(2)(34)\}$ is not a subgroup of S_4.

13 Prove or disprove that

(a) $G = \{e_3, (12)(3), (13)(2), (1)(23)\}$ is a subgroup of S_3.

(b) $S = \{e_5, (12345), (13524), (14253), (15432)\}$ is a subgroup of S_5.

(c) $S = \{e_5, (12345), (13245), (14235), (15234)\}$ is a subgroup of S_5.

14 Let $p \in S_m$. Define $p^1 = p$ and $p^n = p^{n-1}p$, $n > 1$. Describe the infinite sequence $p^1, p^2, p^3, \ldots$

(a) if $p = e_m$.

(b) if $m = 2$ and $p = (12)$.

(c) if $m = 3$ and $p = (123)$.

(d) if $m = 4$ and $p = (1234)$.

(e) if $m = 5$ and $p = (12345)$.

(f) if $m = 6$ and $p = (123456)$.

15 Let $p \in S_m$. Prove that $\{p^n : n \geq 1\}$ is closed. (See Exercise 14.)

16 Let $f, g \in S_m$. Suppose $fg = e_m$. Prove that $gf = e_m$. In other words, $g = f^{-1}$ if and only if *either* criterion in Theorem 3.1.7 is satisfied.

17 Write out the Cayley table for the *alternating group* $A_4 = \{e_4, (12)(34), (13)(24), (14)(23), (123)(4), (124)(3), (132)(4), (134)(2), (142)(3), (143)(2), (1)(234), (1)(243)\}$, thus proving that it is a permutation group.

18 Find four different permutation groups of degree 5. (Prove that each of them is closed).

19 Let $f \in F_{n,n}$. If $g, h \in F_{n,n}$ are (both) inverses of f, prove that $g = h$.

20 Prove that function composition is associative.

3.2. PERMUTATION GROUPS

> Perfection is achieved, not when there is nothing more to add, but when there is nothing left to take away.
>
> — Antoine de Saint Exupery

It is customary to omit cycles of length one when using disjoint cycle notation. Instead of $p = (1748)(2)(36)(5)$, for example, one usually writes $p = (1748)(36)$. The 1-cycles are still there, they just can't be seen. It's as if they were invisible. The convention is that numbers which do not appear are understood to be fixed points.

3.2.1 Example. A Cayley table for S_3 with the 1-cycles suppressed can be found in Figure 3.2.1. (Compare with Fig. 3.1.1.) □

With the fixed points suppressed, how is one to know whether (12) is a permutation in S_2, a permutation in S_3 with an invisible 1-cycle, or, for that matter, a permutation in S_8 with six fixed points? Let us agree that whenever the number of fixed points is an issue (most of the time), the degree of the permutation (the m in S_m) will have to be made clear, one way or another. A second issue arising from the new convention leads to another abuse of language.

	e_3	(12)	(13)	(23)	(123)	(132)
e_3	e_3	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e_3	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e_3	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e_3	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e_3
(132)	(132)	(23)	(12)	(13)	e_3	(123)

Figure 3.2.1. Cayley Table for S_3.

3.2.2 Definition. A cycle is *nontrivial*[*] if its length is greater than 1. A permutation having just one nontrivial cycle in its disjoint cycle factorization will, itself, be referred to as a *cycle*. A *k-cycle* in S_m is any permutation of cycle type $[k, 1^{m-k}]$.

Observe that, apart from e_3, every permutation in S_3 is either a 2-cycle or a 3-cycle.

With both the 1-cycles and the little circle representing function composition suppressed, how should $(123)(45) \in S_6$ be viewed? Is it a "single" permutation, or a composition of $f = (123)$ and $g = (45)$? In fact, the composition $(123) \circ (45)$ *is* the permutation with disjoint cycle factorization $(123)(45)$. Omission of the 1-cycles and the little circle leads to confusing the composition $(123)(45)$ with the permutation $(123)(45)$. Since the two are equal, this confusion is harmless.

Observe that no similar ambiguity arises for $(123)(34) \in S_6$. Because the cycles are not disjoint, this one can *only* be viewed as the composition of $f = (123)$ and $h = (34)$. The disjoint cycle factorization of $p = f \circ h$ is (1234). (Confirm it.)

Another technical issue is this: In the disjoint cycle factorization of a permutation, the order of the "factors" is immaterial, e.g., $(123)(45) = (45)(123)$. On the other hand, viewing $(123)(45) = (123) \circ (45)$ as the composition of $f = (123)$ and $g = (45)$ raises an obvious concern. Function composition is not commutative!

Recall that for mathematical statements *true* means "always true", which leaves *false* meaning *not* "always true". That's not the same thing as "always false". In fact,

$$\begin{aligned}(123) \circ (45) &= (123)(45) \\ &= (45)(123) \\ &= (45) \circ (123),\end{aligned}$$

i.e., permutations $f = (123)$ and $g = (45)$ commute. Indeed, from Lemma 2.4.4, the inequivalent cycles of a permutation are disjoint. Because disjoint cycles always commute, the "obvious concern" from the previous paragraph turns out to be a false alarm. But, enough about conventions. Let's get back to the combinatorics of permutations.

Recall that the nonempty closed subsets of S_m are members of an aristocracy; they are the *subgroups*. There is nothing inherently difficult about this concept. The difficult part is verifying closure, an exercise that seems to require constructing an entire Cayley table. One way around this difficulty might be to create closed subsets *by design*.

[*]This language is more than a little ironic. As we will see, the *significance* of the 1-cycles is far from "trivial".

3.2.3 Definition. If $p \in S_m$, let $p^0 = e_m$ and $p^n = p \circ p^{n-1}$, $n \geq 1$. Denoted $o(p)$, the *order*[*] of p is the smallest positive integer k such that $p^k = e_m$.

Observe that $o(e_m) = 1$ for all m. (In particular, *order* is independent of *degree*.) Before getting to a proof of the existence of $o(p)$, let's see some examples.

3.2.4 Example. Let $p = (123456) \in S_m$ (where $m \geq 6$). Then (check the computations)

$$\begin{aligned}
p^1 &= pe_m = p = (123456),\\
p^2 &= pp^1 = (123456)(123456) = (135)(246),\\
p^3 &= pp^2 = (123456)(135)(246) = (14)(25)(36),\\
p^4 &= pp^3 = (123456)(14)(25)(36) = (153)(264),\\
p^5 &= pp^4 = (123456)(153)(264) = (165432),\\
p^6 &= pp^5 = (123456)(165432) = e_m,
\end{aligned}$$

so $o(p) = 6$. (It follows from Lemma 2.4.1 that $o(g) = k$ for any k-cycle $g \in S_m$.) Observe that the next few *powers* of p are

$$p^7 = pp^6 = pe_m = p, \qquad p^8 = pp^7 = pp = p^2, \qquad p^9 = pp^8 = pp^2 = p^3,$$

and so on. In particular, $p^{12} = p^6 = e_m$.

If $f = (12)(3456) \in S_7$, then f is a permutation of degree 7. To find its order, observe that

$$\begin{aligned}
f^1 &= f = (12)(3456),\\
f^2 &= (12)(3456)(12)(3456) = (35)(46)\\
f^3 &= (12)(3456)(35)(46) = (12)(3654)\\
f^4 &= (12)(3456)(12)(3654) = e_7,
\end{aligned}$$

so $o(f) = 4$. (Does $f^{12} = e_7$?) □

3.2.5 Lemma. *Let n be a positive integer. Suppose $p \in S_m$ has order $o(p) = k$. Then $p^n = e_m$ if and only if k is a factor of n.*

Proof. Dividing n by k yields a quotient q and remainder $r = n - kq$, where $0 \leq r < k$. Because function composition is associative, $p^n = p^{kq+r} = (p^k)^q p^r = (e_m)^q p^r = e_m p^r = p^r$. In particular, $p^n = e_m$ if and only if $p^r = e_m$. Because $r < k = o(p), p^r = e_m$ if and only if $r = 0$ if and only if $n = kq$. ■

[*]The word *order* has already caused so much semantic difficulty that it may seem unwise to give it still another meaning!

3.2.6 Theorem. *If $p \in S_m$, then $o(p)$ is the least common multiple of the lengths of the cycles in the disjoint cycle factorization of p. (In particular, $o(p)$ exists.)*

Proof. If $p = e_m$, there is nothing to prove. So, suppose $p \neq e_m$. Then

$$p = C_p(i_1)C_p(i_2)\cdots C_p(i_r),$$

where $C_p(i_t), 1 \leq t \leq r$, are the nontrivial inequivalent cycles of p. In the aftermath of Definition 3.2.2, this means $p = p_1p_2\cdots p_r$, where the cycle $p_t \in S_m$ differs from $C_p(i_t)$ at most by some fixed points. Because inequivalent cycles of p are disjoint, and disjoint cycles commute, $p^n = p_1^n p_2^n \cdots p_r^n$.

Observe that $e_m = p^n = p_1^n(p_2^n \cdots p_r^n)$ if and only if

$$(p_1^n)^{-1} = p_2^n \cdots p_r^n. \tag{3.8}$$

If $p_1^n \neq e_m$, then $p_1^n(i) = j$ for some $j \neq i$. Because any fixed point of p_1 is a fixed point of p_1^n, this can happen only if $i,j \in C_p(i_1)$, only if both i and j are fixed points of $p_2, p_3, \ldots, p_r$. So, the left-hand side of Equation (3.8) sends j to i, but the right-hand side fixes j. This contradiction proves that $p_1^n = e_m$. Since any one of the cycles could have been first, $p^n = e_m$ if and only if $p_t^n = e_m$, $1 \leq t \leq r$. By Lemma 3.2.5 (and Lemma 2.4.1), $p_t^n = e_m$ if and only if n is a multiple of $o(p_t)$, the length of $C_p(i_t)$. Thus, $p^n = e_m$ if and only if n is a common multiple of these lengths, the least of which is $o(p)$. ■

3.2.7 Example. Let $f = (3,8,5,6,7,2,9,4,1) \in S_9$. Apart from establishing that $o(f)$ exists, Theorem 3.2.6 illustrates one of the benefits of disjoint cycle notation. From the expression $f = (13579)(2846)$, it is easy to see that $o(f) = 20$.

What about $p = (2,3,1,5,4)$? Can you see that $o(p) = 6$ *without* expressing it in the form $p = (123)(45)$? Let's confirm that $o(p) = 6$. (Check the computations.)

$$\begin{aligned}
p^2 &= (123)(45)(123)(45) = (132),\\
p^3 &= (123)(45)(132) = (45),\\
p^4 &= (123)(45)(45) = (123),\\
p^5 &= (123)(45)(123) = (132)(45),\\
p^6 &= (123)(45)(132)(45) = e_5.
\end{aligned}$$

Beyond confirming Theorem 3.2.6, this example illustrates some other facts:

1. While every fixed point of p is a fixed point of p^n for all n, the converse is false. For example, $p^2 = (132)$ fixes 4 and 5, but $p = (123)(45)$ does not.
2. Apart from knowing to write e_5 in the last step, the degree of p was irrelevant to the computation of its order.
3. Because $p \circ p^5 = e_5$, it must be that $p^5 = p^{-1}$. Similarly, $p^4 = (p^2)^{-1} = (p^{-1})^2$, call it p^{-2}, and $p^3 = p^{-3}$. □

3.2.8 Theorem. *Let $p \in S_m$. If $o(p) = k > 1$, then $p^{-1} = p^{k-1}$.*

Proof. By Exercises 16 and 19 of Section 3.1, p^{-1} is a name for the unique permutation $f \in S_m$ that solves the equation $pf = e_m$. So, the theorem is a consequence of $pp^{k-1} = p^k = e_m$. ■

3.2.9 Definition. *Let $p \in S_m$. The cyclic group generated by p is $\langle p \rangle = \{p^n : 0 \le n < o(p)\}$.*

3.2.10 Example. If $o(p) = k$, then $p^k = e_m$, so

$$\begin{aligned}\langle p \rangle &= \{e_m, p, p^2, \ldots, p^{k-1}\} \\ &= \{p, p^2, \ldots, p^{k-1}, p^k\}.\end{aligned}$$

Observe that $o(\langle p \rangle) = k = o(p)$; the number of elements in the subgroup $\langle p \rangle$ is equal to the smallest positive integer k such that $p^k = e_m$. In particular, calling k the *order* of p is no great abuse of language after all.

As in Example 3.2.4,

$$\begin{aligned}p^{k+1} &= pp^k = pe_m = p, \\ p^{k+2} &= pp^{k+1} = pp = p^2, \\ p^{k+3} &= pp^{k+2} = pp^2 = p^3,\end{aligned}$$

and so on. Evidently, the infinite sequence

$$p^0, p^1, p^2, \ldots = e_m, p^1, \ldots, p^{k-1}, e_m, p^1, \ldots, p^{k-1}, e_m, p^1, \ldots, p^{k-1}, e_m, \ldots$$

is *cyclic* with period k. In particular,

$$\begin{aligned}\{p^n : n \ge 0\} &= \{p^n : 0 \le n < k\} \\ &= \{e_m, p, p^2, \ldots, p^{k-1}\} \\ &= \langle p \rangle,\end{aligned} \tag{3.9}$$

which explains why $\langle p \rangle$ is a *cyclic* group. □

We now justify the word *group* in Definition 3.2.9.

3.2.11 Theorem. *If $p \in S_m$, then $\langle p \rangle$ is a subgroup of S_m.*

Proof. Because (associativity and induction) $p^r p^s = p^{r+s}, r, s \ge 0$, the nonempty subset of S_m on the left-hand side of Equation (3.9) is closed. ■

Theorem 3.2.11 gives us the means to construct infinitely many permutation groups. Let m be a fixed but arbitrary positive integer and let p be a fixed but

arbitrary permutation in S_m. Then $G = \langle p \rangle$ is a permutation group of degree m and order $o(G) = o(p)$.

Is every permutation group cyclic? No. In order for G to be cyclic, it must have a generator, i.e., there must be some $p \in G$ such that $o(p) = o(G)$. Consider $G = S_3$, for example. From Theorem 3.2.6 and Fig. 3.2.1, the order of an element of S_3 is 1, 2, or 3. Because S_3 contains no element of order 6, it is not cyclic. On the other hand, every $p \in S_3$ is the generator of a cyclic subgroup of S_3, e.g., $\langle (123) \rangle = \{e_3, (123), (132)\}$.

More generally, if p is an arbitrary element of an arbitrary permutation group G then, because G is closed, every element of $\langle p \rangle$ must be an element of G, i.e.,

$$p \in G \Rightarrow \langle p \rangle \subset G. \tag{3.10}$$

From this important observation, we can deduce the following.

3.2.12 Corollary. *Let G be a permutation group of degree m. Then*

1. $e_m \in G$ *and*

2. $p \in G \Rightarrow p^{-1} \in G$.

Proof. Because G cannot be empty, it contains a permutation that may as well be denoted p. Suppose $o(p) = k$. If $k = 1$, then $p^{-1} = e_m = p \in G$. Otherwise, by Implication (3.10), $\langle p \rangle = \{e_m, p, \ldots, p^{k-1}\} \subset G$. Thus, $e_m \in G$ and, by Theorem 3.2.8, $p^{-1} = p^{k-1} \in G$. ■

Let's summarize. Suppose G is a permutation group of degree m. Then, by definition, G is nonempty and closed with respect to the associative operation of function composition. By Corollary 3.2.12, G contains the identity permutation and the inverse of each of its elements.* In addition, the cyclic subgroup idea provides lots of examples. Another way to obtain examples comes from the following construction.

3.2.13 Definition. Let G be a permutation group of degree m. The *stabilizer subgroup* of $x \in \{1, 2, \ldots, m\}$ is the subset of G consisting of those permutations that fix x, i.e.,

$$G_x = \{p \in G : p(x) = x\}. \tag{3.11}$$

By Corollary 3.2.12, $e_m \in G$. Because $e_m(x) = x$, $e_m \in G_x$. So G_x is not empty. If $f, g \in G_x$, then $fg(x) = f(g(x)) = f(x) = x$, so $fg \in G_x$. Therefore, G_x is closed and so, as its name implies, G_x is a subgroup.

*These are the axioms for an abstract group.

3.2.14 Example. Let $G = S_4$. If $x = 4$, then, because we have decided to make the fixed points invisible, G_x *looks* like S_3. Because we made a mental note not to forget the fixed points, $G_x \neq S_3$. □

3.2.15 Example. Let $G = \langle f \rangle$, where $f = (12)(3456) \in S_7$. From Example 3.2.4, $G = \{e_7, (12)(3456), (35)(46), (12)(3654)\}$. If $x = 1$ or $x = 2$, then $G_x = \{e_7, (35)(46)\} = \langle f^2 \rangle$. If $3 \leq x \leq 6$, then $G_x = \{e_7\} = \langle e_7 \rangle$. If $x = 7$, then $G_x = G$.

Suppose $G = \langle p \rangle$, where $p = (123)(45) \in S_5$. Then, from Example 3.2.7, $G = \{e_5, (123)(45), (132), (45), (123), (132)(45)\}$. In this case, $G_1 = G_2 = G_3 = \{e_5, (45)\} = \langle p^3 \rangle$ and $G_4 = G_5 = \{e_5, (132), (123)\}$. (Observe that $\langle p^2 \rangle = \langle (123) \rangle = \langle p^4 \rangle$.) □

3.2.16 Definition. If G and H are subgroups of S_m and if H is a subset of G, then H is a *subgroup* of G.

We have found two ways to create groups by design, namely, the cyclic subgroups $\langle p \rangle$, where p is a permutation, and the stabilizer subgroups G_x, where G is an existing group and x is a number. While stabilizer subgroups can be cyclic (see Example 3.2.15), they can also be noncyclic (see Example 3.2.14).

The discussion of stabilizer subgroups has opened the door to some other possibilities. If G is a permutation group of degree m, consider the set $S = \{g \in G : g(x) = y\}$, where $y \neq x$. Because $e_m(x) = x \neq y$, S is precluded from being a subgroup by part 1 of Corollary 3.2.12.

That's interesting. The subset G_x consisting of the permutations that map x to x is a subgroup of G, but the subset S consisting of the permutations that map x to $y \neq x$ is not. Nevertheless, at least when it isn't empty, S is a close relative of G_x. If $f \in S$ and $p \in G_x$, then $fp(x) = f(p(x)) = f(x) = y$, i.e., $g = fp \in S$. In other words, for any $f \in S$, $fp \in S$ for every $p \in G_x$.

3.2.17 Definition. Let G be a permutation group of degree m and suppose $f \in G$. If H is a subgroup of G, then the subset

$$fH = \{fp : p \in H\} \subset G \tag{3.12}$$

is a (left) *coset* of H.

3.2.18 Theorem. *Let G be a permutation group of degree m. Suppose $f \in G$. If $f(x) = y$, then the subset of G consisting of all the permutations that send x to y is the coset fG_x, i.e.,*

$$fG_x = \{g \in G : g(x) = y\}. \tag{3.13}$$

Proof. By the discussion preceding Definition 3.2.17, $fG_x \subset S = \{g \in G : g(x) = y\}$. To prove the converse, suppose $g \in G$. If $g(x) = y = f(x)$, then $f^{-1}g(x) = f^{-1}(g(x)) = f^{-1}(y) = x$. Therefore, $f^{-1}g = p$ for some $p \in G_x$, i.e., $g = fp \in fG_x$. ■

3.2.19 Example. Suppose $G = \langle (123)(45) \rangle = \{e_5, (123)(45), (132), (45), (123), (132)(45)\}$. Then

$$\begin{aligned} G_1 &= \{g \in G : g(1) = 1\} \\ &= \{e_5, (45)\}. \end{aligned}$$

If $f = (123)(45)$, then $f(1) = 2$. Observe that

$$\begin{aligned} fG_1 &= (123)(45)\{e_5, (45)\} \\ &= \{(123)(45), (123)\} \\ &= \{g \in G : g(1) = 2\}, \end{aligned}$$

confirming Theorem 3.2.18. If $h = (123)$, then $h(1) = 2$. Although $h \neq f, hG_1 = (123)\{e_5, (45)\} = \{(123), (123)(45)\} = fG_1$.

Similarly, $G_5 = \{e_5, (132), (123)\}$. If $f = (45)$, then f maps $x = 5$ to $y = 4$. Because disjoint cycles commute,

$$\begin{aligned} fG_5 &= \{(45), (132)(45), (123)(45)\} \\ &= \{g \in G : g(5) = 4\}. \end{aligned}$$ □

3.2.20 Example. Let $G = \{e_4, (12), (34), (12)(34)\}$. (Confirm that G is closed but that it is not cyclic.) The stabilizer subgroup $G_1 = \{e_4, (34)\} = \langle (34) \rangle$. If $f = (12)$, then $f(1) = 2$. By Theorem 3.2.18, the subset of G consisting of all permutations that map 1 to 2 is

$$\begin{aligned} fG_1 &= (12)\{e_4, (34)\} \\ &= \{(12), (12)(34)\}. \end{aligned}$$

Indeed, the complement of fG_1 in G is G_1, no element of which maps 1 to 2. □

Suppose G is a permutation group of degree m. Let $x, y \in \{1, 2, \ldots, m\}$. If a total of k permutations of G fix x, how many map x to y? Suppose, e.g., that G is the group from Example 3.2.20. If $x = 1$, then a total of $k = o(G_1) = 2$ permutations of G fix x. If $y = 2$, then $o(fG_1) = 2$ as well. If $y = 3$, however, no permutation of G maps x to y.

Okay, let's rephrase the question. Suppose a total of k permutations of G fix x. If $f(x) = y \neq x$ for some $f \in G$, how many permutations of G map x to y? Because $\{g \in G : g(x) = y\} = fG_x = \{fp : p \in G_x\}$, it seems that $o(fG_x) = o(G_x)$, *unless* $fp = fq$ for some $p, q \in G_x$, where $p \neq q$. But, if $fp = fq$, then $p = e_m p = (f^{-1}f)p = f^{-1}(fp) = f^{-1}(fq) = (f^{-1}f)q = e_m q = q$, i.e., $p = q$. Thus,

$$o(fG_x) = o(G_x). \tag{3.14}$$

3.2. EXERCISES

1 Compute $o(p)$ if

(a) $p = (123)(4567)(89)$. **(b)** $p = (123)(45678)$.

(c) $p = (12)(34)(56)(78)$. **(d)** $p = (123)(456)(789)$.

2 Let $G = S_4$.

(a) With the 1-cycles omitted, exhibit the disjoint cycle factorizations of all 24 permutations in G.

(b) How many of the permutations of G are cycles?

(c) How many of the permutations of G are derangements?

3 Exhibit the disjoint cycle factorization of $p^n, 1 \leq n \leq 10$, when

(a) $p = (1234)$. **(b)** $p = (12345)$.

(c) $p = (123456)$. **(d)** $p = (12345678)$.

4 Let $p = (147926853) \in S_9$. *Without* computing p^5, explain how you can tell that $p^5(1) = 6$.

5 Show that the permutation group

(a) $G = \{e_4, (12)(34), (12), (34)\}$ is not cyclic.

(b) $G = \{e_4, (12)(34), (1324), (1423)\}$ is cyclic.

(c) $G = A_4$, from Exercise 17, Section 3.1, is not cyclic.

6 Show that the cyclic group $G = \{e_4, (12)(34), (1324), (1423)\}$ from Exercise 5(b) has two generators, i.e., find $p, q \in G$ such that $p \neq q$ but $\langle p \rangle = \langle q \rangle = G$.

7 Find all the generators of $G = \langle p \rangle$ when

(a) $p = (1234)$. **(b)** $p = (12345)$. **(c)** $p = (14325)$.

(d) $p = (123456)$. **(e)** $p = (1234567)$. **(f)** $p = (12345678)$.

8 Let $G = \{e_4, (12), (34), (12)(34)\}$. Exhibit G_x when

(a) $x = 1$. **(b)** $x = 2$. **(c)** $x = 3$.

9 Let $G = \{e_4, (1234), (1432), (13), (24), (12)(34), (13)(24), (14)(23)\}$.

(a) Show that G is a subgroup of S_4.

(b) Exhibit G_x when $x = 3$.

(c) Exhibit G_4.

(d) Find $p, q \in G, p \neq q$, such that $p(3) = 2 = q(3)$.

(e) Show that $pG_3 = qG_3$, where p and q are the permutations you found in part (d).

(f) How many different cyclic subgroups does G have?

10 Let G be a permutation group and suppose $f \in G$. Prove that $fG_x = G_x$ if and only if $f(x) = x$.

11 If n is a positive integer, prove that $(p^n)^{-1} = (p^{-1})^n$ for all $p \in S_m$.

12 Let H be a subgroup of a permutation group G. If $f, g \in G$, define $f \sim g$ to mean that $g^{-1}f \in H$.

(a) Prove that $\sim$ is an equivalence relation on G.

(b) If $g \in G$, prove that the equivalence class to which g belongs is the coset $gH = \{gh : h \in H\}$.

(c) Prove that $o(gH) = o(H)$ for all $g \in G$.

(d) Prove that $o(G) = o(H)r$, where r is the number of different equivalence classes.

(e) Prove Lagrange's theorem: $o(H)$ exactly divides $o(G)$.

13 Prove that $o(p^{-1}) = o(p)$ for all $p \in S_m$.

14 Prove that $\langle p^{-1} \rangle = \langle p \rangle$ for all $p \in S_m$.

15 Prove or disprove that $\langle p^2 \rangle = \langle p \rangle$ for all $p \in S_m$.

16 Another name for a 2-cycle is a *transposition*. So, a transposition in S_m is a permutation of cycle type $[2, 1^{m-2}], m \geq 2$.

(a) Express $p = (123) \in S_3$ as a product (composition) of two transpositions.

(b) Express $p = (1234) \in S_4$ as a product of three transpositions.

(c) Express $p = (123)(4567) \in S_m (m \geq 7)$ as a product of five transpositions.

(d) Show that every permutation $p \in S_m$ is a product of $m - c(p)$ transpositions, where $c(p)$ is the total number of cycles, including cycles of length 1, in the disjoint cycle factorization of p.

17 Express (12345) as a product of four transpositions in two different ways. (See Exercise 16 for the definition of transposition.)

18 Prove or disprove that every permutation in $S_m, m \geq 3$, is a product (composition) of 3-cycles. (*Hints*: The 3-cycles need not be disjoint; "3-cycles" is not the same as "three cycles".)

19 Suppose $p \in G$, where G is a permutation group of degree m. If $p(x) = y$, show that $G_y p = pG_x$.

20 A permutation $p \in S_m$ is *self-inverse* if $p^{-1} = p$.

(a) Describe, in words, how to identify self-inverse permutations from the Cayley table for S_m.

(b) Describe the possible cycle types for self-inverse permutations.

21 A permutation $p \in S_m$ is *idempotent* if $p^2 = p$. Describe the possible cycle types for the idempotent permutations.

22 Consider the m-cycle $p = (12 \ldots m) \in S_m$. Suppose r is a fixed positive integer, $1 \leq r \leq m$. Show that p^r is a product (composition) of d disjoint cycles each of length m/d, where d is the greatest common divisor of m and r.

23 Let $p \in S_m$, where $m \geq 2$. It can be proved that if p can be written one way as a product of k transpositions and some other way as a product of r transpositions, then $(-1)^k = (-1)^r$. (See Exercise 16 for the definition of "transposition".) In other words, every $p \in S_m$ is either *odd* or *even* depending on whether it can be written as the product of an odd or an even number of transpositions. Let $A_m = \{ p \in S_m : p \text{ is even} \}$.

(a) Prove that A_m is a subgroup of S_m. (It is called the *alternating group* of degree m.)

(b) Prove that the set of odd permutations, $S_m \backslash A_m$, is not a subgroup.

(c) Prove that $S_m \backslash A_m = (12)A_m$ is a coset of A_m.

(d) Prove that $o(A_m) = \frac{1}{2}m!$.

(e) Confirm that A_4 is the group in Exercise 17, Section 3.1.

24 Describe the cycle types of the permutations $p \in S_m$ that satisfy

(a) $p^{-1} = p^2 \neq p$.

(b) $p^{-1} = p^3 \neq p$.

25 Let $p \in S_m$. Prove that the cyclic group $\langle p \rangle$ is the intersection of all subgroups of S_m that contain p.

3.3. BURNSIDE'S LEMMA

> When I am working on a problem I never think about beauty. But when I have finished, if the solution is not beautiful, I know it is wrong.
>
> — Buckminster Fuller

Getting from point a to point b can sometimes be a problem. Consider the case in which $a, b \in V = \{1, 2, \ldots, m\}$. Let G be subgroup of S_m, and suppose the only way to get from a to b is via some permutation $p \in G$ that maps a to b. If G were a transportation system, the ideal situation would be one in which, for any $a, b \in V$, there is a $p \in G$ such that $p(a) = b$. But, few real-life systems are ideal. Take the San Francisco Bay Area, for example, where public transportation is relatively good. If a and b are both in Oakland, an AC-Transit bus will take passengers from point a to point b. If a and b are in San Francisco, MUNI will do the job. Getting from point a in Oakland to point b in San Francisco, however, is another matter. If the system were enlarged to include BART,* there would be no problem. But, anyone restricted to AC-Transit or MUNI would be out of luck.

*The Bay Area Rapid Transit district.

3.3.1 Definition. If G is a permutation group of degree m, then $x, y \in V = \{1, 2, \ldots, m\}$ are *equivalent modulo* G, written

$$x \equiv y \pmod{G} \tag{3.15}$$

if there is a permutation $p \in G$ such that $p(x) = y$.

For the case modeled by Bay Area buses, any two points in Oakland are equivalent, as are any two points in "the City". Without BART, however, no point of Oakland is equivalent to any point in San Francisco. The two cities are in different transit districts or *equivalence classes*, language that depends on the next result.

3.3.2 Theorem. *If G is a permutation group of degree m, then equivalence modulo G is an equivalence relation.*

To prove the theorem, it will be necessary to verify the following: For all $x, y, z \in V = \{1, 2, \ldots, m\}$,

1. $x \equiv x \pmod{G}$.

2. $x \equiv y \pmod{G} \Rightarrow y \equiv x \pmod{G}$.

3. $x \equiv y \pmod{G}$ and $y \equiv z \pmod{G} \Rightarrow x \equiv z \pmod{G}$.

Proof of Theorem 3.3.2. By Corollary 3.2.12, $e_m \in G$. Because $e_m(x) = x, 1 \leq x \leq m$, criterion 1 is verified.

If $x \equiv y \pmod{G}$, there is a permutation $p \in G$ such that $p(x) = y$. By Corollary 3.2.12, $p^{-1} \in G$. Because $p(x) = y$ if and only if $p^{-1}(y) = x$, criterion 2 is proved.

If $x \equiv y \pmod{G}$ and $y \equiv z \pmod{G}$, there are permutations $f, g \in G$ such that $f(x) = y$ and $g(y) = z$. Because G is closed, $p = gf \in G$. Since $p(x) = gf(x) = g(f(x)) = g(y) = z$, criterion 3 is established. ■

Equivalence classes arising from the action of a permutation group are of fundamental importance in combinatorial enumeration.

3.3.3 Definition. Let G be a permutation group of degree m. Equivalence classes modulo G are called *orbits* of G. The orbit of G containing x is

$$O_x = \{p(x) : p \in G\}. \tag{3.16}$$

In this definition, x and $p(x)$ are numbers. In particular, the orbits of G are subsets, not of G, but of $V = \{1, 2, \ldots, m\}$. From the general theory of equivalence relations, if O_x and O_y overlap at all, they are identical, i.e., *the different orbits of G comprise a partition of V.* In the bus metaphor, the orbit of a point in San Francisco is the entire city, and the San Francisco orbit is disjoint from the Oakland orbit.

3.3.4 Example. If $G = \{e_4, (12), (34), (12)(34)\}$, then $O_1 = \{p(1) : p \in G\} = \{1, 2, 1, 2\}$, multiplicities included. Eliminating repetitions, $O_1 = \{1, 2\}$. Because

$2 \in O_1$, it follows from the general theory that $O_2 = O_1$. This can, of course, be confirmed directly: $O_2 = \{p(2) : p \in G\} = \{2, 1, 2, 1\}$, multiplicities included. Similarly $O_3 = \{3, 4\} = O_4$. (Check it.)

It is important to distinguish the subset $\{3, 4\}$ from the cycle (34), and the orbit $O_1 = \{1, 2\}$ from the stabilizer subgroup $G_1 = \{e_4, (34)\}$. Whereas the orbit $O_x \subset \{1, 2, \ldots, m\}$, the stabilizer subgroup $G_x \subset G \subset S_m$. In particular, O_x is a set of numbers and G_x is a set of permutations.

Equivalence modulo $H = \{e_4, (12)(34), (13)(24), (14)(23)\}$ is trivial. There is only one orbit, namely, $O_1 = O_2 = O_3 = O_4 = \{1, 2, 3, 4\}$. (Check it.) Ironically, what is *trivial* for permutation groups is *ideal* for transportation systems. Equivalence modulo H is trivial because, for all $a, b \in \{1, 2, 3, 4\}$, there is a permutation in H that maps a to b. As we will soon see, however, permutation groups affording trivial equivalence relations are, themselves, anything but trivial. □

3.3.5 Definition. Let G be a permutation group of degree m. Then G is *transitive* if it has only one orbit, i.e., if for every choice of x and y in $V = \{1, 2, \ldots, m\}$ there exists a permutation $p \in G$ such that $p(x) = y$.

3.3.6 Example. While the group

$$H = \{e_4, (12)(34), (13)(24), (14)(23)\},$$

from Example 3.3.4, is transitive, the group

$$K = \{e_5, (12)(34), (13)(24), (14)(23)\}$$

is not. The difference, of couse, is a matter of degree. Being of degree 4, the single orbit of H is $O_1 = O_2 = O_3 = O_4 = \{1, 2, 3, 4\}$. Because it is of degree 5, the orbits of K are $O_1 = O_2 = O_3 = O_4 = \{1, 2, 3, 4\}$ and $O_5 = \{5\}$.

Perhaps the easiest way to see that S_m is transitive is via sequence notation. Suppose $i, j \in V = \{1, 2, \ldots, m\}$. If $f = (f(1), f(2), \ldots, f(m)) \in F_{m,m}$, then $f(i)$ is the number in the ith component of the sequence. With j occupying that position, there are $(m-1)!$ permutations $f \in S_m$ map i to j. □

3.3.7 Lemma. *Let G be a permutation group of degree m. If $x \in \{1, 2, \ldots, m\}$, then the number of elements in the orbit to which x belongs is*

$$o(O_x) = \frac{o(G)}{o(G_x)}. \tag{3.17}$$

Proof. The set $O_x = \{p(x) : p \in G\}$ appears to contain $o(G)$ elements but, as we saw in Example 3.3.4, this includes the multiplicities that arise when $p_1(x) = y = p_2(x)$ for two different permutations $p_1, p_2 \in G$. However, from Theorem 3.2.18, if $f(x) = y$, then $\{p \in G : p(x) = y\} = fG_x$. Hence, as p runs through G, y occurs as the value of $p(x)$ exactly $o(fG_x)$ times. Moreover, by Equation (3.14), the multiplicity $o(fG_x) = o(G_x)$ is the same for every $y \in O_x$. ■

Having counted the elements in each orbit, how hard can it be to count the number of orbits? If every orbit had the same size, counting them would be as easy as dividing m by $o(O_x)$ for some fixed but arbitrary $x \in \{1, 2, \ldots, m\}$. However, orbits need not have the same size. (See, e.g., Example 3.3.6, where the orbits of K are $O_1 = \{1, 2, 3, 4\}$ and $O_5 = \{5\}$.)

There is, in fact, a *beautiful* way to calculate the number of orbits of a permutation group, a method that is as powerful as it is unexpected. The significance of this result may justify a brief anecdote about its history.

William Burnside (1852–1927) published the lemma in his 1897 book on finite groups, along with a footnote citing an 1887 article by Georg Frobenius (1849–1917) as its source. When the footnote was inadvertently omitted from the book's second edition, the result came to be known as "Burnside's lemma". In fact, the same idea had appeared even earlier in an 1847 article by Cauchy (1789–1857).* Before we can state this famous result, one more bit of notation is needed.

3.3.8 Definition. Denote by $F(p)$ *the number of fixed points* of $p \in S_m$.

3.3.9 Burnside's Lemma. *Let G be a permutation group with a total of t orbits. Then t is the average of the numbers of fixed points of the permutations in G. That is,*

$$\frac{1}{o(G)} \sum_{g \in G} F(g) = t. \tag{3.18}$$

3.3.10 Example. For the group $H = \{e_4, (12)(34), (13)(24), (14)(23)\}$, from Example 3.3.6, $F(e_4) = 4$, and $F((12)(34)) = F((13)(24)) = F((14)(23)) = 0$. Because the average of these four numbers is $1, H$ has just one orbit, confirming that it is transitive.

If $K = \{e_5, (12)(34), (13)(24), (14)(23)\}$, then $F(e_5) = 5$, and $F((12)(34)) = F((13)(24)) = F((14)(23)) = 1$. (This would be a natural time to have misgivings about suppressing 1-cycles.) The average of these numbers of fixed points is $(5 + 1 + 1 + 1)/4 = 2$, consistent with our observation in Example 3.3.6 that K partitions $\{1, 2, 3, 4, 5\}$ into two orbits. □

3.3.11 Example. Because S_m is transitive, it has just one orbit. It follows from Brunside's lemma that, on average, the permutations of S_m have one fixed point. (Recall from Section 2.3 that the fraction of permutations in S_m having exactly one fixed point is something else entirely.)

In $S_3, F(e_3) = 3, F(12) = F(13) = F(23) = 1$, and $F(123) = F(132) = 0$. So (as predicted),

$$[3 + 1 + 1 + 1 + 0 + 0]/6 = 1. \qquad \square$$

*For more details, see Peter M. Neumann, A lemma that is not Burnside's *Math. Scientist* 4 (1979), 133–141.

Proof of Burnside's Lemma. Define $S = \{(g,j) : g \in G \text{ and } g(j) = j\}$. Then S is the set of all ordered pairs (g,j) in which j is a fixed point of g. Because $F(g)$ of these ordered pairs begin with g,

$$o(S) = \sum_{g \in G} F(g). \tag{3.19}$$

On the other hand, exactly $o(G_j)$ permutations of G fix j. Therefore,

$$\begin{aligned} o(S) &= \sum_{j=1}^{m} o(G_j) \\ &= \sum_{j=1}^{m} \frac{o(G)}{o(O_j)}, \end{aligned} \tag{3.20}$$

by a rearrangement of Equation (3.17).

Let $C_1, C_2, \ldots, C_t$ be the distinct orbits of G, so that $O_j \in \{C_1, C_2, \ldots, C_t\}, 1 \le j \le m$. Then, continuing from Equation (3.20),

$$o(S) = o(G) \sum_{i=1}^{t} \sum_{j \in C_i} \frac{1}{o(C_i)}.$$

Note that, in the second of these summations, $1/o(C_i)$ is added to itself $o(C_i)$ times, i.e.,

$$\begin{aligned} o(S) &= o(G) \sum_{i=1}^{t} \frac{o(C_i)}{o(C_i)} \\ &= to(G). \end{aligned} \tag{3.21}$$

Comparing Equations (3.19) and (3.21) completes the proof. ■

3.3.12 Corollary. *If G is a subgroup of S_m, then*

$$\frac{1}{o(G)} \sum_{g \in G} F(g) \ge 1 \tag{3.22}$$

with equality if and only if G is transitive.

Proof. Because $t = 1$ if and only if G is transitive, the result is an immediate consequence of Equation (3.18). ■

3.3.13 Example. From Example 3.3.4, the orbits of $G = \{e_4, (12), (34), (12)(34)\}$ are $\{1,2\}$ and $\{3,4\}$. Averaging the fixed points of the permutations in G yields $\frac{1}{4}(4+2+2+0) = 2 > 1$, confirming that G is not transitive. □

A subgroup G of S_m is *doubly* transitive if, for all $x_1, x_2, y_1, y_2 \in \{1, 2, \ldots, m\}$, where $x_1 \neq x_2$ and $y_1 \neq y_2$, there is a permutation $p \in G$ such that $p(x_1) = y_1$ *and* $p(x_2) = y_2$.

This definition looks complicated, in part, because of technical considerations: If $x_1 \neq x_2$ but $y_1 = y_2$, then *no* one-to-one function could send x_1 to y_1 and x_2 to y_2; if $x_1 = x_2$ but $y_1 \neq y_2$, then *no function* could send x_1 to y_1 and x_2 to y_2. Informally, G is doubly transitive if, for all appropriate sequences $x = (x_1, x_2)$ and $y = (y_1, y_2)$, there is a permutation $p \in G$ that maps x to y.

Would it surprise you to learn that, if $m \geq 2$, then

$$\frac{1}{o(G)} \sum_{g \in G} F(g)^2 \geq 2 \tag{3.23}$$

with equality if and only if G is doubly transitive? It is hard to look at Inequalities (3.22)–(3.23) and not conjecture that, if $m \geq 3$, then the average over $g \in G$ of $F(g)^3$ is not less than 3 with equality if and only if G is *triply* transitive.

Let's test this hypothesis. The numbers of fixed points of the permutations in S_3 are listed in Example 3.3.11. The average of their third powers is $\frac{1}{6}(3^3 + 1^3 + 1^3 + 1^3 + 0^3 + 0^3) = \frac{30}{6} = 5$. Five? What happened to 3? Maybe we glided too nimbly over the details of what "triply transitive" might mean. If S_3 turns out not to be triply transitive, there is still hope for the conjecture. On the other hand, maybe the correct lower bound is not 3 but 5. (After all, $1, 2, 3, \ldots$ is not the only sequence of positive integers.) Before doing anything else, let's give a proper definition of multiple transitivity.

3.3.14 Definition. Let G be a subgroup of S_m. Suppose $1 \leq r \leq m$. Then G is *r-fold transitive* if, for all one-to-one functions $f, g \in F_{r,m}$, there exists a permutation $p \in G$ such that $pf = g$.

Using one-to-one functions enormously simplifies the *statement* of Definition 3.3.14. To see what it *means*, recall that $f = (x_1, x_2, \ldots, x_r) \in F_{r,m}$ is one-to-one if and only if the x's are all different. Thus, G is r-fold transitive if and only if, for each of the $P(m, r)^2$ ways to choose one-to-one functions $f = (x_1, x_2, \ldots, x_r)$ and $g = (y_1, y_2, \ldots, y_r)$ from $F_{r,m}$, there is a permutation $p \in G$ such that

$$p(x_i) = p(f(i)) = pf(i) = g(i) = y_i, \qquad 1 \leq i \leq r.$$

In other words, G is r-fold transitive if and only if, for any of the $P(m, r)^2$ ways to choose (without replacement, where order matters) sequences of distinct integers $(x_1, x_2, \ldots, x_r)$ and $(y_1, y_2, \ldots, y_r)$ from $\{1, 2, \ldots, m\}$, there exists a $p \in G$ such that, simultaneously, $p(x_1) = y_1, p(x_2) = y_2, \ldots$, and $p(x_r) = y_r$.

Evidently, "transitive" is the same as "1-fold transitive" and "doubly transitive" is the same as "2-fold transitive". Moreover, every $(r + 1)$-fold transitive group is r-fold transitive.

3.3.15 Example. Recall that $H = \{e_4, (12)(34), (13)(24), (14)(23)\}$ is transitive. Suppose $(x_1, x_2) = (1, 2)$ and $(y_1, y_2) = (2, 3)$. The only permutation in H that maps $x_1 = 1$ to $y_1 = 2$ is $p = (12)(34)$. Because $p(2) \neq 3$, no permutation in H simultaneously sends x_1 to y_1 *and* x_2 to y_2, i.e., H is not doubly transitive.

What about S_4? Any function in $F_{4,4}$ of the form $(2, 3, r, s)$ maps $x_1 = 1$ to $y_1 = 2$ and $x_2 = 2$ to $y_2 = 3$. Two of these functions are permutations, namely, $p_1 = (2, 3, 1, 4)$ and $p_2 = (2, 3, 4, 1)$. (In disjoint cycle notation, $p_1 = (123)$ and $p_2 = (1234)$.) More generally, if $f, g \in F_{r,m}$ are fixed but arbitrary one-to-one functions, then $(m - r)!$ permutations $p \in S_m$ satisfy $pf = g$. In particular, S_m is r-fold transitive, $1 \leq r \leq m$. (Compare with the last part of Example 3.3.6.) □

Consider another example. Suppose G is permutation group of degree $m \geq 2$. Let $j \in V = \{1, 2, \ldots, m\}$ be fixed but arbitrary. Because $p(j) = j$ for all p in the stabilizer subgroup G_j, the set $\{j\}$ is an orbit of G_j. Thus, G_j is not transitive. Suppose, however, we ignore the orbit $\{j\}$ and think of G_j as a permutation group of degree $m - 1$ acting on

$$\begin{aligned} V_j &= V \backslash \{j\} \\ &= \{1, 2, \ldots, j-1, j+1, \ldots, m\}. \end{aligned}$$

If G is $(r + 1)$-fold transitive on V, then G_j is r-fold transitive on V_j. This observation even has a partial converse.

3.3.16 Lemma. *Let G be a permutation group of degree $m \geq 3$. Let $V = \{1, 2, \ldots, m\}$, and suppose $1 \leq r < m$. If the stabilizer subgroup G_j is r-fold transitive on $V_j = V \backslash \{j\}, 1 \leq j \leq m$, then G is $(r + 1)$-fold transitive on V.*

Proof. Let $(x_1, x_2, \ldots, x_{r+1})$ and $(y_1, y_2, \ldots, y_{r+1})$ be two one-to-one functions in $F_{r+1,m}$. Because $m \geq 3$, there is some $t \in V$ such that $x_1 \neq t \neq y_1$. By hypothesis, there is a permutation $f \in G_t$ such that $f(x_1) = y_1$. Suppose $f(x_k) = z_k, 2 \leq k \leq r + 1$. Since f is one-to-one, and the y's are all different, $z_k \neq y_1 \neq y_k$, $2 \leq k \leq r + 1$. So, another application of the hypothesis yields a permutation $g \in G_{y_1}$ such that $g(z_k) = y_k, 2 \leq k \leq r + 1$. If $p = gf$, then $p(x_1) = g(f(x_1)) = g(y_1) = y_1$, and $p(x_k) = g(f(x_k)) = g(z_k) = y_k, 2 \leq k \leq r + 1$, i.e., $p \in G$ and $p(x_k) = y_k, 1 \leq k \leq r + 1$. ■

Let's return to our conjecture based on Inequalities (3.22) and (3.23). Because S_3 is 3-fold transitive, the only way to salvage the conjecture is by replacing the lower bound with 5. All right. Suppose, we could prove the modified conjecture. Then, what comes after 5?

3.3.17 Example. Let's see what we get when we average the fourth powers of the numbers of fixed points of the permutations in a 4-fold transitive group, e.g.,

$$\frac{1}{4!} \sum_{g \in S_4} F(g)^4.$$

The cycle types of the permuations in S_4 are $[4]$, $[3,1]$, $[2^2]$, $[2,1^2]$, and $[1^4]$. Permutations with cycle types $[4]$ and $[2^2]$ don't have fixed points. There are $P(4,3)/3 = [4 \times 3 \times 2]/3 = 8$ permutations of cycle type [3,1] each of which has one fixed point. Permutations of type $[2,1^2]$ have two fixed points, and there are $C(4,2) = 6$ of these. Finally, e_4 has four fixed points. So,

$$\begin{aligned}\frac{1}{4!}\sum_{g\in S_4} F(g)^4 &= \tfrac{1}{24}[8 \times 1^4 + 6 \times 2^4 + 4^4] \\ &= \tfrac{1}{24}[8 + 96 + 256] \\ &= \tfrac{360}{24} = 15.\end{aligned}$$

□

If there is a theorem here, it involves the sequence

$$1, 2, 5, 15, \ldots$$

Amazingly enough, that sequence is familiar. The first four terms, at least, are Bell numbers, sums of Stirling numbers of the second kind.

3.3.18 Theorem. *Let G be a permutation group of degree m. If $1 \le r \le m$, then*

$$\frac{1}{o(G)}\sum_{g\in G} F(g)^r \ge B_r,$$

the rth Bell number, with equality if and only if G is r-fold transitive.

Proof. The proof is by induction on r. The $r = 1$ case having already been established in Corollary 3.3.12, we may assume $r \ge 2$. If $m = 2$, then $G = S_2$ or $G = \{e_2\}$. As the result is easily seen to be valid in both of these cases, we may assume $m \ge 3$.

As in the proof of Burnside's lemma, a certain set is counted in two different ways. Let

$$T = \{(g, i_1, i_2, \ldots, i_r) : g \in G \quad \text{and} \quad g(i_k) = i_k, 1 \le k \le r\}.$$

By the fundamental counting principle, $F(g)^r$ of the elements of T begin with g. Thus,

$$o(T) = \sum_{g\in G} F(g)^r.$$

Any element of T that ends with $j = i_r$ must begin with a permutation $g \in G_j$. By the fundamental counting principle, there are $F(g)^{r-1}$ ways to choose the intermediate $r - 1$ entries. Therefore,

$$o(T) = \sum_{j=1}^{m}\sum_{g\in G_j} F(g)^{r-1}.$$

Setting these two different-looking values of $o(T)$ equal to each other produces

$$\sum_{g\in G} F(g)^r = \sum_{j=1}^{m} \sum_{g\in G_j} F(g)^{r-1}. \tag{3.24}$$

Of course, every $g \in G_j$ has at least one fixed point, namely j. Let $F_1(g) = F(g) - 1$. Then, for $g \in G_j, F_1(g)$ is the number of fixed points of the restriction of g to

$$V_j = \{1, 2, \ldots, j-1, j+1, \ldots, m\}.$$

Substituting $F(g) = F_1(g) + 1$ in Equation (3.24) produces

$$\begin{aligned}
\sum_{g\in G} F(g)^r &= \sum_{j=1}^{m} \sum_{g\in G_j} [F_1(g) + 1]^{r-1} \\
&= \sum_{j=1}^{m} \sum_{g\in G_j} \sum_{k=0}^{r-1} C(r-1,k) F_1(g)^k \\
&= \sum_{j=1}^{m} \sum_{k=0}^{r-1} C(r-1,k) \sum_{g\in G_j} F_1(g)^k \\
&\geq \sum_{j=1}^{m} o(G_j) \sum_{k=0}^{r-1} C(r-1,k) B_k \\
&= B_r \sum_{j=1}^{m} o(G_j)
\end{aligned} \tag{3.25}$$

by the binomial theorem, induction, and the Bell recurrence relation (Theorem 2.2.7). Moreover, by the induction hypothesis, equality holds in Equation (3.25) if and only if G_j is $(r-1)$-fold transitive for all j, if and only if (Lemma 3.3.16) G is r-fold transitive. Finally, by Equations (3.20) and (3.21), $\sum_{j=1}^{m} o(G_j) = to(G) \geq o(G)$, with equality if and only if $t = 1$, if and only if G is transitive. Because an r-fold transitive group is transitive, the proof is complete. ■

The ability of mathematicians to list all finite doubly transitive permutation groups* has robbed Theorem 3.3.18 of one application, but there are others. Recall the enumeration in Section 2.3 of the permutations in S_m that have exactly k fixed points: There are $C(m,k)$ ways to choose the numbers to be fixed and $D(m-k)$ ways to derange the remaining $m-k$ numbers. Therefore,

$$\sum_{g\in S_m} F(g)^r = \sum_{k=1}^{m} C(m,k) D(m-k) k^r,$$

*See, e.g., P. J. Cameron, Permutation groups, Chapter 12 in *Handbook of Combinatorics* (R. L. Graham, M. Grötschel, and L. Lovász, Eds., MIT Press, Cambridge, MA, 1995. From the list of doubly transitive groups, the r-fold transitive groups ($r \geq 2$) can be determined by inspection. In particular, the only 6-fold transitive groups are $S_m (m \geq 6)$ and $A_m (m \geq 8)$, where A_m is the alternating group of even permutations found in Exercise 23, Section 3.2.

where $D(0) = 1$. If $r \leq m$ then, from Theorem 3.3.18,

$$\begin{aligned} B_r &= \frac{1}{m!} \sum_{g \in S_m} F(g)^r \\ &= \sum_{k=1}^{m} \frac{D(m-k)k^r}{(m-k)!\,k!}, \end{aligned} \tag{3.26}$$

a formula for the Bell numbers in terms of the derangement numbers. There is more. From Equation (2.18) in Section 2.3, $D(m-k)/[(m-k)!] = \sum_{t=0}^{m-k} (-1)^t/t!$. Therefore,

$$B_r = \sum_{k=1}^{m} \frac{k_r}{k!} \sum_{t=0}^{m-k} \frac{(-1)^t}{t!}.$$

Since this identity is valid for all $m \geq r$, we may as well let m go to infinity.* Because

$$\lim_{m \to \infty} \sum_{t=0}^{m-k} \frac{(-1)^t}{t!} = \frac{1}{e},$$

it follows that

$$B_r = \frac{1}{e} \sum_{k=1}^{\infty} \frac{k^r}{k!}, \tag{3.27}$$

a formula due to G. Dobinski.†

Further applications of Burnside's Lemma depend upon the notion of a symmetry group, the topic of the next section.

3.3. EXERCISES

1 Let $G = \{e_4, (23), (14), (14)(23)\}$. Exhibit O_x when

(a) $x = 1$ **(b)** $x = 2$ **(c)** $x = 3$.

2 Let $G = \langle (123)(45) \rangle \subset S_5$.

(a) Exhibit G_x when $x = 3$.

(b) Exhibit O_x when $x = 3$.

(c) Confirm that $o(O_3) = o(G)/o(G_3)$.

*This involves questions of convergence, bringing us to the boundary between combinatorics and analysis.

†G. Dobinski, *Grunert's Arch.* 61 (1877), 333–336.

(d) Exhibit G_5.

(e) Exhibit O_5.

(f) Confirm that $o(O_5) = o(G)/o(G_5)$.

(g) Compute the average of the numbers of fixed points of the permutations in G.

3 Let $G = \{e_4, (1234), (1432), (13), (24), (12)(34), (13)(24), (14)(23)\} \subset S_4$.

(a) Prove that the group G is transitive, directly from the definition.

(b) Prove that G is transitive by averaging numbers of fixed points.

(c) Is G doubly transitive?

4 What are the orbits of the cyclic group

(a) $\langle (123)(45) \rangle \subset S_5$? **(b)** $\langle (123)(45) \rangle \subset S_6$?

(c) $\langle (1234) \rangle \subset S_4$? **(d)** $\langle (1234) \rangle \subset S_8$?

5 Average the numbers of fixed points in the cyclic group

(a) $\langle (123)(45) \rangle \subset S_5$. **(b)** $\langle (123)(45) \rangle \subset S_6$.

(c) $\langle (1234) \rangle \subset S_4$. **(d)** $\langle (1234) \rangle \subset S_8$.

6 Average $F(g)^2$ as g runs over the cyclic group

(a) $\langle (123)(45) \rangle \subset S_5$. **(b)** $\langle (123)(45) \rangle \subset S_6$.

(c) $\langle (1234) \rangle \subset S_4$. **(d)** $\langle (1234) \rangle \subset S_8$.

7 Let $A_4 = \{e_4, (123), (124), (132), (134), (142), (143), (234), (243), (12)(34), (13)(24), (14)(23)\} \subset S_4$.

(a) Find the number of orbits of A_4 using Burnside's lemma.

(b) Use Inequality (3.23) to show that A_4 is doubly transitive.

(c) Use Theorem 3.3.18 to decide whether A_4 is 3-fold transitive.

8 Confirm the validity of Theorem 3.3.18 when $r = m = 2$.

9 Let G be a permutation group of degree m.

(a) If G is transitive, prove that $o(G_x) = o(G_y)$ for all $x, y \in \{1, 2, \ldots, m\}$.

(b) Prove that G is transitive if and only if the following condition is satisfied: For every $x \in \{1, 2, \ldots, m\}$, there exists a permutation $p \in G$ such that $p(1) = x$.

10 Let $G = \{e_2\}$. Show that G_j is transitive on $\{1, 2\} \backslash \{j\}$ for each $j \in \{1, 2\}$ and yet G is not doubly transitive.

11 By a direct computation along the lines of Example 3.3.17, confirm that

(a) $\frac{1}{24} \sum_{g \in S_4} F(g)^r = B_r, \ 1 \leq r \leq 3$.

(b) $\frac{1}{120} \sum_{g \in S_5} F(g)^r = B_r, 1 \leq r \leq 5$.

12 By evaluating the right-hand side, confirm that

(a) $B_3 = \sum_{k=1}^{3} \frac{k^3}{k!} \sum_{t=0}^{3-k} \frac{(-1)^t}{t!}$. **(b)** $B_3 = \sum_{k=1}^{6} \frac{k^3}{k!} \sum_{t=0}^{6-k} \frac{(-1)^t}{t!}$.

13 How close is $(1/e)\sum_{k=1}^{6}(k^3/k!)$ to $B_3 = 5$?

14 Hugh Edgar pointed out that the conclusion of Theorem 3.3.18 does not follow without the hypothesis $r \leq m$. Show that

(a) $\frac{1}{24}\sum_{g\in S_4} F(g)^5 = B_5 - 1$.

(b) $\frac{1}{120}\sum_{g\in S_5} F(g)^6 = B_6 - 1$.

15 Let G be a subgroup of S_m. Prove that

$$\frac{1}{o(G)}\sum_{g\in G} F(g)^{m+1} \geq B_{m+1} - 1$$

with equality if and only if $G = S_m$.

16 Denote by $D_{r,m}$ the subset of $F_{r,m}$ consisting of all $P(m,r)$ one-to-one functions. For each $p \in S_m$, denote by $\hat{p} : D_{r,m} \to D_{r,m}$ the *induced action* of p on $D_{r,m}$ defined by $\hat{p}(f) = p \circ f$, $f \in D_{r,m}$.

(a) Show that $\hat{p}\hat{q} = \widehat{pq}$ for all $p, q \in S_m$.

(b) Suppose G is a subgroup of S_m. Explain why $\hat{G} = \{\hat{p} : p \in G\}$ can be viewed as a subgroup of $S_{P(m,r)}$.

(c) Prove that G is an r-fold transitive subgroup of S_m if and only if $\hat{G}$ acts transitively on $D_{r,m}$.

17 Let G be a transitive permutation group of degree $m > 1$. Prove that G contains a derangement.

18 A permutation group G of degree m is *semiregular* if $G_x = \{e_m\}$ for all $x \in V = \{1, 2, \ldots, m\}$.

(a) If G is semiregular, prove that $o(O_x) = o(G)$ for every $x \in V$.

(b) If G is a semiregular permutation group of degree m, prove that $o(G)|m$, i.e., that the cardinality of G exactly divides its degree.

(c) Suppose G is a transitive permutation group of degree m. Prove that G is semiregular if and only if $o(G) = m$. (A transitive semiregular permutation group is said to be *regular*.)

19 Let G be an r-fold transitive permutation group of degree m. Prove or disprove that $P(m,r)|o(G)$, i.e., that $o(G)$ is some integer multiple of the product $m(m-1)\cdots(m-r+1)$.

20 Let G be a permutation group of degree m. Suppose $x, y \in V = \{1, 2, \ldots, m\}$. Define $H = G_x$, the stabilizer subgroup of x. Then, both G and H partition V into a disjoint union of orbits. For the purposes of this exercise only, denote by Gx (not to be confused with G_x) the orbit of G to which x belongs and by Hy the orbit of $H = G_x$ to which y belongs. Prove that

$$o(G) = o(Gx)o(Hy)o(H_y),$$

where $H_y = \{p \in G_x : p(y) = y\} = \{p \in G : p(x) = x \text{ and } p(y) = y\}$.

3.4. SYMMETRY GROUPS

Permutation groups arise naturally in discussions of symmetry. Imagine the square in Fig. 3.4.1*a* drawn on a sheet of plain paper which is then passed through a copy machine to produce an overhead projection transparency. If the transparency were aligned on top of the paper, so that the two squares were superimposed, you would see what appeared to be a single square. However, if the point of a compass were placed at the intersection of the diagonals of that square and (just) the transparency rotated 36 degrees in the clockwise direction, you would see two overlapping squares. Therefore, a 36° clockwise rotation is *not* a symmetry of the square. Had the transparency been rotated exactly 90°, the squares again would be superimposed, and again you would see what appeared to be just one square. Thus, a 90° clockwise rotation *is* a symmetry of the square.

It would be useful to have a list of the different symmetries of a square. This requires us to be a little more precise about what we mean by a *symmetry* and a lot more precise about what we mean by *different*.

Suppose the vertices of the square in Fig. 3.4.1*a* are numbered, as shown in Fig. 3.4.1*b*. Never mind that a 90° rotation is not a symmetry of the labeled figure. The labels are only there to facilitate our discussion. While they rotate with the square, they are not part of it. (Since we are imagining things anyway, feel free to imagine that the numbers are transparent.

A 90° clockwise rotation acts as a permutation of the vertices. Vertex 1 is sent to the position formerly occupied by vertex 2, vertex 2 goes to the place previously held by vertex 4, and so on. It seems natural to associate the permutation $p = (1243)$ with a 90° clockwise rotation.

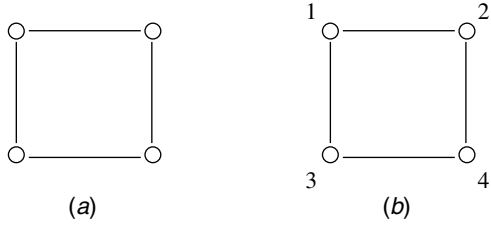


Figure 3.4.1

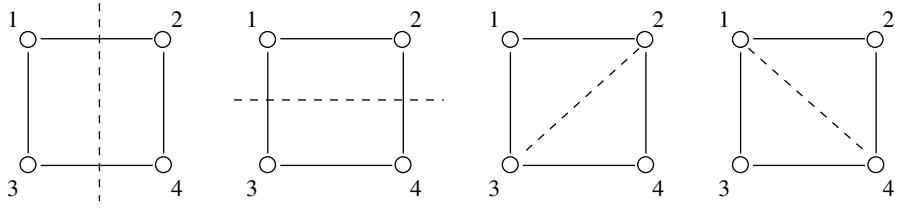


Figure 3.4.2

What about a 90° counterclockwise rotation? That corresponds to $q = (1342)$, the same permutation associated with a *clockwise* rotation of 270°! To be a symmetry, what matters is where the figure ends up, not the route it took getting there. Two symmetries are the same if and only if they afford the same permutation. A 90° counterclockwise rotation and a 270° clockwise rotation are different geometric routes to the same symmetry.

Because each symmetry of the square corresponds to a unique permutation of its vertices, we may as well use permutations as convenient descriptive names for symmetries. (Be careful. This discussion is taking place in the context of some fixed but arbitrary numbering of the vertices. While the symmetries may not depend on these numbers, their permutation names will.)

Just four symmetries come from rotating the square around the compass point, i.e., about an axis through its center, perpendicular to the square. They are (1243), (1342), (14) (23), and e_4. (The 360° rotation and the 0° rotation are two routes to the symmetry whose permutation name is e_4.) Four more symmetries arise from rotations about axes that lie in the plane of the square. (See Fig. 3.4.2.)

With respect to the vertex numbering of Fig. 3.4.1*a*, the set of all symmetries of the square is

$$D_4 = \{e_4, (1243), (14)(23), (1342), (12)(34), (13)(24), (14), (23)\}. \tag{3.28}$$

Many remarkable things can be said about D_4, none of which address the question that seems to be foremost in people's minds. Let's deal with that issue first. Why is it called D_4? Here are some responses: (1) It had to be called something; (2) "D_n" is the name traditionally given to the symmetries of the regular n-gon; (3) "D" stands for *dihedral*, a name that someone once must have thought was descriptive.

Let's talk substance. Perhaps the most obvious substantive thing to be said about D_4 is that it contains 8 permutations. Only one-third of the 24 permutations in S_4 are symmetries of the square. The (painful) effect of applying the permutation (12) to the hapless square is illustrated in Fig. 3.4.3.

What if two symmetries are performed in succession? From the geometric perspective, this process is easy to understand. Following a symmetry with a symmetry produces another symmetry. So far, so good. But which one? How is the

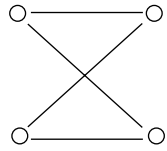
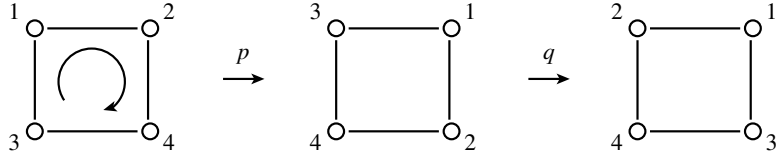


Figure 3.4.3

unique permutation that describes a combination of symmetries related to their individual permutation descriptions?

3.4.1 Example. Suppose we follow 90° clockwise rotation $p = (1243)$ with q, a 180° rotation about an axis through the lower left and upper right-hand corners of the square. Which of the eight elements of D_4 describes the combined symmetry?



Vertex 1 is sent by p to the position formerly occupied by vertex 2, a location on the axis of rotation of $q = (14)$. Since q fixes a vertex in that position, the combination of p followed by q sends 1 to 2. Note that it is not the number of vertex 1 that determines where it is sent by symmetry $q = (14)$; it is the number of the *position* that vertex 1 occupies when symmetry q is applied.

Vertex 2 is sent by p to vertex 4's original position, and symmetry q sends a vertex in that place to vertex 1's initial position. Therefore, p followed by q sends 2 to 1. Evidently, (12) is a cyclic in the disjoint cycle factorization of the combined symmetry.

Vertex 3 is sent by p to the initial position of vertex 1, and q sends a vertex in that place to the position originally occupied by vertex 4. Finally, the combined symmetry sends 4 to 3. So, the combination, first $p = (1243)$, then $q = (14)$, yields $(12)(34)$, a 180° rotation about an axis through the midpoints of sides 1—2 and 3—4. □

The most remarkable thing about the process of describing the combined symmetry, first p then q, is that it is identical to the process for computing the composition qp, i.e., $(14) \circ (1243) = (12)(34)$. Let's formalize this discovery.

3.4.2 Theorem. *Let p and q be symmetries of some object F. Then the permutation afforded by the combined symmetry first p then q is the composition qp.*

When we elected to use permutations as convenient descriptive names for symmetries, there was no reason to believe that a combination of symmetries would

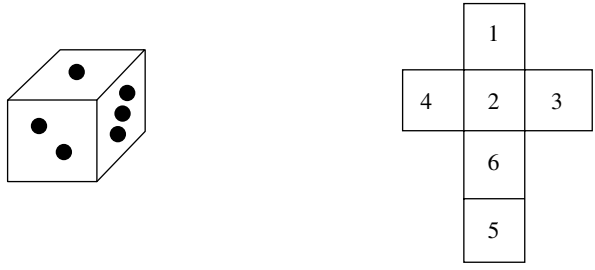


Figure 3.4.4. The numbered faces of a die.

have any connection at all to the composition of their corresponding permutation names. This unexpected relationship has some profound consequences. For one thing, the set of permutations representing the family of all symmetries of an object is closed. In particular, D_4 is more than a subset of S_4, it is a sub*group*.

3.4.3 Definition. Let G be a subgroup of S_m. If it is possible to label some object F in such a way that every element of G is a symmetry of F, then G is a *symmetry group*.

Among the symmetries of the square are those that can be achieved under the constraint that the superimposed transparency remain flat on top of the original. More generally, a *plane symmetry* is one that can be performed entirely within the two-dimensional plane. The plane symmetries of the square comprise a symmetry group, namely $\langle(1243)\rangle = \{e_4, (1243), (14)(23), (1342)\}$. Ironically, these are the symmetries that can be described as rotations about an axis perpendicular to the plane, while the remaining, nonplanar symmetries can all be construed as rotations around axes in the plane. (Nonplanar symmetries can also be visualized as *reflections*.)

Let's consider a real-life example, the cube. It is conventional in "the real world" to number, not the vertices, but the faces of cubes. The standard way to number dice is illustrated in Fig. 3.4.4.

How many symmetries does a cube have? Let's begin with an analogy. The square is a two-dimensional form lying in the plane. It seemed natural to partition the symmetries of the square into two types, planar and nonplanar. The cube is a three-dimensional figure. Its symmetries naturally split between those that can be accomplished entirely within three-dimensional space, and those that cannot. The three-dimensional symmetries are all rotations (of the kind taking place 24/7 in gambling casinos from Atlantic City to Las Vegas). The remaining symmetries are reflections.*

* Just as the nonplanar symmetries of the square can be visualized as rotations through a third dimension, reflections of the cube can be construed as rotations through a fourth dimension. But, we will not make use of this idea. For us, a *rotational symmetry* of the cube is a three-dimensional rotation.

Let't count the *rotational* symmetries of a cube. Any one of the six numbered faces of a die can be rotated to the top. Holding the top and bottom faces with your forefinger and thumb, any one of the four remaining faces can be rotated to the front. Once the top and front faces are specified, the remaining faces are completely determined. So, a cube has $6 \times 4 = 24$ different orientations and, hence, 24 different rotational symmetries.

3.4.4 Example. Let's say a die (numbered as in Fig. 3.4.4) is in *standard position* if face 1 is on top and face 2 is in front. (Then face 6 is on the bottom, and face 5 is in the back.) With the die in standard position, hold the bottom and top faces with your thumb and forefinger and rotate face 2 to the left 90° (that is, clockwise when viewed from the top, looking down on face 1). As face 2 moves, other faces move too. The faces around the "equator" all rotate to new locations. While the squares comprising faces 1 and 6 "experience" a symmetry, they wind up in their original positions. The permutation name for this symmetry is (2453).

Here is another example. (Try to get your hands on a die for this one.) Place your forefinger on vertex $\{1, 2, 3\}$ (at the intersection of faces 1, 2, and 3) and your thumb on vertex $\{4, 5, 6\}$. Rotate face 1 into the position formerly occupied by face 3. This time, all six faces change position. The resulting symmetry is (132)(456).

The complete rotational symmetry group of the cube is shown in Fig. 3.4.5. □

Perhaps it is inconsistent to describe the symmetries of a square as permutations of its *vertices* and the symmetries of a cube as permutations of its *faces*. Why not view the symmetries of a cube as vertex permutations? What difference would it make? The symmetries themselves are independent of whether we *describe* them in terms of faces or vertices, or edges for that matter. One practical sort of difference is that, as permutations of the faces, the symmetries of the cube comprise a subgroup of S_6. As vertex permutations, they form a subgroup of S_8, and as edge permutations, they constitute a subgroup of S_{12}.*

There is some nice geometry associated with expressing the rotational symmetries of a cube as permutations of the vertices. Imagine two congruent, square-based

e_6	(2453)	(16) (24) (35)		
	(1265)	(15) (26) (34)	(132) (456)	(123) (465)
(25) (34)	(1364)	(14) (25) (36)	(153) (246)	(135) (264)
(16) (25)	(2354)	(16) (23) (45)	(124) (365)	(142) (356)
(16) (34)	(1562)	(12) (34) (56)	(145) (263)	(154) (236)
	(1463)	(13) (25) (46)		

Figure 3.4.5. The rotational symmetry group of the cube.

*As abstract groups, these manifestations of the rotational symmetry group of the cube are all isomorphic to S_4.

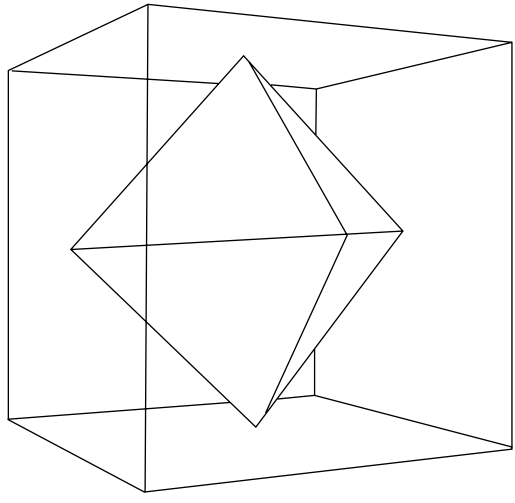


Figure 3.4.6. A regular octahedron inside a cube.

pyramids. The object that results from gluing the square bases together, so that they disappear into the interior, is an *octahedron*. So, an octahedron is a polyhedron with 8 triangular faces, 6 vertices (each surrounded by four faces), and 12 edges. If each of the faces is equilateral, the octahedron is said to be *regular.*

From Fig. 3.4.6, one sees that a regular octahedron will fit inside an appropriately sized cubical box in such a way that each vertex of the octahedron is aligned with the center of the corresponding face of the box (and each vertex of the cube is centered directly above a face of the octahedron). If one of the 24 rotational symmetries of the cube is applied (gently) to the box, the result is also a symmetry of the octahedron inside. In other words, every rotational symmetry of the cube is simultaneously a rotational symmetry of the regular octahedron (and vice versa). The cube and the regular octahedron share the same rotational symmetry group! The manifestation of this group as permutations of the eight vertices of the cube is identical to its manifestation as permutations of the eight faces of the octahedron. Indeed, this group is commonly known to mathematicians as the *octahedral group*.

While this discussion is pleasant enough, it doesn't seem to be getting us any closer to a concrete realization of the octahedral group as a subgroup of S_8. As a step in that direction, let's agree to number the vertices of a die as follows:

$$\begin{array}{llll} \mathbf{1} = \{1,2,3\}, & \mathbf{2} = \{1,2,4\}, & \mathbf{3} = \{1,3,5\}, & \mathbf{4} = \{1,4,5\}, \\ \mathbf{5} = \{2,3,6\}, & \mathbf{6} = \{2,4,6\}, & \mathbf{7} = \{3,5,6\}, & \mathbf{8} = \{4,5,6\}, \end{array} \tag{3.29}$$

where, e.g., $\mathbf{6} = \{2,4,6\}$ means that (**boldface**) number **6** is assigned to the vertex formed by the intersection of the even-numbered faces.

If some symmetry of the cube, manifested as a permutation of its six faces, corresponds to $p \in S_6$ then, as a permutation of the eight vertices of the cube, that same symmetry corresponds to the permutation $\tilde{p} \in S_{\mathbf{8}}$ defined by

$$\tilde{p}(\{i,j,k\}) = \{p(i), p(j), p(k)\}.$$

We will say that $\tilde{p}$ is *induced* by p. If, e.g., $p = (25)(34) \in S_6$, then

$$\begin{aligned} \tilde{p}(\mathbf{1}) &= p(\{1,2,3\}) \\ &= \{p(1), p(2), p(3)\} \\ &= \{1,5,4\} \\ &= \mathbf{4}. \end{aligned} \tag{3.30}$$

Similarly,

$$\begin{aligned} \tilde{p}(\mathbf{4}) &= \tilde{p}(\{1,4,5\}) \\ &= \{p(1), p(4), p(5)\} \\ &= \{1,3,2\} \\ &= \mathbf{1}. \end{aligned} \tag{3.31}$$

Evidently, $(\mathbf{14})$ is a cycle in the disjoint cycle factorization of $\tilde{p}$. In the same way, $\tilde{p}(\mathbf{2}) = \{p(1), p(2), p(4)\} = \{1,5,3\} = \mathbf{3}$, $\tilde{p}(\mathbf{3}) = \{p(1), p(3), p(5)\} = \{1,4,2\} = \mathbf{2}$, and so on. Continuing in this way, we find that $\tilde{p} = (\mathbf{14})(\mathbf{23})(\mathbf{58})(\mathbf{67})$. Notice that $o(\tilde{p}) = 2$, as it should. Because $\tilde{p}$ and $p = (25)(34)$ represent the same symmetry, they have the same order.

3.4.5 Example. As a permutation of die numbered faces, $p = (2453) \in S_6$ is a rotational symmetry of the cube. Before describing its induced action, observe that the least common multiple of the lengths of the disjoint cycles of $\tilde{p}$ is $o(\tilde{p}) = o(p) = 4$. Therefore, every cycle of $\tilde{p}$ has length 2^k, where $0 \leq k \leq 2$. Moreover, at least one cycle of $\tilde{p}$ must have length equal to 4. Let's confirm these deductions:

$$\begin{aligned} \tilde{p}(\mathbf{1}) &= \tilde{p}(\{1,2,3\}) = \{p(1), p(2), p(3)\} = \{1,4,2\} = \mathbf{2}, \\ \tilde{p}(\mathbf{2}) &= \tilde{p}(\{1,2,4\}) = \{p(1), p(2), p(4)\} = \{1,4,5\} = \mathbf{4}, \\ \tilde{p}(\mathbf{4}) &= \tilde{p}(\{1,4,5\}) = \{p(1), p(4), p(5)\} = \{1,5,3\} = \mathbf{3}, \\ \tilde{p}(\mathbf{3}) &= \tilde{p}(\{1,3,5\}) = \{p(1), p(3), p(5)\} = \{1,2,3\} = \mathbf{1}. \end{aligned}$$

So, $(\mathbf{1243})$ is a cycle of $\tilde{p}$. Beginning a new cycle with $\mathbf{5}$,

$$\begin{aligned} \tilde{p}(\mathbf{5}) &= \tilde{p}(\{2,3,6\}) = \{p(2), p(3), p(6)\} = \{4,2,6\} = \mathbf{6}, \\ \tilde{p}(\mathbf{6}) &= \tilde{p}(\{2,4,6\}) = \{p(2), p(4), p(6)\} = \{4,5,6\} = \mathbf{8}, \\ \tilde{p}(\mathbf{8}) &= \tilde{p}(\{4,5,6\}) = \{p(4), p(5), p(6)\} = \{5,3,6\} = \mathbf{7}, \\ \tilde{p}(\mathbf{7}) &= \tilde{p}(\{3,5,6\}) = \{p(3), p(5), p(6)\} = \{2,3,6\} = \mathbf{5}. \end{aligned}$$

So, $\tilde{p} = (\mathbf{1243})(\mathbf{5687})$.

p	$\tilde{p}$	p	$\tilde{p}$
(25)(34)	(**14**) (**23**) (**58**) (**67**)	(2453)	(**1243**) (**5687**)
(16)(25)	(**17**) (**28**) (**35**) (**46**)	(1265)	(**1573**) (**2684**)
(16)(34)	(**16**) (**25**) (**38**) (**47**)	(1364)	(**1562**) (**3784**)
		(2354)	(**1342**) (**5786**)
(132)(456)	(**235**) (**476**)	(1562)	(**1375**) (**2486**)
(153)(246)	(**147**) (**285**)	(1463)	(**1265**) (**3487**)
(124)(365)	(**164**) (**358**)		
(145)(263)	(**167**) (**283**)	(16)(24)(35)	(**18**) (**26**) (**37**) (**45**)
(123)(465)	(**253**) (**467**)	(15)(26)(34)	(**18**) (**27**) (**34**) (**56**)
(135)(264)	(**174**) (**258**)	(14)(25)(36)	(**18**) (**24**) (**36**) (**57**)
(142)(356)	(**146**) (**385**)	(16)(23)(45)	(**15**) (**27**) (**36**) (**48**)
(154)(236)	(**176**) (**238**)	(12)(34)(56)	(**12**) (**36**) (**45**) (**78**)
e_6	$e_{\mathbf{8}}$	(13)(25)(46)	(**13**) (**27**) (**45**) (**68**)

Figure 3.4.7. Two manifestations of the octahedral group.

For each rotational symmetry p, manifested as a permutation of the (die numbered) faces of a cube, the corresponding induced vertex permutation $\tilde{p}$ can be found in Fig. 3.4.7. (Note that $\tilde{p}_1$ and $\tilde{p}_2$ can have the same cycle structure even when p_1 and p_2 do not.) □

3.4.6 Example. Whatever its manifestation, the octahedral group G contains only *some* of the symmetries of the cube, namely, the 24 rotations. What about reflections? Suppose a die in standard position (with face 1 on top and face 2 in front) is laid on a mirror. Imagine the image rising straight up out of the mirror until it is superimposed on the die, with face 6 of the reflection overlapping face 1 of the die, face 1 of the reflection overlapping face 6 of the die, and the remaining faces of the image overlapping the correspondingly numbered faces of the cube. As a permutation of the faces, this reflection is $r = (16) \in S_6$. (Note, e.g., from Fig. 3.4.5, that $r \notin G$.)

Given one reflection, it is easy to generate more. If $p \in G$ is any rotational symmetry, then the composition $q = pr$ is a symmetry. Might q be a rotation? If so, then $r = p^{-1}q \in G$, a contradiction. Since it cannot be a rotation, pr must be another reflection. Because $p_1 r = p_2 r$ if and only if $p_1 = p_2$, the set $Gr = \{pr : p \in G\}$ contains 24 different reflections. Moreover, since the die and its reflected image rotate together, Gr contains all possible reflections, i.e., $H = G \cup Gr$ is the (full) symmetry group of the cube. As permutations of its six faces, all 48 symmetries of the cube are given in Fig. 3.4.8. □

p	$p(16)$	p	$p(16)$
(25) (34)	(16) (25) (34)	(2453)	(16) (2453)
(16) (25)	(25)	(1265)	(15) (26)
(16) (34)	(34)	(1364)	(14) (36)
		(2354)	(16) (2354)
(132) (456)	(145632)	(1562)	(12) (56)
(153) (246)	(124653)	(1463)	(13) (46)
(124) (365)	(153624)		
(145) (263)	(132645)	(16) (24) (35)	(24) (35)
(123) (465)	(154623)	(15) (26) (34)	(1265) (34)
(135) (264)	(142635)	(14) (25) (36)	(1364) (25)
(142) (356)	(135642)	(16) (23) (45)	(23) (45)
(154) (236)	(123654)	(12) (34) (56)	(1562) (34)
e_6	(16)	(13) (25) (46)	(1463) (25)

Figure 3.4.8. The 48 symmetries of the cube.

3.4. EXERCISES

1 Suppose the vertices of the square in Fig. 3.4.1*b* are permuted according to the permutation $p = (13) \in S_4$. Draw a picture of the resulting "twisted" polygon.

2 Let R be a rectangle of length 5 and width 3. Consecutively number its vertices 1–4 in clockwise order.

(a) Use this numbering to write down the group of symmetries of R as permutations of its vertices.

(b) How would the group in part (a) differ from the group of symmetries of R as permutations of its edges?

(c) How sensible is it to discuss the symmetries of R as permutations of its face?

3 Denote by D_3 the group of symmetries of an equilateral triangle as permutations of its vertices.

(a) Show that $D_3 = S_3$.

(b) Which of the six symmetries are plane symmetries?

4 How many symmetries does an isosceles right triangle have? How many of them are plane symmetries?

5 Suppose the vertices of a regular pentagon are consecutively numbered 1–5, in clockwise order. Use this numbering to exhibit

(a) the group of plane symmetries of the pentagon.

(b) D_5, the group of all 10 symmetries of the pentagon.

6 Suppose the vertices of a regular hexagon are consecutively numbered 1–6, in clockwise order. Use this numbering to exhibit

(a) the group of plane symmetries of the hexagon.

(b) D_6, the group of all symmetries of the hexagon.

7 Denote by D_n the group of all symmetries of the regular n-gon. Prove that $o(D_n) = 2n$, $n \geq 3$

8 Recall (Example 3.4.4) that a die is in *standard position* if its top face is numbered 1 and its front face is numbered 2. The symmetry (1265) might be described, in words, as a 90° rotation around an axis through the centers of faces 3 and 4. Similarly, (123) (465) is a 120° rotation around an axis running diagonally through the cube from vertex $\{1, 2, 3\}$ to vertex $\{4, 5, 6\}$. Describe, in words, the symmetry

(a) (16) (25). **(b)** (16) (34).

(c) (16) (24) (35). **(d)** (16) (23) (45).

(e) (1463). **(f)** (154) (236).

9 A regular tetrahedron is a pyramid with a triangular base in which each of the four triangular faces is equilateral. Assign numbers 1–4 to the faces of a regular tetrahedron in some fixed but arbitrary way.

(a) Prove that a regular tetrahedron has 12 rotational symmetries.

(b) Exhibit the rotational symmetries of a regular tetrahedron as a permutation group of degree 4.

10 Prove that the group of all symmetries of a regular tetrahedron is S_4. (See Exercise 9.)

11 The 24 rotational symmetries of a cube expressed as permutations of its vertices can be found in Fig. 3.4.7 (in the columns labeled $\tilde{p}$). Express the remaining 24 symmetries (the reflections) as permutations of the vertices. (*Hint*: Example 3.4.6.)

12 Express the 12 rotational symmetries of a regular tetrahedron (see Exercise 9) as permutations of its six *edges*. (*Hint*: An edge is formed by the intersection of two faces. Unlike a cube, every pair of faces of a tetrahedron meet to form an edge. Number the edges in dictionary order, i.e., $\mathbf{1} = \{1, 2\}, \mathbf{2} = \{1, 3\}, \mathbf{3} = \{1, 4\}, \mathbf{4} = \{2, 3\}, \mathbf{5} = \{2, 4\}$, and $\mathbf{6} = \{3, 4\}$. Let G be the group of rotational symmetries as permutations of the four faces. For each $p \in G$, let $\tilde{p}$ be the natural action induced on the edges, i.e., $\tilde{p}(\{i,j\}) = \{p(i), p(j)\}$. Express $\tilde{G} = \{\tilde{p} : p \in G\}$ as a subgroup of S_6.)

13 Suppose the vertices of a square are numbered, not as shown in Fig. 3.4.1*b*, but in consecutive clockwise order. With respect to this numbering scheme, the permutation names of the elements of D_4 will not be the same as those given in

Equation (3.28). Exhibit their permutation names with respect to this consecutive clockwise numbering scheme.

14 Let G be the rotational symmetry group of the cube expressed as permutations of its (die numbered) faces. For each $p \in G$, let $\tilde{p}$ be the corresponding vertex permutation. If $\tilde{G} = \{\tilde{p} : p \in G\}$, define $f : G \to \tilde{G}$ by $f(p) = \tilde{p}$. (See Fig. 3.4.7.)

(a) Prove that $f(pq) = f(p)f(q), p, q \in G$.

(b) Deduce that $f(p^{-1}) = f(p)^{-1}, p \in G$.

15 Prove that D_4 (Equation (3.28)) is transitive but not doubly transitive

(a) from the definitions and geometric considerations.

(b) using Equations (3.22) and (3.23).

16 Prove that the octahedral group (Fig. 3.4.5) is transitive but not doubly transitive

(a) from the definitions and geometric considerations.

(b) using Inequalities (3.22) and (3.23).

17 In general, a polyhedron is *regular* if each of its faces is congruent to the same regular polygon and each of its vertices is formed by the intersection of the same number of faces. The cube, regular tetrahedron, and regular octahedron are examples of regular polyhedra. (If two regular tetrahedra are glued together so as to make a face of each disappear into the interior of the resulting figure, the outcome is not a regular polyhedron because some vertices are formed by the intersection of three faces and some by four.) The regular *dodecahedron*, illustrated in Fig. 3.4.9*a*, is a regular polyhedron each of whose 12 faces is a regular pentagon.

(a) Prove that a regular dodecahedron has 20 vertices and 30 edges.

(b) Prove that a regular dodecahedron has 60 rotational symmetries.

18 A *fullerene*[*] is a pure carbon molecule, C_n, in which the n carbon atoms sit at the vertices of a polyhedral "cage" whose faces consist of 12 pentagons and $\frac{1}{2}n - 10$ hexagons. The first fullerenes, C_{60} and C_{70}, were isolated in 1990. The smaller version, C_{60}, is in the shape of a (traditional) soccer ball. Also known as a *truncated icosahedron*, each vertex of a soccer ball lies at the intersection of two hexagonal faces and one pentagonal face. (See Fig. 3.4.9*b*.)

(a) Compute the number of hexagonal faces of C_{60}.

(b) Compute the number of edges of a truncated icosahedron.

(c) Compute the number of rotational symmetries of a truncated icosahedron.

(d) In what sense does a truncated icosahedron fail to be a regular polyhedron? (See Exercise 17.)

[*] Named for R. Buckminster Fuller (1895–1983).

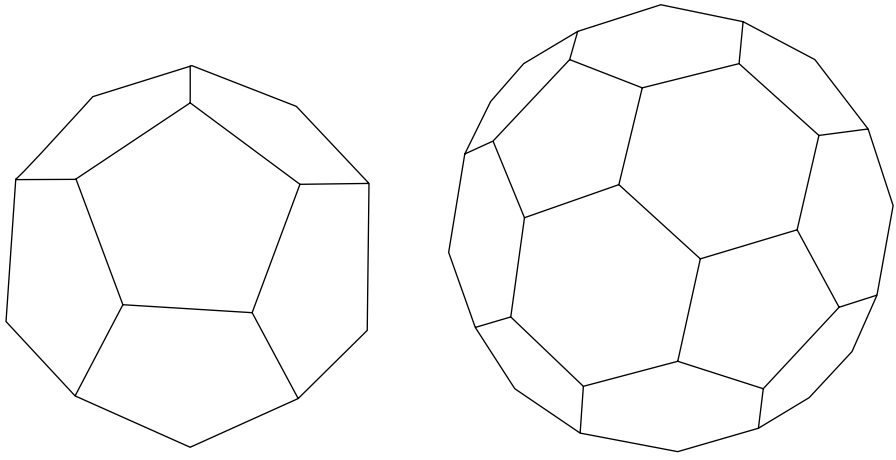


Figure 3.4.9. (*a*) A regular dodecahedron; (*b*) a truncated icosahedron.

19 Prove that no regular polyhedron (see Exercise 17) has hexagonal faces.

20 Prove that there are exactly five regular polyhedra. (*Hint*: Exercise 19.)

21 Leonhard Euler proved that if a convex polyhedron has F faces, E edges, and V vertices, then $F + V = E + 2$. Confirm Euler's formula for a

(a) cube. **(b)** tetrahedron.

(c) octahedron. **(d)** square-based pyramid.

(e) truncated icosahedron (see Exercise 18).

22 Having six square faces and eight equilateral triangular faces, a *cuboctahedron* is carved from a cube by truncating (slicing off) each vertex with a plane that passes through the midpoints of the three edges incident with it.* Every edge of a cuboctahedron has the same length, namely $1/\sqrt{2}$ times the length of an edge of the original cube.

(a) Confirm Euler's formula (Exericse 21) for the cuboctahedron.

(b) Discuss the symmetries of a cuboctahedron.

*Its counterpart, the truncated octahedron, has 8 regular hexagonal faces and 6 equilateral triangular faces. William Thomson, Lord Kelvin (1824–1907), proposed the truncated octahedron as the shape of a space-filling cell that minimizes the ratio of surface area to volume. In 1994, D. Weaire and R. Phelan discovered another cell with 14 faces that improves on Lord Kelvin's by 0.3%. It is not known whether this new cell is optimal.

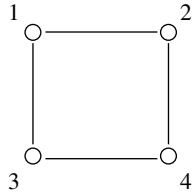


Figure 3.5.1

3.5. COLOR PATTERNS

A mathematician, like a painter or a poet, is a maker of patterns.
— G. H. Hardy

Let's take some of the materials left lying around from our last discussion, e.g., squares and cubes, and recycle them into decorations for Independence Day. We might, e.g., take a square and color its vertices red, white, or blue. With respect to the vertex numbering of Fig. 3.5.1, any such *coloring* can be identified with a unique function $f : \{1, 2, 3, 4\} \to \{r, w, b\}$. Some colorings, along with the matching functions, are given in Fig. 3.5.2.

Surely, it would be going too far to claim that there is room for "artistic expression" in decorating squares. Is there room even for some individuality? How many different colorings are there? Because coloring the vertices of a square involves four decisions, each having three choices, there must be $3^4 = 81$ different colorings. The set C, consisting of all functions $f : \{1, 2, 3, 4\} \to \{r, w, b\}$, contains 81 elements.

Wait a minute. Look carefully at the four colorings illustrated in Fig. 3.5.2. How different will they be after the paint dries and the squares are free to rotate? It seems 81 is the right answer to the wrong question. Let's try to formulate the right question.

Say two colorings (elements of C) are *equivalent* if one can be obtained from the other by a plane rotation of the square. This relation partitions C into equivalence classes; let's call them color *patterns*. The four colorings in Fig. 3.5.2, e.g., comprise a single color pattern. The right question is, how many color patterns are there?

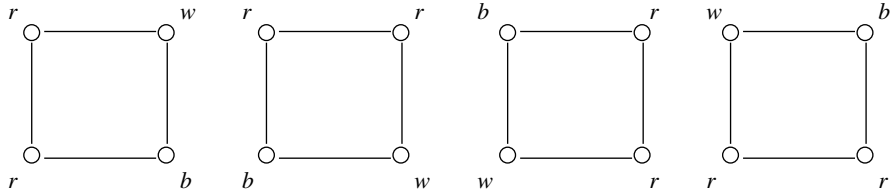


Figure 3.5.2

Before we can count color patterns, we need to understand the relation a little better. Consider, e.g., f_1 and f_2 in Fig. 3.5.2. Geometrically, the *coloring* f_2 can be obtained from f_1 by a 90° rotation. With respect to the vertex numbering of Fig. 3.5.1, this is the symmetry whose permutation name is $p = (1243)$. However, *function* $f_2 \neq p \circ f_1$. In fact, pf_1 is meaningless. The image of f_1 is a set of colors. It is no subset of domain$(p) = \{1,2,3,4\}$. The composition of p and f_1 makes sense, but only in the order $f_1 p$. Well, maybe $f_1 p = f_2$. Let's see:

$$\begin{aligned} f_1p(1) &= f_1(p(1)) = f_1(2) = w, \\ f_1p(2) &= f_1(p(2)) = f_1(4) = b, \\ f_1p(3) &= f_1(p(3)) = f_1(1) = r, \\ f_1p(4) &= f_1(p(4)) = f_1(3) = r. \end{aligned}$$

So, $f_1 p = (w,b,r,r) = f_4$, not f_2. The correct combination of f_1, f_2, and p is (confirm it!)

$$f_2 = f_1 \circ p^{-1}. \tag{3.32}$$

When a fixed but arbitrary symmetry $q \in D_4$ is applied to an f-colored square, another coloring is produced, namely, the one corresponding to fq^{-1}. This is interesting. Associated with each symmetry of the square is a permutation of *colored* squares, i.e., permutation $q \in S_4$ *acts* on the 81-element set C. It's almost as if q were a permutation in S_{81}. Let's explore this idea more generally.

3.5.1 Definition. Denote by $C_{m,n}$ (not to be confused with $C(m,n)$) the set of all functions

$$f : \{1,2,\ldots,m\} \to \{x_1, x_2, \ldots, x_n\}.$$

The *action* of $p \in S_m$ *induced* on $C_{m,n}$ is defined by

$$\hat{p}(f) = f \circ p^{-1}, \qquad f \in C_{m,n}. \tag{3.33}$$

A couple of comments may be in order: (1) There is no *mathematical* reason to introduce $C_{m,n}$. It is a clone of $F_{m,n}$, the set of all functions from $\{1,2,\ldots,m\}$ into $\{1,2,\ldots,n\}$. However, thinking of the elements of $C_{m,n}$ as colorings may make the mathematicians easier to understand. (2) While $\hat{p}$ (in Equation (3.33)) is similar to $\tilde{p}$ (from Section 3.4), $\hat{p}$ and $\tilde{p}$ are not clones. They are two different induced actions of $p \in S_m$.

3.5.2 Lemma. *For any permutation $p \in S_m$, the function $\hat{p} : C_{m,n} \to C_{m,n}$ is one-to-one and onto. Moreover, if $p, q \in S_m$, then*

$$\hat{p}\hat{q} = \widehat{pq}. \tag{3.34}$$

Proof. Suppose $f, g \in C_{m,n}$. Then $\hat{p}(f) = \hat{p}(g)$, if and only if $fp^{-1} = gp^{-1}$, if and only if $f = g$, proving that $\hat{p}$ is one-to-one. Because $\hat{p} : C_{m,n} \to C_{m,n}$, and $C_{m,n}$ is finite, $\hat{p}$ is onto. Finally, for a fixed but arbitrary $f \in C_{m,n}$,

$$\begin{aligned}\hat{p}\hat{q}(f) &= \hat{p}(\hat{q}(f)) \\ &= \hat{p}(fq^{-1}) \\ &= (fq^{-1})p^{-1} \\ &= f(q^{-1}p^{-1}) \\ &= f(pq)^{-1} \\ &= \widehat{pq}(f).\end{aligned}$$

■

This brings us to a matter of "*national security.*" For the rest of this section, information will be restricted on a *need-to-know* basis. From Lemma 3.5.2, $\hat{p}$ is a permutation acting on $C_{m,n}$. If the functions in $C_{m,n}$ are numbered, from 1 to n^m, then all $\hat{p}$ needs to know are the *numbers* of the agents being permuted; $\hat{p}$ does not need to know their true identities. This little metaphor is leading to another abuse of language, namely, that $\hat{p}$ may as well be viewed as an element of S_{m^n}.

Setting $x_1 = r,\ x_2 = w$, and $x_3 = b$ allows $C_{4,3}$ to be identified with C, the set of red–white–blue vertex colorings of the square. Let $R = \{e_4, (1243), (14)(23), (1342)\}$ be the symmetry group of plane rotations of the square (with respect to the vertex numbering of Fig. 3.5.1), and define $\hat{R} = \{\hat{p} : p \in R\}$. Then, by Lemma 3.5.2 and our *national security* metaphor, $\hat{R}$ may be regarded as a subset of S_{81}. In fact, $\hat{R}$ is a subgroup. If $\hat{p}, \hat{q} \in \hat{R}$, then, by Equation (3.34), $\hat{p}\hat{q} \in \hat{R}$, proving that $\hat{R}$ is closed.

Suppose $f, g \in C = C_{4,3}$. As colorings, f and g are equivalent if and only if g can be obtained from f by a rotation of the square. Translating this statement into function language, f and g are equivalent if and only if there is a symmetry $p \in R$ such that $g = fp^{-1}$, if and only if there is a $\hat{p} \in \hat{R}$ such that $\hat{p}(f) = g$, if and only if (viewed as elements of S_{81}) f and g are equivalent modulo $\hat{R}$.

Evidently, this artificially contrived $\hat{R}$ affords another way to *state* the problem. How does it bring us any closer to a *solution*? In fact, $\hat{R}$ is not so much artificially contrived as artfully crafted. Having identified color patterns with orbits of $\hat{R}$, we can use Burnside's lemma to count them! The number of color patterns is the average of the numbers of fixed points of the permutations in $\hat{R}$. Because $o(\hat{R}) = o(R)$ and it doesn't matter whether we sum over $\hat{p} \in \hat{R}$ or $p \in R$, the number of color patterns is

$$\frac{1}{o(\hat{R})}\sum_{\hat{p}\in\hat{R}} F(\hat{p}) = \frac{1}{o(R)}\sum_{p\in R} F(\hat{p}). \tag{3.35}$$

It remains to evaluate $F(\hat{p})$.

If $p = (1243) \in R$, then p is the permutation name for a 90° clockwise rotation of the square in Fig. 3.5.1 and $f \in C_{4,3}$ is a fixed point of $\hat{p}$ if and only if $\hat{p}(f) = f$, if

and only if the *function* $f = fp^{-1}$, if and only if the *coloring* f is unchanged when the square is turned 90°, if and only if p is a symmetry of the *colored* square. But, the only colored squares left unchanged by a 90° rotation are those in which all four vertices are colored the same. Because there are three colors, there are three such colorings. In other words, if $p = (1243)$, then $F(\hat{p}) = 3$. The same analysis applies to $p = (1342)$, the permutation name for a 90° counterclockwise rotation.

What about $p = (14)(23)$. A rotation of 180° switches vertex 1 with vertex 4 and vertex 2 with vertex 3. Thus, $\hat{p}(f) = f$ if and only if $f(1) = f(4)$ and $f(2) = f(3)$. In this case, counting the fixed points of $\hat{p}$ involves two decisions, one for each cycle of p. (That's right, p.) Because there are 3 choices for each decision, $\hat{p}(f) = f$ for 3^2 colorings $f \in C$, i.e., $F(\hat{p}) = 9$.

An algorithm is emerging. If p is the permutation name for a generic symmetry, then the vertices whose numbers belong to a cycle of p are *cycled* among themselves. A necessary and sufficient condition for f to be a fixed point of $\hat{p}$ is that f be constant on the vertices within each cycle of p. If the disjoint cycle factorization of p contains a total of $c(p)$ cycles (including cycles of length 1), then $3^{c(p)}$ colorings meet this criterion, i.e., $F(\hat{p}) = 3^{c(p)}$. (If there were 4 colors, $F(\hat{p})$ would be $4^{c(p)}$.)

Let's try this new algorithm on the remaining element of G, namely e_4. Because $c(e_4) = 4$, we are predicting that $F(\hat{e}_4) = 3^4 = 81$, and that's right. After all, $\hat{e}_4$ is being identified with e_{81}, a permutation with 81 fixed points.

Substituting these values for $F(\hat{p}), p \in R$, into Equation (3.35) yields that the number of inequivalent red–white–blue vertex colorings of a square is $\frac{1}{4}(81 + 3 + 9 + 3) = 24$. In other words, the 81 colorings of $C = C_{4,3}$ are partitioned by the plane symmetries of the square into 24 patterns. Symbolically,

$$C_{4,3} = P_1 \cup P_2 \cup \cdots \cup P_{24},$$

where

$$\begin{aligned} P_i &= \{\hat{p}(g) : p \in R\} \\ &= \{gp^{-1} : p \in R\} \\ &= \{gp : p \in R\} \end{aligned}$$

for any coloring $g \in P_i$. Moreover, because $P_i = O_g$, the orbit of $\hat{R}$ to which g belongs, $o(P_i) = o(O_g)$ is the quotient of $o(\hat{R})$ and the cardinality of the stabilizer subgroup $\hat{R}_g$. (See Lemma 3.3.7.)

Amazing! But, is 24 really correct? It has the virtue, at least, of being an integer. But would you stake your life on its being the *right* integer? What about confirming it with a brute-force list?

A *system of distinct representatives* (SDR) for the color patterns consists of one coloring from each pattern. Imagine searching for a SDR for the color patterns of red–white–blue vertex colored squares and arriving at the list displayed in Fig. 3.5.3. (Convince yourself that no two listed colorings are equivalent, modulo a plane

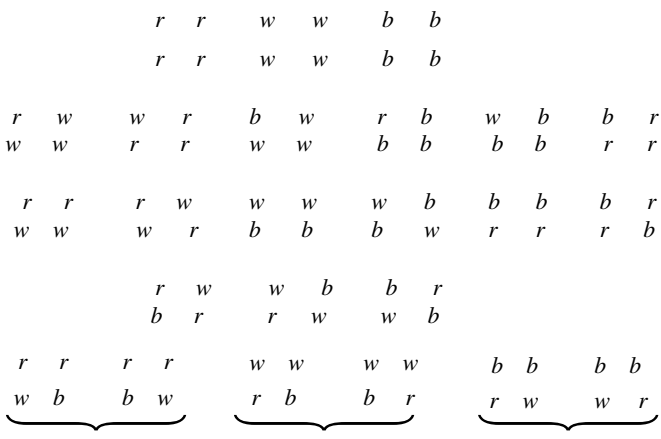


Figure 3.5.3

rotation.) Assuming ignorance or doubt about the total number of patterns, the only way to be sure the list is complete is to confirm that each of the remaining $81 - 24 = 57$ colorings is equivalent to one of those listed. On the other hand, given that the total number of color patterns is 24, once 24 inequivalent colorings are found, the list must be complete.

We've been treating these Independence Day decorations as if they were colored squares on plain paper. What about coloring squares on transparencies so that, in addition to plane rotations, the colored squares can be flipped over? Because this changes the symmetry group, it probably changes the number of color patterns, but by how much? What would you guess is the number of color patterns modulo $D_4 = \{e_4, (1243), (14)(23), (1342), (12)(34), (13)(24), (14), (23)\}$? Does doubling the symmetry group halve the number of color patterns? Let's see. By Burnside's lemma,

$$\begin{aligned}\frac{1}{8}\sum_{p\in D_4} F(\hat{p}) &= \frac{1}{8}\sum_{p\in D_4} 3^{c(p)} \\ &= \frac{1}{8}(81 + 3 + 9 + 3 + 9 + 9 + 27 + 27) \\ &= 21.\end{aligned}$$

This explains the braces in Fig. 3.5.3. They indicate which patterns, inequivalent modulo R, coalesce to form single patterns modulo D_4.

Let's extend these notions to a more general setting.

3.5.3 Lemma. *Let $c(p)$ be the total number of cycles, including cycles of length 1, in the disjoint cycle factorization of $p \in S_m$. Denote the induced action of p on $C_{m,n}$ by $\hat{p}$. Then the number of fixed points of $\hat{p}$ is $F(\hat{p}) = n^{c(p)}$.*

Proof. If $f \in C_{m,n}$, then $\hat{p}(f) = fp^{-1} = f$, if and only if $fp^{-1}(i) = f(i), 1 \le i \le m$, if and only if $f(i) = fp(i), 1 \le i \le m$, if and only if $f(i) = f(j)$ whenever i and j are

				(132) (456)
		(2453)	(16) (24) (35)	(153) (246)
		(1265)	(15) (26) (34)	(124) (365)
	(25) (34)	(1364)	(14) (25) (36)	(145) (263)
e_6	(16) (25)	(2354)	(16) (23) (45)	(123) (465)
	(16) (34)	(1562)	(12) (34) (56)	(135) (264)
		(1463)	(13) (25) (46)	(142) (356)
				(154) (236)

Figure 3.5.4

in the same cycle of p. So, the number of f's fixed by p is equal to the number of ways to make a sequence of $c(p)$ decisions each having n choices. ■

3.5.4 Theorem. *Suppose G is a permutation group of degree m. Let $\hat{G} = \{\hat{p} : p \in G\}$ be the induced action of G on $C_{m,n}$. Then equivalence modulo $\hat{G}$ partitions $C_{m,n}$ into a disjoint union of color patterns. The number of patterns is*

$$t = \frac{1}{o(G)} \sum_{p \in G} n^{c(p)}, \tag{3.36}$$

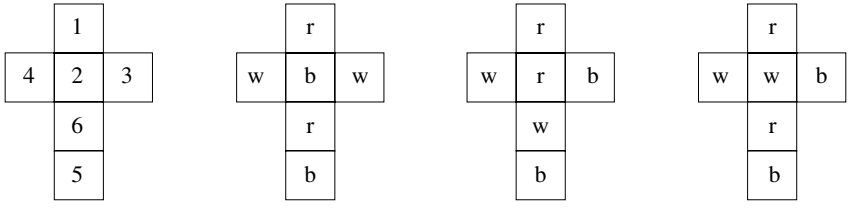
where $c(p)$ is the total number of cycles (including cycles of length 1) in the disjoint cycle factorization of p.

Proof. The result is an immediate consequence of Lemma 3.5.3 and Burnside's lemma. ■

3.5.5 Example. Suppose each face of a *cube* is painted red, white, or blue. There are $3^6 = 729$ ways to do it. Say two colored cubes are equivalent if one of them can be rotated so as to appear identical to the other one. Let's use Theorem 3.5.4 to count the resulting color patterns. Imported from Fig. 3.4.5, the octahedral group of rotational symmetries of the cube is exhibited in Fig. 3.5.4. Letting this group play the role of G in Equation (3.36) yields (don't forget the invisible 1-cycles)

$$\frac{1}{24}[3^6 + 3 \times 3^4 + 6 \times 3^3 + 6 \times 3^3 + 8 \times 3^2] = 1368/24$$
$$= 57.$$

Consider the colorings $f_1 = (r, b, w, w, b, r), f_2 = (r, r, b, w, b, w)$, and $f_3 = (r, w, b, w, b, r)$ exhibited in Fig. 3.5.5. In each of these colorings, two faces are red, two are white, and two are blue. Because the white faces are opposite each other in f_1 but adjacent in f_3, these two colorings are inequivalent. Moreover, because the red



(*a*) $f_1 = (r,b,w,w,b,r)$ $f_2 = (r,r,b,w,b,w)$ $f_3 = (r,w,b,w,b,r)$

Figure 3.5.5

faces are adjacent in f_2, it is equivalent neither to f_1 nor to f_3. Thus, we have distinct representatives for three of the 57 color patterns. While it is helpful to know there are (only) 54 patterns to go, it would help even more to know the color distributions of the remaining patterns. How many more patterns, e.g., are comprised of colorings that have two red faces, two white faces, and two blue faces? That kind of information comes from a refinement of Theorem 3.5.4 known as Pólya's theorem,* the subject of the next section. □

3.5. EXERCISES

1 Suppose four colors are available to color the vertices of a square, say red, white, blue, and yellow.

(a) Find $g = \hat{p}(f)$ if $p = (14)(23)$ and $f = (r, w, b, y)$.

(b) Find $g = \hat{p}(f)$ if $p = (1243)$ and $f = (r, w, b, y)$.

(c) Suppose $g = (r, r, w, b) \in P$, where P is one of the red–white–blue–yellow color patterns modulo the group of plane rotations of the square. With respect to the vertex numbering of Fig. 3.5.1, list all the elements of $P \subset C_{4,3}$.

(d) Suppose $g = (r, r, w, b) \in P$, where P is one of the red–white–blue–yellow color patterns modulo D_4. List all the elements of $P \subset C_{4,3}$.

(e) How many red–white–blue–yellow color patterns are there modulo the group of plane rotations?

(f) How many red–white–blue–yellow color patterns are there modulo D_4?

2 Suppose just two colors are available to decorate the vertices of a square, say red and white. Counting the distinct representatives in Fig. 3.5.3 that don't involve any b's, one discovers that there are a total of six red–white color patterns modulo the symmetry group $G = \langle(1243)\rangle$ of plane rotations.

* Named for George Pólya (1888–1985).

(a) How many different colorings are equivalent, modulo G, to $f = (r, r, w, w)$?
(b) How many different colorings are equivalent, modulo G, to $f = (r, w, r, w)$?
(c) Confirm that $\frac{1}{4}\sum_{p\in G} 2^{c(p)} = 6$.
(d) Use Theorem 3.5.4 to compute the number of inequivalent red–white vertex colorings of the square modulo D_4.

3 Say that two vertex colorings of a regular pentagon are equivalent if one can be obtained from the other by a plane rotation. Suppose n colors are available.
(a) Use Theorem 3.5.4 to show that there are eight color patterns when $n = 2$.
(b) Find a system of distinct representatives for the eight color patterns in part (a).
(c) Show that there are 51 color patterns when $n = 3$.
(d) Compute the number of color patterns when $n = 4$.
(e) If n is relatively prime to 5, prove that $n^4 + 4$ is a multiple of 5.
(f) If n is relatively prime to 5, prove that $n^4 - 1$ is a multiple of 5.
(g) Let p be, not a permutation, but a prime number. If n is relatively prime to p, prove that p is a factor of $n^{p-1} - 1$.

4 Which of the eight inequivalent color patterns in Exercise 3(b) are equivalent modulo the group D_5 of all 10 symmetries of a regular pentagon?

5 Show that there are 39 inequivalent 3-colorings of the vertices of a regular pentagon modulo D_5.

6 Suppose n colors are available to decorate the vertices of a regular hexagon. Compute the number of color patterns modulo D_6 (see Exercise 6(b), Section 3.4) when
(a) $n = 2$. **(b)** $n = 3$. **(c)** $n = 4$.

7 Three of the six rotationally inequivalent red–white–blue colorings of the faces of a cube in which each color is used twice are given in Fig. 3.5.5. Exhibit the other three
(a) using pictures. **(b)** using functions.

8 Modulo its group of 12 rotational symmetries (see Exercise 9, Section 3.4), how many inequivalent n-colorings of the faces of a regular tetrahedron are there when
(a) $n = 2$? **(b)** $n = 3$? **(c)** $n = 4$?

9 Modulo the group of all its symmetries, how many inequivalent n-colorings of the faces of a regular tetrahedron are there when
(a) $n = 2$? **(b)** $n = 3$? **(c)** $n = 4$?

10 Express $o(\{p \in S_m : c(p) = r\})$ in terms of Stirling numbers.

11 Prove that the falling factorial function

$$x^{(m)} = (-1)^m \sum_{p \in S_m} (-x)^{c(p)}.$$

12 There is a natural one-to-one correspondence between binary words of length 3 and points in three-dimensional space. The word 010, e.g., corresponds to the point (0, 1, 0).

(a) Show that the $2^3 = 8$ different binary words of length 3 correspond to the vertices of a cube.

(b) Show that there is a one-to-one correspondence between $(3, M, d)$ codes and vertex colorings of the cube using 2 colors.

(c) If two $(3, M, d)$ codes are defined to be equivalent when the corresponding vertex 2-colorings of the cube are equivalent modulo its group of 48 symmetries, how many inequivalent $(3, M, d)$ codes are there? (*Hint*: Exercise 11, Section 3.4.)

(d) Suppose $\mathscr{C}_1$ is a $(3, M, d_1)$ code and $\mathscr{C}_2$ is a $(3, M_2, d_2)$ code. If $\mathscr{C}_1$ and $\mathscr{C}_2$ are equivalent (in the sense of part (e)), show that $M_1 = M_2$. Is $d_1 = d_2$?

13 In how many inequivalent ways can the eight faces of an octahedron be colored, modulo the group of its 24 rotational symmetries,

(a) using two colors?

(b) using three colors?

(c) using ten colors?

14 In how many inequivalent ways can the eight faces of an octahedron be colored, modulo the group of all 48 of its symmetries,

(a) using two colors? (*Hint*: Compare with Exercise 12(c).)

(b) using three colors?

(c) using ten colors?

15 Express the number of inequivalent vertex colorings of a regular octagon, modulo its group of plane symmetries, as a polynomial in n, the number of available colors.

16 In how many inequivalent ways can the six *edges* of a regular tetrahedron be 2-colored,

(a) modulo the group of its 12 rotational symmetries. (Hint: Exercise 12, Section 3.4.)

(b) modulo the group of all 24 of its symmetries.

17 Fifteen billiard balls can be racked into a triangular array as shown in Fig. 3.5.6. Assume the balls are available in (unlimited quantitites of) red, white, and blue. Modulo the symmetry group of plane rotations of the rack, how many inequivalent color patterns of balls are possible?

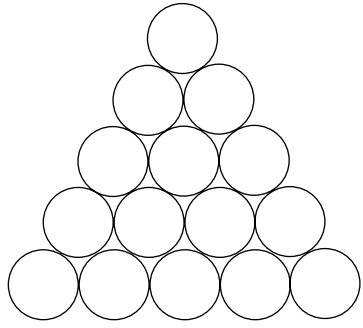


Figure 3.5.6

18 Nuclear magnetic resonance (NMR) is produced by a magnetic field associated with unpaired nuclear *spins*. There are two possibilities for the spin of an ordinary hydrogen nucleus (a proton): spin *up* and spin *down*. The NMR phenomenon is observed by placing a sample in a steady magnetic field and simultaneously exciting the sample with radio waves. The frequency of the radiation and the strength of the magnetic field can be adjusted to produce absorption of the radio waves. (Among the triumphs of quantum mechanics is a theoretical understanding of these, and other, *spectral lines*.)

Free hydrogen can exist either as atomic hydrogen, H_1, or as molecular hydrogen, H_2. Suppose some random cubic meter of intergalactic space contains four hydrogen atoms. Imagine using NMR spectroscopy to determine whether the hydrogens are in atomic or molecular form. The first step is to analyze the various possibilities. Suppose we ''color'' each of the nucleii using two colors: up and down.

(a) The group of symmetries for the system $4H_1$ is S_4. Show, in this case, that five nuclear magnetic *states* (inequivalent 2-colorings) are possible. (Give two arguments, one based on common sense and one based on Theorem 3.5.4.)

(b) Numbering the atoms of one molecule 1 and 2, and the atoms of the second 3 and 4, show that the group of symmetries for the system $2H_2$ is $\{e_4, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$.

(c) How many states are possible for the system $2H_1 + H_2$?

19 If $A = (a_{i,j})$ is an $m \times m$ matrix, then

$$\det(A) = \sum_{p \in S_m} (-1)^{m-c(p)} \prod_{t=1}^{m} a_{t,p(t)}.$$

The *permanent* function is defined by

$$\operatorname{per}(A) = \sum_{p \in S_m} \prod_{t=1}^{m} a_{t,p(t)},$$

i.e., the permanent is the determinant without the alternating minus signs. Let J_m be the $m \times m$ matrix each of whose entries is 1. Prove that

(a) $\text{per}(J_m) = m!$.

(b) $\text{per}(J_m - I_m) = D(m)$, the mth derangement number.

20 Suppose G is a group of symmetries of some objcet O. Denote by $N(G, n)$ the number of inequivalent colorings of the faces of O modulo $\hat{G}$ when n colors are available.

(a) Prove that $N(G, s) < N(G, t)$ whenever $s < t$.

(b) Prove that $N(G, n) \leq N(H, n)$ whenever H is a subgroup of G.

(c) Must the inequality in part (b) be strict when H is a proper subgroup of G?

21 Let $\hat{p}$ be the induced action of $p \in S_m$ defined by $\hat{p}(f) = fp^{-1}$, $f \in C_{m,n}$. If $n > 1$, prove that $\hat{p} = \hat{q}$ if and only if $p = q$.

3.6. PÓLYA'S THEOREM

A little inaccuracy sometimes saves a ton of explanation.
— H. H. Munro

Modulo its symmetry group of plane rotations, there are 24 inequivalent ways to color the vertices of a square red, white or blue, a number obtained by identifying equivalence classes of colorings with the orbits of an artfully crafted permutation group. A system of distinct representatives (SDR) for the 24 color patterns, described by means of geometric pictures, can be found in Fig. 3.5.3. With respect to the vertex numbering in Fig. 3.6.1, the function manifestation of the SDR appears in Fig. 3.6.2.

During a previous discussion of balls and urns, it was productive at one point to deviate from the usual sequence notation and describe functions using *words*, e.g., substituting *rrbw* for (r, r, b, w). It is a well-documented phenomenon of human nature that people typically see what they expect to see. Told to expect a word, we look at *rrbw* and our thoughts turn to pronunciation. Told to expand $(r + w + b)^4$, we look at *rrbw* and our thoughts turn to algebraic expressions like r^2wb. Told nothing about what to expect, we could misinterpret *rrbw*.

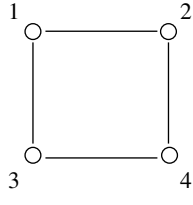


Figure 3.6.1

(r, r, r, r) (w, w, w, w) (b, b, b, b)

(r, w, w, w) (w, r, r, r) (b, w, w, w) (r, b, b, b) (w, b, b, b) (b, r, r, r)

(r, r, w, w) (r, w, w, r) (w, w, b, b) (w, b, b, w) (b, b, r, r) (b, r, r, b)

(r, w, b, r) (w, b, r, w) (b, r, w, b)

(r, r, w, b) (r, r, b, w) (w, w, r, b) (w, w, b, r) (b, b, r, w) (b, b, w, r)

Figure 3.6.2

What are the implications of a misinterpretation? Suppose we abbreviate the function (r, r, b, w) with *rrbw* and then, due to some distraction or lapse of concentration, find ourselves writing r^2wb. Let's call it the *weight* of (r, r, b, w). In passing from a coloring to its weight, something gets lost. From the weight, we can determine which colors are used and how often, but not which vertices get which colors. Nevertheless, replacing *(r,r,b,w)* with the algebraic expression r^2wb is surprisingly useful.

Observe, first, that equivalent colorings have the same weight. (Rotating a colored square isn't going to change the number of its red vertices.) So, it makes sense to define the *weight* of a *pattern* to be the weight common to every coloring in the pattern. What makes things interesting is that inequivalent colorings can also have the same weight. Exactly three of the 24 inequivalent colorings represented in Fig. 3.6.2, e.g., have weight r^2wb, namely, $(r, w, b, r), (r, r, w, b)$, and (r, r, b, w). The *pattern inventory* tracks just this sort of information. It is the polynomial obtained by summing the weights of the distinct patterns. The pattern inventory for the rotationally inequivalent red–white–blue vertex colorings of the square can be obtained by replacing each function in Fig. 3.6.2 by its weight and then summing the resulting monomials. After combining like terms, the outcome is

$$W_G(r, w, b) = (r^4 + w^4 + b^4) + (rw^3 + r^3w + w^3b + rb^3 + wb^3 + r^3b) + 2(r^2w^2 + w^2b^2 + r^2b^2) + 3(r^2wb + rw^2b + rwb^2). \tag{3.37}$$

Note that $W_G(1, 1, 1) = 24$, reflecting the fact that each pattern contributes one monomial to W_G.

Starting from a system of distinct representatives for the color patterns, as we just did, it is easy to write down the pattern inventory. The hard part is finding the SDR! The focus of this section involves reversing the process, *starting* with the pattern inventory and using it as a guide while assembling a system of distinct representatives. If, e.g., you were in the midst of listing an SDR, perhaps having just found a second pattern of weight r^2w^2, you would know from Equation (3.37) not to waste time searching for a nonexistent third pattern of the same weight.

All right, how does one find the pattern inventory without first constructing a system of distinct representatives? Let's approach it like a mystery and begin with the clues. From Equation (3.37), $W_G(r, w, b)$ is a homogeneous polynomial

of degree 4 (because there are four vertices) in 3 variables (because there are three colors). Moreover, from the physical nature of the problem, $W_G(r,w,b)$ is a *symmetric* polynomial. So, it is a linear combination of minimal symmetric polynomials:

$$W_G(r,w,b) = M_{[4]}(r,w,b) + M_{[3,1]}(r,w,b) + 2M_{[2^2]}(r,w,b) + 3M_{[2,1^2]}(r,w,b). \tag{3.38}$$

(Confirm the equivalence of Equations (3.37) and (3.38).)

One way to proceed might be to look for an analogue of the multinomial theorem, a formula for the coefficient of M_π in the *expansion* of W_G as a linear combination of minimal symmetric polynomials. If such a formula exists, it has not yet been found. What has been discovered is a little different. It is an algorithm for expressing W_G as a *polynomial* in the power sums $M_k = M_{[k]}$, $1 \le k \le m$. (This is a little like ordering a hamburger and being served a hot dog!)

So far, our discussion has been limited to the motivating example of red–white–blue vertex colored squares. If that sort of thing were all Pólya's theorem is good for, it would not be worth mentioning. To enable the full range of applications, we need to retrace our steps in a more general setting.

Recall that $C_{m,n}$ is the set of all n^m functions

$$f : \{1,2,\ldots,m\} \to \{x_1,x_2,\ldots,x_n\}$$

and that each $p \in S_m$ induces a one-to-one function $\hat{p} : C_{m,n} \to C_{m,n}$ defined by $\hat{p}(f) = fp^{-1}$. If G is a permutation group of degree m, then $\hat{G} = \{\hat{p} : p \in G\}$ can be viewed as a permutation group of degree n^m acting on $C_{m,n}$. When G is a symmetry group and $\{x_1,x_2,\ldots,x_n\}$ is a set of colors, the orbits of $C_{m,n}$ modulo $\hat{G}$ are the color patterns. Finally, from Burnside's lemma and the fact that the number of fixed points of $\hat{p}$ is $F(\hat{p}) = n^{c(p)}$, the total number of color patterns modulo $\hat{G}$ is

$$t = \frac{1}{o(G)} \sum_{p \in G} n^{c(p)}, \tag{3.39}$$

where $c(p)$ is the number of cycles in the disjoint cycle factorization, not of $\hat{p}$, but of p.

3.6.1 Definition. Treating the colors $x_1,x_2,\ldots,x_n$ that comprise the range of $f \in C_{m,n}$ as independent variables, the weight of f is

$$w(f) = \prod_{i=1}^{m} f(i).$$

Evidently, $w(f)$ is a monomial of (total) degree m.

3.6.2 Example. In the case of red–white–blue vertex colorings of the square, $n = 3, x_1 = r, x_2 = w$, and $x_3 = b$. If, e.g., $f = (r, r, b, w)$, then

$$\begin{aligned} w(f) &= f(1)f(2)f(3)f(4) \\ &= rrbw \\ &= r^2wb. \end{aligned}$$

□

Example 3.6.2 shows that Definition 3.6.1 is consistent with our original notion of weight. We now confirm, in the general setting, that equivalent colorings have the same weight.

3.6.3 Lemma. *For all $p \in S_m$ and all $f \in C_{m,n}$,*

$$w(\hat{p}(f)) = w(f). \tag{3.40}$$

In particular, $w(f) = w(g)$ whenever f and *g are equivalent modulo $\hat{G}$.*

Proof. Let $g = \hat{p}(f) = fp^{-1}$. Then $gp = f$. Because multiplication is commutative and $p \in S_m$,

$$\begin{aligned} w(g) &= \prod_{i=1}^{m} g(i) \\ &= \prod_{i=1}^{m} gp(i) \\ &= \prod_{i=1}^{m} f(i) \\ &= w(f). \end{aligned}$$

■

Suppose P is one of the color patterns (orbits) of $C_{m,n}$ modulo $\hat{G}$. If $f, g \in P$, then $g = \hat{p}(f)$ for some $p \in G$ and, by Lemma 3.6.3, $w(g) = w(f)$. This brings us, at last, to a formal definition of pattern inventory.

3.6.4 Definition. Suppose G is a permutation group of degree m. Let $P_1, P_2, \ldots, P_t$ be the distinct color patterns (orbits) of $C_{m,n}$ modulo $\hat{G}$. The *weight* of P_i is the common value of $w(f), f \in P_i$. The sum of the weights of the orbits is the *pattern inventory*

$$W_G(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{t} w(P_i). \tag{3.41}$$

Because $W_G(1, 1, \ldots, 1) = t$, the number of patterns, it follows from Equation (3.39) that

$$W_G(1, 1, \ldots, 1) = \frac{1}{o(G)} \sum_{p \in G} n^{c(p)}. \tag{3.42}$$

Now that all the formal definitions are in place, let's return to the issue of *evaluating* $W_G(x_1, x_2, \ldots, x_n)$. While it is important to keep m and G general, no real generality is lost if we take $n = 3$ and set $x_1 = r$, $x_2 = w$, and $x_3 = b$.

Consider a fixed but arbitrary nonnegative integer solution to the equation $i + j + k = m$. By definition, the coefficient of $r^i w^j b^k$ in $W_G(r, w, b)$ is the number of color patterns of weight $r^i w^j b^k$. Denote the union of these patterns by $C_{m,n}(i, j, k)$. Then $C_{m,n}(i, j, k)$ is the set of all *colorings* of weight $r^i w^j b^k$.

If $p \in G$ then, by Lemma 3.6.3, $\hat{p}$ permutes the elements of $C_{m,n}(i, j, k)$ among themselves. Define $\hat{p}_{(i,j,k)}$ to be the restriction of $\hat{p}$ to $C_{m,n}(i, j, k)$, and let $\hat{G}_{(i,j,k)} = \{\hat{p}_{(i,j,k)} : p \in G\}$. Then $\hat{G}_{(i,j,k)}$ is a permutation group acting on $C_{m,n}(i, j, k)$. Moreover, two colorings of $C_{m,n}(i, j, k)$ are equivalent modulo $\hat{G}_{(i,j,k)}$ if and only if they are equivalent modulo $\hat{G}$. So, the number of orbits of $\hat{G}$ having weight $r^i w^j b^k$ is equal to the *total* number of orbits of $\hat{G}_{(i,j,k)}$. Let's apply Burnside's lemma to $\hat{G}_{(i,j,k)}$ and deduce that the number of color patterns modulo $\hat{G}$ of weight $r^i w^j b^k$ is given by*

$$\frac{1}{o(G)} \sum_{p \in G} F(\hat{p}_{(i,j,k)}). \tag{3.43}$$

Because Formula (3.43) is the coefficient of $r^i w^j b^k$ in $W_G(r, w, b)$, it must be that

$$\begin{aligned} W_G(r, w, b) &= \sum_{i+j+k=m} \left(\frac{1}{o(G)} \sum_{p \in G} F(\hat{p}_{(i,j,k)}) \right) r^i w^j b^k \\ &= \frac{1}{o(G)} \sum_{p \in G} \left(\sum_{i+j+k=m} F(\hat{p}_{(i,j,k)}) r^i w^j b^k \right) \end{aligned} \tag{3.44}$$

It remains to evaluate

$$\sum_{i+j+k=m} F(\hat{p}_{(i,j,k)}) r^i w^j b^k. \tag{3.45}$$

Consider an example. If $m = 7$, the colorings can be identified with functions $f : \{1, 2, 3, 4, 5, 6, 7\} \to \{r, w, b\}$. Let $q = (12)(34)(567)$. Then f is a fixed point of $\hat{q}$ if and only if $f(1) = f(2)$, $f(3) = f(4)$, and $f(5) = f(6) = f(7)$. As we saw in the last section, the number of fixed points, $F(\hat{q})$, is equal to the number of ways to make a sequence of $c(q) = 3$ decisions each having three choices (namely, r, w, or b). Therefore, $F(\hat{q}) = 3^{c(q)} = 27$.

Of the 27 fixed points of $\hat{q}$, one is $f_1 = (r, r, w, w, b, b, b)$, a coloring of weight $w(f_1) = r^2 w^2 b^3$. Another fixed point of $\hat{q}$ is $f_2 = (w, w, r, r, b, b, b)$. Because

* While this statement is correct, it is not completely justified by the discussion. The problem is that $p \to \hat{p}_{(i,j,k)}$ need not be one-to-one. The argument can be made rigorous by using the tools of abstract group homomorphisms, their kernels, and the corresponding quotient groups.

$w(f_2) = r^2w^2b^3 = w(f_1), F(\hat{q}_{(2,2,3)}) \geq 2$. A third fixed point of $\hat{q}$ is (b, b, w, w, w, w, w), having weight w^5b^2. If we listed all 27 fixed points of $\hat{q}$ and summed their weights, the result would be

$$\begin{aligned}\sum_{i+j+k=m} F(\hat{q}_{(i,j,k)})r^iw^jb^k \\ &= (r^7 + w^7 + b^7) + 2(r^5w^2 + r^5b^2 + r^2w^5 + r^2b^5 + w^5b^2 + w^2b^5) \\ &\quad + (r^4w^3 + r^4b^3 + r^3w^4 + r^3b^4 + w^4b^3 + w^3b^4) \\ &\quad + 2(r^2w^2b^3 + r^2w^3b^2 + r^3w^2b^2), \end{aligned} \tag{3.46}$$

the special case of Formula (3.45) corresponding to $p = q$. (From the term $2r^2w^2b^3$, we deduce that f_1 and f_2 are the only fixed points of $\hat{q}$ that have weight $r^2w^2b^3$.)

Because $f \in C_{7,3}$ is a fixed point of $\hat{q}$ if and only if f is constant on the three cycles of $q = (12)(34)(567) \in S_7$, Equation (3.46) is an inventory of the weights $w(f) = c_1^2c_2^2c_3^3$, where $c_1 \in \{r, w, b\}$ is the color $f(1) = f(2)$, $c_2 \in \{r, w, b\}$ is the (not necessarily different) color $f(3) = f(4)$, and $c_3 \in \{r, w, b\}$ is the color $f(5) = f(6) = f(7)$. But, there is another way to inventory *these same weights*! From the alternative view of distributivity used, e.g., to prove the binomial theorem,

$$\begin{aligned}\sum_{i+j+k=m} F(\hat{q}_{(i,j,k)})r^iw^jb^k \\ &= (r^2 + w^2 + b^2)^2(r^3 + w^3 + b^3) \\ &= M_2(r, w, b)^2M_3(r, w, b),\end{aligned}$$

where $M_k(r, w, b) = r^k + w^k + b^k$ is the kth power sum. (Confirm that the right-hand side of this equation is equal to the right-hand side of Equation (3.46).)

Returning to the general case, let $c_i(p)$ be, not some color, but the number of cycles of length i in the disjoint cycle factorization of $p \in S_m$. Using the arguments illustrated above for $q = (12)(34)(567)$, it follows that the weights of the fixed points of $\hat{p}$ are inventoried by

$$\begin{aligned}\sum_{i+j+k=m} F(\hat{p}_{(i,j,k)})r^iw^jb^k \\ &= (r + w + b)^{c_1(p)}(r^2 + w^2 + b^2)^{c_2(p)} \cdots (r^m + w^m + b^m)^{c_m(p)} \\ &= M_1(r, w, b)^{c_1(p)}M_2(r, w, b)^{c_2(p)} \cdots M_m(r, w, b)^{c_m(p)}\end{aligned}$$

for any $p \in S_m$. Substituting this identity into Equation (3.44) yields

$$W_G(r, w, b) = \frac{1}{o(G)} \sum_{p \in G} M_1(r, w, b)^{c_1(p)}M_2(r, w, b)^{c_2(p)} \cdots M_m(r, w, b)^{c_m(p)}.$$

p	$C_1(p)$	$C_2(p)$	$C_3(p)$	$C_4(p)$
e_4	4	0	0	0
(1243)	0	0	0	1
(14) (23)	0	2	0	0
(1342)	0	0	0	1

Figure 3.6.3

The generalization to n colors is this:

3.6.5 Pólya's Theorem.[*] *If G is a subgroup of S_m, then the pattern inventory for the orbits of $C_{m,n}$ modulo $\hat{G}$ is*

$$W_G(x_1, x_2, \ldots, x_n) = \frac{1}{o(G)} \sum_{p \in G} M_1^{c_1(p)} M_2^{c_2(p)} \ldots M_m^{c_m(p)}, \tag{3.47}$$

where $M_k = M_{[k]}(x_1, x_2, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k$, the kth power sum of the x's.

So, there it is: an algorithm, depending only on G, for expressing the pattern inventory, W_G, as a polynomial in the power sums. The unfortunate thing is that it should *look* so complicated. In fact, there is *less* here than meets the eye.

Note that Pólya's theorem is consistent with our earlier formula for the *number* of patterns: If $x_1 = x_2 = \cdots = x_n = 1$, then $M_k = n$ for all k. Because

$$c_1(p) + c_2(p) + \cdots + c_m(p) = c(p), \tag{3.48}$$

the total number of cycles of p, Equation (3.42) is an easy consequence of Equation (3.47).

3.6.6 Example. Let's apply Pólya's theorem to red–white–blue colorings of the vertices of a square, modulo the group $G = \langle (1243) \rangle$ of plane rotations. Substituting the information from Fig. 3.6.3 into Equation (3.47) yields

$$W_G(r, w, b) = \frac{1}{4}[(r + w + b)^4 + 2(r^4 + w^4 + b^4) + (r^2 + w^2 + b^2)^2]. \tag{3.49}$$

From the multinomial theorem,

$$\begin{aligned}(r + w + b)^4 = {} & M_{[4]}(r, w, b) + 4M_{[3,1]}(r, w, b) \\ & + 6M_{[2,2]}(r, w, b) + 12M_{[2,1^2]}(r, w, b),\end{aligned}$$

[*] Pólya's 1937 paper revolutionized combinatorial enumeration. In 1960, F. Harary pointed out that many of Pólya's ideas had been anticipated in 1927 by J. H. Redfield. However, it was only after Pólya had articulated and explained the ideas that anyone was able to make sense of Redfield's paper.

p	#	$C_1(p)$	$C_2(p)$	$C_3(p)$	$C_4(p)$	$C_5(p)$	$C_6(p)$
e_6	1	6	0	0	0	0	0
(25) (34)	3	2	2	0	0	0	0
(2453)	6	2	0	0	1	0	0
(16) (24) (35)	6	0	3	0	0	0	0
(132) (456)	8	0	0	2	0	0	0

Figure 3.6.4

and

$$\begin{aligned}(r^2+w^2+b^2)^2 &= M_{[2]}(r^2,w^2,b^2)+2M_{[1^2]}(r^2,w^2,b^2)\\ &= M_{[4]}(r,w,b)+2M_{[2^2]}(r,w,b).\end{aligned}$$

Together with Equation (3.49) and

$$2(r^4+w^4+b^4)=2M_{[4]}(r,w,b),$$

these identities produce

$$\begin{aligned}W_G(r,w,b) &= \frac{1}{4}[4M_{[4]}(r,w,b)+4M_{[3,1]}(r,w,b)+8M_{[2^2]}(r,w,b)+12M_{[2,1^2]}(r,w,b)]\\ &= M_{[4]}(r,w,b)+M_{[3,1]}(r,w,b)+2M_{[2^2]}(r,w,b)+3M_{[2,1^2]}(r,w,b),\end{aligned}$$

which is precisely Equation (3.38). □

3.6.7 Example. Let's work out the pattern inventory for the 57 red–white–blue color patterns for the faces of the cube, modulo the group G consisting of its 24 rotational symmetries. To get started, we need an analogue of Fig. 3.6.3, but it need not have 24 rows. To evaluate Equation (3.47), all we really need are the numbers of permutations of each cycle type. Because (Example 3.5.5) the permutations of G come in five different cycle types, only five rows are needed. In Fig. 3.6.4, the column labeled "#" contains the number of permutations of G having the same cycle type as the permutation in column "p". Substituting this information into Pólya's theorem, we obtain

$$\begin{aligned}W_G(r,w,b) = \frac{1}{24}[&(r+w+b)^6+3(r+w+b)^2(r^2+w^2+b^2)^2\\ &+6(r+w+b)^2(r^4+w^4+b^4)+6(r^2+w^2+b^2)^3\\ &+8(r^3+w^3+b^3)^2].\end{aligned} \tag{3.50}$$

Equation (3.50) is the hot dog. It is an expression for the pattern inventory as a polynomial in the power sums. What stands between us and the coefficient of M_π in

the expansion of W_G (the hamburger) is a pile of computations. The silver lining is that we do not always need the coefficient of M_π for *every* $\pi \vdash m$. It might happen, e.g., that our interest does not extend beyond patterns of weight rw^2b^3.

Okay, what is the coefficient of rw^2b^3 in Equation (3.50)? Because every term of the product $6(r+w+b)^2(r^4+w^4+b^4)$ contains a fourth power, it contributes nothing of the form rw^2b^3. Since neither $6(r^2+w^2+b^2)^3$ nor $8(r^3+w^3+b^3)^2$ involves a first power, they cannot contribute terms of the form rw^2b^3 either. From the multinomial theorem, $(r+w+b)^6$ contributes $60rw^2b^3$.

What about $3(r+w+b)^2(r^2+w^2+b^2)^2$? Because, the single r must come from the factor $(r+w+b)^2$, the contribution from this term is the product

$$3 \times 2rb \times 2w^2b^2 = 12rw^2b^3.$$

So, the coefficient of rw^2b^3 in $W_G(r,w,b)$ is $\frac{1}{24}(60+12) = 3$. Of the 57 rotationally inequivalent red–white–blue color patterns of the cube, there are exactly 3 in which one face is painted red, two faces are painted white, and three are painted blue.* (It is important to understand that Pólya's theorem tells us nothing about how to find distinct representatives for the three color patterns of weight rw^2b^3.)

With the tedious computations all completed, Equation (3.50) yields the hamburger

$$\begin{aligned} W_G(r,w,b) &= M_{[6]}(r,w,b) + M_{[5,1]}(r,w,b) + 2M_{[4,2]}(r,w,b) \\ &\quad + 2M_{[4,1^2]}(r,w,b) + 2M_{[3^2]}(r,w,b) \\ &\quad + 3M_{[3,2,1]}(r,w,b) + 6M_{[2^3]}(r,w,b) \\ &= (r^6+w^6+b^6) + (r^5w+\cdots+wb^5) + 2(r^4w^2+\cdots+w^2b^4) \\ &\quad + 2(r^4wb+rw^4b+rwb^4) + 2(r^3w^3+r^3b^3+w^3b^3) \\ &\quad + 3(r^3w^2b+\cdots+rw^2b^3) + 6r^2w^2b^2. \end{aligned} \tag{3.51}$$

Suppose some businessman wanted to manufacture and sell red–white–blue painted cubes in all 57 varieties. He might organize his stock in 57 drawers, one for each pattern, and make use of a system of distinct representatives to label the drawers. It might even make sense to organize the drawers into filing cabinets according to weight. Given the one-to-one correspondence between weights, $r^iw^jb^k$, and nonnegative integer solutions of the equation $i+j+k=6$, this scheme would require $C(6+3-1,6) = 28$ filing cabinets each having 1, 2, 3, or 6 drawers. A customer interested in colorings with 1 red, 2 white, and 3 blue faces could be led to the cabinet labeled rw^2b^3 and offered a choice of three drawers (the coefficient of $M_{[3,2,1]}(r,w,b)$ in $W_G(r,w,b)$). □

*By symmetry, $3M_{[3,2,1]}(r,w,b)$ must be a summand of $W_G(r,w,b)$.

3.6. EXERCISES

1 Consider $G = \langle(1243)\rangle$, the group of plane rotations of the square illustrated in Fig. 3.6.1.

(a) Show that $W_G(r,b) = M_{[4]}(r,b) + M_{[3,1]}(r,b) + 2M_{[2^2]}(r,b)$.

(b) Express $W_G(r,b)$ as a polynomial in the power sums $M_k = M_{[k]}(r,b), 1 \le k \le 2$.

2 Consider the red–white–blue vertex color patterns of a square, modulo $G = D_4$. Compute the pattern inventory $W_G(r,w,b)$

(a) using Fig. 3.5.3.

(b) using Pólya's theorem.

3 Let $G = \langle(123)\rangle$, the group of plane rotations of a equilateral triangle, expressed as permutations of its vertices.

(a) Show that, as a polynomial in the power sums $M_k = M_{[k]}(r,w,b)$, $1 \le k \le 3$,

$$W_G(r,w,b) = \tfrac{1}{3}M_1^3 + \tfrac{2}{3}M_3.$$

(b) Show that, as a linear combination of minimal symmetric polynomials,

$$W_G(r,w,b) = M_{[3]}(r,w,b) + M_{[2,1]}(r,w,b) + 2M_{[1^3]}(r,w,b).$$

(c) Exhibit a system of distinct representatives for the red–white–blue color patterns of the vertices of an equilateral triangle modulo $\hat{G}$.

4 Let $G = D_3$, the group of all symmetrics of an equilateral triangle, expressed as permutations of its vertices.

(a) Show that

$$W_G(r,w,b) = \tfrac{1}{6}[(r+w+b)^3 + 3(r+w+b)(r^2+w^2+b^2) + 2(r^3+w^3+b^3)].$$

(b) Show that, as a linear combination of minimal symmetric polynomials,

$$W_G(r,w,b) = M_{[3]}(r,w,b) + M_{[2,1]}(r,w,b) + M_{[1^3]}(r,w,b).$$

(c) Which red–white–blue color pattern(s) modulo the group of plane rotations of the equilateral triangle coalesce into a single pattern modulo $D_3 = S_3$? (*Hint*: Exercise 3(c).)

(d) If (r,w,b) is dropped from each term in part (b), the result is $W_G = M_{[3]} + M_{[2,1]} + M_{[1^3]}$. How would this expression change if a fourth color, say green, were added to the palette? How would it change if there were just two colors, say black and blue?

(e) Prove that $W_G(r,w,b) = H_3(r,w,b)$, the homogeneous symmetric function of degree 3 from Exercise 25, Section 1.8.

5 Let $G = \langle (12345) \rangle$, the group of rotational symmetries of a regular pentagon, expressed as permutations of its (consecutively numbered) vertices.

(a) Show that

$$W_G(r, w, b) = \tfrac{1}{5}[(r + w + b)^5 + 4(r^5 + w^5 + b^5)].$$

(b) Show that $W_G(1, 1, 1) = 51$.

(c) Show that

$$W_G(r, w, b) = M_{[5]}(r, w, b) + M_{[4,1]}(r, w, b) + 2M_{[3,2]}(r, w, b) + 4M_{[3,1^2]}(r, w, b) + 6M_{[2^2,1]}(r, w, b).$$

(d) Exhibit a system of distinct representatives for the four color patterns of weight rw^3b.

(e) Exhibit a system of distinct representatives for the six color patterns of weight rw^2b^2.

6 Consider red–white–blue vertex colorings of the regular pentagon modulo D_5, the group of all 10 of its symmetries. (See Exercise 5 in Sections 3.4 and 3.5.)

(a) Show that

$$W_{D_5}(r, w, b) = \tfrac{1}{10}[(r + w + b)^5 + 5(r + w + b)(r^2 + w^2 + b^2)^2 + 4(r^5 + w^5 + b^5)].$$

(b) Show that $W_{D_5}(1, 1, 1) = 39$.

(c) Show that

$$W_{D_5}(r, w, b) = M_{[5]}(r, w, b) + M_{[4,1]}(r, w, b) + 2M_{[3,2]}(r, w, b) + 2M_{[3,1^2]}(r, w, b) + 4M_{[2^2,1]}(r, w, b).$$

(d) Use part (c) to prove that $W_{D_5}(1, 1, 1) = 39$.

(e) Exhibit a system of distinct representatives for the two color patterns of weight rw^3b.

(f) Compare and contrast your answer to part (e) with your answer to Exercise 5(d).

(g) Exhibit a system of distinct representatives for the four color patterns of weight rw^2b^2.

(h) Compare and contrast your answer to part (g) with your answer to Exercise 5(e).

(i) If green were to become available, so that the set of colors is $\{r, w, b, g\}$, show that

$$W_{D_5}(r, w, b, g) = \tfrac{1}{10}[(r + w + b + g)^5 + 5(r + w + b + g)(r^2 + w^2 + b^2 + g^2)^2 + 4(r^5 + w^5 + b^5 + g^5)].$$

(j) Show that $W_{D_5}(1,1,1,1) = 136$.

(k) Show that

$$W_{D_5}(r,w,b,g) = M_{[5]} + M_{[4,1]} + 2M_{[3,2]} + 2M_{[3,1^2]} + 4M_{[2^2,1]} + 6M_{[2,1^3]},$$

where $M_\pi = M_\pi(r,w,b,g)$.

(l) Use your answer to part (k) to confirm that $W_{D_5}(1,1,1,1) = 136$.

(m) Express $W_{D_5}(r,w,b,g,p)$ as a linear combination of minimal symmetric polynomials $M_\pi(r,w,b,g,p), \pi \vdash 5$.

7 Consider vertex color patterns of a regular hexagon modulo $G = D_6$, the group of all 12 of its symmetries. (See Exercise 6(b), Section 3.4.)

(a) Express $W_G(r,w,b)$ as a linear combination of minimal symmetric polynomials $M_\pi = M_\pi(r,w,b), \pi \vdash 6$.

(b) Exhibit a system of distinct representatives for the color patterns of weight r^3w^2b.

(c) Exhibit a system of distinct representatives for the color patterns of weight $r^2w^2b^2$.

8 Exhibit six rotationally equivalent red–white–blue colorings of the faces of a cube, all having weight $r^2w^2b^2$, and indicate which pairs are equivalent by a reflection. (*Hint*: Exercise 7, Section 3.5.)

9 Let G be the group of 24 rotational symmetries of a (regular) octahedron expressed as permutations of its eight faces. (So, G is comprised of the permutations $\tilde{p}$ in Fig. 3.4.7.) Express $W_G(r,w,b)$ as a linear combination of the minimal symmetric polynomials $M_\pi = M_\pi(r,w,b), \pi \vdash 8$.

10 Modulo its group of 24 rotational symmetries, the faces of a regular octahedron have 333 inequivalent red–white–blue color patterns. (See Exericse 9.) How many of these have weight

(a) r^8? **(b)** r^7b? **(c)** $r^3w^3b^2$?

(d) $r^4w^2b^2$? **(e)** w^4b^4? **(f)** r^4wb^3?

11 Use Pólya's theorem to compute the number of red–white–blue color patterns of the faces of a cube that have weight $r^2w^2b^2$, modulo the group of all 48 of its symmetries. (*Hint*: Be sure your solution is consistent with Exercise 8.)

12 Show that

$$(x_1 + x_2 + \cdots + x_n)^m = \sum_{f \in C_{m,n}} w(f).$$

13 Let G be the group of 12 rotational symmetries of the faces of a regular tetrahedron. Express $W_G(r,w,b,y)$ as a linear combination of minimal symmetric polynomials $M_\pi = M_\pi(r,w,b,y), \pi \vdash 4$.

14 Let G be the group of all 24 symmetries of the faces of a regular tetrahedron.

(a) Express $W_G(r, w, b, g)$ as a linear combination of minimal symmetric polynomials $M_\pi = M_\pi(r, w, b, g), \pi \vdash 4$.

(b) Prove that $W_G(r, w, b, g) = H_4(r, w, b, g)$, the homogeneous symmetric function of degree 4 from Exercise 25, Section 1.8.

15 Let G be the group of 12 rotational symmetries of the regular tetrahedron expressed as permutations of its six edges. (See Exercise 12, Section 3.4.) If two colors are available, x and y, how many rotationally inequivalent 2-colorings of the edges of the tetrahedron have weight

(a) x^6? **(b)** x^5y? **(c)** x^4y^2? **(d)** x^3y^3?

16 Let G be the group of all 24 symmetries of a regular tetrahedron expressed as permutations of its six edges. (See Exercise 15.) Expand $W_G(x, y)$ as a linear combination of minimal symmetric polynomials $M_\pi = M_\pi(x, y), \pi \vdash 4$.

17 How many rotationally inequivalent ways are there to rack 15 billiard balls in a triangular array if there are 5 balls each of three different colors, say, red, white, and blue? (*Hint*: See Exercise 17, Section 3.5.)

18 Suppose G is a group of symmetries of the "features" (e.g., vertices, faces, or edges) of some geometric object. How many red–white–blue color patterns (modulo G) of the features use *all three colors* if

(a) G is the group of plane rotations of the vertices of a square?

(b) G is the rotational group of the faces of a cube?

(c) $G = D_5$, acting on the vertices of a regular pentagon?

(d) $G = D_6$, acting on the vertices of a regular hexagon?

(e) G is the group of 12 rotational symmetries of the edges of a regular tetrahedron?

(f) (get ready for some serious computation) G is the group of 24 rotational symmetries of the faces of a regular octahedron.

19 The chemical formula for benzene is C_6H_6. It is possible to form new compounds by substituting various atoms, or groups of atoms, for one or more of the hydrogens. *Benzenediol*, e.g., is the generic name for $C_6H_4(OH)_2$, obtained by subsituting OH groups for two hydrogens. Benzenediol comes in three variations, *pyrocatechol* (melting point 105°C), *resorcinol* (melting point 110°C) and *hydroquinone* (melting point 171°C). Moreover, *dichlorobenzene* ($C_6H_4Cl_2$), *dinitrobenzene* ($C_6H_4(NO_2)_2$), and a host of other compounds obtained by substituting for two of the hydrogens in benzene invariably come in families of three. From this (and other information), Baron August Kekulé von Stradonitz was able to deduce the structure of benzene.

Consider two early models (neither of which seems to satisfy the valence condition). In one model, the six carbon atoms are found at the vertices of a regular hexagon and are bonded to their two nearest neighbors and to one hydrogen atom. In the other model, the carbon atoms are found at the vertices

of a regular octahedron and are bonded to their four nearest neighbors and to one hydrogen atom. (Note that both of these models satisfy the chemical formula C_6H_6.) Now, replace two of the six hydrogen atoms with bromine. Color a carbon atom H if it is bonded to hydrogen and B if it is bonded to bromine.

(a) Modulo D_6, how many inequivalent 2-colorings of the vertices of a regular hexagon have weight H^4B^2?

(b) Modulo its group of rotational symmetries, how many inequivalent 2-colorings of the vertices of a regular octahedron have weight H^4B^2?

(c) Which model, the hexagon or octahedron, is consistent with the experimental data?

(d) Is Pólya's theorem the right way to solve this problem? Why or why not?

20 In how many inequivalent ways, modulo its rotation group, can the faces of a truncated icosahedron (see Fig. 3.4.9) be 2-colored if all the hexagons have to be the same color and all the pentagons have to be the same color?

3.7. THE CYCLE INDEX POLYNOMIAL

The cycle index knows many things.

— George Pólya

Suppose G is a group of symmetries of the m features* of some geometric object. Let $\{x_1, x_2, \ldots, x_n\}$ be a set of *colors*.† Then the pattern inventory $W_G(x_1, x_2, \ldots, x_n)$ is a polynomial, symmetric in the *variables* $x_1, x_2, \ldots, x_n$. Thus, by Theorem 1.9.11, $W_G(x_1, x_2, \ldots, x_n)$ is a polynomial in the power sums

$$\begin{aligned} M_t &= M_{[t]}(x_1, x_2, \ldots, x_n) \\ &= x_1^t + x_2^t + \cdots + x_n^t, \qquad 1 \le t \le n. \end{aligned}$$

In fact, Pólya's theorem is neither more nor less than an algorithm for constructing that mysterious polynomial. A little preparation will help clarify this point.

We are assuming G is a permutation group of degree m (because our geometric object has m features). Recall that $c_t(p)$ is the number of cycles of length t in the disjoint cycle factorization of $p \in G$. Because each integer in $\{1, 2, \ldots, m\}$ is contained in exactly one of these cycles,

$$m = c_1(p) + 2c_2(p) + \cdots + tc_t(p) + \cdots + mc_m(p). \tag{3.52}$$

(Equation (3.52) is not the same as $c(p) = c_1(p) + c_2(p) + \cdots + c_m(p)$.)

* *Features* could be vertices, edges, faces, or even hyperfaces.

† Colors might be anything from *red* and *white* to *in* and *out* or *spin up* and *spin down*.

3.7.1 Definition. Let G be a permutation group of degree m. If $s_1, s_2, \ldots, s_m$ are independent variables, the *cycle index polynomial* of G is

$$\begin{aligned} Z_G(s_1, s_2, \ldots, s_m) &= \frac{1}{o(G)} \sum_{p \in G} s_1^{c_1(p)} s_2^{c_2(p)} \cdots s_m^{c_m(p)} \\ &= \frac{1}{o(G)} \sum_{p \in G} \prod_{t=1}^{m} s_t^{c_t(p)}. \end{aligned} \tag{3.53}$$

3.7.2 Example. If $G = \{e_4, (12), (34), (12)(34)\}$, then

$$Z_G(s_1, s_2, s_3, s_4) = \tfrac{1}{4}\left(s_1^4 + 2s_1^2 s_2 + s_2^2\right). \tag{3.54}$$

(Don't forget the cycles of length 1.) For the *dihedral* group $D_4 = \{e_4, (1243), (14)(23), (1342), (12)(34), (13)(24), (14), (23)\}$,

$$Z_{D_4}(s_1, s_2, s_3, s_4) = \tfrac{1}{8}(s_1^4 + 2s_4 + 3s_2^2 + 2s_1^2 s_2). \tag{3.55}$$

Finally, let $H = \{e_4, (13)(24), (12)(34), (14)(23)\}$. Then H is a subgroup of D_4. The cycle index polynomial* of H is

$$Z_H(s_1, s_2, s_3, s_4) = \tfrac{1}{4}(s_1^4 + 3s_2^2). \tag{3.56}$$

Nominally among the variables of all three cycle index polynomials, s_3 actually appears in none of them. Similarly, s_4 is missing from the right-hand sides of Equations (3.54) and (3.56). □

Well, that's it. The cycle index polynomial is the mystery polynomial. In particular, Pólya's theorem can be restated as

$$\begin{aligned} W_G(x_1, x_2, \ldots, x_n) &= \frac{1}{o(G)} \sum_{p \in G} M_1^{c_1(p)} M_2^{c_2(p)} \cdots M_m^{c_m(p)}, \\ &= Z_G(M_1, M_2, \ldots, M_m). \end{aligned} \tag{3.57}$$

That is to say, the pattern inventory $W_G(x_1, x_2, \ldots, x_n)$ is obtained from the cycle index polynomial $Z_G(s_1, s_2, \ldots, s_m)$ by substituting $s_k = x_1^k + x_2^k + \cdots + x_n^k, 1 \leq k \leq m$.

Computing a cycle index polynomial can be a bit complicated. Here are two hints to help avoid common mistakes:

* As abstract groups, G and H are isomorphic, yet their cycle index polynomials are different.

1. $Z_G(s_1, s_2, \ldots, s_m)$ is an average of monomials, one for each permutation in G. So, the sum of its coefficients is 1.
2. In *each* monomial term $\prod s_t^{c_t(p)}$, the sum of the products, $tc_t(p)$, is the degree of G (See Equation (3.52).)

Confirm that these rules hold in Example 3.7.2 and for the cycle index polynomial

$$Z_{S_4}(s_1, s_2, s_3, s_4) = \frac{1}{24}(s_1^4 + 3s_2^2 + 6s_4 + 6s_1^2 s_2 + 8s_1 s_3). \tag{3.58}$$

Obviously important because of its association with Pólya's theorem, the cycle index polynomial emerges in other contexts as well. Notice, e.g., that s_1 occurs in $\prod s_t^{c_t(p)}$ if and only if $c_1(p) > 0$, if and only if p has a fixed point. It follows that the mth derangement number $D(m)$ can be read directly from Z_{S_m} (or, more accurately, from $m!Z_{S_m}$). Apart from $m!$ in the denominator, $D(m)$ is the sum of the coefficients of the terms that do not contain s_1. From Equation (3.58), e.g.,

$$D(4) = 3 + 6 = 9.$$

3.7.3 Definition. To simplify the notation, denote the cycle index polynomial for S_m by Z_m, i.e.,

$$\begin{aligned} Z_m &= Z_m(s_1, s_2, \ldots, s_m) \\ &= Z_{S_m}(s_1, s_2, \ldots, s_m). \end{aligned}$$

We will return momentarily to the substitution $s_k = x_1^k + x_2^k + \cdots + x_n^k$, $1 \le k \le m$. Meanwhile, the next result involves a different substitution.

3.7.4 Theorem. *Setting $s_k = x$ in $m!Z_m(s_1, s_2, \ldots, s_m)$, $1 \le k \le m$, yields*

$$m!Z_m(x, x, \ldots, x) = \sum_{r=1}^{m} s(m, r)x^r,$$

where $s(m, r)$ is a Stirling number of the first kind, $1 \le r \le m$.

Proof

$$m!Z_m(x, x, \ldots, x) = \sum_{p \in S_m} x^{c(p)},$$

where $c(p) = c_1(p) + c_2(p) + \cdots + c_m(p)$ is the number of cycles in the disjoint cycle factorization of p. The coefficient of x^r on the right-hand side of the equation

is $o(\{p \in S_m : c(p) = r\}) = s(m, r)$, the number of permutations whose disjoint cycle factorizations consist of (exactly) r cycles. ■

3.7.5 Example. From Equation (3.58),

$$24Z_4(s_1, s_2, s_3, s_4) = s_1^4 + 3s_2^2 + 6s_4 + 6s_1^2 s_2 + 8s_1 s_3.$$

So,

$$\begin{aligned} 24Z_4(x, x, x, x) &= x^4 + 3x^2 + 6x + 6x^3 + 8x^2 \\ &= x^4 + 6x^3 + 11x^2 + 6x. \end{aligned}$$

By Theorem 3.7.4, the coefficients (in reverse order) are $s(4, 1) = 6, s(4, 2) = 11, s(4, 3) = 6$, and $s(4, 4) = 1$, consistent with the fourth row of Fig. 2.5.2.

Wait a minute. It is customary when writing a polynomial in the single variable x to begin with the highest power of x. It is clear from Example 3.7.5, however, that reversing the terms of $24Z_4(x, x, x, x)$ gives $6x + 11x^2 + 6x^3 + x^4 = s(4, 1)x + s(4, 2)x^2 + s(4, 3)x^3 + s(4, 4)x^4 = g_4(x)$, the *generating function* from Equation (2.29).

3.7.6 Corollary. *Setting $s_k = x$ in $m!Z_m(s_1, s_2, \ldots, s_m), 1 \le k \le m$, yields*

$$\sum_{p \in S_m} x^{c(p)} = x(x + 1)(x + 2) \cdots (x + m - 1).$$

Proof. Theorems 2.5.4 and 3.7.4. ■

This might be a good time to reconfirm that

$$x(x + 1)(x + 2)(x + 3) = x^4 + 6x^3 + 11x^2 + 6x.$$

Recall (Theorem 1.7.5) that there are $C(m + n - 1, m)$ different monomials of degree m in n variables. Thus, a fixed but arbitrary coloring $f \in C_{m,n}$ might have any one of $C(m + n - 1, m)$ different weights $w = w(f)$. Our interest in the pattern inventory stems from the fact that inequivalent colorings can have the same weight. The coefficient of w in $W_G(x_1, x_2, \ldots, x_n)$ is the number of color patterns of weight w.

Suppose $f, g \in C_{m,n}$. Then $w(f) = w(g)$ if and only if the sequences $f = (f(1), f(2), \ldots, f(m))$ and $g = (g(1), g(2), \ldots, g(m))$ contain the same colors, with the same multiplicities, if and only if the sequence g is some rearrangement of the sequence f, if and only if $g = fp$ for some permutation $p \in S_m$, if and only if $\hat{p}(g) = gp^{-1} = f$ for some $p \in S_m$. In other words, two color patterns modulo S_m are equal if and only if they have the same weight. It follows that the pattern inventory for S_m is a sum of all $C(m + n - 1, m)$ monomials of degree m in $x_1, x_2, \ldots, x_n$, each occurring with multiplicity 1.

Let's work out the pattern inventory for S_4 when $n = 3$. Setting $x_1 = x, x_2 = y$, and $x_3 = z$ in Equations (3.57) and (3.58) yields (check it)

$$\begin{aligned} W_{S_4}(x,y,z) &= Z_4(x+y+z,\ x^2+y^2+z^2,\ x^3+y^3+z^3,\ x^4+y^4+z^4) \\ &= \frac{1}{24}[(x+y+z)^4 + 3(x^2+y^2+z^2)^2 + 6(x^4+y^4+z^4) \\ &\quad + 6(x+y+z)^2(x^2+y^2+z^2) + 8(x+y+z)(x^3+y^3+z^3)] \\ &= [x^4+y^4+z^4] + [x^3y+x^3z+xy^3+xz^3+y^3z+yz^3] \\ &\quad + [x^2y^2+x^2z^2+y^2z^2] + [x^2yz+xy^2z+xyz^2] \\ &\quad + M_{[4]}(x,y,z) + M_{[3,1]}(x,y,z) + M_{[2^2]}(x,y,z) + M_{[2,1^2]}(x,y,z). \end{aligned} \tag{3.59}$$

As predicted, each of the $C(4+3-1,4) = 15$ monomials of degree 4 occurs exactly once in Equation (3.59).

3.7.7 Definition. The mth *homogeneous symmetric function* $H_m(x_1, x_2, \ldots, x_n)$ is the sum of all $C(m+n-1,m)$ monomials of (total) degree m in the variables $x_1, x_2, \ldots, x_n$, i.e.,

$$H_m(x_1, x_2, \ldots, x_n) = \sum_{\pi} M_\pi(x_1, x_2, \ldots, x_n),$$

where the summation is over the partitions π of m having at most n parts.

Definition 3.7.7 is extended by defining $H_0(x_1, x_2, \ldots, x_n) = 1$.

3.7.8 Theorem. *The mth homogeneous symmetric function*

(a) $H_m(x_1, x_2, \ldots, x_n) = Z_m(M_1, M_2, \ldots, M_m)$,

where $M_t = M_{[t]}(x_1, x_2, \ldots, x_n) = x_1^t + x_2^t + \ldots + x_n^t, 1 \le t \le m$, *and*

(b) $$H_m(x_1, x_2, \ldots, x_n) = \sum_{f \in G_{m,n}} \prod_{i=1}^{m} x_{f(i)},$$

where $G_{m,n} \subset F_{m,n}$ *is the set of all* $C(m+n-1,m)$ *nondecreasing functions from* $\{1, 2, \ldots, m\}$ *into* $\{1, 2, \ldots, n\}$.

Proof. Part (a) summarizes the previous discussion. Since the terms in a product of commuting variables can be rearranged into nondecreasing order, part (b) is just a restatement of the definition. ■

The homogeneous symmetric functions have many properties reminiscent of the more glamorous elementary symmetric functions. For one thing, Theorem 3.7.8(b) is the natural analog of Theorem 2.1.9:

$$E_m(x_1, x_2, \ldots, x_n) = \sum_{f \in Q_{m,n}} \prod_{i=1}^{m} x_{f(i)},$$

where $Q_{m,n}$ is the subset of $F_{m,n}$ consisting of the $C(m,n)$ (strictly) increasing functions. Another similarity involves Stirling numbers. Recall (Corollary 2.5.5) that the Stirling number of the first kind, $s(m,n) = E_{m-n}(1,2,\ldots,m-1)$.

3.7.9 Theorem. *The Stirling number of the second kind,* $S(m,n) = H_{m-n}(1,2,\ldots,n), 1 \le n \le m$.

Proof. Define $h(m,n) = H_{m-n}(1,2,\ldots,n), 1 \le n \le m$. Because the arrays $h(m,n)$ and $S(m,n)$ satisfy the same initial conditions and the same recurrence (see Exercise 11, Section 2.1), they must be identical. ■

The next identity relates binomial coefficients to cycle structure.

3.7.10 Corollary. *If m and n are any two positive integers, then*

$$C(m+n-1,m) = \frac{1}{m!}\sum_{p\in S_m} n^{c(p)}.$$

Proof. Set $x_1 = x_2 = \cdots = x_n = 1$ in Theorem 3.7.8 or set $x = n$ in Corollary 3.7.6. ■

Pólya's theorem can be found in a 1937 paper entitled Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen (Combinatorial Enumeration for Groups, Graphs, and Chemical Compounds).* The part about graphs will be discussed in Chapter 5. That application requires the cycle index polynomial of the so-called *pair group*, bringing us to the final topic of this chapter.

3.7.11 Definition. Let $V = \{1,2,\ldots,m\}$, and define $V^{(2)}$ to be the family of all $C(m,2)$ two-element subsets of V. For each $p \in S_m$, let $\tilde{p}$ be the natural action of p on $V^{(2)}$ defined by $\tilde{p}(\{i,j\}) = \{p(i),p(j)\}$.† The *pair group* $S_m^{(2)} = \{\tilde{p} : p \in S_m\}$.

Because $\tilde{p}\tilde{q} = \widetilde{pq}$ for all $p,q \in S_m$ (see Exercise 6), $S_m^{(2)}$ is closed, i.e., it is a permutation group acting on $V^{(2)}$. Because $o(V^{(2)}) = C(m,2)$, we may view $S_m^{(2)}$ as a subgroup of $S_{C(m,2)}$. (Since $o(S_m^{(2)}) = m!$ is much less than $[\frac{1}{2}m(m-1)]! = o(S_{C(m,2)})$, $S_m^{(2)}$ is a relatively small subgroup of $S_{C(m,2)}$.)

*See G. Pólya and R. C. Read, Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds, Springer-Verlag, New York, 1987.

†Similar induced actions can be found in Section 3.4.

p	$\tilde{p}$	p	$\tilde{p}$	p	$\tilde{p}$
e_4	$\mathbf{e_6}$	(123)	(**142**) (**356**)	(1234)	(**1463**) (**25**)
(12)	(**24**) (**35**)	(124)	(**153**) (**246**)	(1243)	(**1562**) (**34**)
(13)	(**14**) (**36**)	(132)	(**124**) (**365**)	(1324)	(**16**) (**2453**)
(14)	(**15**) (**26**)	(134)	(**145**) (**263**)	(1342)	(**1265**) (**34**)
(23)	(**12**) (**56**)	(142)	(**135**) (**264**)	(1423)	(**16**) (**2354**)
(24)	(**13**) (**46**)	(143)	(**154**) (**236**)	(1432)	(**1364**) (**25**)
(34)	(**23**) (**45**)	(234)	(**123**) (**465**)	(12) (34)	(**25**) (**34**)
(13) (24)	(**16**) (**34**)	(243)	(**132**) (**456**)	(14) (23)	(**16**) (**25**)

Figure 3.7.1. The pair group $S_4^{(2)} = \{p : p \in S_4\}$.

3.7.12 Example. If $m = 4$, then $V^{(2)} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\}$. Numbering the elements of $V^{(2)}$ in dictionary order, using **boldface** numerals, we have

$$\mathbf{1} = \{1,2\}, \qquad \mathbf{2} = \{1,3\}, \qquad \mathbf{3} = \{1,4\},$$
$$\mathbf{4} = \{2,3\}, \qquad \mathbf{5} = \{2,4\}, \qquad \mathbf{6} = \{3,4\}.$$

Suppose $p = (123) \in S_4$. Let's compute the disjoint cycle factorization of $\tilde{p} \in S_4^{(2)}$:

$$\tilde{p}(\mathbf{1}) = \tilde{p}(\{1,2\}) = \{p(1), p(2)\} = \{2,3\} = \mathbf{4},$$
$$\tilde{p}(\mathbf{4}) = \tilde{p}(\{2,3\}) = \{p(2), p(3)\} = \{3,1\} = \mathbf{2},$$
$$\tilde{p}(\mathbf{2}) = \tilde{p}(\{1,3\}) = \{p(1), p(3)\} = \{2,1\} = \mathbf{1}.$$

So, (**142**) is a cycle of $\tilde{p}$. Continuing,

$$\tilde{p}(\mathbf{3}) = \tilde{p}(\{1,4\}) = \{p(1), p(4)\} = \{2,4\} = \mathbf{5},$$
$$\tilde{p}(\mathbf{5}) = \tilde{p}(\{2,4\}) = \{p(2), p(4)\} = \{3,4\} = \mathbf{6},$$
$$\tilde{p}(\mathbf{6}) = \tilde{p}(\{3,4\}) = \{p(3), p(4)\} = \{1,4\} = \mathbf{3}.$$

Therefore, $\tilde{p} = (\mathbf{142})(\mathbf{356}) \in S_4^{(2)}$. All $4! = 24$ elements of the pair group $S_4^{(2)}$ can be found in Fig. 3.7.1. □

Using Fig. 3.7.1, it is easy to produce the cycle index polynomial

$$Z_{S_4^{(2)}}(s_1, s_2, \ldots, s_6) = \frac{1}{24}(s_1^6 + 9s_1^2 s_2^2 + 8s_3^2 + 6s_2 s_4). \tag{3.60}$$

On the other hand, if all we want is its cycle index polynomial, it is not necessary to compute the disjoint cycle factorization of *every* element of $S_m^{(2)}$.

3.7.13 Lemma. *Let $\tilde{p}$ and $\tilde{q}$ be the elements of $S_m^{(2)}$ induced by the permutations p and q of S_m, respectively. If p and q have the same structure, then $\tilde{p}$ and $\tilde{q}$ have the same cycle structure.*

Proof. Let $p \in S_m$. Fix $i,j \in \{1,2,\ldots,m\}$. Let p_1 be the permutation obtained by interchanging the positions of i and j in the disjoint cycle factorization of p. Then p_1 has the same cycle structure as p. Moreover, $\tilde{p}_1$ can be obtained by interchanging the positions of $\mathbf{r_k} = \{i,k\}$ and $\mathbf{t_k} = \{j,k\}$ in the disjoint cycle factorization of $\tilde{p}$ for each k different from i and j. In particular, $\tilde{p}_1$ and $\tilde{p}$ have the same cycle structure. Because p and q have the same cycle structure if and only if q can be obtained from p by a sequence of such interchanges, the proof is complete. ■

3.7.14 Example. The converse of Lemma 3.7.13 is false. If $p = (12)$ and $q = (13)(24)$, then (Fig. 3.7.1) both $\tilde{p}$ and $\tilde{q}$ have cycle type $[2^2, 1^2]$. □

It follows from Lemma 3.7.13 that the cycle index polynomial for $S_m^{(2)}$ is just a modification of Z_m.

3.7.15 Example. Recall from Equation (3.58) that

$$Z_4(s_1,s_2,s_3,s_4) = \frac{1}{24}(s_1^4 + 3s_2^2 + 6s_4 + 6s_1^2 s_2 + 8s_1 s_3). \tag{3.61}$$

To see how Z_4 can be modified to obtain the cycle index polynomial for the pair group $S_4^{(2)}$, observe that since $\tilde{e}_4 = \mathbf{e_6}$, the monomial of s_1^4 in Z_4 should be replaced with s_1^6. Because (see Fig. 3.7.1) the induced action on $V^{(2)}$ of $p = (12)(34)$ is $\tilde{p} = (\mathbf{25})(\mathbf{34})$, the term $3s_2^2$ in Z_4, corresponding to the three permutations in S_4 of cycle type $[2^2]$, is replaced with $3s_1^2 s_2^2$. For the same reason, $6s_4$ is replaced with $6s_2 s_4$ and $6s_1^2 s_2$ with $6s_1^2 s_2^2$. When $8s_3^2$ is substituted for $8s_1 s_3$ and like terms are combined, the transformation of Equation (3.61) into Equation (3.60) is complete. □

3.7.16 Example. The cycle index polynomial for $S_5^{(2)}$ is

$$\tfrac{1}{120}[s_1^{10} + 10s_1^4 s_2^3 + 20s_1 s_3^3 + 15s_1^2 s_2^4 + 30s_2 s_4^2 + 20s_1 s_3 s_6 + 24s_5^2]. \qquad \square$$

3.7.17 Example. The cycle index polynomial for $S_6^{(2)}$ is

$$\tfrac{1}{720}[s_1^{15} + 15s_1^7 s_2^4 + 40s_1^3 s_3^4 + 60s_1^3 s_2^6 + 180s_1 s_2 s_4^3 + 144s_5^3 + 120s_1 s_2 s_3^2 s_6 + 40s_3^5 + 120s_3 s_6^2]. \qquad \square$$

3.7. EXERCISES

1 Compute Z_3, the cycle index polynomial for S_3.

2 Use the result of Exercise 1

(a) to compute the derangement number $D(3)$.

(b) to confirm Theorem 3.7.4 when $m = 3$.

(c) and Theorem 3.7.8(a) to compute $H_3(x, y)$.
(d) Use Theorem 3.7.8(b) to compute $H_3(x, y)$.
(e) Use Theorem 3.7.9 and your answer to parts (c) and (d) to compute $S(5, 2)$.
(f) Modify the approach of part (e) to compute $S(6, 3)$.

3 Confirm Corollary 3.7.10 when $m = 3$.

4 Compute the cycle index polynomial for the cyclic group
(a) $G = \langle(12345)\rangle$. **(b)** $G = \langle(123456)\rangle$.
(c) $G = \langle(1234567)\rangle$. **(d)** $G = \langle(12345678)\rangle$.

5 Let G be the rotational symmetry group of a cube.
(a) If G is expressed as permutations of the faces of the cube, show that

$$Z_G(s_1, s_2, \ldots, s_6) = \tfrac{1}{24}[s_1^6 + 3s_1^2s_2^2 + 6s_1^2s_4 + 6s_2^3 + 8s_3^2].$$

(Note that s_5 and s_6 are missing from the right-hand side of this expression.)
(b) If G is expressed as permutations of the vertices of the cube, show that

$$Z_G(s_1, s_2, \ldots, s_8) = \tfrac{1}{24}[s_1^8 + 9s_2^4 + 6s_4^2 + 8s_1^2s_3^2].$$

6 Let $\tilde{p}$ and $\tilde{q}$ be the elements $S_m^{(2)}$ induced by the permutations p and q of S_m, respectively. Prove that
(a) $\tilde{p}\tilde{q} = \widetilde{pq}$. **(b)** $\tilde{p}^{-1} = \widetilde{p^{-1}}$.

7 Use Fig. 3.7.1 to confirm Exercise 6(b) when
(a) $p = (123)$. **(b)** $p = (1234)$.
(c) $p = (1324)$. **(d)** $p = (1423)$.

8 Compute $Z_5(s_1, s_2, \ldots, s_5)$, the cycle index polynomial for S_5.

9 Use the result of Exercise 8
(a) to compute the derangement number $D(5)$.
(b) to confirm Theorem 3.7.4 when $m = 5$.
(c) and Theorem 3.7.8(a) to compute $H_5(x, y)$.
(d) Use Theorem 3.7.8(b) to compute $H_5(x, y)$.
(e) Use Theorem 3.7.9 and your answer to parts (c) and (d) to compute $S(7, 2)$.

10 Suppose the group of symmetries of the m faces of some object is $G = S_m$.
(a) Show that two colorings of the faces of the object are equivalent if and only if they have the same weight.
(b) Give a combinatorial argument, independent of Corollary 3.7.10, to show that the number of inequivalent n-colorings of the m faces of the object is $C(m + n - 1, m)$.

11 Show that the partial derivative of Z_5 with respect to s_1 is Z_4.

12 Show that the partial derivative of Z_m with respect to s_m is $(m-1)!$.

13 Confirm Example 3.7.16.

14 Define $Z_0 = 1$ (and recall that $Z_m = Z_m(s_1, s_2, \ldots, s_m)$). It can be shown that

$$mZ_m = \sum_{k=1}^{m} s_k Z_{m-k}.$$

(a) Confirm this result when $m = 4$.

(b) Use this result to compute Z_6. (*Hint*: Exercise 8.)

(c) Confirm your answer to part (b) by computing Z_6 directly from the definition of cycle index polynomial.

15 Use the result of Exercise 14(b) or (c) to

(a) evaluate the derangement number $D(6)$.

(b) confirm the $m = 6$ case of Theorem 3.7.4.

16 Show that the pair group $S_4^{(2)}$ is the group of (all 24) symmetries of a regular tetrahedron expressed as permutations of its six edges. (See Exercise 16, Section 3.6.)

17 Let G be the rotational symmetry group of a regular dodecahedron, expressed as permutations of its 12 faces. (See Exercise 17, Section 3.4.) Show that

$$Z_G(s_1, s_2, \ldots, s_{12}) = \tfrac{1}{60}(s_1^{12} + 16s_2^6 + 20s_3^4 + 24s_1^2 s_5^2).$$

18 Prove that

$$\frac{1}{m!}\sum_{r=1}^{m} s(m,r)n^r = C(m+n-1, m).$$

19 Prove that

$$k^m = \sum_{r=1}^{m} (-1)^{m+r} r! S(m,r) C(k+r-1, r).$$

20 Prove that

$$Z_m(s_1, s_2, \ldots, s_m) = \sum \frac{s_1^{k_1} s_2^{k_2} \ldots s_m^{k_m}}{1^{k_1} k_1! 2^{k_2} k_2! \ldots m^{k_m} k_m!},$$

where the sum is over all nonnegative integer sequences $k_1, k_2, \ldots, k_m$ satisfying $k_1 + 2k_2 + 3k_3 + \cdots + mk_m = m$. (*Hint*: Exercise 19, Section 2.4.)

21 The analogue of Theorem 3.7.8(a) for elementary symmetric functions, namely,

$$E_m(x_1, x_2, \ldots, x_n) = (-1)^m Z_m(-M_1, -M_2, \ldots, -M_m),$$

can be proved using Newton's identities. Show that

(a) Equation (1.40) in Section 1.9 is the $m = 2$ case of this equation.

(b) Equation (1.41) is the $m = 3$ case of this equation.

(c) Equation (1.42) is the $m = 4$ case of this equation.

22 If

$$U_m = \begin{pmatrix} s_1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ s_2 & s_1 & 2 & 0 & \cdots & 0 & 0 \\ s_3 & s_2 & s_1 & 3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ s_{m-1} & s_{m-2} & s_{m-3} & s_{m-4} & \cdots & s_1 & m-1 \\ s_m & s_{m-1} & s_{m-2} & s_{m-3} & \cdots & s_2 & s_1 \end{pmatrix},$$

then $\text{per}(U_m) = m! Z_m(s_1, s_2, \ldots, s_m)$, where "per" is the *permanent* function defined in Exercise 19, Section 3.5. Confirm this formula when

(a) $m = 2$. **(b)** $m = 3$. **(c)** $m = 4$.

23 Let L_m be the matrix obtained from U_m (Exercise 22) by replacing s_t with $M_t = M_{[t]}(x_1, x_2, \ldots, x_n), 1 \le t \le m$. Then (Exercise 20, Section 1.9), $\det(L_m) = m! E_m(x_1, x_2, \ldots, x_n)$. It follows from Theorem 3.7.8(a) and Exercise 22 that $\text{per}(L_m) = m! H_m(x_1, x_2, \ldots, x_n)$. Confirm this formula for H_m when

(a) $m = 2$. **(b)** $m = 3$. **(c)** $m = 4$.

24 Confirm the computations leading to Equation (3.59).

25 Use Theorem 3.7.9 to compute

(a) $S(6, 4)$. **b** $S(5, 3)$.

26 Prove Cauchy's identity: $\sum (1^{k_1} k_1! 2^{k_2} k_2! \cdots m^{k_m} k_m!)^{-1} = 1$, where the sum is over all nonnegative integer sequences $k_1, k_2, \ldots, k_m$ satisfying $k_1 + 2k_2 + 3k_3 + \cdots + mk_m = m$. (*Hint*: Exercise 20.)

4

Generating Functions

On a superficial level, a generating function is simply a way to exhibit a sequence of numbers $a_0, a_1, a_2, \ldots$. However, the act of writing

$$g(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

has some surprising consequences. Because the left-hand side of this expression *looks* like a function, it is tempting to treat the right-hand side as if it were one, a "mistake" having some interesting implications.

Those sequences $a_0, a_1, a_2, \ldots$ with the property that a_n is a polynomial function of n are characterized in the first section. *Ordinary* generating functions and some of their properties are discussed in Section 4.2. Applications, e.g., to Newton's binomial theorem, are the focus of Section 4.3. Section 4.4 deals with some variations on the generating function idea. Techniques for solving recurrences occupy the final section.

Apart from the observation in Section 4.2 that the pattern inventory is a generating function, one that doesn't generate anything but is generated by the cycle index polynomial, Chapter 4 is independent of Chapter 3. Readers may go directly from Chapter 2 to Chapter 4. Natural places to exit from Chapter 4 are the ends of Sections 4.1 or 4.3, just before Definition 4.4.9 in Section 4.4, or at the end of Section 4.4.

4.1. DIFFERENCE SEQUENCES

A standard feature of American education in the mid-twentieth century was the so-called IQ test. Typical of these tests were pattern recognition problems like this:

$$6, 13, 20, 27, \_\_\,, \tag{4.1}$$

it being understood that one should find the next number in the sequence after 27. Because the next Sunday after June 27, 2004, is the fourth of July, it may be

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

that the answer is 4. Doubtless the author of the test had another answer in mind,* probably 34.

4.1.1 Definition. The notation $\{a_n\}$ is used to denote the sequence $a_0, a_1, a_2, \ldots$.

Note that the first *number* in the sequence $\{a_n\}$ is the zeroth *term*, a_0. The 4th number in Sequence (4.1) is $27 = a_3$. (While this system may seem awkward now, it will simplify our work later on.)

4.1.2 Definition. The sequence $\{a_n\}$ is *arithmetic* if, for all $n \geq 0$, the difference $a_{n+1} - a_n = d$ is a constant, independent of n.

An arithmetic sequence satisfies the pattern, or *recurrence*, $a_{n+1} = a_n + d$, $n \geq 0$. *Given* that Sequence (4.1) comprises an arithmetic sequence, then $d = 7$, and there can be no ambiguity about the 5th number. It is $a_4 = 27 + 7 = 34$. So far, so good. Now you know how to exhibit intelligence by the standards of the last century.

What if you were asked to determine, not a_4, but a_{400}? Using the recurrence $a_{400} = a_{399} + 7$ is not much help. The key to *solving* Sequence (4.1) is to think of it symbolically, as

$$6, 6 + 7, (6 + 7) + 7, (6 + 7 + 7) + 7, \ldots$$

From this perspective, it is clear that a_n is a sum of $n + 1$ numbers, one 6 and n 7's, i.e., $a_n = 7n + 6$. So, $a_{400} = 7 \times 400 + 6 = 2806$. This solution illustrates the tension between mathematics and computation. Doing the arithmetic at each step leads to $a_{400} = a_{399} + 7$. Not doing the arithmetic reveals a pattern leading to the mathematical abstraction $a_n = 7n + 6$.

More generally, every arithmetic sequence takes the form

$$a_0, a_0 + d, a_0 + 2d, a_0 + 3d, \ldots$$

So, the nth term of an arithmetic sequence (the $(n + 1)$st number in the sequence) is

$$a_n = dn + a_0. \tag{4.2}$$

An expression like Equation (4.2), in which a_n is given as an explicit function of n, is called a *closed formula*, or *solution*, for $\{a_n\}$.

Associated with the sequence $\{a_n\}$ is a natural function of the nonnegative integers, namely, $f(n) = a_n$, $n \geq 0$. Conversely, to any function f of the nonnegative integers, there corresponds a natural sequence, namely, $\{f(n)\}$. Informally, a closed formula for $\{a_n\}$ is a "nice" description of the corresponding function, e.g., $\{a_n\}$ is arithmetic if and only if it corresponds to a function of the form $f(n) = dn + a_0$, i.e., to a polynomial of degree (at most) 1.

*Do high IQ scores correlate best with an ability to recognize patterns, an ability to choose most plausible patterns, or an ability to read the minds of the authors of the tests?

Consider the sequence $\{n^2\}$, i.e.,

$$0, 1, 4, 9, 16, 25, \ldots$$

It is *not* arithmetic. For one thing, the closed formula $f(n) = n^2$ is a nonlinear polynomial. For another, while a_{n+1} is obtained from a_n by adding an odd number, that number changes. The difference, $a_{n+1} - a_n = (n+1)^2 - n^2 = 2n + 1$, is not constant.

4.1.3 Definition. Let $\{a_n\}$ be a fixed but arbitrary sequence. Its *difference sequence*, denoted $\{\Delta a_n\}$, is defined by $\Delta a_n = a_{n+1} - a_n$, $n \geq 0$.

Perhaps $\Delta(a_n)$ would be a better notation. Certainly, Δa_n should not be confused with a product of Δ and a_n. Whatever the notation, $\{a_n\}$ is an arithmetic sequence if and only if its difference sequence $\{\Delta a_n\}$ is constant, that is, $\Delta a_n = d$, $n \geq 0$. When $a_n = n^2$, $\Delta a_n = 2n + 1$. In other words, $\{\Delta n^2\} = \{2n + 1\}$.

If $f(n) = a_n$, $n \geq 0$, then $\Delta a_n = \Delta f(n) = f(n+1) - f(n)$. It seems that

$$\Delta f(n) = \frac{f(n+1) - f(n)}{1} \tag{4.3}$$

is a kind of *discrete derivative*.

It can be revealing to look at a sequence and its difference sequence (*also called sequence of differences) side by side. In the case of* $\{n^2\}$*, the side-by-side comparison looks like this:*

$$\begin{array}{cccccccccc} 0, & 1, & 4, & 9, & 16, & 25, & 36, & 49, & \ldots \\ 1, & 3, & 5, & 7, & 9, & 11, & 13, & \ldots \end{array}$$

Evidently, the difference sequence of the sequence of perfect squares is the sequence of odd numbers. More useful to our present objective is the fact that the difference sequence is arithmetic. This suggests looking at the difference sequence of a difference sequence. The following *difference array* gives two generations of difference sequences for $\{n^2\}$:

$$\begin{array}{cccccccccc} 0, & 1, & 4, & 9, & 16, & 25, & 36, & 49, & \ldots \\ 1, & 3, & 5, & 7, & 9, & 11, & 13, & \ldots \\ 2, & 2, & 2, & 2, & 2, & 2, & \ldots \end{array}$$

Denote by $\{\Delta^2 a_n\}$ the difference sequence of the difference sequence, Then, e.g., $\{\Delta^2 n^2\} = \{2\}$, the constant sequence each of whose terms is 2. In general,

$$\begin{aligned} \Delta^2 a_n &= \Delta a_{n+1} - \Delta a_n \\ &= a_{n+2} - 2a_{n+1} + a_n, \end{aligned} \tag{4.4}$$

$$
\begin{array}{cccccccc}
a_0, & a_1, & a_2, & a_3, & a_4, & a_5, & a_6, & \cdots \\
\Delta a_0, & \Delta a_1, & \Delta a_2, & \Delta a_3, & \Delta a_4, & \Delta a_5, & \cdots & \\
\Delta^2 a_0, & \Delta^2 a_1, & \Delta^2 a_2, & \Delta^2 a_3, & \Delta^2 a_4, & \cdots & & \\
\Delta^3 a_0, & \Delta^3 a_1, & \Delta^3 a_2, & \Delta^3 a_3, & \cdots & & & \\
 & & \cdots & & & & &
\end{array}
$$

Figure 4.1.1. A generic difference array.

Letting $\Delta^0 a_n = a_n$ and $\Delta^1 a_n = \Delta a_n$, we can define $\Delta^{r+1} a_n = \Delta(\Delta^r a_n)$ for all $r \geq 1$, i.e.,

$$\Delta^{r+1} a_n = \Delta^r a_{n+1} - \Delta^r a_n, \qquad r \geq 1. \tag{4.5}$$

Successive generations of difference sequences are displayed in Fig. 4.1.1.

4.1.4 Example. The difference array for $\{n^3\}$ is

$$
\begin{array}{cccccccccc}
0, & 1, & 8, & 27, & 64, & 125, & 216, & 343, & \ldots \\
1, & 7, & 19, & 37, & 61, & 91, & 127, & \ldots & \\
6, & 12, & 18, & 24, & 30, & 36, & \ldots & & \\
6, & 6, & 6, & 6, & 6, & \ldots & & &
\end{array}
$$

While one could write out additional rows, there isn't much point in doing so. If the fourth row, corresponding to $\{\Delta^3 n^3\}$, is constant, then each row after the fourth consists entirely of zeros. But, is the fourth row really constant? Let's see.

If $\{a_n\}$ is any sequence, then $\Delta a_n = a_{n+1} - a_n$. From Equation (4.4), $\Delta^2 a_n = a_{n+2} - 2a_{n+1} + a_n$. From Equation (4.5),

$$
\begin{aligned}
\Delta^3 a_n &= \Delta^2 a_{n+1} - \Delta^2 a_n \\
&= (a_{n+3} - 2a_{n+2} + a_{n+1}) - (a_{n+2} - 2a_{n+1} + a_n) \\
&= a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n.
\end{aligned} \tag{4.6}
$$

Substituting $a_n = n^3$ into Equation (4.6) yields

$$
\begin{aligned}
\Delta^3 n^3 &= (n+3)^3 - 3(n+2)^3 + 3(n+1)^3 - n^3 \\
&= (n^3 + 9n^2 + 27n + 27) - 3(n^3 + 6n^2 + 12n + 8) + 3(n^3 + 3n^2 + 3n + 1) - n^3 \\
&= 6
\end{aligned}
$$

for all n. □

Is it too early to guess a pattern? Might $\{\Delta^4 a_n\}$ be constant when $a_n = n^4$? More generally, might $\{\Delta^r a_n\}$ be constant when $\{a_n\} = \{n^r\}$. If so, can the constant be predicted in advance? Before we can answer such questions, we need to know a little more about $\{\Delta^r a_n\}$.

4.1.5 Lemma. *If $\{a_n\}$ is a sequence then, for all $n \geq 0$,*

$$\Delta^r a_n = \sum_{t=0}^{r} (-1)^{r+t} C(r,t) a_{n+t}.$$

Proof. The identity has already been established for small r (see, e.g., Equations (4.4) and (4.6)). From Equation (4.5) and induction on r,

$$\begin{aligned}
\Delta^{r+1} a_n &= \Delta^r a_{n+1} - \Delta^r a_n \\
&= \sum_{t=0}^{r} (-1)^{r+t} C(r,t) a_{n+1+t} - \sum_{t=0}^{r} (-1)^{r+t} C(r,t) a_{n+t} \\
&= \sum_{t=1}^{r+1} (-1)^{r+t-1} C(r,t-1) a_{n+t} + \sum_{t=0}^{r} (-1)^{r+t-1} C(r,t) a_{n+t} \\
&= a_{n+r+1} + \sum_{t=1}^{r} (-1)^{r+t-1} [C(r,t-1) + C(r,t)] a_{n+t} + (-1)^{r-1} a_n \\
&= \sum_{t=0}^{r+1} (-1)^{r+1+t} C(r+1,t) a_{n+t}.
\end{aligned}$$

■

With the help of Lemma 4.1.5, we can answer our questions about $\{\Delta^r n^r\}$.

4.1.6 Theorem. *Suppose r is a fixed but arbitrary positive integer. Let $a_n = n^r$, $n \geq 0$. Then $\Delta^r a_n = r!$, $n \geq 0$.*

Proof. By Lemma 4.1.5,

$$\begin{aligned}
\Delta^r n^r &= \sum_{t=0}^{r} (-1)^{r+t} C(r,t) (n+t)^r \\
&= \sum_{t=0}^{r} (-1)^{r+t} C(r,t) \sum_{m=0}^{r} C(r,m) n^{r-m} t^m \\
&= \sum_{m=0}^{r} C(r,m) n^{r-m} \sum_{t=0}^{r} (-1)^{r+t} C(r,t) t^m \\
&= \sum_{m=0}^{r} C(r,m) n^{r-m} r! S(m,r)
\end{aligned}$$

by Stirling's identity. Because the Stirling number of the second kind, $S(m,r)$, is equal to 0 when $m < r$ and equal to 1 when $m = r$, the only surviving term in the final summation is $C(r,r) n^{r-r} r! = r!$. ■

4.1.7 Corollary. *Suppose m is a fixed but arbitrary positive integer. Then $\Delta^{r+1}n^m = 0$ for all $n \geq 0$ and all $r \geq m$.*

Proof. From Theorem 4.1.6, $\Delta^{m+1}n^m = \Delta(\Delta^m n^m) = \Delta m! = m! - m! = 0$. If $r > m$, then $\Delta^{r+1}n^m = \Delta^{r-m}(\Delta^{m+1}n^m) = \Delta^{r-m}0 = 0$. ■

Corollary 4.1.7 remains valid when n^m is replaced by any polynomial in n of degree m.

4.1.8 Theorem. *Let m be a fixed but arbitrary positive integer. Suppose f is a polynomial of degree m. If $a_n = f(n)$, $n \geq 0$, then $\Delta^{r+1}a_n = 0$ for all $n \geq 0$ and all $r \geq m$.*

Proof. Suppose $\{y_n\}$ and $\{z_n\}$ are sequences. Let b and c be numbers. Then

$$\begin{aligned}\Delta(by_n + cz_n) &= (by_{n+1} + cz_{n+1}) - (by_n + cz_n)\\ &= b(y_{n+1} - y_n) + c(z_{n+1} - z_n)\\ &= b\,\Delta y_n + c\,\Delta z_n.\end{aligned}$$

So, Δ is linear. Therefore,

$$\begin{aligned}\Delta^2(by_n + cz_n) &= \Delta(\Delta(by_n + cz_n))\\ &= \Delta(b\,\Delta y_n + c\,\Delta z_n)\\ &= b\,\Delta^2 y_n + c\,\Delta^2 z_n,\end{aligned}$$

and, more generally, $\Delta^k(by_n + cz_n) = b\,\Delta^k y_n + c\,\Delta^k z_n$ for all $k \geq 1$. If $f(x) = c_0x^m + c_1x^{m-1} + \cdots + c_m$ and $a_n = f(n)$, $n \geq 0$, then

$$\begin{aligned}\Delta^{r+1}a_n &= \Delta^{r+1}f(n)\\ &= \Delta^{r+1}(c_0n^m + c_1n^{m-1} + \cdots + c_m)\\ &= c_0\,\Delta^{r+1}n^m + c_1\,\Delta^{r+1}n^{m-1} + \cdots + c_m\,\Delta^{r+1}(1)\\ &= 0\end{aligned}$$

by linearity and Corollary 4.1.7. ■

4.1.9 Example. Consider the sequence $\{a_n\}$ the first few terms of which are

$$1, 6, 15, 28, 45, 66, 91, \ldots$$

Successive terms of this fragment of a sequence differ by 5, 9, 13, 17, 21, and 25, respectively. If this pattern were to continue, the difference sequence would be arithmetic, with $\Delta a_n = 4n+5$, $n \geq 0$, and the second difference sequence would be $\{4\}$. This is consistent with the nth term of the (original) sequence being of the form $f(n) = an^2 + bn + c$. Substituting $n = 0, 1$, and 2, respectively, yields the linear system

$$\begin{aligned} c &= 1 \\ a + b + c &= 6 \\ 4a + 2b + c &= 15 \end{aligned}$$

which has the unique solution $a = 2$, $b = 3$, and $c = 1$. Computations confirm that

$$\begin{aligned} a_n &= f(n) \\ &= 2n^2 + 3n + 1, \qquad 0 \leq n \leq 6. \end{aligned}$$

□

Some interesting questions are suggested by Example 4.1.9: (1) Is the converse of Theorem 4.1.8 always true? (2) If so, is there some easy way to find the polynomial function f, short of solving a system of linear equations? The answers to these questions are yes and yes. To see why, consider the $n = 0$ case of Lemma 4.1.5, i.e.,

$$\Delta^r a_0 = \sum_{t=0}^{r} (-1)^{r+t} C(r,t) a_t.$$

Multiply both sides of this equation by $C(n,r)$ and sum on r to obtain

$$\sum_{r=0}^{n} C(n,r)\, \Delta^r a_0 = \sum_{r=0}^{n} \sum_{t=0}^{r} (-1)^{r+t} C(n,r) C(r,t) a_t.$$

Because $C(r,t) = 0$ when $t > r$, we can let the second sum on the right-hand side run from $t = 0$ to $t = n$. That makes it easy to reverse the order of the summations so as to obtain

$$\begin{aligned} \sum_{r=0}^{n} C(n,r)\, \Delta^r a_0 &= \sum_{t=0}^{n} a_t \sum_{r=0}^{n} (-1)^{r+t} C(n,r) C(r,t) \\ &= \sum_{t=0}^{n} a_t \delta_{n,t} \\ &= a_n \end{aligned} \tag{4.7}$$

by the alternating-sign theorem for inverting Pascal matrices.*

*Strictly speaking, we have used an extension of the alternating-sign theorem found in Exercise 25, Section 1.5.

For the sequence fragment in Example 4.1.9, $\Delta^0 a_0 = a_0 = 1$, $\Delta^1 a_0 = \Delta a_0 = 5$, $\Delta^2 a_0 = 4$, and $\Delta^r a_0 = 0$ for all $r \geq 3$. Thus, according to Equation (4.7),

$$\begin{aligned} a_n &= C(n,0) \times 1 + C(n,1) \times 5 + C(n,2) \times 4 \\ &= 1 + 5n + 4n(n-1)/2 \\ &= 2n^2 + 3n + 1, \end{aligned}$$

precisely the polynomial obtained in the example by solving a system of linear equations.

If $f(n) = a_n$, $n \geq 0$, then $\Delta^r a_n = \Delta^r f(n)$, $r, n \geq 0$. In particular, $\Delta^r a_0 = \Delta^r f(0)$ for all $r \geq 0$. Hence, by Equation (4.7),

$$\begin{aligned} f(n) &= \sum_{r=0}^{n} C(n,r)\, \Delta^r f(0) \\ &= \sum_{r=0}^{n} \frac{\Delta^r f(0)}{r!} n^{(r)} \end{aligned}$$

because $C(n,r) = n^{(r)}/r!$. Since $n^{(r)} = 0$, $r > n$, this last equation can be expressed in the form

$$f(n) = \sum_{r=0}^{\infty} \frac{\Delta^r f(0)}{r!} n^{(r)}, \tag{4.8}$$

a discrete analog of the Maclaurin* series from calculus.

If f happens to be a polynomial of degree m, a combination of Theorem 4.1.8 and Equation (4.8) yields that

$$f(n) = \sum_{r=0}^{m} \frac{\Delta^r f(0)}{r!} n^{(r)}.$$

Conversely, if $\{\Delta^m a_n\}$ is constant, so that $\{\Delta^r a_n\} = \{0\}$ for all $r > m$, then $\Delta^r f(0) = \Delta^r a_0 = 0$, $r > m$, and Equation (4.8) becomes

$$f(n) = \sum_{r=0}^{m} \frac{\Delta^r a_0}{r!} n^{(r)}. \tag{4.9}$$

Since $n^{(r)}$ is a polynomial (in n) of degree r, Equation (4.9) implies that $f(n)$ is a polynomial of degree at most m. (If $\{\Delta^m a_n\}$ is a *nonzero* constant, f is a polynomial of degree exactly m.) This proves the following strong converse of Theorem 4.1.8.

*After Colin Maclaurin (1698–1746).

4.1.10 Theorem. *Let $\{a_n\}$ be a sequence. If the mth difference sequence $\{\Delta^m a_n\}$ is constant, i.e., if $\Delta^{m+1} a_n = 0$ for all $n \geq 0$, then there exists a polynomial f of degree at most m such that $a_n = f(n)$ for all $n \geq 0$. Moreover,*

$$f(n) = \sum_{r=0}^{m} C(n,r)\,\Delta^r a_0. \tag{4.10}$$

Proof. Equation (4.10) follows either by replacing $n^{(r)}/r!$ with $C(n,r)$ in Equation (4.9) or by replacing a_n with $f(n)$ in Equation (4.7). ■

Theorem 4.1.10 is a "strong" converse of Theorem 4.1.8 because it does more than establish the existence of f. Equation (4.10) is an explicit formula; it is the "easy way" to find f (short of solving a linear system of equations). Note, in particular, that if $\{\Delta^m a_n\}$ is a constant sequence then f, hence $\{a_n\}$, is completely determined by the $m+1$ numbers $a_0, \Delta a_0, \ldots, \Delta^m a_0$ from the first column (or *leading edge* of the difference array for $\{a_n\}$.

4.1.11 Example. Suppose $\{a_n\}$ is a sequence the first column of whose difference array is 1, 5, 4, 6, with zeros thereafter. Compute a_{100}. Solution: Let $f(n) = a_n$, $n \geq 0$. Because $\Delta^r a_0 = 0$, $r \geq 4$, Equation (4.10) yields

$$\begin{aligned} a_n &= \sum_{r=0}^{3} C(n,r)\,\Delta^r a_0 \\ &= C(n,0) \times 1 + C(n,1) \times 5 + C(n,2) \times 4 + C(n,3) \times 6 \\ &= 1 + 5n + 4n(n-1)/2 + 6n(n-1)(n-2)/6 \\ &= 1 + 5n + 2n^2 - 2n + n^3 - 3n^2 + 2n \\ &= n^3 - n^2 + 5n + 1, \end{aligned}$$

so $a_{100} = 10^6 - 10^4 + 500 + 1 = 990{,}501$. □

4.1.12 Example. Let m be a fixed positive integer and $\{a_n\}$ be the sequence whose nth term is $a_n = n^m$, $n \geq 0$. From Equation (4.10) (and Corollary 4.1.7), we obtain

$$n^m = \sum_{r=0}^{m} C(n,r)\,\Delta^r a_0.$$

On the other hand, from Corollary 2.2.3,

$$n^m = \sum_{r=1}^{m} r!\,S(m,r)\,C(n,r),$$

0,	1,	16,	81,	256,	625,	1296,	2401,	⋯
1,	15,	65,	175,	369,	671,	1105,	⋯	
14,	50,	110,	194,	302,	434,	⋯		
36,	60,	84,	108,	132,	⋯			
24,	24,	24,	24,	⋯				
0,	0,	0,	⋯					
	⋯							

Figure 4.1.2. The difference array for $\{n^4\}$.

where $S(m,r)$ is a Stirling number of the second kind. Together with the fact that $C(n,r) = n^{(r)}/r!$, these equations imply that $r!S(m,r) = \Delta^r a_0$, $0 \le r \le m$. (See Exercise 17, below.) The numbers comprising the leading edge of the difference array for the sequence $\{n^m\}$ are $\Delta^r a_0 = r!S(m,r)$, $r \ge 0$.

Let's check it out. For $m = 4$, $0!S(4,0) = 1 \times 0 = 0$, $1!S(4,1) = 1 \times 1 = 1$, $2!S(4,2) = 2 \times 7 = 14$, $3!S(4,3) = 6 \times 6 = 36$, $4!S(4,4) = 24 \times 1 = 24$, and $5!S(4,5) = 120 \times 0$. Compare the sequence

$$0,\ 1,\ 14,\ 36,\ 24,\ 0, \ldots$$

with the first column of the difference array for $\{n^4\}$ shown in Fig. 4.1.2. □

4.1.13 Example. Perhaps the techniques of this section can be made to yield additional new insights about Stirling numbers of the second kind. Consider, e.g., the sequence

$$S(k,0),\ S(k+1,1),\ S(k+2,2),\ S(k+3,3), \ldots,$$

where k is fixed but arbitrary. (The previous example involved $S(m,r)$ where m was fixed. This time, $m - r = k$ is fixed.) When $k = 2$, the first few terms of the sequence are

$$0,\ 1,\ 7,\ 25,\ 65,\ 140,\ 266,\ 462, \ldots$$

The initial portion of the difference array for this sequence is illustrated in Fig. 4.1.3. If the fourth difference sequence, corresponding to the fifth row of the difference array, really is the constant sequence $\{3\}$ then, from Equation (4.10), there is some polynomial f_2 of degree 4 such that $S(2+n,n) = f_2(n)$ for all $n \ge 0$. Moreover, from the leading edge of Fig. 4.1.3,

$$\begin{aligned} f_2(n) &= C(n,1) + 5C(n,2) + 7C(n,3) + 3C(n,4) \\ &= [C(n,1) + C(n,2)] + 4[C(n,2) + C(n,3)] + 3[C(n,3) + C(n,4)] \\ &= C(n+1,2) + 4C(n+1,3) + 3C(n+1,4) \\ &= [C(n+1,2) + C(n+1,3)] + 3[C(n+1,3) + C(n+1,4)] \\ &= C(n+2,3) + 3C(n+2,4). \end{aligned}$$

0,	1,	7,	25,	65,	140,	266,	462,	⋯
1,	6,	18,	40,	75,	126,	196,	⋯	
5,	12,	22,	35,	51,	70,	⋯		
7,	10,	13,	16,	19,	⋯			
3,	3,	3,	3,	⋯				

Figure 4.1.3. Difference array for $\{S(2+n,n)\}$.

Can this be right? Does $S(n+2,n) = C(n+2,3) + 3C(n+2,4)$ for all $n \geq 0$? (See Exercise 23.) If so, what about $S(n+3,n)$? (See Exercise 24.) □

4.1. EXERCISES

1 Compute a_{497} if $\{a_n\}$ is an arithmetic sequence satisfying

(a) $a_0 = 1$ and $a_1 = 4$.

(b) $a_2 = 76$ and $a_4 = 80$.

(c) $a_{461} = 1860$ and $a_{462} = 1864$.

2 Equation (4.2) expresses the nth term of an arithmetic sequence $\{a_n\}$ in terms of a_0, n, and d. Some people prefer to denote the first number in a sequence, not by a_0, but by a_1. This system has the advantage that the nth number and the nth term of the sequence are both a_n. If an arithmetic sequence begins with a_1 and satisfies $a_{n+1} = a_n + d$, $n \geq 1$, give a formula for a_n in terms of a_1, n, and d.

3 Let $\{a_n\}$ be the sequence $3, 4, 9, 18, \ldots$ defined by $a_0 = 3$ and $a_{n+1} = a_n + 4n + 1$, $n \geq 0$.

(a) Compute $a_4, a_5, \ldots, a_8$.

(b) Compute Δa_n.

(c) Starting with a first row consisting of the nine numbers $a_0, a_1, \ldots, a_8$, exhibit the rest of the difference array for $\{a_n\}$.

(d) Prove that $a_n = 2n^2 - n + 3$, $n \geq 0$.

(e) Let $\{b_n\}$ be the sequence defined by $\Delta b_n = a_n$, $n \geq 0$. Find a polynomial g such that $b_n = g(n)$ for all $n \geq 0$.

4 Let $\{a_n\}$ be the sequence $3, 4, 8, 17, \ldots$, where $a_0 = 3$ and $a_{n+1} = a_n + (n+1)^2$, $n \geq 0$. Find a polynomial f such that $a_n = f(n)$, $n \geq 0$, by

(a) using Equation (4.10).

(b) writing the sequence in the form

$$3, 3 + 1^2, 3 + 1^2 + 2^2, \ldots$$

and using the formula for the sum of the squares of the first n positive integers.

5 Let $\{a_n\}$ be the sequence $1, 2, 4, 8, \ldots$, where $a_0 = 1$ and $a_{n+1} = 2a_n$, $n \geq 0$.

(a) Exhibit the difference array for $\{a_n\}$.

(b) Prove that there does not exist a polynomial f such that $a_n = f(n)$ for all $n \geq 0$.

6 Recall that the Fibonacci sequence $\{F_n\}$ is defined by $F_0 = F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$, $n \geq 1$. Prove that there is no polynomial f such that $F_n = f(n)$ for all $n \geq 0$.

7 Let $\{a_n\}$ be an arithmetic sequence. Prove that the sum of the first k numbers in the sequence is given by the formula

$$a_0 + a_1 + \cdots + a_{k-1} = (a_0 + a_{k-1})k/2.$$

8 Compute the sum of the first 100 numbers $(a_0 + a_1 + \cdots + a_{99})$ of the arithmetic sequence $\{a_n\}$ that begins

(a) $1, 2, 3, \ldots$ **(b)** $1, 3, 5, \ldots$

(c) $2, 4, 6, \ldots$ **(d)** $7, 11, \ldots$

(e) $7, 13, \ldots$ **(f)** $123, 133, \ldots$

9 Let $\{a_n\}$ be a sequence that satisfies $\Delta^{m+1} a_n = 0$, $n \geq 0$. Prove that the sum of the first k numbers in the sequence is given by the formula

$$\sum_{n=0}^{k-1} a_n = \sum_{r=0}^{m} C(k, r+1)\, \Delta^r a_0.$$

10 Show that the formula in Exercise 7 is the $m = 1$ case of the formula in Exercise 9.

11 Let $\{a_n\}$ be the sequence $3, 4, 9, 18, \ldots$ defined by $a_0 = 3$ and $a_{n+1} = a_n + 4n + 1$, $n \geq 0$.

(a) Show that $\Delta^0 a_0 = 3$, $\Delta^1 a_0 = 1$, $\Delta^2 a_0 = 4$, and $\Delta^t a_n = 0$ for all $t \geq 3$ and all $n \geq 0$.

(b) Confirm the $k = 4$ case of the formula in Exercise 9 for this sequence by showing that $3 + 4 + 9 + 18 = 3 \times C(4, 1) + 1 \times C(4, 2) + 4 \times C(4, 3)$.

(c) Compute the sum $3 + 4 + 9 + 18 + \cdots + 123$ by filling in the missing entries (indicated by the ellipsis) and doing all the additions.

(d) Compute the sum $3 + 4 + 9 + 18 + \cdots + 123$ by first using Exercise 3(a) to deduce that $123 = a_8$ and then using Exercise 9.

(e) Show that $3 + 4 + 9 + 18 + \cdots + 1131 = 9575$.

(f) Compute the sum $3 + 4 + 9 + 18 + \cdots + 19,506$.

12 Let $\{a_n\}$ be the sequence $3, 4, 8, 17, \ldots$ from Exercise 4. Use Exercise 9 to compute the sum $a_0 + a_1 + \cdots + a_{19}$.

13 If $a_n = n^m$ for some fixed positive integer m, then Exercise 9 yields the formula

$$1^m + 2^m + \cdots + k^m = \sum_{r=0}^{m} C(k+1, r+1)\,\Delta^r a_0.$$

Use this formula to find a polynomial f such that

(a) $f(k) = 1^2 + 2^2 + \cdots + k^2$.

(b) $f(k) = 1^3 + 2^3 + \cdots + k^3$.

14 Each of the following is a special case of Equation (4.6) applied to the sequence $\{n^3\}$ from Example 4.1.4. Give a direct, computational confirmation that

(a) $5^3 - 3 \times 4^3 + 3 \times 3^3 - 2^3 = 6$.

(b) $6^3 - 3 \times 5^3 + 3 \times 4^3 - 3^3 = 6$.

(c) $7^3 - 3 \times 6^3 + 3 \times 5^3 - 4^3 = 6$.

(d) $8^3 - 3 \times 7^3 + 3 \times 6^3 - 5^3 = 6$.

15 Use the approach illustrated in Example 4.1.12 to compute the Stirling numbers

(a) $S(3, n)$, $1 \le n \le 3$. **(b)** $S(5, n)$, $1 \le n \le 5$.

16 Let $\{a_n\}$ be a sequence. Prove that there is a polynomial f such that $a_n = f(n)$, $n \ge 0$, if and only if the terms of the sequence satisfy a recurrence of the form $a_{n+1} = a_n + g(n)$, $n \ge 0$, where g is a polynomial.

17 Let m be a fixed positive integer. Prove that $\{x^{(r)}/r! : 0 \le r \le m\}$ is a basis for the vector space of polynomials of degree at most m, where $x^{(r)}$ is the falling factorial function.

18 Let $\mathbb{R}$ be the set of real numbers. If $f : \mathbb{R} \to \mathbb{R}$ is a function, let $\Delta f : \mathbb{R} \to \mathbb{R}$ be its "discrete derivative", i.e., $\Delta f(x) = f(x+1) - f(x)$.

(a) Prove that $\Delta x^{(m)} = m x^{(m-1)}$, where $x^{(m)}$ is the falling factorial function.

(b) Prove that $\Delta 2^x = 2^x$.

(c) Find an analog for discrete differentiation of the "product rule" for ordinary differentiation.

19 The sequence $\{a_n\}$ is said to be *convex* if

$$\frac{a_{n+2} + a_n}{2} \ge a_{n+1}, \qquad n \ge 0.$$

(a) Show that $\{a_n\}$ is convex if and only if each term of its second difference sequence $\{\Delta^2 a_n\}$ is nonnegative.

(b) Compare and contrast part (a) with the theorem from calculus that f is concave up on the open interval I whenever its second derivative $f''(x) > 0$ on I.

(c) Let $p(n)$ be, not the value of a polynomial function at $x = n$, but the number of partitions of n. Show that the sequence $\{a_n\}$ defined by $a_n = p(n+1)$, $n \geq 0$, is convex.

20 Let r be a fixed positive integer. Define $a_n = C(n, r)$, $n \geq 0$. Find a closed formula for Δa_n.

21 Suppose $a_n = f(n)$, $n \geq 0$, where $f(x) = b_r x^r + b_{r-1}x^{r-1} + \cdots + b_1 x + b_0$.

(a) Show that $u = Q_r v$, where $u = (a_0, a_1, \ldots, a_r)^t$, the transpose of $(a_0, a_1, \ldots, a_r)$, $v = (b_0, b_1, \ldots, b_r)^t$, and

$$Q_r = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1^0 & 1^1 & 1^2 & \cdots & 1^r \\ 2^0 & 2^1 & 2^2 & \cdots & 2^r \\ 3^0 & 3^1 & 3^2 & \cdots & 3^r \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r^0 & r^1 & r^2 & \cdots & r^r \end{pmatrix}.$$

(b) Show that

$$Q_3^{-1} = \frac{1}{6}\begin{pmatrix} 6 & 0 & 0 & 0 \\ -11 & 18 & -9 & 2 \\ 6 & -15 & 12 & -3 \\ -1 & 3 & -3 & 1 \end{pmatrix}.$$

(c) Consider the sequence $\{a_n\}$ whose first few terms are $1, 3, 8, 17, \ldots$. Given that $\Delta^4 a_n = 0$, $n \geq 0$, use parts (a) and (b) to find a polynomial $f(x)$ (of degree at most 3) such that $a_n = f(n)$, $n \geq 0$.

(d) Consider the sequence $\{a_n\}$ described in part (c). Use Equation (4.10) to find a polynomial $f(x)$ (of degree at most 3) such that $a_n = f(n)$, $n \geq 0$.

22 Much of our knowledge of ancient Egyptian mathematics comes from the (seventeenth century BC) *Rhind papyrus*. The papyrus contains the following sequence: $7, 49, 343, 2301, \_\_\_$. What is the fifth number in the sequence? Justify your answer. (*Hint*: Anyone can make mistakes.)

23 Prove the identity

(a) $S(n+2, n) = C(n+2, 3) + 3C(n+2, 4)$, from Example 4.1.13.

(b) $S(n+2, n) = n(n+1)(n+2)(3n+1)/24$.

24 Use the technique illustrated in Example 4.1.13 to show that

(a) $S(n+3,n) = C(n+3,4) + 10C(n+3,5) + 15C(n+3,6)$.

(b) $S(n+3,n) = n^2(n+1)^2(n+2)(n+3)/48$.

25 Use Equation (4.10) to express $f(n) = 3n^2 + 2n + 1$ as a linear combination of binomial coefficients.

26 Express the polynomial $f(n)$ from Exercise 25 as a linear combination of falling factorial functions (of n).

27 Consider the sequence $0, 1, 3, 6, 10, 15, \ldots$ whose nth term is $S(n+1,n)$, $n \geq 0$.

(a) Use the technique illustrated in Example 4.1.13 to show that $S(n+1,n) = C(n+1,2)$.

(b) Give a combinatorial proof of the identity $S(n+1,n) = C(n+1,2)$.

28 Suppose $\{a_n\}$ is the sequence determined by the initial condition $a_0 = 0$ and the recurrence $a_n = a_{n-1} + n^2$, $n \geq 1$.

(a) Exhibit the difference array for $\{a_n\}$.

(b) Use part (a) to find a polynomial f such that $a_n = f(n)$, $n \geq 0$.

29 Suppose r and s are nonnegative integers satisfying $r \geq s+2$. Let $n = (2s+1) + (2s+3) + \cdots + (2r-1)$.

(a) Prove that n is a difference of squares.

(b) Prove that $n = ab$, where a and b are integers (strictly) larger than 1 both of which are even or both of which are odd.

30 Show that there are 10 different ways to express 945 as a sum of (two or more) consecutive odd positive integers. (*Hint*: Exercise 29 and the fact that $945 = 3^3 \times 5 \times 7$.)

31 Prove the following identity (attributed to Galileo):

$$\frac{1}{3} = \frac{1+3}{5+7} = \frac{1+3+5}{7+9+11} = \cdots = \frac{1+3+\cdots+(2n-1)}{(2n+1)+\cdots+(4n-1)} = \cdots$$

32 Suppose $n > 1$ is a difference of (positive) squares. Prove that $n = (2s+1) + (2s+3) + \cdots + (2r-1)$, where r and s are nonnegative integers satisfying $r \geq s+2$.

33 Suppose $n = ab$, where a and b are integers (strictly) larger than 1 both of which are even or both of which are odd. Prove that $n = (2s+1) + (2s+3) + \cdots + (2r-1)$, where r and s are nonnegative integers satisfying $r \geq s+2$.

4.2. ORDINARY GENERATING FUNCTIONS

Consider the sequence $3, 6, 12, 24, \ldots$, where $a_0 = 3$ and $a_{n+1} = 2a_n$, $n \geq 0$. Pretty clearly, no row of the difference array

$$\begin{array}{cccccc} 3, & 6, & 12, & 24, & \ldots \\ 3, & 6, & 12, & 24, & \ldots \\ 3, & 6, & 12, & 24, & \ldots \\ & & \ldots & & \end{array}$$

will ever be constant, much less consist entirely of zeros. So, by Theorem 4.1.8, the function defined by $f(n) = a_n$, $n \geq 0$, is not a polynomial. Indeed, by not doing any arithmetic, it is easy to see from the symbolic representation

$$3,\ 3 \times 2,\ (3 \times 2) \times 2,\ (3 \times 2 \times 2) \times 2, \ldots$$

that $f(n) = 3 \times 2^n$, $n \geq 0$.

4.2.1 Definition. The sequence $\{a_n\}$ is *geometric* if it satisfies a recurrence of the form $a_{n+1} = da_n$, $n \geq 0$, where d is a constant, independent of n.

Evidently, the nth term of a generic geometric sequence is given by the closed formula $a_n = a_0 \times d^n$, $n \geq 0$.

Consider the sequence

$$3, 4, 22, 46, 178, 454, \ldots \tag{4.11}$$

defined by $a_0 = 3$, $a_1 = 4$, and $a_n = a_{n-1} + 6a_{n-2}$, $n \geq 2$. This one is neither arithmetic nor geometric. While there is a simple closed formula for a_n, its discovery requires either an inspired guess or a new approach.

4.2.2 Definition. The (ordinary) *generating function* for the sequence $\{a_n\}$ is

$$g(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots \tag{4.12}$$

Generating functions come in assorted sizes, shapes, and flavors. The pattern inventory* $W_G(x_1, x_2, \ldots, x_n)$ is one kind of generating function; Equation (4.12) is another. The name "generating function" is more than a little curious. The pattern inventory doesn't generate anything; it is *generated by* the cycle index polynomial.† Moreover, as we are about to see, it is useful to view $g(x)$ as something *other* than a function!

*The subject of Section 3.6.
†The subject of Section 3.7.

If $g(x)$ is the generating function for Sequence (4.11), then

$$\begin{array}{rcccccccccccc} g(x) &=& 3 &+& 4x &+& 22x^2 &+& 46x^3 &+& 178x^4 &+& \cdots &+& a_n x^n &+& \cdots \\ -xg(x) &=& & - & 3x &-& 4x^2 &-& 22x^3 &-& 46x^4 &-& \cdots &-& a_{n-1}x^n &-& \cdots \\ -6x^2 g(x) &=& & & & - & 18x^2 &-& 24x^3 &-& 132x^4 &-& \cdots &-& 6a_{n-2}x^n &-& \cdots \end{array}$$

Summing these three equations produces

$$g(x)(1 - x - 6x^2) = 3 + x.$$

(The recurrence guarantees that $[a_n - a_{n-1} - 6a_{n-2}]x^n = 0$, $n \geq 2$.) Evidently,

$$g(x) = 3 + 4x + 22x^2 + 46x^3 + 178x^4 + 454x^5 + \cdots \tag{4.13a}$$

$$= \frac{3 + x}{1 - x - 6x^2}. \tag{4.13b}$$

A typical backpacker will sacrifice many things to decrease weight. Freeze-dried food is a good example. Why carry water (even as a constituent of food) if it is available at campsites? Equation (4.13b) might be viewed as a freeze-dried version of Equation (4.13a). (If you had to stuff $g(x)$ into a backpack, which version would you prefer?)

Okay. Imagine yourself at a campsite. What is the easy way to resurrect (or *generate*) the sequence $\{a_n\}$ from $g(x) = (3 + x)/(1 - x - 6x^2)$? One perfectly acceptable alternative is long division. Another is to factor the denominator as $(1 + 2x)(1 - 3x)$, so that

$$g(x) = (3 + x)\left(\frac{1}{1 + 2x}\right)\left(\frac{1}{1 - 3x}\right).$$

Recall that

$$\frac{1}{1 - x} = 1 + x + x^2 + x^3 + x^4 + \cdots, \tag{4.14}$$

so

$$\frac{1}{1 + 2x} = 1 + (-2x) + (-2x)^2 + (-2x)^3 + \cdots \tag{4.15}$$

and

$$\frac{1}{1 - 3x} = 1 + 3x + (3x)^2 + (3x)^3 + \cdots. \tag{4.16}$$

Therefore, $g(x)$ can be expressed as the (formidable *looking*) product

$$g(x) = (3 + x)(1 - 2x + 4x^2 - 8x^3 + \cdots)(1 + 3x + 9x^2 + 27x^3 + \cdots).$$

A third, easier approach is to make use of the method of partial fractions*, i.e., to write

$$g(x) = \frac{3+x}{1-x-6x^2} = \frac{3+x}{(1+2x)(1-3x)} = \frac{1}{1+2x} + \frac{2}{1-3x}.$$

Together with Equations (4.15) and (4.16), this yields

$$\begin{aligned} g(x) &= [1 + (-2x) + (-2x)^2 + \cdots] + 2[1 + 3x + (3x)^2 + \cdots] \\ &= [1 - 2x + 4x^2 - 8x^3 + \cdots] + [2 + 6x + 18x^2 + 54x^3 + \cdots] \\ &= 3 + 4x + 22x^2 + 46x^3 + \cdots, \end{aligned}$$

and the generating function has been reassembled. There is more. Obscured by the rush to compute is a closed formula for a_n. Comparing the coefficients of x^n in

$$g(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$$

and

$$g(x) = [1 + (-2x) + (-2x)^2 + \cdots] + 2[1 + 3x + (3x)^2 + \cdots]$$

yields

$$a_n = (-2)^n + 2(3^n), \qquad n \geq 0. \tag{4.17}$$

It is striking, but is it right? Without checking for convergence, what justifies manipulating the generating "function" just as if it were an honest-to-goodness function? It would appear that our derivation may have some holes in it. On the other hand, *independently of where it came from*, we can prove that Equation (4.17) is a valid identity.

Define a sequence $\{b_n\}$ by $b_n = 2(3^n) + (-2)^n$, $n \geq 0$. Then $b_0 = 2(3^0) + (-2)^0 = 3 = a_0$ and $b_1 = 2(3) - 2 = 4 = a_1$. So, the first two numbers in the sequences $\{a_n\}$ and $\{b_n\}$ are the same. If we could prove that the sequences satisfy the same recurrence, i.e., if $b_n = b_{n-1} + 6b_{n-2}$, $n \geq 2$, it would follow that $b_n = a_n$ for all n.

Observe that

$$2(3^n) = 6(3^{n-1}) = 2(3^{n-1}) + 4(3^{n-1}) = 2(3^{n-1}) + 6[2(3^{n-2})]$$

and

$$(-2)^n = -2(-2)^{n-1} = (-2)^{n-1} - 3(-2)^{n-1} = (-2)^{n-1} + 6(-2)^{n-2}.$$

*You already know how to do partial fractions. If you don't recall all of the details, that's okay. It just means you will have to dig out your old calculus book and do some reviewing.

Summing the extreme left- and right-hand sides, we obtain

$$\begin{aligned} b_n &= 2(3^n) + (-2)^n \\ &= [2(3^{n-1}) + (-2)^{n-1}] + 6[2(3^{n-2}) + (-2)^{n-2}] \\ &= b_{n-1} + 6b_{n-2}. \end{aligned}$$

(Before reading on, confirm that $b_5 = 2(3^5) - 2^5 = 454 = a_5$.)

A *spelunker* is someone who explores caves. Of the many things a spelunker must do well, perhaps the most important is to keep track of where s/he is relative to the way out. Let's pause and outline where we are. We used the sequence $\{a_n\}$ to produce a generating function $g(x) = a_0 + a_1x + a_2x^2 + \cdots$. On one level, the plus signs and powers of x are separators. Like the commas in $a_0, a_1, a_2, \ldots$, they keep the a_i's apart. On a deeper level, just writing $g(x)$ suggests manipulating it as if it were a function. (As Leibniz once observed, good notation can lead to startling insights.) The object of manipulating $g(x)$ was to produce a closed formula (freeze-dried version). The closed formula gave us another way to look at $\{a_n\}$, eventually leading to a solution for a_n. The disturbing part came at the end, where it seemed necessary to validate the solution. One way to avoid this verification step would be to justify the algebraic manipulations leading up to it.

4.2.3 Definition. A *formal power series* in x is an infinite sum of the form $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$, where the *coefficients* $a_0, a_1, a_2, a_3, \ldots$ are fixed constants. It is sometimes convenient to give a shorthand name to a power series, writing, e.g.,

$$\begin{aligned} g(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots \\ &= \sum_{n\geq 0} a_nx^n. \end{aligned}$$

(The expressions $\sum_{n\geq 0} a_nx^n$ and $\sum_{n=0}^{\infty} a_nx^n$ are interchangeable.)

Most of the algebraic manipulations associated with polynomials extend naturally to formal power series. (If all but finitely many of its coefficients are zero, a formal power series *is* a polynomial.) If

$$f(x) = \sum_{n\geq 0} a_nx^n \qquad \text{and} \qquad g(x) = \sum_{n\geq 0} b_nx^n,$$

then $f(x) = g(x)$ if and only if $a_n = b_n$ for all $n \geq 0$. If c and d are constants, then $h(x) = cf(x) + dg(x)$ is the formal power series defined by

$$h(x) = c\sum_{n\geq 0} a_nx^n + d\sum_{n\geq 0} b_nx^n = \sum_{n\geq 0}(ca_n + db_n)x^n. \tag{4.18}$$

Multiplication of polynomials also extends to formal power series:

$$\begin{aligned}(a_0 + a_1x + a_2x^2 + \cdots)(b_0 + b_1x + b_2x^2 + \cdots)\\ = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots.\end{aligned}$$

In general,

$$\left(\sum_{n\geq 0} a_nx^n\right)\left(\sum_{n\geq 0} b_nx^n\right) = \sum_{n\geq 0} c_nx^n, \tag{4.19a}$$

where

$$c_n = \sum_{r=0}^{n} a_rb_{n-r}. \tag{4.19b}$$

4.2.4 Example. Observe that

$$(1 + x + x^2 + x^3 + x^4 + \cdots)(1 - x) = 1. \tag{4.20}$$

In fact, this product is just a variation of Equation (4.14). □

It is instructive to turn Example 4.2.4 around. How *do* we know that

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots?$$

One justification comes from calculus:

$$\begin{aligned}g(x) &= 1 + x + x^2 + x^3 + x^4 + \cdots\\ &= \lim_{n\to\infty} 1 + x + x^2 + \cdots + x^{n-1}\\ &= \lim_{n\to\infty} \frac{1-x^n}{1-x}\\ &= \frac{1}{1-x},\end{aligned}$$

$x \in (-1, 1)$, because $\lim_{n\to\infty} x^n = 0$ whenever $|x| < 1$. But, this argument depends upon viewing $g(x) = 1 + x + x^2 + x^3 + x^4 + \cdots$ as a function, precisely the perspective we are trying to avoid. What we want is a justification that depends only on the algebra of formal power series.

4.2.5 Definition. Let $g(x)$ and $h(x)$ be formal power series. If $g(x)h(x) = 1$, then $h(x)$ is the *reciprocal* of $g(x)$, written $h(x) = 1/g(x)$.

Because multiplication of power series is commutative, $h(x)$ is the reciprocal of $g(x)$ if and only if $g(x)$ is the reciprocal of $h(x)$.

4.2.6 Theorem. *The formal power series $g(x) = \sum_{n\geq 0} a_n x^n$ has a reciprocal if and only if $a_0 \neq 0$. If $g(x)$ has a reciprocal, it is unique.*

Proof. Suppose $g(x)$ has a reciprocal, say $h(x) = \sum_{n\geq 0} b_n x^n$. Then, from Definition 4.2.5 and Equations (4.19a)–(4.19b), $c_0 = a_0 b_0 = 1$, so $a_0 \neq 0$ and $b_0 = 1/a_0$ is uniquely determined by a_0. Furthermore, because

$$c_n = \sum_{r=0}^{n} a_r b_{n-r} = 0, \qquad n \geq 1,$$

the coefficients $b_1 = -a_1 b_0/a_0$, $b_2 = -(a_1 b_1 + a_2 b_0)/a_0$, and so on, are uniquely determined (recursively) by $\{a_n\}$.

Conversely, if $a_0 \neq 0$, define $\{b_n\}$ recursively by $b_0 = 1/a_0$, and

$$b_n = -\sum_{r=1}^{n} a_r b_{n-r}/a_0, \qquad n \geq 1.$$

Then, setting $h(x) = \sum_{n\geq 0} b_n x^n$, our definitions yield

$$\sum_{r=0}^{n} a_r b_{n-r} = \delta_{n,0},$$

i.e. (by Equations (4.19a)–(4.19b)), $g(x)h(x) = 1$. ■

Every step in the derivation of Equation (4.17) can now be justified using (only) algebraic manipulations of formal power series. The solution $a_n = (-2)^n + 2(3^n)$ does not require the generating function for $\{a_n\}$ to be a function. We are on solid ground again.

The freeze drying of generating functions can involve a variety of techniques. No single recipe works in every case. All by itself, the method of partial fractions is pretty much limited to sequences $\{a_n\}$ that satisfy so-called *homogeneous linear recurrences*, i.e., recurrences of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \qquad n \geq k, \tag{4.21}$$

where k is a fixed positive integer, and $c_1, c_2, \ldots, c_k$ are constants, independent of n. The following technical observation will be useful in helping to motivate the development of a useful tool.

4.2.7 Lemma. *If $f(x)$ is the generating function for $\{a_n\}$, then $g(x) = f(x)/(1-x) = f(x)[1/(1-x)]$ is the generating function for $\{s_n\}$, where $s_n = a_0 + a_1 + \cdots + a_n$.*

Proof. From Equation (4.20) and the definition of reciprocals,

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \cdots$$

Therefore, from Equations (4.19a)–(4.19b),

$$f(x)\frac{1}{1-x} = \left(\sum_{n\geq 0} a_n x^n\right)\left(\sum_{n\geq 0} x^n\right) = \sum_{n\geq 0}\left(\sum_{r=0}^{n} a_r\right)x^n. \qquad \blacksquare$$

4.2.8 Example. For a fixed but arbitrary positive integer m, let $g_m(x)$ be the generating function for the sequence $\{s(m,n)\}$ of Stirling numbers of the first kind. Because $s(m,n) = 0$ when $n = 0$ or $n > m$, it follows from Theorem 2.5.4 that

$$\begin{aligned} g_m(x) &= \sum_{n=1}^{m} s(m,n)x^n \\ &= x(x+1)(x+2)\cdots(x+m-1). \end{aligned}$$

Differentiating with respect to x, we obtain (by the product rule) that

$$\sum_{n=1}^{m} n s(m,n)x^{n-1} = \sum_{i=0}^{m-1} \frac{x(x+1)(x+2)\cdots(x+m-1)}{x+i}.$$

Setting $x = 1$ and dividing both sides by $m!$ yields

$$\frac{1}{m!}\sum_{n=1}^{m} n s(m,n) = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{m}, \tag{4.22a}$$

an identity with some interesting implications.

The *harmonic sequence* $\{h_n\}$ is defined by $h_0 = 0$ and

$$h_n = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}, \qquad n > 0.$$

Because $s(m,n)$ is the number of permutations in S_m whose disjoint cycle factorizations consist of exactly n cycles, the left-hand side of Equation (4.22a) is the average, over $p \in S_m$, of the number of cycles in p. That this average should equal h_m is unexpected. There is more! By Theorem 2.5.2, $h_m = s(m+1,2)/m!$. Together with Equation (4.22a), this yields

$$\sum_{n=1}^{m} ns(m,n) = s(m+1,2), \tag{4.22b}$$

another surprising result.

Consider the harmonic generating function

$$\begin{aligned} h(x) &= \sum_{n\geq 0} h_n x^n \\ &= \sum_{n\geq 0} \frac{s(n+1,2)}{n!} x^n. \end{aligned}$$

By Lemma 4.2.7, the formal power series $h(x) = f(x)/(1-x)$, where

$$f(x) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \frac{1}{4}x^4 + \cdots$$

If this expression defined, not only a function, but a *differentiable* function, then

$$\begin{aligned} f'(x) &= 1 + x + x^2 + x^3 + \cdots \\ &= \frac{1}{1-x}. \end{aligned}$$

Antidifferentiating this equation yields (because $f(0) = 0$) $f(x) = -\ln(1-x)$, from which it follows that

$$h(x) = \frac{-\ln(1-x)}{1-x}. \qquad \square$$

Can one do calculus with formal power series without treating them as functions? In a superficial sense, that is not a problem. One can define the formal term-by-term derivative of $g(x) = \sum_{n\geq 0} a_n x^n$ by

$$D_x g(x) = \sum_{n\geq 1} n a_n x^{n-1}$$

and, using Equations (4.18)–(4.19b), prove the usual formulas for differentiating sums and products. The sticky part comes when we want to differentiate *both* sides, e.g., of

$$(1-x)^{-1} = 1 + x + x^2 + x^3 + x^4 + \cdots \tag{4.23}$$

The (ordinary) derivative of the left-hand side is $D_x(1-x)^{-1} = (1-x)^{-2}$. The formal derivative of the right-hand side is

$$D_x(1 + x + x^2 + x^3 + x^4 + \cdots) = 1 + 2x + 3x^2 + 4x^3 + \cdots$$

Despite using the same symbol, D_x, for both operators, setting these two derivatives equal cannot be justified by arguments based solely on algebraic manipulations of formal power series. The justification relies on the fact that the right-hand side of Equation (4.23) has a positive radius of convergence. We need the following result from calculus.

4.2.9 Theorem. *Let r be a positive real number. If the power series*

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$$

converges to $g(x)$ for all x in the interval $I = (-r, r)$, then g is differentiable on I, and the power series

$$D_xg(x) = a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1} + \cdots$$

converges to $g'(x)$ for all $x \in I$. Moreover, for all $x \in I$,

$$\int_0^x g(t)dt = a_0x + \frac{1}{2}a_1x^2 + \frac{1}{3}a_2x^3 + \cdots + \frac{1}{n+1}a_nx^{n+1} + \cdots$$

4.2.10 Example. Consider the sequence

$$2, 4, 31, 100, 421, \ldots,$$

defined by $a_0 = 2$, $a_1 = 4$, $a_2 = 31$, and $a_{n+1} = 4a_n + 3a_{n-1} - 18a_{n-2}$, $n \geq 2$. Let's use generating functions to solve for a_n: Summing the equations

$$\begin{aligned}
g(x) &= 2 + 4x + 31x^2 + 100x^3 + \cdots + a_nx^n + \cdots \\
-4xg(x) &= -8x - 16x^2 - 124x^3 - \cdots - 4a_{n-1}x^n - \cdots \\
-3x^2g(x) &= -6x^2 - 12x^3 - \cdots - 3a_{n-2}x^n - \cdots \\
18x^3g(x) &= 36x^3 + \cdots + 18a_{n-3}x^n + \cdots
\end{aligned}$$

produces $(1-4x-3x^2+18x^3)g(x)=2-4x+9x^2$. (The recurrence guarantees that $[a_n-4a_{n-1}-3a_{n-2}+18a_{n-3}]x^n=0$ for all $n\geq 3$.) So,

$$\begin{aligned} g(x) &= \frac{2-4x+9x^2}{1-4x-3x^2+18x^3} \\ &= \frac{2-4x+9x^2}{(1+2x)(1-3x)^2} \\ &= \frac{1}{1+2x}+\frac{1}{(1-3x)^2} \end{aligned}$$

using partial fractions. (Check it.)

From Equation (4.16),

$$\frac{1}{1-3x}=1+3x+3^2x^2+3^3x^3+\cdots+3^nx^n+\cdots \tag{4.24}$$

What about $1/(1-3x)^2$? The brute-force approach would be to square both sides of Equation (4.24), using Equations (4.19a)–(4.19b) for the right-hand side. But, there is an easier solution. Because $1+x+x^2+x^3+\cdots$ converges to $(1-x)^{-1}$ for all $x\in(-1,1)$, the right-hand side of Equation (4.24) converges to the left-hand side whenever $3x\in(-1,1)$, i.e., for all $x\in(-\frac{1}{3},\frac{1}{3})$. It follows from Theorem 4.2.9 that both sides of Equation (4.24) can be differentiated to obtain

$$\frac{3}{(1-3x)^2}=3+2(3^2)x+3(3^3)x^2+\cdots+n(3^n)x^{n-1}+\cdots,$$

so

$$\begin{aligned} \frac{1}{(1-3x)^2} &= 1+2(3)x+3(3^2)x^2+\cdots+n(3^{n-1})x^{n-1}+\cdots \\ &= \sum_{n\geq 0}(n+1)3^nx^n. \end{aligned} \tag{4.25}$$

Adding Equations (4.15) and (4.25), we obtain

$$\begin{aligned} g(x) &= 2+4x+31x^2+100x^3+\cdots+a_nx^n+\cdots \\ &= \frac{1}{1+2x}+\frac{1}{(1-3x)^2} \\ &= \sum_{n\geq 0}[(-2)^n+(n+1)3^n]x^n. \end{aligned} \tag{4.26}$$

Therefore, $a_n=(-2)^n+(n+1)3^n$, $n\geq 0$. □

The technique that was used in Example 4.2.10 to pass from Equation (4.24) to Equation (4.25) has many uses. For example, successive differentiations of

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots + x^n + \cdots$$

yield

$$\frac{1}{(1-x)^2} = 1 + 2x + 3x^2 + \cdots + (n+1)x^n + \cdots,$$
$$\frac{2}{(1-x)^3} = 2 + 2(3x) + 3(4x^2) + \cdots + (n+1)(n+2)x^n + \cdots,$$

and so on, the formula for the rth derivative being

$$\frac{r!}{(1-x)^{r+1}} = P(r,r) + P(r+1,r)x + P(r+2,r)x^2 + \cdots + P(r+n,r)x^n + \cdots$$

Dividing both sides of this equation by $r!$ yields

$$\frac{1}{(1-x)^{r+1}} = \sum_{n\geq 0} C(r+n,r)x^n, \tag{4.27}$$

the generating function for $\{C(r+n,r)\}$. When both sides of Equation (4.27) are multiplied by x^r, the result is

$$\begin{aligned}\frac{x^r}{(1-x)^{r+1}} &= \sum_{n\geq 0} C(r+n,r)x^{n+r} \\ &= \sum_{n\geq r} C(n,r)x^n \\ &= \sum_{n\geq 0} C(n,r)x^n \end{aligned} \tag{4.28}$$

because $C(n,r) = 0$ whenever $n < r$. Let's summarize.

4.2.11 Theorem. *Let r be a fixed nonnegative integer. If $a_n = C(n,r)$, $n \geq 0$, then a closed formula for the generating function of $\{a_n\}$ is $g(x) = x^r/(1-x)^{r+1}$.*

The nth term of the sequence $\{C(n,r)\}$ is a *value* of the polynomial

$$f(x) = \frac{x^{(r)}}{r!} = \frac{x(x-1)\cdots(x-r+1)}{r!}$$

and a *coefficient* of the generating function $g(x) = x^r/(1-x)^{r+1}$. In other words, $f(n)$ is a closed formula (solution) for the nth term of the sequence, while $x^r/(1-x)^{r+1}$ is a closed formula (freeze-dried version) for the generating function of the sequence.

4.2.12 Example. Speaking of values vs. coefficients, consider the sequence $\{a_n\}$ given by $a_0 = 0$ and $a_{n+1} = a_n + 2n + 1$, $n \geq 0$, the first few terms of which are

$$0, 1, 4, 9, 16, 25, \ldots$$

That's right, it's the familiar sequence of (perfect) squares. In particular, $f(n) = n^2$ solves the sequence in the sense that its nth term is given by $a_n = f(n)$. What about the generating function

$$g(x) = \sum_{n \geq 0} n^2 x^n?$$

As Yogi Berra once remarked, this looks like *déjà vu* all over again: Because $n^2 = C(n,1) + 2C(n,2)$,

$$\begin{aligned} g(x) &= \sum_{n \geq 0} [C(n,1) + 2C(n,2)]x^n \\ &= \sum_{n \geq 0} C(n,1)x^n + 2\sum_{n \geq 0} C(n,2)x^n \\ &= \frac{x}{(1-x)^2} + 2\frac{x^2}{(1-x)^3} \\ &= \frac{x(1+x)}{(1-x)^3} \end{aligned}$$

by Theorem 4.2.11. □

We conclude this section with a combinatorial proof of the Pythagorean theorem due to E. R. Scheinerman.*

4.2.13 Example. Let a, b, and c be the lengths of the sides of a triangle. Then the angle opposite side c is a right angle if and only if $a^2 + b^2 = c^2$. This statement of the Pythagorean theorem is equivalent to the identity $\sin^2(x) + \cos^2(x) = 1$,

*A combinatorial proof of the Pythagorean theorem, *Math. Mag.* 68 (1995), 48–49.

$0 < x < \frac{1}{2}\pi$. (See Exercise 23.) Recall from calculus that the Maclaurin series expansions for sine and cosine are

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots = \sum_{n\geq 0} s_n \frac{x^n}{n!},$$
$$\cos(x) = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots = \sum_{n\geq 0} c_n \frac{x^n}{n!},$$

where

$$s_n = \begin{cases} 0 & \text{if} \quad n = 2k, \\ +1 & \text{if} \quad n = 4k+1, \\ -1 & \text{if} \quad n = 4k-1, \end{cases}$$

$$c_n = \begin{cases} 0 & \text{if} \quad n = 2k+1, \\ +1 & \text{if} \quad n = 4k, \\ -1 & \text{if} \quad n = 4k+2. \end{cases}$$

It follows from Equations (4.19a) – (4.19b) that

$$\begin{aligned} \sin^2(x) &= \sum_{n\geq 0} \left(\sum_{r=0}^{n} \frac{s_r}{r!} \frac{s_{n-r}}{(n-r)!} \right) x^n \\ &= \sum_{n\geq 0} \left(\sum_{r=0}^{n} C(n,r) s_r s_{n-r} \right) \frac{x^n}{n!}. \end{aligned}$$

Similarly,

$$\begin{aligned} \cos^2(x) &= \sum_{n\geq 0} \left(\sum_{r=0}^{n} \frac{c_r}{r!} \frac{c_{n-r}}{(n-r)!} \right) x^n \\ &= \sum_{n\geq 0} \left(\sum_{r=0}^{n} C(n,r) c_r c_{n-r} \right) \frac{x^n}{n!}. \end{aligned}$$

It remains to prove that

$$\sum_{r=0}^{n} C(n,r)(s_r s_{n-r} + c_r c_{n-r}) = \delta_{n,0}.$$

When $n = 0$, the summation on the left-hand side is $s_0^2 + c_0^2 = 0 + 1 = 1$. If n is odd, then one of r and $n-r$ is odd and the other is even, so $s_r s_{n-r} = c_r c_{n-r} = 0$, $0 \leq r \leq n$. If n is positive and even, then (see Exercise 24) the summation on left-hand side becomes

$$\pm \sum_{r=0}^{n} (-1)^r C(n,r) = 0$$

by Lemma 1.5.8. □

4.2. EXERCISES

1 Find a closed formula for the generating function $g(x) = \sum_{n\geq 0} C(m,n)x^n = C(m,0) + C(m,1)x + C(m,2)x^2 + \cdots$, where m is a fixed but arbitrary positive integer.

2 Find a closed formula for the generating function $g(x) = \sum_{n\geq 0} a_n x^n$ when

(a) $a_n = 1$, $n \geq 0$.

(b) $a_0 = 0$ and $a_n = 1$, $n \geq 1$.

(c) $a_0 = a_1 = 0$ and $a_n = 1$, $n \geq 2$.

(d) $a_n = (-1)^n$, $n \geq 0$.

(e) $a_n = n + 1$, $n \geq 0$.

(f) $a_n = n$, $n \geq 0$.

(g) $a_n = (-1)^n n$, $n \geq 0$.

3 Find a closed formula for the generating function of the sequence

(a) $a_0 = 1$, $a_1 = 2$, and $a_n = 3a_{n-1} + 2a_{n-2}$, $n \geq 2$.

(b) $b_0 = 2$, $b_1 = 1$, and $b_n = 2b_{n-1} - 3b_{n-2}$, $n \geq 2$.

(c) $c_0 = 4$, $c_1 = 13$, and $c_n = 2c_{n-1} - c_{n-2}$, $n \geq 2$.

4 Use a closed formula for the generating function of $\{a_n\}$ to express a_n as an explicit function of n when

(a) $a_0 = 7$, $a_1 = 6$, and $a_n = a_{n-1} + 6a_{n-2}$, $n \geq 2$.

(b) $b_0 = 0$, $b_1 = 1$, and $b_n = 2b_{n-1} + 15b_{n-2}$, $n \geq 2$.

(c) $c_0 = 3$, $c_1 = 6$, and $c_n = c_{n-1} + 20c_{n-2}$, $n \geq 2$.

5 Let $\{a_n\}$ be the sequence defined by $a_0 = a_1 = 3$, $a_2 = 29$, and $a_n = 3a_{n-1} + 10a_{n-2} - 24a_{n-3}$, $n \geq 3$. Use generating functions and partial fractions to derive the solution $a_n = 4^n + (-3)^n + 2^n$.

6 The Fibonacci sequence is defined by $F_0 = F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$.

(a) Use generating functions and partial fractions to derive the identity

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

(b) Prove that $F_n = [C(n+1,1) + 5C(n+1,3) + 5^2 C(n+1,5) + \cdots]/2^n$.

(c) Prove that F_n is the integer closest to

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}.$$

(d) According to some, the most visually pleasing shape for a rectangle is one in which the ratio of adjacent sides is $\varphi = (1+\sqrt{5})/2$. Compute, to two decimal places, the ratio F_{n+1}/F_n, $1 \le n \le 9$. Compare the results with the decimal expansion of φ.

(e) Prove that $\lim_{n\to\infty} F_{n+1}/F_n = (1+\sqrt{5})/2$.

7 Suppose $\{a_n\}$ is a sequence for which the formal power series $a_0 + a_1x + a_2x^2 + \cdots$ converges to a function $g(x)$ in some open interval $(-r, r)$. Show that $a_n = g^{[n]}(0)/n!$, $n \ge 0$, where $g^{[0]} = g$ and $g^{[n]}$ is the nth derivative of g, $n \ge 1$.

8 Find a formula for the sum $1 + 2 + 2^2 + \cdots + 2^{m-1}$ of the first m numbers in the geometric sequence $\{2^n\}$.

9 Prove that $\frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \frac{1}{256} + \cdots = \frac{1}{3}$.

10 Recall that a k-part composition of n is a positive integer solution to $x_1 + x_2 + \cdots + x_k = n$. For fixed positive integers k and m, denote by a_n the number of k-part compositions of n *none of which is larger than* m. Prove that the generating function for $\{a_n\}$ is $g(x) = (x + x^2 + \cdots + x^m)^k$.

11 Let $k = 4$ and $m = 3$ in Exercise 10.

(a) Evaluate $g(x) = \sum_{n\ge 0} a_n x^n$, i.e., compute the coefficient a_n of x^n in $(x + x^2 + x^3)^4$, $n \ge 0$.

(b) Confirm that there are exactly a_7 (the coefficient of x^7 from your answer to part (a)) four-part compositions of 7, none of which is larger than 3.

(c) Confirm that there are exactly a_8 four-part compositions of 8, none of which is larger than 3.

(d) Show that the number of four-part compositions of 9, none of which is larger than 3, is equal to the number of four-part compositions of 7, none of which is larger than 3.

(e) Confirm that there are exactly a_9 four-part compositions of 9, none of which is larger than 3.

12 Prove that $(x + x^2 + x^3 + \cdots)^k = \sum_{n\ge 1} C(n-1, k-1)x^n$

(a) using Equations (4.19a)–(4.19b) and induction on k.

(b) using the fact that the number of compositions of n having k parts is $C(n-1, k-1)$.

13 Consider the sequence $\{b_n\}$ defined by $b_n = (-2)^n + (n+1)3^n$. Show that $b_0 = 2$, $b_1 = 4$, $b_2 = 31$, and $b_{n+1} = 4b_n + 3b_{n-1} - 18b_{n-2}$, $n \ge 2$.

14 Prove that the coefficient of x^n in $(1+x)^m/(1-x)$ is 2^m for all $n \ge m$. (*Hint*: Lemma 4.2.7.)

15 Let $g(x)$ be the generating function for $\{a_n\}$. Describe the sequence $\{b_n\}$ whose generating function is $(1-x)g(x)$.

16 Let $g(x) = \sum_{n\geq 0} a_n x^n$ be the generating function for $\{a_n\}$. Solve for a_n if

(a) $g(x) = 1/(1-x)$.

(b) $g(x) = x(x+1)/(1-x)^3$.

(c) $g(x) = x(x^2+4x+1)/(1-x)^4$.

17 Given that $e^x = \sum_{n\geq 0} x^n/n!$, it must be that $e^{2x} = \sum_{n\geq 0}(2x)^n/n! = \sum_{n\geq 0} 2^n x^n/n!$. On the other hand, $e^{2x} = (e^x)^2$. Use Equations (4.19a)–(4.19b) to prove that $\left(\sum_{n\geq 0} x^n/n!\right)^2 = \sum_{n\geq 0} 2^n x^n/n!$.

18 If $g(x) = (1-x)^{-1}$, then $g''(x) = 2(1-x)^{-3} = 2g(x)^3$. Use Equations (4.19a)–(4.19b) and formal term-by-term differentiation to confirm that $g''(x) = 2g(x)^3$ when $g(x) = 1 + x + x^2 + x^3 + \cdots$.

19 For a fixed but arbitrary positive integer m, let $g_m(x) = \sum_{n\geq 1} S(m,n)x^n$. (Don't confuse $g_m(x)$ with $x^m = \sum_{n\geq 1} S(m,n)x^{(n)}$.)

(a) Show that $e^x g_m(x)$ is the generating function for $\{n^m/n!\}$, i.e., that $e^x g_m(x) = \sum_{n\geq 1} n^m x^n/n!$.

(b) Show that $g_m(x) = e^{-x}\sum_{n\geq 1} n^m x^n/n!$.

(c) Use (the right-hand side of) the equation in part (b) to compute $S(4,n)$, $1 \leq n \leq 5$.

(d) Describe the relationship between part (b) and Stirling's identity.

(e) Give the generating function proof of Dobinski's formula for the Bell numbers $B_m = e^{-1}\sum_{n\geq 1} n^m/n!$.

20 Find the *reciprocal* of $g(x) = \sum_{n\geq 0} a_n x^n$ if

(a) $a_n = 2(3^n) + (-2)^n$. (*Hint*: Equation (4.17).)

(b) $a_0 = 2$, $a_1 = 3$, and $a_{n+2} = 5a_{n+1} - 6a_n$, $n \geq 0$.

(c) a_n is the binomial coefficient $C(n+3,3)$, so that $g(x) = 1 + 4x + 10x^2 + 20x^3 + 35x^4 + \cdots$. (*Hint*: Equation (4.27).)

(d) a_n is the Stirling number of the second kind, $S(n+3,3)$, so that $g(x) = 1 + 6x + 25x^2 + 90x^3 + 301x^4 + \cdots$. (*Hint*: The proof of Theorem 4.2.6.)

21 Denote by $K(n)$ the number of ways to choose n elements, with replacement, from the set $A = \{r,s,t\}$, where order doesn't matter, but subject to the conditions that r can be chosen at most three times, s at most twice, and t at most once. Let $g(x)$ be the generating function for $\{K(n)\}$, i.e., $g(x) = \sum_{n\geq 0} K(n)x^n$. Show that $g(x) = (1 + x + x^2 + x^3)(1 + x + x^2)\ (1 + x)$.

22 Let $C(n)$ be the number of ways to choose n elements from the set $\{N,D,Q\}$, where order doesn't matter, but subject to the conditions that N can be chosen at most ten times, D at most five times, and Q at most twice.

(a) Find a closed formula for the generating function for $\{C(n)\}$.

(b) In how many different ways can you change a half-dollar coin using only Nickels, Dimes, and Quarters?

23 Prove the equivalence of the two statements of the Pythagorean theorem given in Example 4.2.13.

24 Let s_n and c_n be the quantities related to sines and cosines defined in Example 4.2.13. Prove that

(a) $\displaystyle\sum_{r=0}^{n} C(n,r)(s_r s_{n-r} + c_r c_{n-r}) = \sum_{r=0}^{n} (-1)^r C(n,r) \quad \text{if } n = 4k.$

(b) $\displaystyle\sum_{r=0}^{n} C(n,r)(s_r s_{n-r} + c_r c_{n-r}) = -\sum_{r=0}^{n} (-1)^r C(n,r) \quad \text{if } n = 4k+2.$

25 Find a closed formula for the generating function $g(x)$ of the sequence

(a) $\{3^n\}$. **(b)** $\{n^3\}$. **(c)** $\{2n^3 + 3n^2\}$.

26 Prove the partial fraction decomposition

$$\frac{n!}{x(x+1)\cdots(x+n)} = \frac{C(n,0)}{x} - \frac{C(n,1)}{x+1} + \frac{C(n,2)}{x+2} - \cdots \pm \frac{C(n,n)}{x+n}.$$

27 Consider the sequence $0, \frac{1}{2}, 1\frac{1}{3}, 2\frac{1}{4}, 3\frac{1}{5}, 4\frac{1}{6}, \ldots$, denoting its nth term by a_n and its generating function by $f(x) = \sum_{n\geq 0} a_n x^n$.

(a) Assuming the pattern continues, find a closed formula for a_n.

(b) Without actually doing it, describe in words how Example 4.2.12 might be used to obtain a closed formula for $f(x)$.

4.3. APPLICATIONS OF GENERATING FUNCTIONS

If we make the substitution $m = r + 1$ in Equation (4.27) and replace $C(m-1+n, m-1)$ with $C(m+n-1, n)$, the result is

$$\frac{1}{(1-x)^m} = \sum_{n\geq 0} C(n+m-1, n)x^n, \tag{4.29}$$

the generating function for the number of ways to choose n times from $\{1, 2, \ldots, m\}$, with replacement, if order doesn't matter. In fact, there is no need to appeal to Equation (4.27). If $x^{n_1}, x^{n_2}, \ldots, x^{n_m}$ are chosen from the m sets of parentheses on the right-hand side of

$$(1-x)^{-m} = (1 + x + x^2 + \cdots)(1 + x + x^2 + \cdots)\cdots(1 + x + x^2 + \cdots),$$

their product will be x^n if and only if $n_1 + n_2 + \cdots + n_m = n$, i.e., the coefficient of x^n in $(1-x)^{-m}$ is the number of nonnegative integer solutions to this equation, a number that we know to be $C(n+m-1, n)$.

Replacing x with $-x$ in Equation (4.29) produces

$$(1+x)^{-m} = \sum_{n\geq 0}(-1)^n C(n+m-1,n)x^n, \tag{4.30a}$$

a binomial-type theorem for negative exponents. With the proper definition of $C(-m,n)$, we can make it look even more like the binomial theorem.

4.3.1 Definition. Let n be a nonnegative integer. If u is any real number, the *extended binomial coefficient* $C(u,0)=1$, and

$$C(u,n) = \binom{u}{n} = \frac{u(u-1)\cdots(u-[n-1])}{n!}, \qquad n>0.$$

4.3.2 Example. If m is a positive integer, then, taking $u=-m$,

$$\begin{aligned} C(-m,n) &= \frac{-m(-m-1)\cdots(-m-[n-1])}{n!} \\ &= \frac{(-1)^n m(m+1)\cdots(m+[n-1])}{n!} \\ &= (-1)^n C(m+n-1,n). \end{aligned}$$

□

In view of Example 4.3.2, Equation (4.30a) can be written

$$(x+1)^{-m} = \sum_{n\geq 0} C(-m,n)x^n. \tag{4.30b}$$

A hundred years before the American Revolution, Isaac Newton* extended this binomial-type theorem even further.

4.3.3 Newton's Binomial Theorem. *Let u be a real number. If $|x|<|y|$, then*

$$(x+y)^u = \sum_{n\geq 0} C(u,n)x^n y^{u-n}.$$

The curious hypothesis $|x|<|y|$ signals a change of perspective. Equations (4.30a)–(4.30b) concern generating functions involving formal power series. Theorem 4.3.3 is a statement about a function of two variables that involves substituting numbers for x and y.

*The first *proof* of Newton's binomial theorem was published in 1812 by Gauss.

n	$f^{[n]}(x)$	$f^{[n]}(0)/n!$
0	$(1+x)^{\frac{1}{2}}$	1
1	$\frac{1}{2}(1+x)^{-\frac{1}{2}}$	$\frac{1}{2}$
2	$-\frac{1}{4}(1+x)^{-\frac{3}{2}}$	$-\frac{1}{8}$
3	$\frac{3}{8}(1+x)^{-\frac{5}{2}}$	$\frac{1}{16}$
4	$-\frac{15}{16}(1+x)^{-\frac{7}{2}}$	$\frac{-5}{128}$

Figure 4.3.1. Maclaurin coefficients for $(x+1)^{1/2}$.

Proof of Theorem 4.3.3. When u is a positive integer, the result is just the binomial theorem, which holds without restrictions on x and y. Otherwise, because

$$(x+y)^u = y^u\left(\frac{x}{y}+1\right)^u,$$

it suffices to prove the result when $y=1$. If $f(x)=(x+1)^u$, then (confirm it) $f^{[n]}(0)/n! = C(u,n)$, resulting in the Maclaurin series expansion

$$(x+1)^u = \sum_{n\geq 0} C(u,n)x^n. \tag{4.31}$$

Because

$$\lim_{n\to\infty}\frac{|C(u,n+1)x^{n+1}|}{|C(u,n)x^n|} = \lim_{n\to\infty}\frac{|u-n|}{n+1}|x| = |x|,$$

Equation (4.31) converges absolutely for all $|x|<1$ by the ratio test. ■

4.3.4 Example. Suppose $f(x)=(x+1)^{1/2}$. From computations summarized in Fig. 4.3.1, the Maclaurin series expansion for $f(x)$ is

$$(x+1)^{1/2} = 1+\frac{1}{2}x-\frac{1}{8}x^2+\frac{1}{16}x^3-\frac{5}{128}x^4+\cdots \tag{4.32}$$

Comparing coefficients of x^n in Equations (4.31) and (4.32), it must be the case, e.g., that $C\left(\frac{1}{2},4\right)=-\frac{5}{128}$. Let's check it out. From Definition 4.3.1,

$$\begin{aligned} C\left(\frac{1}{2},4\right) &= \frac{1}{2}\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)\left(\frac{1}{2}-3\right)\frac{1}{4!} \\ &= \frac{1}{2}\left(\frac{-1}{2}\right)\left(\frac{-3}{2}\right)\left(\frac{-5}{2}\right)\frac{1}{4!} = \frac{-15/16}{24} = \frac{-5}{128}. \end{aligned}$$

□

Shifting from binomial coefficients to Stirling numbers of the second kind, let $f_r(x)$ be the generating function for $\{S(n,r)\}$, i.e.,

$$\begin{aligned} f_r(x) &= \sum_{n\geq 0} S(n,r)x^n \\ &= S(r,r)x^r + S(r+1,r)x^{r+1} + S(r+2,r)x^{r+2} + \cdots \end{aligned}$$

Then (from Fig. 2.1.2),

$$f_1(x) = x + x^2 + x^3 + x^4 + x^5 + x^6 + \cdots = \frac{x}{1-x} \tag{4.33}$$

$$f_2(x) = x^2 + 3x^3 + 7x^4 + 15x^5 + 31x^6 + \cdots \tag{4.34}$$

$$f_3(x) = x^3 + 6x^4 + 25x^5 + 90x^6 + 301x^7 + \cdots$$

and so on. If $r > 1$, then adding

$$-rxf_r(x) = -rS(r,r)x^{r+1} - rS(r+1,r)x^{r+2} - \cdots$$

to $f_r(x)$ gives

$$\begin{aligned} (1-rx)f_r(x) &= S(r,r)x^r + [S(r+1,r) - rS(r,r)]x^{r+1} \\ &\qquad + [S(r+2,r) - rS(r+1,r)]x^{r+2} + \cdots \\ &= S(r-1,r-1)x^r + S(r,r-1)x^{r+1} + S(r+1,r-1)x^{r+2} + \cdots \\ &= xf_{r-1} \end{aligned}$$

by the recurrence $S(k+1,r) = S(k,r-1) + rS(k,r)$ (and the fact that $S(r,r) = 1 = S(r-1,r-1)$). So, for all $r > 1$, $f_r(x) = xf_{r-1}/(1-rx)$. Together with Equation (4.33), this implies

$$f_2(x) = \frac{x}{1-2x}f_1(x) = \frac{x^2}{(1-2x)(1-x)}, \tag{4.35}$$

$$f_3(x) = \frac{x}{1-3x}f_2(x) = \frac{x^3}{(1-3x)(1-2x)(1-x)}, \tag{4.36}$$

and so on. Along with induction, these observations prove the following.

4.3.5 Theorem. *Let r be a fixed but arbitrary positive integer. Denote by $f_r(x)$ the generating function for the sequence $\{S(n,r)\}$ of Stirling numbers of the second kind, i.e., $f_r(x) = \sum_{n\geq 0} S(n,r)x^n$. Then*

$$f_r(x) = x^r \prod_{t=1}^{r} \frac{1}{1-tx}. \tag{4.37}$$

4.3.6 Example. From Equation (4.35),

$$\sum_{n\geq 2} S(n,2)x^n = x^2 \frac{1}{(1-2x)(1-x)}. \tag{4.38}$$

Using partial fractions,

$$\begin{aligned}\frac{1}{(1-2x)(1-x)} &= \frac{2}{(1-2x)} - \frac{1}{1-x} \\ &= 2[1+2x+(2x)^2+(2x)^3+\cdots] - [1+x+x^2+x^3+\cdots] \\ &= \sum_{n\geq 0}(2^{n+1}-1)x^n \qquad (4.39) \\ &= 1+3x+7x^2+15x^3+31x^4+\cdots\end{aligned}$$

Multiplying by x^2, we recover Equation (4.34):

$$f_2(x) = x^2+3x^3+7x^4+15x^5+31x^6+\cdots$$

So far, so good. Now let's see what was overlooked in the rush to compute: Multiplying Equation (4.39) by x^2 yields

$$\begin{aligned}\sum_{n\geq 2} S(n,2)x^n &= f_2(x) \\ &= \sum_{n\geq 0}(2^{n+1}-1)x^{n+2} \\ &= \sum_{n\geq 2}(2^{n-1}-1)x^n.\end{aligned}$$

Comparing the coefficient of x^n on either side of this equation yields the closed formula $S(n,2) = 2^{n-1}-1$.

Similarly, from Equation (4.36) (check the computations),

$$\begin{aligned}\sum_{n\geq 3} S(n,3)x^n &= x^3\left[\frac{9/2}{1-3x} - \frac{4}{1-2x} + \frac{1/2}{1-x}\right] \\ &= x^3\left[\tfrac{9}{2}(1+3x+(3x)^2+\cdots) - 4(1+2x+(2x)^2+\cdots).\right. \\ &\qquad \left.+\tfrac{1}{2}(1+x+x^2+\cdots)\right].\end{aligned}$$

Therefore, $S(n,3) = \frac{1}{2}(3^{n-1}-2^n+1)$.

What is the generalization? If partial fractions are used with Equation (4.37), the result is a generating function proof of Stirling's identity,

$$S(n,r) = \frac{1}{r!}\sum_{t=1}^{r}(-1)^{r-t}C(r,t)t^n. \qquad \square$$

With the convention $p(0) = 1$, the *partition generating function* is

$$\begin{aligned} P(x) &= \sum_{n\geq 0} p(n)x^n \\ &= 1 + x + 2x^2 + 3x^3 + 5x^4 + 7x^5 + 11x^6 + 15x^7 + 22x^8 + \cdots \end{aligned}$$

There is no closed formula for $P(x)$, but there is an interesting formula.

4.3.7 Theorem. *The partition generating function*

$$P(x) = \prod_{k\geq 1}\frac{1}{1-x^k}. \tag{4.40}$$

Whoa! An infinite product?

4.3.8 Example. The coefficient of x^4 in the infinite product

$$\begin{aligned} \prod_{k\geq 1}(1 + x^k + x^{2k} + \cdots) = (1 + x + x^2 + \cdots)(1 + [x^2] + [x^2]^2 + \cdots) \\ \times (1 + [x^3] + [x^3]^2 + \cdots)(1 + [x^4] + [x^4]^2 + \cdots)\cdots \end{aligned}$$

is the same as the coefficient of x^4 in the *finite* product

$$(1 + x + x^2 + x^3 + x^4)(1 + [x^2] + [x^2]^2)(1 + [x^3])(1 + [x^4]). \qquad \square$$

Proof of Theorem 4.3.7. Recall the shorthand notation for partitions, e.g.,

$$[4^3, 3^5, 2^4, 1^6] = [4,4,4,3,3,3,3,3,2,2,2,2,1,1,1,1,1,1],$$

where exponents denote the multiplicities of repeated parts. Thus, e.g., 4^3 contributes not $4 \times 4 \times 4 = 64$, but $4 + 4 + 4 = 12$ to the sum $4 \times 3 + 3 \times 5 + 2 \times 4 + 1 \times 6 = 41$. In particular, $[4^3, 3^5, 2^4, 1^6] \vdash 41$. More generally, $[\ldots, 4^{r_4}, 3^{r_3}, 2^{r_2}, 1^{r_1}] \vdash n$ if and only if

$$\cdots + 4r_4 + 3r_3 + 2r_2 + 1r_1 = n. \tag{4.41}$$

The distributivity of multiplication over addition implies that a product of finitely many finite sums can be evaluated by choosing one term from each summand (set of parentheses), multiplying the choices together, adding the resulting products for all possible ways of making the selections, and "combining like terms". With the

$[4]$	$r_4 = 1$	$1 \times 1 \times 1 \times [x^4] \times 1 \times \cdots$
$[3,1]$	$r_1 = r_3 = 1$	$x \times 1 \times [x^3] \times 1 \times 1 \times \cdots$
$[2^2]$	$r_2 = 2$	$1 \times [x^2]^2 \times 1 \times 1 \times 1 \times \cdots$
$[2,1^2]$	$r_1 = 2, r_2 = 1$	$x^2 \times x^2 \times 1 \times 1 \times 1 \times \cdots$
$[1^4]$	$r_1 = 4$	$x^4 \times 1 \times 1 \times 1 \times 1 \times \cdots$

Figure 4.3.2

added constraint that 1 must be the choice from all but finitely many summands, this process extends to evaluating the infinite product

$$(1+x+x^2+x^3+\cdots)(1+[x^2]+[x^2]^2+[x^2]^3+\cdots)\times(1+[x^3]+[x^3]^2+[x^3]^3+\cdots)\cdots$$

There is a natural one-to-one correspondence between the different choices that produce x^n in this process, and the distinct partitions of n. If

$$\begin{aligned} &x^{r_1} \text{ is chosen from } (1+x+x^2+x^3+\cdots),\\ &[x^2]^{r_2} = x^{2r_2} \text{ from } (1+[x^2]+[x^2]^2+[x^2]^3+\cdots),\\ &[x^3]^{r_3} = x^{3r_3} \text{ from } (1+[x^3]+[x^3]^2+[x^3]^3+\cdots), \end{aligned}$$

and so on, then the product $x^{r_1} \times x^{2r_2} \times \cdots \times x^{nr_n} = x^n$, if and only if $r_1 + 2r_2 + \cdots + nr_n = n$. By Equation (4.41), this is equivalent to $[n^{r_n}, \ldots, 2^{r_2}, 1^{r_1}] \vdash n$. So, the coefficient of x^n on the right-hand side of Equation (4.40) is exactly $p(n)$. ■

In the proof of Theorem 4.3.7, the correspondence between partitions of $n = 4$, solutions of $r_1 + 2r_2 + 3r_3 + 4r_4 = 4$, and selections yielding x^4 is tabulated in Fig. 4.3.2.

4.3.9 Example. In how many ways can change be made for a dollar? Not counting a dollar coin as "change", the available coins are pennies, nickels, dimes, quarters, and half dollars.

The answer is the number of nonnegative integer solutions to the equation

$$p + 5n + 10d + 25q + 50h = 100.$$

This is a partition problem in which the parts are restricted to the values 1, 5, 10, 25, and 50.

With *no* restrictions on the denominations of the coins, the answer be the coefficient of x^{100} in the infinite product

$$\prod_{k\geq 1}(1-x^k)^{-1} = (1+x+x^2+\cdots)\times(1+[x^2]+[x^2]^2+\cdots)\times \\ (1+[x^3]+[x^3]^2+\cdots)\times\cdots$$

With the restrictions imposed by U.S. coins, the answer involves just those contributions in which 1 is the mandatory choice from all summands but the 1st, 5th, 10th, 25th, and 50th, i.e., the number of ways to change a dollar is the coefficient of x^{100} in the product

$$(1+x+x^2+\cdots)(1+[x^5]+[x^5]^2+\cdots)(1+[x^{10}]+[x^{10}]^2+\cdots)\times \\ (1+[x^{25}]+[x^{25}]^2+\cdots)(1+[x^{50}]+[x^{50}]^2+\cdots).$$

Thus, e.g., the contribution

$$1\times[x^5]^4\times[x^{10}]^3\times 1\times[x^{50}] = x^{100}$$

corresponds to changing the dollar with four nickels, three dimes, and a half dollar; making change with four quarters corresponds to $1\times 1\times 1\times[x^{25}]^4\times 1$, and so on. □

There are other interesting ways to restrict the parts of partitions.

4.3.10 Example. The $p(6)=11$ partitions of 6 are $[6],[5,1],[4,2],[4,1^2],[3^2],[3,2,1],[3,1^3],[2^3],[2^2,1^2],[2,1^4]$, and $[1^6]$. Some of these expressions are complicated by exponents (indicating multiplicities). The simpler ones, $[6],[5,1],[4,2]$, and $[3,2,1]$, are those having distinct parts. Denote by $p_{\text{dist}}(n)$ the number of partitions of n, each of whose parts is different. Then, e.g, $p_{\text{dist}}(6)=4$. The generating function for $\{p_{\text{dist}}(n)\}$ is

$$\begin{aligned} h(x) &= \sum_{n\geq 0} p_{\text{dist}}(n)x^n \\ &= (1+x)(1+x^2)(1+x^3)(1+x^4)\cdots, \end{aligned} \tag{4.42}$$

where, by convention, $p_{\text{dist}}(0)=1$. □

4.3.11 Example. Let $p_{\text{odd}}(n)$ be the number of partitions of n each of whose parts is odd. From Example 4.3.10, the odd-part partitions of 6 are $[5,1],[3^2],[3,1^3]$, and $[1^6]$, so $p_{\text{odd}}(6)=4$. The generating function for $\{p_{\text{odd}}(n)\}$ is

$$\begin{aligned} g(x) &= \sum_{n\geq 0} p_{\text{odd}}(n)x^n \\ &= \left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^3}\right)\left(\frac{1}{1-x^5}\right)\cdots \end{aligned} \tag{4.43}$$

where, by convention, $p_{\text{odd}}(0)=1$. □

From Examples 4.3.10 and 4.3.11, $p_{\text{odd}}(6) = p_{\text{dist}}(6)$. This coincidence turns out not to be an accident.

4.3.12 Theorem. *Let $p_{odd}(n)$ be the number of partitions of n each of whose parts is odd and $p_{dist}(n)$ the number having distinct parts. Then, for every positive integer n, $p_{odd}(n) = p_{dist}(n)$.*

Proof. From Example 4.3.10, the generating function for $p_{\text{dist}}(n)$ is

$$\begin{aligned} h(x) &= (1+x)(1+x^2)(1+x^3)(1+x^4)\cdots \\ &= \left(\frac{1-x^2}{1-x}\right)\left(\frac{1-[x^2]^2}{1-x^2}\right)\left(\frac{1-[x^3]^2}{1-x^3}\right)\left(\frac{1-[x^4]^2}{1-x^4}\right)\cdots \end{aligned}$$

After canceling $1-x^2$, $1-x^4$, and so on, i.e., every term from the numerator and every second term from the denominator, we are left with $g(x)$ from Example 4.3.11 on the right-hand side. ■

Let's return to the partition generating function

$$\begin{aligned} P(x) &= \sum_{n\geq 0} p(n)x^n \\ &= 1 + x + 2x^2 + 3x^3 + 5x^4 + 7x^5 + 11x^6 + 15x^7 + 22x^8 + \cdots \\ &= \prod_{k\geq 1} \frac{1}{1-x^k}. \end{aligned} \tag{4.44}$$

Because the constant coefficient $p(0) = 1 \neq 0$ (by convention), the formal power series $P(x)$ has a reciprocal, call it $f(x) = \sum_{n\geq 0} a_n x^n$. Then, as in the proof of Theorem 4.2.6, $a_0 = 1/p(0) = 1$. Because

$$\begin{aligned} 0 &= p(0)a_1 + p(1)a_0 \\ &= 1 \times a_1 + 1 \times 1, \\ a_1 &= -1; \end{aligned} \tag{4.45a}$$

since

$$\begin{aligned} 0 &= p(0)a_2 + p(1)a_1 + p(2)a_0 \\ &= 1 \times a_2 + 1 \times (-1) + 2 \times 1, \\ a_2 &= -1; \end{aligned} \tag{4.45b}$$

because

$$\begin{aligned} 0 &= p(0)a_3 + p(1)a_2 + p(2)a_1 + p(3)a_0 \\ &= 1 \times a_3 + 1 \times (-1) + 2 \times (-1) + 3 \times 1, \\ a_3 &= 0; \end{aligned} \tag{4.45c}$$

and so on. But, this is the hard way to proceed. The easy way is to invert both sides of Equation (4.44), obtaining

$$\begin{aligned} f(x) &= \prod_{k\geq 1}(1 - x^k) \\ &= (1-x)(1-x^2)(1-x^3)(1-x^4)(1-x^5)\cdots \\ &= 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + x^{22} + x^{26} - x^{35} - \cdots \end{aligned} \tag{4.46}$$

Judging from the first few terms, it appears that many coefficients of $f(x)$ are zero and those that are not all seem to be ± 1. After the first term, the signs seem to alternate in pairs. Within these pairs, the exponents appear to drift further apart, one unit at a time. Finally, the first exponent in each pair comes from the sequence

$$1, 5, 12, 22, 35, \ldots$$

Applying the techniques of Section 4.1 to this fragment suggests that its nth term is given by the polynomial function $C(n,0) + 4C(n,1) + 3C(n,2) = \frac{1}{2}(2 + 5n + 3n^2)$. (Confirm it!) If this formula is valid for all n, then the sequence is well known! It consists of the so-called *pentagonal* numbers (Fig. 4.3.3).

Historically, the pentagonal number sequence is written so as to begin, not with a zeroth, but with a first term. This perspective can be accommodated by setting $m = n + 1$. Starting with $m = 1$, the mth term of the pentagonal number sequence is

$$\tfrac{1}{2}(2 + 5[m-1] + 3[m-1]^2) = m(3m-1).$$

4.3.13 Euler's Pentagonal Number Theorem. *The reciprocal of the partition generating function $P(x)$ is*

$$\begin{aligned} f(x) &= \sum_{n\geq 0} a_n x^n \\ &= \prod_{k\geq 1}(1 - x^k) \\ &= 1 + \sum_{m\geq 1}(-1)^m (x^{m(3m-1)/2} + x^{m(3m+1)/2}). \end{aligned} \tag{4.47}$$

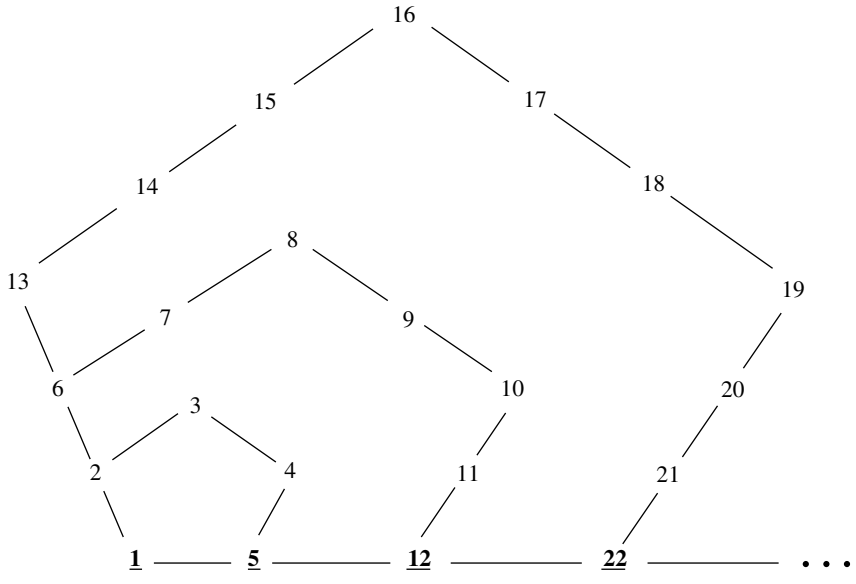


Figure 4.3.3. Pentagonal Numbers.

(Confirm that the first few terms of Equation (4.47) are precisely those given by Equation (4.46).)

4.3.14 Example. Apart from historical footnotes, what good is Equation (4.47)? For one thing, an independent way to compute the coefficients of $1/P(x) = f(x) = \sum_{n\geq 0} a_n x^n$ gives us another way to look at $P(x) = 1/f(x)$. Let's reconsider the approach illustrated by Equations (4.45a)–(4.45c), but this time from "the reverse-angle". The coefficient, e.g., of x^9 in the product $f(x)P(x)$ is

$$0 = a_0 p(9) + a_1 p(8) + a_2 p(7) + \cdots + a_8 p(1) + a_9 p(0).$$

Substituting $a_0 = a_5 = a_7 = 1$, $a_1 = a_2 = -1$, and $a_3 = a_4 = a_6 = a_8 = a_9 = 0$ from Equation (4.46) [an explicit representation of Equation (4.47)], yields

$$0 = p(9) - p(8) - p(7) + p(4) + p(2).$$

Upon substituting the values $p(2) = 2$, $p(4) = 5$, $p(7) = 15$, and $p(8) = 22$ from Equation (4.44), this yields $p(9) = 30$. Similarly,

$$0 = p(10) - p(9) - p(8) + p(5) + p(3).$$

from which it follows that

$$\begin{aligned} p(10) &= 30 + 22 - 7 - 3 \\ &= 42. \end{aligned}$$

(Confirm these values by summing rows 9 and 10 of Figure 1.8.2.) □

4.3. EXERCISES

1 Evaluate the extended binomial coefficient

(a) $\binom{-3}{4}$. **(b)** $\binom{-4}{3}$. **(c)** $C\left(\frac{2}{3}, 2\right)$. **(d)** $C\left(-\frac{2}{3}, 2\right)$.

2 Show that $2n \times C\left(\frac{1}{2}, n\right) = C\left(-\frac{1}{2}, n-1\right)$.

3 Show that $C(-u, n) = (-1)^n C(u+n-1, n)$ for any real number u and any nonnegative integer n.

4 Prove that $(-1)^m C(-n, m-1) = (-1)^n C(-m, n-1)$.

5 Prove that $(-4)^n C\left(-\frac{1}{2}, n\right) = C(2n, n)$.

6 Prove Pascal's relation $C(u+1, n) = C(u, n-1) + C(u, n)$ for the extended binomial coefficients.

7 Confirm that the formulas $S(m,2) = 2^{m-1} - 1$ and $S(m,3) = \frac{1}{2}(3^{m-1} - 2^m + 1)$, obtained in Example 4.3.6, are the $r = 2$ and $r = 3$ cases, respectively, of Stirling's identity.

8 Consider $f_4(x) = x^4/[(1-x)(1-2x)(1-3x)(1-4x)]$ from Equation (4.37).

(a) Expand $f_4(x)$ using partial fractions.

(b) Use your answer to part (a) to show that $S(m,4) = \frac{1}{6}[4^{m-1} - 3^m + 3(2^{m-1}) - 1]$.

(c) Use part (b) to compute $S(8,4)$.

(d) Show that part (b) is the $r = 4$ case of Stirling's identity.

9 Prove that the generating function for the Fibonacci numbers

$$F(x) = 1 + x + 2x^2 + 3x^3 + 5x^4 + 8x^5 + 13x^6 + \cdots$$

has radius of convergence $\varphi = (1 + \sqrt{5})/2$.

10 In the manner of Example 4.3.4, show that the first few terms in the Maclaurin series expansion for $f(x) = (1-x)^{-1/2}$ are $1 + \frac{1}{2}x + \frac{3}{8}x^2 + \frac{5}{16}x^3 + \frac{35}{128}x^4 + \cdots$

11 For things to work out properly in Exercise 10, $C\left(-\frac{1}{2}, 4\right)$ had better be $\frac{35}{128}$. Use Definition 4.3.1 to confirm that it is.

12 By Newton's binomial theorem,

$$(1+x)^{1/2} = 1 + C\left(\tfrac{1}{2}, 1\right)x + C\left(\tfrac{1}{2}, 2\right)x^2 + C\left(\tfrac{1}{2}, 3\right)x^3 + \cdots$$

Since the square of the left-hand side of this equation is $1 + x$, the square of the right-hand side must be $1 + x$. In particular, the coefficient of x^n in the square of the right-hand side must be zero for all $n \geq 2$. From Equations (4.19a)–(4.19b), the coefficient, e.g., of x^2 is $2C\left(\frac{1}{2}, 2\right) + C\left(\frac{1}{2}, 1\right)^2$.

(a) Use Definition 4.3.1 to confirm that $2C\left(\frac{1}{2}, 2\right) + C\left(\frac{1}{2}, 1\right)^2 = 0$.

(b) Use Equations (4.19a)–(4.19b) to express the coefficient of x^3 in the square of the right-hand side; then use Definition 4.3.1 to confirm that it is zero.

(c) Use Equations (4.19a)–(4.19b) to express the coefficient of x^4 in the square of the right-hand side; then use Definition 4.3.1 to confirm that it is zero.

(d) Further confirm parts (a)–(c) by truncating the right-hand side of Equation (4.32) at the ellipsis ("$\cdots$") and squaring what's left.

13 Show that $(1 - 4x)^{-1/2} = 1 + 2x + 6x^2 + 20x^3 + 70x^4 + \cdots$.

14 Show that $(1 - 4x)^{-1/2}$ is the generating function for $C(2n, n)$ by

(a) using Newton's binomial theorem and Exercise 5.

(b) showing that $a_0 = 1$ and $a_{n+1} = (4n + 2)a_n/(n + 1)$, $n \geq 0$, in the Maclaurin series expansion $(1 - 4x)^{-1/2} = \sum_{n\geq 0} a_n x^n$.

15 Let $g(x)$ be the generating function for the Catalan sequence $\{C(2n, n)/(n + 1)\}$. Show that $g(x) = (1 - \sqrt{1 - 4x})/2x$.

16 Suppose A is a nonempty subset of positive integers. Let $p_A(n)$ be the number of partitions of n each of whose parts is an element of A. Find a closed for $g(x) = \sum_{n\geq 0} p_A(n)x^n$, where $p_A(0)$ is assumed to be 1.

17 Find a closed formula for $g(x) = \sum_{n\geq 0} a_n x^n$ when $a_0 = 1$ and a_n is the number of partitions of n,

(a) no part of which is repeated more than twice.

(b) no part of which is repeated more than three times.

18 For a fixed but arbitrary positive integer k, let

$$p(n; k) = \begin{cases} 0 & \text{if } n < 0, \\ 1 & \text{if } n = 0, \end{cases}$$

and the number of partitions of n each of whose parts is at most k, $n > 0$.

(a) Show that $p(n; k) = p(n; k - 1) + p(n - k; k)$.

(b) If $g_k(x) = \sum_{n\geq 0} p(n; k)x^n$ is the generating function for $\{p(n; k)\}$, show that

$$g_k(x) = \prod_{i=1}^{k} (1 - x^i)^{-1}.$$

(c) Show that $p_k(n) = p(n; k) - p(n; k - 1)$, where $p_k(n)$ is the number of k-part partitions of n.

(d) Let $f_k(n) = \sum_{n\geq 0} p_k(n)x^n$ be the generating function for $\{p_k(n)\}$. Use parts (b) and (c) to show that

$$f_k(x) = x^k \prod_{i=1}^{k} (1 - x^i)^{-1}.$$

(e) Find a closed formula for the generating function for the partitions of n each of whose parts is *different* and at most k.

19 Let $q_m(n)$ be the number of partitions of n having m parts each of which is different (so that $\sum_{m\geq 1} q_m(n) = p_{\text{dist}}(n)$).

(a) Show that $q_3(10) = 4$.

(b) Show that $q_3(12) = 7$.

(c) Show that $q_m(n) = q_m(n-m) + q_{m-1}(n-m)$.

(d) Show that $1 + \sum_{n\geq m\geq 1} q_m(n)x^n t^m = \prod_{i\geq 1}(1+tx^i)$.

(e) Prove that $q_m(n) = p_m(n - C(m,2))$, the number of m-part partitions of $n - C(m,2)$ (with no restrictions on the parts).

20 Recall that $p_m(n)$ is the number of m-part partitions of n. Let $f_m(x) = \sum_{n\geq 0} p_m(n)x^n$ be the generating function for $\{p_m(n)\}$.

(a) Show that $f_m(x)$ is the coefficient of t^m in

$$P(x,t) = \prod_{i\geq 1} \frac{1}{1-tx^i}.$$

(b) Compute the mth partial derivative of $P(x,t)$ with respect to t and use it to show that

$$f_m(x) = \frac{x^m}{(1-x)(1-x^2)\cdots(1-x^m)}.$$

21 Prove that $\sum_{m\geq 1}\sum_{r=1}^{m} S(m,r)x^m t^{(r)} = xt/(1-xt)$.

22 In the manner of Example 4.3.14 (and using Equation (4.46)),

(a) show that $p(11) = 56$.

(b) show that $p(12) = p(0) - p(5) - p(7) + p(10) + p(11)$.

(c) evaluate $p(12)$.

23 Prove that $S(m+1, n+1) = \sum_{r=n}^{m} S(r,n)(n+1)^{m-r}$.

24 Use Exercise 23 and Fig. 2.1.2 to show that

(a) $S(8,5) = 1050$. **(b)** $S(9,6) = 2646$.

25 Show that there are 292 ways to change a dollar.

26 How many ways are there to change a

(a) quarter? **(b)** half-dollar?

27 Let b_n be the number of nonnegative integer solutions to $x_1 + x_2 + x_3 + x_4 = n$. Find a closed formula for the generating function of the sequence $\{b_n\}$ if

(a) $x_i \leq 10$, $1 \leq i \leq 4$.

(b) x_i is odd, $1 \le i \le 4$.

(c) $2 \le x_1 \le 5$, $7 \le x_2 \le 9$, $4 \le x_3$, and $x_4 \le 6$.

(d) there are no additional restrictions on the x_i.

28 Confirm Theorem 4.3.12 by showing that

(a) $(1 + x + x^2 + \cdots)(1 + x^3 + x^6 + \cdots)(1 + x^5 + \cdots)(1 + x^7 + \cdots) = 1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + 4x^6 + 5x^7 + \cdots$

(b) $(1 + x)(1 + x^2)(1 + x^3)(1 + x^4)(1 + x^5)(1 + x^6)(1 + x^7) \cdots = 1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + 4x^6 + 5x^7 + \cdots$

29 Let a_n be the number of ways to distribute n unlabeled balls into eight labeled urns. Find a closed formula for the generating function of the sequence $\{a_n\}$ if

(a) no urn is left empty.

(b) no urn is left with fewer than three balls.

30 Show that

(a) in the partial fraction expression

$$\frac{1}{(1-x)(1-2x)\cdots(1-rx)} = \frac{a_1}{1-x} + \frac{a_2}{1-2x} + \cdots + \frac{a_r}{1-rx},$$
$$a_t = (-1)^{r-t} t^{r-1} / [(t-1)!(r-t)!], \quad 1 \le t \le r.$$

(b) the Stirling number $S(n, r)$ is the coefficient of x^n in the expression

$$f_r(x) = x^r \sum_{t=1}^{r} (-1)^{r-t} \frac{t^{r-1}}{(t-1)!(r-t)!} [1 + tx + (tx)^2 + (tx)^3 + \cdots].$$

(c) as advertised in Example 4.3.6, Equation (4.37) leads to a new proof of Stirling's identity.

31 Let k be a fixed but arbitrary positive integer. Denote by $a_k(n)$ the number of (equally likely) ways to obtain a sum of n by rolling k (fair) dice.

(a) Find a closed formula for the generating function $g_k(x) = \sum_{n \ge 0} a_k(n) x^n$.

(b) Show that $g_4(x) = (x - x^7)^4 \sum_{n \ge 0} C(n+3, 3) x^n$.

(c) Show that $a_4(20) = C(19, 3) - 4C(13, 3) + 6C(7, 3)$.

(d) Evaluate $a_4(20)$.

(e) Evaluate $a_4(24)$.

32 Given an integer $k \ge 2$, show that the number of partitions of n, none of whose parts is (exactly) divisible by k, is equal to the number of partitions of n no part of which has multiplicity as large as k.

33 Let $a_1, a_2, \ldots, a_m$ be fixed but arbitrary real numbers, and Let $E_n = E_n(a_1, a_2, \ldots, a_m)$. Denote by $e(x)$ (not to be confused with e^x) the

generating function for $\{E_n\}$ so that $e(x) = E_0 + E_1x + E_2x^2 + \cdots$. Prove that

$$e(x) = (1 + a_1x)(1 + a_2x)\cdots(1 + a_mx).$$

34 Let $a_1, a_2, \ldots, a_m$ be fixed but arbitrary real numbers, and let $M_n = M_n(a_1, a_2, \ldots, a_m) = a_1^n + a_2^n + \cdots + a_m^n$ be their nth power sum. Define

$$M(x) = \sum_{n\geq 0}(-1)^n M_{n+1}x^n.$$

(a) Show that $M(x) = \sum_{r=1}^m a_r(1 + a_rx)^{-1}$.

(b) Show that $M(x) = \sum_{r=1}^m D_x \ln(1 + a_rx)$.

(c) Show that $M(x) = D_x \ln\left[\prod_{r=1}^m (1 + a_rx)\right]$

(d) Show that $M(x) = D_x \ln(e(x))$, where $e(x)$ is not e^x, but the generating function from Exercise 33.

(e) Show that $M(x) = e'(x)/e(x)$, where $e(x)$ is the function from part (d).

(f) Show that $e'(x) = M(x)e(x)$ is the generating function version of Newton's identities.

35 Let $a_1, a_2, \ldots, a_m$ be fixed but arbitrary numbers. Their nth homogeneous symmetric function $H_n = H_n(a_1, a_2, \ldots, a_m)$ is the sum of all $C(n + m - 1, n)$ monomials of degree n in $a_1, a_2, \ldots, a_m$, i.e., $H_n(a_1, a_2, \ldots, a_m) = \sum M_\alpha(a_1, a_2, \ldots, a_m)$, where the summation is over all partitions α of n having at most m parts. Let $h(x)$ be the generating function for $\{H_n\}$, assuming that $H_0 = 1$, i.e., $h(x) = 1 + H_1x + H_2x^2 + \cdots$.

(a) Show that $h(x) = [(1 - a_1x)(1 - a_2x)\cdots(1 - a_mx)]^{-1}$.

(b) Explain how/why part (a) is a generalization of Equation (4.29).

(c) Prove that $e(-x)h(x) = 1$, where $e(x)$ is the function in Exercise 33.

(d) For every $n \geq 1$, prove that $\sum_{r=0}^n (-1)^r E_r H_{n-r} = 0$, where E_r is defined in Exercise 33.

(e) Confirm, by direct computation, that

$$H_3(a, b, c) - E_1(a, b, c)H_2(a, b, c) + E_2(a, b, c)H_1(a, b, c) - E_3(a, b, c) = 0.$$

(f) Prove that the elementary symmetric functions $E_n(x_1, x_2, \ldots, x_m)$, $1 \leq n \leq m$, can be expressed as polynomials in the homogeneous symmetric functions $H_n(x_1, x_2, \ldots, x_m)$, $1 \leq n \leq m$.

(g) Prove the following analog of the fundamental theorem of symmetric polynomials: Any polynomial symmetric in the variables $x_1, x_2, \ldots, x_m$ is a polynomial in the homogeneous symmetric functions $H_n(x_1, x_2, \ldots, x_m)$, $1 \leq n \leq m$.

(h) Let H be the $(n + 1) \times (n + 1)$ matrix whose (i, j)-entry is zero if $j > i$ and $H_{i-j}(x_1, x_2, \ldots, x_m)$ if $j \leq i$. Similarly, let E by the $(n + 1)$-square

matrix whose (i,j)-entry is zero if $j > i$ and $(-1)^{i+j}E_{i-j}(x_1, x_2, \ldots, x_m)$ otherwise. Prove that $H^{-1} = E$.

36 Prove that $S(n+r, r) = H_n(1, 2, \ldots, r)$. (*Hint*: Theorem 4.3.5 and Exercise 35(a). Compare with Exercise 11(c), Section 2.1.)

37 Prove that $\sum_{r=0}^{n}(-1)^r C(n,r)C(2n-r-1, n-r) = 0$, $n \geq 1$.

38 Let $Z_n = Z_n(s_1, s_2, \ldots, s_n)$ be the cycle index polynomial for S_n discussed in Section 3.7. Let $f(x) = \sum_{n\geq 0} Z_n x^n$ be the generating function for $\{Z_n\}$. Using Theorem 3.7.8(a) and Exercise 35(a), MacMahon showed that $f(x) = e^w$, where

$$w = s_1 x + \tfrac{1}{2}s_2 x^2 + \tfrac{1}{3}s_3 x^3 + \tfrac{1}{4}s_4 x^4 + \cdots$$

Let $f(x) = e^w$, and confirm that $f^{[n]}(0)/n! = Z_n(s_1, s_2, \ldots, s_n)$ when

(a) $n = 0$. **(b)** $n = 1$. **(c)** $n = 2$.

(d) $n = 3$. **(e)** $n = 4$.

39 Let r and s be fixed but arbitrary positive integers. Denote by $a_{(r,s)}(n)$ the number of partitions of n that have at most s parts each of which is at most r. Define $a_{(r,s)}(0) = 1$. Then (Exercise 27, Section 1.8), $\sum_{n\geq 0} a_{(r,s)}(n) = C(r+s, r)$. Denote by $f_{(r,s)}(x) = \sum_{n\geq 0} a_{(r,s)}(n)x^n$ the generating function for these numbers.

(a) Show that $f_{(2,2)}(x) = 1 + x + 2x^2 + x^3 + x^4$.

(b) Show that $f_{(3,2)}(x) = 1 + x + 2x^2 + 2x^3 + 2x^4 + x^5 + x^6$.

(c) The *q-binomial coefficient* is $C_q(r+s, r) = f_{(r,s)}(q)$. (From parts (a) and (b), e.g., $C_q(4,2) = 1 + q + 2q^2 + q^3 + q^4$ and $C_q(5,2) = 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6$.) Show that $C_q(r+s, 0) = 1 = C_q(r+s, r+s)$.

(d) Show that $C_q(r+s, r) = C_q(r+s, s)$. (See part (c).)

(e) Show that $C_q(r+s, r) = C_q(r+s-1, r) + q^s C_q(r+s-1, r-1)$.

(f) Show that

$$C_q(r+s, s) = \frac{(1-q)(1-q^2)\cdots(1-q^{r+s})}{(1-q)(1-q^2)\cdots(1-q^r) \times (1-q)(1-q^2)\cdots(1-q^s)}.$$

(g) Prove that

$$f_{(r,s)}(x) = \frac{(1-x)(1-x^2)\cdots(1-x^{r+s})}{(1-x)(1-x^2)\cdots(1-x^r) \times (1-x)(1-x^2)\cdots(1-x^s)}.$$

(h) Use the formula from part (g) to confirm part (a).

(i) Use the formula from part (g) to confirm part (b).

(j) Show that $\lim_{q\to 1} C_q(m,r) = C(m,r)$, binomial coefficient m-choose-r.

(k) Denote by $W(r,s)$ the set of binary words of length $r+s$, with r bits (letters) equal to 0 and s bits equal to 1. Suppose $w = b_1 b_2 \cdots b_m \in W$ (so that $m = r+s$). As in Section 1.8, Exercise 27(d), the inversion number of b_i is 0 if $b_i = 1$, and it is the number of 1's to the left of b_i if $b_i = 0$. Define Inv (w), the *inversion number* of w, to be the sum of the inversion numbers of its bits, and show that

$$\sum_{w\in W(r,s)} q^{\mathrm{Inv}(w)} = C_q(r+s,r).$$

40 Denote by $K(n)$ the number of ways to choose n elements from the set $A = \{r,s,t\}$, with replacement, where order doesn't matter, but subject to the conditions that r can be chosen at most three times, s at most twice, and t at most once. Then $K(n)$ is the number of n-element sub*multisets* of A subject to the multiplicity conditions on r, s, and t. When $n = 5$, e.g., the possible submultisets are $\{r,r,r,s,s\}$, $\{r,r,r,s,t\}$, and $\{r,r,s,s,t\}$, so that $K(5) = 3$. Letting

$$g(x) = \sum_{n\geq 0} K(n)x^n$$

be the generating function for $\{K(n)\}$, show that

(a) $g(x) = (1+x+x^2+x^3)(1+x+x^2)(1+x)$.

(b) $g(x) = 1+3x+5x^2+6x^3+5x^4+3x^5+x^6$.

(c) $g(x) = [(1-x^4)(1-x^3)(1-x^2)]/(1-x)^3$. (Compare with Equation (4.29).)

4.4. EXPONENTIAL GENERATING FUNCTIONS

Form ever follows function.

— Louis Henri Sullivan

Recall that the Bell numbers are sums of Stirling numbers of the second kind;

$$B_n = \sum_{r=1}^{n} S(n,r)$$

is the (total) number of partitions of $\{1,2,\ldots,n\}$. Setting $B_0 = 1$, the Bell numbers satisfy the recurrence

$$B_{n+1} = \sum_{r=0}^{n} C(n,r)B_r. \tag{4.48}$$

Let's see if we can find a closed formula for the generating function

$$\begin{aligned} g(x) &= \sum_{n\geq 0} B_n x^n \\ &= 1 + x + 2x^2 + 5x^3 + 15x^4 + 52x^5 + \cdots \end{aligned}$$

While it is true that

$$B_n = c_1 B_{n-1} + c_2 B_{n-2} + \cdots + c_n B_0,$$

neither the coefficient $c_r = C(n-1, n-r)$ nor the number of terms is independent of n. Equation (4.48) is not a homogeneous linear recurrence as defined by Equation (4.21). Partial fractions are of no use here. A new idea is needed.

Let's see what happens if we multiply by e^x, the generating function for $\{1/n!\}$:

$$\begin{aligned} g(x)e^x &= \left(\sum_{n\geq 0} B_n x^n\right)\left(\sum_{n\geq 0} \frac{1}{n!} x^n\right) \\ &= \sum_{n\geq 0}\left(\sum_{r=0}^{n} B_r \frac{1}{(n-r)!}\right) x^n \\ &= \sum_{n\geq 0} \frac{1}{n!}\left(\sum_{r=0}^{n} B_r \frac{n!}{(n-r)!}\right) x^n. \end{aligned} \tag{4.49}$$

This is the point at which we might expect Equation (4.48) to be helpful. And, it would be, if there were just an $r!$ in the denominator of Equation (4.49). (We were able to multiply and divide by $n!$, and then move $1/n!$ outside the parentheses, because $n!$ is independent of the index of summation r. The same approach clearly will not work for $r!$.)

Playing by the usual rules, there appears to be no way to solve the problem of the missing $r!$. So, let's change the rules. If we can't find a closed formula for $g(x) = \sum_{n\geq 0} B_n x^n$, let's instead consider

$$g(x) = \sum_{n\geq 0} \frac{B_n}{n!} x^n.$$

The effect of repeating the same steps with this new formal power series is to replace B_r in Equation (4.49) with $B_r/r!$. With the new $g(x)$, we obtain

$$\begin{aligned} g(x)e^x &= \sum_{n\geq 0} \frac{1}{n!}\left(\sum_{r=0}^{n} \frac{B_r}{r!} \frac{n!}{(n-r)!}\right) x^n \\ &= \sum_{n\geq 0} \frac{1}{n!}\left(\sum_{r=0}^{n} C(n,r) B_r\right) x^n \end{aligned}$$

$$
\begin{aligned}
&= \sum_{n\geq 0} \frac{1}{n!} B_{n+1} x^n \\
&= \sum_{n\geq 0} (n+1) \frac{B_{n+1}}{(n+1)!} x^n \\
&= D_x g(x), \qquad (4.50)
\end{aligned}
$$

the formal (term-by-term) derivative of $g(x)$.*

Assuming that the revised power series has a positive radius of convergence, we may treat $D_x g(x)$ as the ordinary derivative $g'(x)$. In this case, dividing both sides of Equation (4.50) by $g(x)$ and antidifferentiating, we obtain

$$\int \frac{g'(x)}{g(x)} dx = \int e^x \, dx.$$

It follows that $\ln(g(x)) = e^x + C$. Substituting $g(0) = 1$ gives $\ln(1) = e^0 + C$, or $0 = 1 + C$. Hence, $\ln(g(x)) = e^x - 1$. Exponentiating both sides gives

$$
\begin{aligned}
g(x) &= \exp(e^x - 1) \\
&= e^{e^x - 1}.
\end{aligned}
$$

4.4.1 Definition. The *exponential generating function* for the sequence $\{a_n\}$ is

$$g(x) = \sum_{n\geq 0} a_n x^n / n!.$$

Evidently, the exponential generating function for $\{a_n\}$ is the ordinary generating function for $\{a_n/n!\}$. If m is a fixed but arbitrary positive integer then, e.g.,

$$(1+x)^m = C(m,0) + C(m,1)x + C(m,2)x^2 + \cdots$$

is the ordinary generating function for $\{C(m,n)\}$ and, since

$$\sum_{n\geq 0} C(m,n) x^n = \sum_{n\geq 0} \frac{P(m,n)}{n!} x^n,$$

$(1+x)^m$ is the exponential generating function for $\{P(m,n)\}$.

4.4.2 Theorem. *The exponential generating function for the sequence $\{B_n\}$ of Bell numbers is $\exp(e^x - 1)$.*

*To those familiar with the use of *integrating factors* in differential equations, this may make the decision to multiply by e^x a little less mysterious.

Our derivation of Theorem 4.4.2 falls short of a proof because it relies on the assumption that $g(x) = \sum_{n\geq 0}(B_n/n!)x^n$ has a positive radius of convergence. If we knew a lot more about the Bell numbers, we might be able to prove this fact using one of the familiar *tests* from calculus. (Having $n!$ in the denominator can do no harm whenever convergence is an issue.)

Alternatively, we know from calculus that the Maclaurin series for $\exp(x)$ converges for all x. Thus, another way to prove Theorem 4.4.2 would be to show that $B_n/n!$ is the coefficient of x^n in the Maclaurin series expansion of $\exp(e^x - 1)$. This is the approach taken in Exercise 5.

Had we known to look for an *exponential* generating function from the beginning, the clever but mysterious "let's see what happens if we multiply by e^x" would have been unnecessary. Multiplying both sides of Equation (4.48) by $x^n/n!$ and summing on n yield

$$\sum_{n\geq 0}\frac{B_{n+1}}{n!}x^n = \sum_{n\geq 0}\left(\sum_{r=0}^{n}\frac{1}{(n-r)!}\frac{B_r}{r!}\right)x^n.$$

By Equations (4.19a)–(4.19b), this is equivalent to

$$\sum_{n\geq 0}(n+1)\frac{B_{n+1}}{(n+1)!}x^n = \left(\sum_{n\geq 0}\frac{1}{n!}x^n\right)\left(\sum_{n\geq 0}\frac{B_n}{n!}x^n\right),$$

i.e., to $D_x g(x) = e^x g(x)$, bringing us to Equation (4.50) by a more direct route.

Why introduce a new kind of generating function? Because it makes our work *easier*. At first blush, this might seem strange. After all, there is nothing particularly *easy* about deriving the closed formula $\exp(e^x - 1)$, nor is this formula especially simple. On the other hand, suppose your job depended on being able to find a closed formula for *some* generating function for $\{B_n\}$. If you think it would be easier to solve the ordinary generating function problem, by all means go for it!

4.4.3 Example. Of what use is the formula $\exp(e^x - 1)$? Observe that

$$\begin{aligned}
\sum_{n\geq 0}(B_n/n!)x^n &= e^{e^x-1}\\
&= e^{\sum_{r\geq 1}x^r/r!}\\
&= \prod_{r\geq 1}e^{x^r/r!}\\
&= \prod_{r\geq 1}\left(\sum_{t\geq 0}[x^r/r!]^t/t!\right)\\
&= (1 + [x^1/1!] + [x^1/1!]^2/2! + [x^1/1!]^3/3! + \cdots)\\
&\quad \times (1 + [x^2/2!] + [x^2/2!]^2/2! + [x^2/2!]^3/3! + \cdots)\\
&\quad \times (1 + [x^3/3!] + [x^3/3!]^2/2! + [x^3/3!]^3/3! + \cdots)\\
&\quad \times \cdots
\end{aligned}$$

Comparing the coefficient of x^n on either side of this equation, we obtain (after multiplying by $n!$) that

$$B_n = \sum_{1t_1+2t_2+\cdots+kt_k=n} \frac{n!}{(1!)^{t_1}t_1! \times (2!)^{t_2}t_2! \times \cdots \times (k!)^{t_k}t_k!}. \tag{4.51}$$

This is interesting for many reasons, not the least of which is that the left-hand side pertains to the number of partitions (into disjoint subsets) of $\{1,2,\ldots,n\}$. Because $1t_1+2t_2+\cdots+kt_k=n$ if and only if $[k^{t_k},\cdots,2^{t_2},1^{t_1}]\vdash n$, the right-hand side involves partitions of (the integer) n.

The partitions of 4 are

$$\begin{aligned}
[4] &\text{ corresponding to } t_1=0,\ t_2=0,\ t_3=0,\ \text{and } t_4=1;\\
[3,1] &\text{ corresponding to } t_1=1,\ t_2=0,\ t_3=1,\ \text{and } t_4=0;\\
[2^2] &\text{ corresponding to } t_1=0,\ t_2=2,\ t_3=0,\ \text{and } t_4=0;\\
[2,1^2] &\text{ corresponding to } t_1=2,\ t_2=1,\ t_3=0,\ \text{and } t_4=0;\\
[1^4] &\text{ corresponding to } t_1=4,\ t_2=0,\ t_3=0,\ \text{and } t_4=0.
\end{aligned}$$

Substituting these values into Equation (4.51), we obtain

$$\begin{aligned}
B_4 &= \left[\frac{4!}{(4!)^1 1!} + \frac{4!}{(1!)^1 1!(3!)^1 1!} + \frac{4!}{(2!)^2 2!} + \frac{4!}{(1!)^2 2!(2!)^1 1!} + \frac{4!}{(1!)^4 4!}\right]\\
&= 1+4+3+6+1 = 15.
\end{aligned}$$

□

4.4.4 Example. Without recognizing them as such, we have already seen many examples of exponential generating functions. Consider, e.g., the sequence $\{c_n\}$ defined by

$$c_n = \begin{cases} 0 & \text{if } n = 2k+1,\\ +1 & \text{if } n = 4k,\\ -1 & \text{if } n = 4k+2, \end{cases}$$

the first few terms of which are $1,0,-1,0,1,0,-1,\ldots$. The exponential generating function for $\{c_n\}$,

$$1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots = \cos(x),$$

can be found in Example 4.2.13. What about the sequence $\{d_n\}$ defined by $d_n = |c_n|$? Its exponential generating function is

$$1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \frac{x^6}{6!} + \cdots = \frac{e^x + e^{-x}}{2} = \cosh(x),$$

the *hyperbolic* cosine.

If m is fixed, the ordinary generating function for $\{m^n\}$ is $\sum_{n\geq 0} m^n x^n = \sum_{n\geq 0}(mx)^n = (1-mx)^{-1}$ and its exponential generating function is $\sum_{n\geq 0} m^n x^n/n! = \sum_{n\geq 0}(mx)^n/n! = e^{mx} = \exp(mx)$. What about $\{n^m\}$? According to Exercise 19, Section 4.2,

$$\sum_{n\geq 0} n^m x^n/n! = e^x \sum_{n=1}^{m} S(m,n)x^n. \tag{4.52}$$

By Newton's binomial theorem (with $|x| < \frac{1}{2}$,

$$(1-2x)^{-3/2} = 1/0! + 3x/1! + (3\times 5)x^2/2! + (3\times 5\times 7)x^3/3! + \cdots$$

is the exponential generating function for the sequence $\{a_n\}$, where $a_n = 1\times 3\times 5\times \ldots \times (2n+1)$ is the product of the first $n+1$ odd integers. (Confirm it!) □

If $f(x)$ and $g(x)$ are exponential generating functions for $\{a_n\}$ and $\{b_n\}$, respectively, then

$$\begin{aligned} f(x)g(x) &= \left(\sum_{n\geq 0} a_n x^n/n!\right)\left(\sum_{n\geq 0} b_n x^n/n!\right) \\ &= \sum_{n\geq 0}\left(\sum_{r=0}^{n} \frac{a_r}{r!}\frac{b_{n-r}}{(n-r)!}\right)x^n \\ &= \sum_{n\geq 0}\left(\sum_{r=0}^{n} C(n,r)a_r b_{n-r}\right)x^n/n! \end{aligned}$$

the exponential generating function for the sequence $\{c_n\}$ defined by

$$c_n = \sum_{r=0}^{n} C(n,r)a_r b_{n-r}. \tag{4.53}$$

(Compare and contrast Equations (4.19b) and (4.53).)

If $a_n = 1$ for all n, then $f(x) = e^x$ and, after a change of variable, the right-hand side of Equation (4.53) becomes

$$\sum_{r=0}^{n} C(n,n-r)b_r = \sum_{r=0}^{n} C(n,r)b_r. \tag{4.54}$$

Comparing the right-hand sides of Equations (4.48) and (4.54) should strip away any remaining mystery about the curious decision to "see that happens if we multiply by e^x."

Recall that a derangement is a permutation with no fixed points. From Equation (2.18) in Section 2.3,

$$\frac{D(n)}{n!} = \frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}.$$

Therefore, the (exponential) generating function

$$\begin{aligned} g(x) &= \sum_{n\geq 0} \frac{D(n)}{n!} x^n \\ &= \sum_{n\geq 0} \left(\sum_{r=0}^{n} \frac{(-1)^r}{r!} \right) x^n. \end{aligned}$$

It follows, from either Lemma 4.2.7 or Equations (4.19a)–(4.19b), that

$$\begin{aligned} g(x) &= \left(\sum_{n\geq 0} (-1)^n \frac{x^n}{n!} \right) \left(\sum_{n\geq 0} x^n \right) \\ &= e^{-x}(1-x)^{-1}. \end{aligned}$$

Let's summarize.

4.4.5 Theorem. *The exponential generating function for the derangement numbers is*

$$\sum_{n\geq 0} D(n)x^n/n! = \frac{1}{(1-x)e^x}. \tag{4.55}$$

Speaking of fixed points and derangements leads to cycle structure and Stirling numbers of the first kind. Let k be a fixed but arbitrary positive integer and define

$$h_k(x) = \sum_{n\geq k} s(n,k)x^n/n!, \tag{4.56}$$

the exponential generating function for $\{s(n,k)\}$.

Recalling that $s(n,1) = (n-1)!$,

$$h_1(x) = x + x^2/2 + x^3/3 + \cdots \tag{4.57}$$

The right-hand side of Equation (4.57) is the Maclaurin series expansion for $-\ln(1-x)$.

If $k > 1$, the derivative of Equation (4.56) is

$$\begin{aligned} D_x h_k(x) &= \sum_{n\geq k} \frac{s(n,k)}{(n-1)!} x^{n-1} \\ &= \sum_{n\geq k-1} \frac{s(n+1,k)}{n!} x^n \\ &= \sum_{n\geq k-1} \frac{s(n,k-1) + n s(n,k)}{n!} x^n \\ &= \sum_{n\geq k-1} \frac{s(n,k-1)}{n!} x^n + \sum_{n\geq k} n \frac{s(n,k)}{n!} x^n \\ &= h_{k-1}(x) + x \sum_{n\geq k} \frac{s(n,k)}{(n-1)!} x^{n-1} \\ &= h_{k-1}(x) + x D_x h_k(x). \end{aligned}$$

So, $(1-x)D_x h_k(x) = h_{k-1}(x)$. Assuming a positive radius of convergence for Equation (4.56),

$$h_k(x) = \int \frac{h_{k-1}(x)}{1-x} dx. \tag{4.58}$$

4.4.6 Theorem. *Let k be a fixed positive integer. Then the exponential generating function for $\{s(n,k)\}$, the sequence of Stirling numbers of the first kind, is*

$$\sum_{n\geq k} s(n,k) x^n/n! = \frac{[-\ln(1-x)]^k}{k!}.$$

Proof. The $k = 1$ case follows from Equation (4.57) and the Maclaurin series expansion of $-\ln(1-x)$. Because this expansion has a positive radius of convergence, namely $r = 1$, Theorem 4.2.9 can be applied to the $k = 2$ case of Equation (4.58) to obtain

$$\begin{aligned} h_2(x) &= \int \frac{-\ln(1-x)}{1-x} dx \\ &= \tfrac{1}{2}[-\ln(1-x)]^2 \end{aligned}$$

(where the constant of integration is $s(0,2) = 0$). Moreover, also from Theorem 4.2.9, $h_2(x)$ has radius of convergence $r = 1$. The general formula follows from Equation (4.58) using induction on k (and integration by substitution). ■

What about Stirling numbers of the second kind? Recall that, apart from some minus signs, the matrix manifestations of the two arrays of Stirling numbers are inverses of each other. Given the appearance of natural logarithms in Theorem 4.4.6, it is natural to wonder whether the inverse of the logarithm function will emerge in a discussion of

$$g_r(x) = \sum_{n\geq 0} S(n,r)x^n/n!.$$

Let's see.

By Stirling's identity (Corollary 2.2.4),

$$g_r(x) = \sum_{n\geq 0}\left(\frac{1}{r!}\sum_{t=0}^{r}(-1)^{r+t}C(r,t)t^n\right)x^n/n!,$$

so

$$\begin{aligned} r!g_r(x) &= \sum_{t=0}^{r}(-1)^{r+t}C(r,t)\sum_{n\geq 0}(tx)^n/n! \\ &= \sum_{t=0}^{r}(-1)^{r+t}C(r,t)e^{tx} \\ &= \sum_{t=0}^{r}C(r,t)(e^x)^t(-1)^{r-t} \\ &= (e^x-1)^r. \end{aligned}$$

Therefore,

$$g_r(x) = (e^x-1)^r/r!.$$

We have proved the following:

4.4.7 Theorem. *Let r be a fixed positive integer. The exponential generating function for the sequence $\{S(n,r)\}$ of Stirling numbers of the second kind is*

$$\sum_{n\geq r} S(n,r)x^n/n! = (e^x-1)^r/r!. \tag{4.59}$$

4.4.8 Example. If the truth be known, it is a rare sequence for which even one variety of generating function has a nice closed formula. When $\{a_n\}$ has closed formula generating functions of more than one kind, they tend to be very different.

Recall that the ordinary generating function for $\{m^n\}$ is $(1 - mx)^{-1}$ and its exponential generating function is $e^{mx} = \exp(mx)$. The ordinary generating function for $\{S(n, r)\}$ is

$$\sum_{n \geq r} S(n, r)x^n = x^r \prod_{t=1}^{r} (1 - tx)^{-1}$$

(Theorem 4.3.5), while its exponential generating function is $(e^x - 1)^r/r!$. □

Because the Bell numbers are sums of Stirling numbers of the second kind, Theorem 4.4.7 should yield another proof of Theorem 4.4.2. Setting $S(0, 0) = 1$ and summing both sides of Equation (4.59) on r, we obtain

$$\sum_{r \geq 0} \sum_{n \geq 0} S(n, r)x^n/n! = \sum_{r \geq 0} (e^x - 1)^r/r!.$$

So,

$$\sum_{n \geq 0} (\sum_{r \geq 0} S(n, r))x^n/n! = \exp(e^x - 1), \tag{4.60}$$

i.e.,

$$\sum_{n \geq 0} B_n x^n/n! = \exp(e^x - 1).$$

Asked to find a generating function for the Bell numbers, we found an "exponential" generating function instead. There is, of course, nothing particularly sacred about the sequence

$$1, x, x^2, x^3, \cdots$$

Not only does

$$\frac{1}{0!}, \frac{x}{1!}, \frac{x^2}{2!}, \frac{x^3}{3!}, \cdots$$

work just as well, it enhances the likelihood of convergence. It is natural to wonder if other sequences might yield interesting results. For example, what about basing a generating function on

$$1^x, 2^x, 3^x, 4^x, \cdots ?$$

4.4.9 Definition. The *Dirichlet*[*] *generating function* of $\{a_n\}$ is the formal series

$$f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}.$$

[*]After Peter Gustav Lejeune Dirichlet (1805–1859).

There are several things to note right away about this definition. First, the variable has changed from x to s. This is an inconsequential change, having more to do with tradition than mathematics. The second is that we have used, not n^s, but n^{-s}. This is a consequence of some experience; it turns out to be more useful. Finally, the summation starts with $n = 1$, which is necessary to avoid dividing by zero.

4.4.10 Example. Let $\{a_n\}$ be the trivial sequence defined by $a_n = 1$ for all n. Its Dirichlet generating function is the *Riemann zeta function*,*

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}. \tag{4.61}$$

□

The Dirichlet generating function analogue of Equations (4.19b) and (4.53) may help to suggest why they are important in number theory.

4.4.11 Theorem. *Let $f(s)$ and $g(s)$ be Dirichlet generating functions for the sequences $\{a_n\}$ and $\{b_n\}$, respectively. Then $f(s)g(s)$ is the Dirichlet generating function for $\{c_n\}$, where*

$$c_n = \sum_{km=n} a_k b_m,$$

the sum over all (ordered) factorizations $n = km$.

Proof

$$\begin{aligned} f(s)g(s) &= \left(a_1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_4}{4^s} + \cdots\right)\left(b_1 + \frac{b_2}{2^s} + \frac{b_3}{3^s} + \frac{b_4}{4^s} + \cdots\right) \\ &= (a_1b_1) + (a_1b_2 + a_2b_1)2^{-s} + (a_1b_3 + a_3b_1)3^{-s} + (a_1b_4 + a_2b_2 + a_4b_1)4^{-s} \\ &\quad + (a_1b_5 + a_5b_1)5^{-s} + (a_1b_6 + a_2b_3 + a_3b_2 + a_6b_1)6^{-s} + \cdots \end{aligned}$$

In general,

$$\frac{a_k}{k^s}\frac{b_m}{m^s} = \frac{a_k b_m}{n^s}$$

if and only if $km = n$, i.e., $a_k b_m$ is a summand in the coefficient of n^{-s} if and only if $km = n$. ■

*Named after Georg Friedrich Bernhard Riemann (1826–1866). See, e.g., G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, Oxford, 1979, for a discussion of the zeta function.

4.4.12 Definition. Read "d divides n", the notation "$d|n$" means that there exists an integer q such that $n = dq$, i.e., that d *exactly* divides n, or that n is a multiple of d.

Using this notation, the conclusion of Theorem 4.4.11 can be written as

$$c_n = \sum_{d|n} a_d b_{n/d}, \tag{4.62}$$

from which it follows, e.g., that

$$\begin{aligned}\zeta^2(s) &= \sum_{n\geq 1}\left(\sum_{d|n} 1\times 1\right) n^{-s} \\ &= \sum_{n\geq 1}\frac{d(n)}{n^s},\end{aligned}$$

the Dirichlet generating function for the sequence $\{d(n)\}$, where $d(n)$ is the number of (exact, positive-integer) divisors of n.

4.4.13 Example. If $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, where $p_1, p_2, \ldots, p_r$ are different primes, then (Example 1.1.4)

$$\begin{aligned}d(n) &= (a_1+1)(a_2+1)\cdots(a_r+1) \\ &= d(p_1^{a_1})d(p_2^{a_2})\cdots d(p_r^{a_r}).\end{aligned} \tag{4.63}$$

If m and n are relatively prime, then no prime divisor of m is a prime divisor of n, and vice versa. It follows from Equation (4.63), therefore, that $d(mn) = d(m)d(n)$. □

4.4.14 Definition. A *number-theoretic* function is one whose domain is the set of positive integers. A number-theoretic function f is *multiplicative* if $f(mn) = f(m)f(n)$ whenever m and n are relatively prime.

If n is a positive integer and $0 \neq f$ is a multiplicative number-theoretic function, then $f(n) = f(1\times n) = f(1)f(n)$, from which it follows that $f(1) = 1$.

4.4.15 Lemma. *Let f be a multiplicative number-theoretic function. If $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$, where $p_1, p_2, \ldots, p_r$ are different primes, then*

$$f(n) = f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_r^{a_r}). \tag{4.64}$$

Conversely, a (numerical valued) function f, defined arbitrarily on positive-integer powers of primes, can be extended to a multiplicative number-theoretic function by defining $f(1) = 1$ and $f(n)$ by Equation (4.64) for all composite positive n.

The proof is left to the exercises.

If f is any multiplicative number-theoretic function, then the Dirichlet generating function for the sequence defined by $a_n = f(n), n \geq 1$, can be expressed in an interesting way.

4.4.16 Theorem. *If f is a multiplicative number-theoretic function, then*

$$\sum_{n\geq 1} \frac{f(n)}{n^s} = \prod_p [1 + f(p)p^{-s} + f(p^2)p^{-2s} + f(p^3)p^{-3s} + \cdots], \tag{4.65}$$

where the product is over the (positive) prime numbers p.

Proof. Consider a generic positive integer $n = 2^a 3^b 5^c \ldots$. In the product

$$\left[1 + \frac{f(2)}{2^s} + \frac{f(2^2)}{2^{2s}} + \cdots\right]\left[1 + \frac{f(3)}{3^s} + \frac{f(3^2)}{3^{2s}} + \cdots\right]\left[1 + \frac{f(5)}{5^s} + \frac{f(5^2)}{5^{2s}} + \cdots\right]\cdots,$$

only the first set of brackets contains terms with 2's in the denominator, and only one of these denominators is 2^{as}. Thus, for a product comprised of one term from each set of brackets to have a denominator equal to n^s, the unique choice from the first set must be $f(2^a)/2^{as}$. Similarly, the unique choice from the second set of brackets must be $f(3^b)/3^{bs}$, the unique choice from the third set must be $f(5^c)/5^{cs}$, and so on. In particular, n^{-s} is produced only once on the right-hand side of Equation (4.65), and its coefficient is

$$\begin{aligned} f(2^a)f(3^b)f(5^c)\cdots &= f(2^a 3^b 5^c \cdots) \\ &= f(n) \end{aligned}$$

because f is multiplicative. ■

4.4.17 Example. Suppose $f(n) = 1$ for all n. Then, because f is a multiplicative number-theoretic function, we can use Theorem 4.4.16 to obtain an identity for its Dirichlet generating function $\zeta(s)$. Evidently, the Riemann zeta function

$$\begin{aligned} \zeta(s) &= \prod_p \left(1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots\right) \\ &= \prod_p \frac{1}{1 - p^{-s}}. \end{aligned}$$

□

4.4.18 Example. The multiplicative number-theoretic *Möbius function*[*] μ is defined by

$$\mu(p^a) = \begin{cases} +1 & \text{if} \quad a = 0, \\ -1 & \text{if} \quad a = 1, \\ 0 & \text{if} \quad a \geq 2 \end{cases}$$

[*]Named for August Ferdinand Möbius (1790–1868).

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1	−1	0

Figure 4.4.1. The Möbius function.

when $n = p^a$ is a power of a prime and (using Lemma 4.4.15) by

$$\mu(n) = \mu(p_1^{a_1})\mu(p_2^{a_2}) \cdots \mu(p_r^{a_r})$$

when $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ is composite. So, $\mu(1) = 1, \mu(n) = (-1)^k$ if the prime factorization of n consists of k distinct primes, and $\mu(n) = 0$ whenever n is (exactly) divisible by the square of a prime. The first few values of μ are listed in Fig. 4.4.1.

Denote by $M(s)$ the Dirichlet generating function for the Möbius sequence, defined by $a_n = \mu(n), n \geq 1$. Then, by Theorem 4.4.16 and Example 4.4.17,

$$M(s) = \sum_{n \geq 1} \frac{\mu(n)}{n^s} = \prod_p (1 - p^{-s}) = \frac{1}{\zeta(s)}. \tag{4.66}$$

□

4.4.19 Corollary. *If sequences* $\{a_n\}$ *and* $\{b_n\}$ *satisfy*

$$a_n = \sum_{d|n} b_d, \qquad n \geq 1, \tag{4.67}$$

then

$$b_n = \sum_{d|n} \mu(n/d) a_d. \tag{4.68}$$

Proof. Let $A(s)$ and $B(s)$ be the Dirichlet generating functions for $\{a_n\}$ and $\{b_n\}$, respectively. Then, by Equations (4.62) and (4.67), $A(s) = B(s)\zeta(s)$. So, by Equation (4.66), $A(s)M(s) = B(s)$. Equation (4.68) now follows from another application of Equation (4.62). ■

The transformation from Equation (4.67) to Equation (4.68) is commonly referred to as *Möbius inversion*.

4.4.20 Example. Let $s(n) = \sum_{d|n} d$, the sum of the divisors of n. (Then, e.g., n is *perfect* if and only if $s(n) = 2n$.) It follows from Möbius inversion that

$$n = \sum_{d|n} \mu(n/d) s(d). \tag{4.69}$$

Let's confirm Equation (4.69), e.g., for $n = 6$ (the first perfect number):

$$\begin{aligned}\sum_{d|6} \mu(6/d)s(d) &= \mu(6)s(1) + \mu(3)s(2) + \mu(2)s(3) + \mu(1)s(6)\\ &= s(1) - s(2) - s(3) + s(6)\\ &= 1 - (1+2) - (1+3) + (1+2+3+6)\\ &= 6.\end{aligned}$$

What about another example, maybe $n = 8$. (Because $s(8) = 1 + 2 + 4 + 8 = 15 < 2 \times 8$, 8 is *deficient*.) Observe that

$$\begin{aligned}\sum_{d|8} \mu(8/d)s(d) &= \mu(8)s(1) + \mu(4)s(2) + \mu(2)s(4) + \mu(1)s(8)\\ &= 0 \times s(1) + 0 \times s(2) - s(4) + s(8)\\ &= -(1+2+4) + (1+2+4+8)\\ &= 8.\end{aligned}$$

□

4.4. EXERCISES

1 Let $g(x)$ be the exponential generating function for the sequence $\{a_n\}$. Find a closed formula for a_n if

(a) $g(x) = xe^{2x}$. **(b)** $g(x) = e^x + e^{3x}$.

(c) $g(x) = e^x(x + x^2)$. **(d)** $g(x) = e^x(x + 3x^2 + x^3)$.

2 Find a closed formula for the exponential generating function of the sequence

(a) $\{n\}$.

(b) $\{n^4\}$.

(c) $0, 1, 0, -1, 0, 1, 0, -1, \ldots$

(d) $0, 1, 0, 1, 0, 1, 0, 1, \ldots$

3 The purpose of this exercise is to outline another approach to the proof of Theorem 4.4.7. Let r be a fixed but arbitrary positive integer, and let $g_r(x) = \sum_{n \geq r} S(n, r)x^n/n!$ be the exponential generating function for $\{S(n, r)\}$.

(a) Show that $g_1(x) = e^x - 1$.

(b) Show that the derivative $D_x q_r(x) = rg_r(x) + g_{r-1}(x),\ r > 1$.

(c) Define $f_r(x) = (e^x - 1)^r/r!$ and show that $f_1(x) = e^x - 1$.

(d) Show that $D_x f_r(x) = rf_r(x) + f_{r-1}(x),\ r > 1$.

(e) Show that $g_r(0) = f_r(0)$.

(f) Prove Theorem 4.4.7.

(g) Confirm directly that $S(n,r) = f_r^{(n)}(0)$, the nth derivative of $f_r(x)$ evaluated at $x = 0$.

4 Use Equation (4.51) to confirm that

(a) $B_3 = 5$.

(b) $B_5 = 52$.

5 Let $f(x) = \exp(e^x - 1)$. Show that

(a) $f'(x) = \exp(e^x + x - 1)$.

(b) $f''(x) = \exp(e^x + 2x - 1) + \exp(e^x + x - 1)$.

(c) $f'''(x) = \exp(e^x + 3x - 1) + 3\exp(e^x + 2x - 1) + \exp(e^x + x - 1)$.

(d) $f^{[4]}(x) = \sum_{r=1}^{4} S(4,r)\exp(e^x + rx - 1)$.

(e) $f^{[n]}(x) = \sum_{r=1}^{n} S(n,r)\exp(e^x + rx - 1)$.

(f) $f^{[n]}(0) = B_n$.

(g) $f(x) = \sum_{n\geq 0} B_n x^n/n!$.

6 Recall that the Maclaurin series expansion of $\ln(1-x)$ is

$$-x - \tfrac{1}{2}x^2 - \tfrac{1}{3}x^3 - \tfrac{1}{4}x^4 - \cdots$$

(a) Find a closed formula for the exponential generating function of the sequence defined by $a_n = (n-1)!, n \geq 1$.

(b) Find a closed formula for the exponential generating function of the sequence defined by $a_n = (-1)^n(n-1)!,\ n \geq 1$.

(c) Show that

$$x = (e^x - 1) - \tfrac{1}{2}(e^x - 1)^2 + \tfrac{1}{3}(e^x - 1)^3 - \tfrac{1}{4}(e^x - 1)^4 + \cdots$$

7 Use Exercise 6(c) to prove that

$$0!S(n,1) - 1!S(n,2) + 2!S(n,3) - 3!S(n,4) + \cdots + (-1)^{n-1}(n-1)!S(n,n) = 0$$

for all $n \geq 2$.

8 If $f(x) = (1-x)^{-1}e^{-x}$ then, by Theorem 4.4.5 and the general theory of Maclaurin series, $f^{[n]}(0) = D(n), n \geq 0$. Compute $f^{[n]}(x)$ and confirm that $f^{[n]}(0) = D(n), 0 \leq n \leq 4$.

9 Let $h_2(x)$ be the exponential generating function for $\{s(n,2)\}$.

(a) Show that $D_x h_2(x) = \dfrac{-\ln(1-x)}{1-x}$.

(b) Show that $D_x h_2(x) = \sum_{n\geq 0} s(n+1,2)x^n/n!$.

(c) Use parts (a) and (b) to obtain a new derivation of the closed formula for the (ordinary) generating function of the harmonic numbers given in Example 4.2.8.

10 Give the (exponential) generating function proof that

$$\sum_{r=0}^{n}(-1)^r C(n,r) = 0,\ n \geq 1. \quad (\textit{Hint}: e^x \times e^{-x} = 1.)$$

11 Give the generating function proof that

(a) $\sum_{r=0}^{n}(-1)^r C(m+r-1,r)C(m,n-r) = 0, n \geq 1.$

(b) $\sum_{k=r}^{n} C(k,r) = C(n+1,r+1).$

(c) $D(n) = nD(n-1) + (-1)^n.$

12 Explain why $(x+1)^m(x+1)^n = (x+1)^{m+n}$ is the generating function proof of Vandermonde's identity (Exercise 15, Section 1.5).

13 Perhaps the most curious thing to occur in this section was the invitation to "see what happens if we multiply by e^x." If $g(x)$ is the exponential generating function for the sequence of derangement numbers $\{D(n)\}$ (with $D(0) = 1$), "see what happens" if you multiply by e^x.

14 Show that the derangement numbers satisfy

$$n\frac{D(n)}{n!} = (n-1)\frac{D(n-1)}{(n-1)!} + \frac{D(n-2)}{(n-2)!}.$$

(*Hint*: Exercise 13, Section 2.3.)

15 Let $g(x) = 1 + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \frac{3}{8}x^4 + \frac{11}{30}x^5 + \cdots$ be the exponential generating function for the derangement numbers. Use Exercise 14 to prove that $(1-x)g'(x) = xg(x)$.

16 Use Exercise 15 as the basis for another proof of Theorem 4.4.5.

17 Find a closed formula for the two-variable generating function

$$f(x,y) = \sum_{m\geq 0}\sum_{n\geq 0} C(m,n)x^m y^n.$$

18 Let $g(x) = \sum_{n\geq 0} a_n x^n$ be the ordinary generating function for the sequence $\{a_n\}$.

(a) Show that the "discrete derivative", $\Delta g(x) = g(x+1) - g(x)$, is the ordinary generating function for the sequence $\{b_n\}$ defined by

$$b_n = \sum_{m>n} a_m C(m,n), \qquad n \geq 0.$$

(b) Show that the ordinary generating function for the difference sequence $\{\Delta a_n\}$ is $[(1-x)g(x) - a_0]/x$.

19 Tabulate the values of $\mu(n), 13 \leq n \leq 27$.

20 Prove that the Euler totient function (Definition 2.3.9) is a multiplicative number-theoretic function (*Hint*: Theorem 2.3.11.)

21 This exercise involves the Euler totient function from Definition 2.3.9.

(a) Prove that $n = \sum_{d|n} \varphi(d)$.

(b) Confirm the formula in part (a) when $n = 6$.

(c) Confirm the formula in part (a) when $n = 10$.

(d) Prove that $\varphi(n) = n \sum_{d|n} \mu(d)/d$.

(e) Confirm the formula in part (d) when $n = 6$.

(f) Confirm the formula in part (d) when $n = 10$.

22 Prove that $n/\varphi(n) = \sum_{d|n} \mu(d)^2/\varphi(d)$, where φ is the Euler totient function from Definition 2.3.9.

23 If n is a positive integer, prove that $\sum_{d|n} \mu(d) = \delta_{n,1}$.

24 Let $f(n) = 1$ if n is "square free" (not divisible by the square of any prime) and zero otherwise. Prove that f is a multiplicative number-theoretic function.

25 Prove that $\sum_{k|n} \mu(n/k)d(k) = 1$, $n \geq 1$, where $d(k)$ is the number of divisors of k.

26 If f is a multiplicative number-theoretic function, show that the number-theoretic function g defined by $g(n) = \sum_{d|n} f(d)$, $n \geq 1$, is multiplicative.

27 Let $a_1, a_2, \ldots, a_m$ be fixed but arbitrary real numbers. Let $M_n = a_1^n + a_2^n + \cdots + a_m^n$ be their nth-power sum.

(a) Let $E_0 = 1$ and $E_n = E_n(a_1, a_2, \ldots, a_m)$, $n \geq 1$, be the nth elementary symmetric function of the a's. Prove that $e(x)$, the ordinary generating function for $\{E_n\}$, satisfies the identity $e(x) = \exp\left[\sum_{n\geq 1}(-1)^{n+1}(M_n/n)x^n\right]$.

(b) Let $H_0 = 1$ and $H_n = H_n(a_1, a_2, \ldots, a_m)$, $n \geq 1$, be the nth homogeneous symmetric function of the a's, i.e.,

$$H_n = \sum M_\alpha(a_1, a_2, \ldots, a_m),$$

the sum, over all partitions α of n having at most m parts, of the minimal symmetric polynomial M_α. Prove that $h(x)$, the ordinary generating function for $\{H_n\}$, satisfies the identity $h(x) = \exp\left[\sum_{n\geq 1}(M_n/n)x^n\right]$.

28 Prove Lemma 4.4.15.

29 Starting with $b_0 = 1$, the *Bernoulli numbers* satisfy the implicit recurrence $\sum_{r=0}^{n} C(n+1, r)b_r = 0$, $n \geq 1$. Show that the exponential generating function for the Bernoulli numbers has the closed formula $g(x) = x/(e^x - 1)$.

30 Say that the permutation $p \in S_n$ *fluctuates* if the integers in the sequence $p = (p(1), p(2), \ldots, p(n))$ alternately rise and fall, i.e., if $p(2k-1) < p(2k)$, $1 \le k \le \lfloor n/2 \rfloor$, and $p(2k+1) > p(2k)$, $1 \le k \le \lfloor (n-1)/2 \rfloor$. In sequence notation, the five "fluctuating" permutations in S_4 are $(1,3,2,4)$, $(1,4,2,3)$, $(2,3,1,4)$, $(2,4,1,3)$, and $(3,4,1,2)$. Denote the number of fluctuating permutations in S_n by ξ_n. Setting $\xi_0 = 1$, the first few terms of the sequence $\{\xi_n\}$ of *Euler numbers* are

$$1, 1, 1, 2, 5, 16, 61, \ldots$$

(a) List the 16 fluctuating permutations in S_5.

(b) The Euler numbers obey the recurrence $\xi_0 = \xi_1 = 1$ and

$$2\xi_{n+1} = \sum_{r=0}^{n} C(n,r)\xi_r \xi_{n-r}, \qquad n \ge 1.$$

Use this relation (along with $\xi_0, \ldots, \xi_6$ given above) to show that $\xi_7 = 272$.

(c) Show that the exponential generating function for $\{\xi_n\}$ has the closed formula $\sec(x) + \tan(x)$. (*Hint*: Use part (b) with the Maclaurin series expansions of secant and tangent.)

31 (L. Lovász) Let $s_0 = 1$ and $s_n = \sum_{r=1}^{n} r!S(n,r)$, $n \ge 1$.

(a) Show that s_n, $n \ge 1$, is the number of functions

$$f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

that are onto $\{1, 2, \ldots, r\}$ for some $r \in \{1, 2, \ldots, n\}$.

(b) Show that $s_n = \sum_{r \ge 1} C(n,r)s_{n-r}$, $n \ge 1$.

(c) Letting $g(x) = \sum_{n \ge 0} s_n x^n/n!$ be the exponential generating function for $\{s_n\}$, show that $g(x) = (2 - e^x)^{-1}$.

(d) Show that $(2 - e^x)^{-1} = \frac{1}{2}\sum_{k \ge 0}(e^x/2)^k$.

(e) Show that $(2 - e^x)^{-1} = \sum_{n \ge 0}\sum_{k \ge 0}(k^n/2^{k+1})x^n/n!$.

(f) Show that $\sum_{n=1}^{m} n!S(m,n) = \sum_{r \ge 1} r^m/2^{r+1}$.

(g) Show that $\sum_{n=1}^{3} n!S(3,n) = 13$.

(h) Write a computer program based on the following algorithm and use it to approximate the right-hand side of the equation in part (f) when $m = 3$:

```
1. M = 3.
2. K = 100.
3. S = 0.
4. For R = 1 to K
5. S = S + R^M/2^(r+1).
6. Next R.
7. Return S.
```

32 Let $W(n)$ be the number of n-letter "words" that can be made from the alphabet $A = \{r, s, t\}$ subject to the conditions that letter r can be repeated at most three times, s at most twice, and t at most once.

(a) Show that $W(5) = 60$.

(b) Show that the exponential generating function for $\{W(n)\}$ is $(1 + x/1! + x^2/2! + x^3/3!)(1 + x/1! + x^2/2!)(1 + x/1!)$.

(c) Compare and contrast with Exercise 40, Section 4.3.

33 Let $c(n)$ be the number of n-letter words that can be made from the alphabet $\{N, D, Q\}$ subject to the conditions that N can occur at most 10 times, D at most 5 times, and Q at most twice. Find a closed formula for the exponential generating function for $\{c(n)\}$.

4.5. RECURSIVE TECHNIQUES

> Fibonacci numbers and the golden ratio are ubiquitous in nature. The number $(1 + \sqrt{5})/2$ seems an unlikely candidate for what is arguably the most important ratio in the natural world, yet it possesses a subtle power that drives the arrangements of leaves, seeds, and spirals in many plants from vastly different origins.
>
> — Michael Naylor (*Mathematics Magazine*)

Encountered frequently in the exercises,* the *Fibonacci numbers* are defined by $F_0 = 1$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$. The first few terms of the Fibonacci sequence are

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

It was the French number theorist Edouard Lucas who suggested naming these numbers after Leonardo of Pisa, also known as Fibonacci. Indeed, the sequence

$$1, 3, 4, 7, 11, 18, 29, 47, 76, 123, \ldots$$

defined by $L_0 = 1$, $L_1 = 3$, and $L_n = L_{n-1} + L_{n-2}$, $n \geq 2$, has come to be known as the *Lucas sequence*.

The descriptions of these sequences have two elements. One consists of *initial conditions* that explicitly prescribe the first few terms. The second is a *recurrence* by means of which the remaining terms are determined inductively. Roughly speaking, a recurrence for $\{a_n\}$ is a formula for a_n as a function of previous terms. The Fibonacci and Lucas sequenes, e.g., obey the recurrence $a_n = a_{n-1} + a_{n-2}$, $n \geq 2$.

*Starting as early as Section 1.2.

4.5.1 Example The first few terms of the sequence $\{a_n\}$ defined by initial conditions $a_0 = 0$, $a_1 = 1$, and recurrence $a_n = a_{n-1} - a_{n-2}$, $n \geq 2$, are

$$0, 1, 1, 0, -1, -1, 0, 1, 1, \ldots$$

If $\{b_n\}$ is the sequence defined by the same recurrence, $b_n = b_{n-1} - b_{n-2}$, $n \geq 2$, and the *boundary conditions* $b_1 = 1$ and $b_3 = 2$, then

$$\begin{aligned} b_2 &= b_1 - b_0 \\ &= 1 - b_0 \end{aligned}$$

and

$$\begin{aligned} 2 &= b_3 \\ &= b_2 - b_1 \\ &= (1 - b_0) - 1 \\ &= -b_0. \end{aligned}$$

So, $b_0 = -2$, $b_2 = 3$, and the first few terms of $\{b_n\}$ are

$$-2, 1, 3, 2, -1, -3, -2, 1, 3, \ldots$$

What about defining $\{b_n\}$ using the same recurrence, but with boundary conditions $b_0 = 0$ and $b_3 = 1$? In this case, $b_2 = b_1 - b_0 = b_1$ and $b_3 = b_2 - b_1 = 0 \neq 1$. In other words, there is no such sequence! □

Initial conditions are special kinds of boundary conditions that specify the first few *consecutive* terms of a sequence. For the remainder of this section, we will focus exclusively on sequences prescribed by initial conditions and a recurrence.

Recall, from Equation (4.21) in Section 4.2, that a *homogeneous linear recurrence with constant coefficients* is a relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}, \qquad n \geq k, \tag{4.70}$$

where k is a fixed positive integer and $c_1, c_2, \ldots, c_k$ are constants.

4.5.2 Example. As we saw in Theorem 2.2.7, the Bell numbers satisfy the recurrence $B_0 = 1$ and

$$B_n = \sum_{r=0}^{n-1} C(n-1, r) B_r, \qquad n \geq 1.$$

While it is homogeneous, this recurrence fails to be linear because the number of summands on the right-hand side is not constant. Moreover, because it depends on n, binomial coefficient $C(n-1,r)$ is not constant in the sense of Equation (4.70). □

4.5.3 Theorem. *If $\{a_n\}$ satisfies the homogeneous linear recurrence $a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$, $n \geq k$, with constant coefficients, then the (ordinary) generating function*

$$f(x) = \sum_{n\geq 0} a_n x^n$$

has the closed formula $f(x) = h(x)/q(x)$, where

$$q(x) = 1 - c_1x - c_2x^2 - \cdots - c_kx^k$$

and $h(x)$ is a polynomial of degree at most $k-1$.

Proof. It follows from the recurrence that, for all $n \geq k$, the coefficient of x^n in

$$q(x)f(x) = f(x) - c_1xf(x) - c_2x^2f(x) - \cdots - c_kx^kf(x)$$

is $a_n - c_1a_{n-1} - c_2a_{n-2} - \cdots - c_ka_{n-k} = 0$. ■

In Section 4.2, partial fractions were used to convert

$$f(x) = \frac{h(x)}{1 - c_1x - c_2x^2 - \cdots - c_kx^k} \tag{4.71}$$

into a form from which a solution (closed formula) for a_n could easily be determined. That technique depended upon being able to factor $q(x) = 1 - c_1x - c_2x^2 - \cdots - c_kx^k$.

4.5.4 Example. Consider the sequence

$$1, 6, 24, 84, 276, \ldots$$

defined by $a_0 = 1$, $a_1 = 6$, and $a_n = 5a_{n-1} - 6a_{n-2}$, $n \geq 2$. Then $q(x) = 1 - 5x + 6x^2$, and it follows from Theorem 4.5.3 that the generating function for the sequence has the closed formula

$$\begin{aligned} f(x) &= \frac{h(x)}{1 - 5x + 6x^2} \\ &= \frac{h(x)}{(1-2x)(1-3x)}. \end{aligned}$$

Because $h(x)$ is a polynomial of degree at most 1, there exist constants s and t such that

$$\begin{aligned} f(x) &= \frac{s}{1-2x} + \frac{t}{1-3x} \\ &= s(1 + 2x + 2^2x^2 + 2^3x^3 + \cdots) + t(1 + 3x + 3^2x^2 + 3^3x^3 + \cdots), \end{aligned}$$

so

$$a_n = s(2^n) + t(3^n), \qquad n \geq 0. \tag{4.72}$$

So far, the initial conditions have not been used, i.e., *any* sequence that satisfies the recurrence $a_n = 5a_{n-1} - 6a_{n-2}$, $n \geq 2$, is solved by Equation (4.72). Let's call it a *general solution* of the recurrence.

Using the initial conditions $a_0 = 1$ and $a_1 = 6$, we see that s and t in Equation (4.72) satisfy the simultaneous equations $1 = s + t$ and $6 = 2s + 3t$, from which it follows that $s = -3$ and $t = 4$. Hence, the solution to this *particular* sequence is

$$a_n = -3(2^n) + 4(3^n), \qquad n \geq 0. \tag{4.73}$$

(Confirm that Equation (4.73) produces the correct fifth number of the sequence, namely, $a_4 = 276$.) □

The numbers 2 and 3 in Equation (4.72) came from the factorization $q(x) = 1 - 5x + 6x^2 = (1 - 2x)(1 - 3x)$. They are the *reciprocals* of the roots of $q(x)$. From a purely mechanical perspective, it seems more natural to work, not with $q(x)$, but with the polynomial $u(x) = x^2q(1/x) = x^2 - 5x + 6 = (x - 2)(x - 3)$, whose roots are 2 and 3.

4.5.5 Definition. The *characteristic polynomial* afforded by the homogeneous linear recurrence $a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$, $n \geq k$, is $u(x) = x^k - c_1x^{k-1} - c_2x^{k-2} - \cdots - c_{k-1}x - c_k$.

Beyond the "mechanical perspective", there is a better reason to introduce the characteristic polynomial. As the method of partial fractions shows, homogeneous linear recurrences of the form $a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k}$ are solved by linear combinations of exponentials. (See, e.g., the general solution in Equation (4.72).) But, in order for $a_n = r^n$ to solve the recurrence, it is necessary that

$$r^n = c_1r^{n-1} + c_2r^{n-2} + \cdots + c_kr^{n-k}.$$

Upon dividing by r^{n-k} and rearranging terms, this identity becomes

$$r^k - c_1r^{k-1} - c_2r^{k-2} - \cdots - c_k = 0,$$

i.e., for $a_n = r^n$ to solve the recurrence, r must be a root of $u(x)$.

4.5.6 Theorem. *Let $\{a_n\}$ be a sequence determined by the initial values $a_0, a_1, \ldots, a_{k-1}$ and the homogeneous linear recurrence $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$, $n \geq k$. If the distinct roots $r_1, r_2, \ldots, r_s$ of the corresponding characteristic polynomial $u(x)$ have multiplicities $m_1, m_2, \ldots, m_s$, respectively, then there exists a polynomial p_i of degree at most $m_i - 1$, $1 \leq i \leq s$, such that*

$$a_n = p_1(n) r_1^n + p_2(n) r_2^n + \cdots + p_s(n) r_s^n, \qquad n \geq 0. \tag{4.74}$$

Proof. From Theorem 4.5.3 and Definition 4.5.5, the generating function for $\{a_n\}$ is

$$f(x) = \frac{h(x)}{(1 - r_1 x)^{m_1} (1 - r_2 x)^{m_2} \cdots (1 - r_s x)^{m_s}},$$

where the degree of $h(x)$ is less than $m_1 + m_2 + \cdots + m_s = k$. It follows from the theory of partial fractions that $f(x)$ can be written as a sum of expressions, each of the form

$$\frac{b_1}{1 - rx} + \frac{b_2}{(1 - rx)^2} + \cdots + \frac{b_m}{(1 - rx)^m}, \tag{4.75}$$

where $r = r_i$ and $m = m_i$, $1 \leq i \leq s$. By the binomial theorem for negative exponents (see, e.g., Equation (4.29)),

$$(1 - rx)^{-t} = \sum_{n \geq 0} C(n + t - 1, n) r^n x^n. \tag{4.76}$$

Because $C(n + t - 1, n) = C(n + t - 1, t - 1)$, it follows from Equation (4.76) that the coefficient of x^n in Equation (4.75) is

$$[b_1 C(n + 1 - 1, 0) + b_2 C(n + 2 - 1, 1) + \cdots + b_m C(n + m - 1, m - 1)] r^n.$$

It remains to observe that

$$p(n) = b_1 C(n + 1 - 1, 0) + b_2 C(n + 2 - 1, 1) + \cdots + b_m C(n + m - 1, m - 1)$$

is a polynomial in n of degree (at most) $m - 1$. ■

4.5.7 Corollary. *Let $\{a_n\}$ be a sequence determined by the initial values $a_0, a_1, \ldots, a_{k-1}$ and the homogeneous linear recurrence $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$, $n \geq k$. If the roots $r_1, r_2, \ldots, r_k$ of the corresponding characteristic polynomial all have multiplicity 1, then there exist constants p_i, $1 \leq i \leq k$, such that*

$$a_n = p_1 r_1^n + p_2 r_2^n + \cdots + p_k r_k^n, \qquad n \geq 0.$$

Proof. A polynomial of degree 0 is a constant. ■

4.5.8 Example. Suppose $a_0 = 3$, $a_1 = 2$, $a_2 = 4$, and $a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3}$, $n \geq 3$. Then the first few terms of $\{a_n\}$ (check them) are

$$3, 2, 4, 4, 8, 12, 24, 44, \ldots$$

From the characteristic polynomial $u(x) = x^3 - 2x^2 - x + 2 = (x+1)(x-1)(x-2)$, we obtain the general solution $a_n = p_1(-1)^n + p_2 1^n + p_3 2^n$. Together with the initial conditions $a_0 = 3$, $a_1 = 2$, and $a_2 = 4$, this leads to the system of equations

$$\begin{aligned} 3 &= p_1 + p_2 + p_3 \\ 2 &= -p_1 + p_2 + 2p_3 \\ 4 &= p_1 + p_2 + 4p_3, \end{aligned}$$

the solution to which is $p_1 = \frac{2}{3}$, $p_2 = 2$, and $p_3 = \frac{1}{3}$. Thus,

$$\begin{aligned} a_n &= \tfrac{2}{3}(-1)^n + 2 + \tfrac{1}{3}2^n \\ &= 2 + \tfrac{2}{3}[2^{n-1} + (-1)^n]. \end{aligned}$$

(Confirm that this formula yields $a_7 = 44$.) □

4.5.9 Example. Consider the sequence $\{a_n\}$ defined by $a_0 = 11$, $a_1 = 6$, $a_2 = 18$, $a_3 = 104$, $a_4 = 346$, and

$$a_n = 6a_{n-1} - 13a_{n-2} + 14a_{n-3} - 12a_{n-4} + 8a_{n-5}, \qquad n \geq 5. \tag{4.77}$$

This time the characteristic polynomial is

$$\begin{aligned} u(x) &= x^5 - 6x^4 + 13x^3 - 14x^2 + 12x - 8 \\ &= (x-2)^3(x-i)(x+i). \end{aligned} \tag{4.78}$$

(While it may not be easy to obtain the factorization in Equation (4.78), how hard can it be to check and see that it is correct?) It follows from Equation (4.78) and Theorem 4.5.6 that

$$a_n = p(n)2^n + ci^n + d(-i)^n, \tag{4.79}$$

where $p(n) = rn^2 + sn + t$ is a polynomial of degree at most 2. From the initial conditions (successively substitute $n = 0, 1, 2, 3$, and 4 into Equation (4.79)), we obtain

the following system of five equations in five unknowns:

$$\begin{aligned}
11 &= & & & t &+ c + d \\
6 &= & 2r + & 2s + & 2t &+ ic - id \\
18 &= & 16r + & 8s + & 4t &- c - d \\
104 &= & 72r + & 24s + & 8t &- ic + id \\
346 &= & 256r + & 64s + & 16t &+ c + d,
\end{aligned}$$

the solution to which is $r = s = t = 1$ and $c = d = 5$. (Is it easier to solve the system on your own or to confirm that this solution is correct?) Thus,

$$a_n = (n^2 + n + 1)2^n + 5i^n + 5(-i)^n. \tag{4.80}$$

(Before going on, check to see that Equations (4.77) and (4.80) yield the same value for a_5, namely, 992.)

On reflection, we worked harder than necessary to obtain Equation (4.80). From the initial conditions and recurrence, it is clear (for this sequence at least) that a_n is real, for all $n \geq 0$. Thus, the fact that c and d are equal (but not that their common value is 5) should have been obvious from Equation (4.79). Instead of solving five equations in five unknowns, the problem could have been reduced to solving four equations in four unknowns. □

A *linear recurrence with constant coefficients* is a relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + w(n), \qquad n \geq k, \tag{4.81}$$

where k is a fixed positive integer, $c_1, c_2, \ldots, c_k$ are constants, and $w(n)$ is some function of n. Thus, a linear recurrence is *homogeneous* if and only if $w(n) = 0$.

4.5.10 Example. Consider a recurrence of the form $a_n = a_{n-1} + w(n)$, $n \geq 1$, where $w(n)$ is a polynomial of degree r in n. Then $w(n)$ is the nth number in the difference sequence $\Delta a_n = a_{n+1} - a_n$. By Theorems 4.1.8 and 4.1.10, there is a polynomial $p(x)$, of degree at most $r+1$, such that $a_n = p(n)$ for all $n \geq 0$.

To take a specific example, suppose $a_0 = 3$ and $a_n = a_{n-1} + 2n^2 - n + 1$, $n \geq 1$. Then the difference array for $\{a_n\}$ is

3, 5, 12, 28, 57, 103 …
2, 7, 16, 29, 46, …
5, 9, 13, 17, …
4, 4, 4, …

So, again from Theorem 4.1.10,

$$\begin{aligned} a_n &= 3C(n,0) + 2C(n,1) + 5C(n,2) + 4C(n,3) \\ &= 3 + 2n + \tfrac{5}{2}(n^2 - n) + \tfrac{2}{3}(n^3 - 3n^2 + 2n) \\ &= \tfrac{2}{3}n^3 + \tfrac{1}{2}n^2 + \tfrac{5}{6}n + 3. \end{aligned} \tag{4.82}$$

(Before going on, check to see that Equation (4.82) produces the correct results for $n = 1, 2$, and 3.) □

For more complicated linear recurrences, we turn to the so-called *method of undetermined coefficients*, a fancy name for *guess and check*.

4.5.11 Example. Consider the sequence

$$5, 1, 34, 39, 226, 415, \ldots \tag{4.83}$$

defined by $a_0 = 5$, $a_1 = 1$, and $a_n = a_{n-1} + 6a_{n-2} - 6n^2 + 26n - 25$, $n \geq 2$. If it were not for the term $6a_{n-2}$, we could use the method of Example 4.5.10, expecting the solution to be a polynomial of degree 3 in n. If $w(n) = -6n^2 + 26n - 25$ were zero, the characteristic polynomial $x^2 - x - 6 = (x-3)(x+2)$ would lead us to expect a solution of the form $s3^n + t(-2)^n$. The idea behind the method of undetermined coefficients is to look for a solution of the form

$$a_n = s3^n + t(-2)^n + an^3 + bn^2 + cn + d. \tag{4.84}$$

This leads to the system of equations

$$\begin{array}{rcrcrcrcrcr} 5 & = & a_0 & = & s & + & t & & & & + d \\ 1 & = & a_1 & = & 3s & - & 2t & + & a & + & b & + & c & + & d \\ 34 & = & a_2 & = & 9s & + & 4t & + & 8a & + & 4b & + & 2c & + & d \\ 39 & = & a_3 & = & 27s & - & 8t & + & 27a & + & 9b & + & 3c & + & d \\ 226 & = & a_4 & = & 81s & + & 16t & + & 64a & + & 16b & + & 4c & + & d \\ 415 & = & a_5 & = & 243s & - & 32t & + & 125a & + & 25b & + & 5c & + & d \end{array}$$

whose solution is $s = 2$, $t = 3$, $b = 1$, and $a = c = d = 0$. So far, so good. We have shown that *if* the solution to Sequence (4.83) has the form given in Equation (4.84), then

$$a_n = 2(3)^n + 3(-2)^n + n^2, \qquad n \geq 0. \tag{4.85}$$

We know that the sequence defined by Equation (4.85) satisfies the initial conditions $a_0 = 5$ and $a_1 = 1$. (These initial conditions gave us the first two of our six

equations.) If we can show that it also satisfies the recurrence $a_n = a_{n-1} + 6a_{n-2} - 6n^2 + 26n - 25$, $n \geq 2$, we will be finished. Let's check it out.

From Equation (4.85),

$$\begin{aligned} a_{n-1} &= 6(3)^{n-2} - 6(-2)^{n-2} + n^2 - 2n + 1, && n \geq 1, \\ 6a_{n-2} &= 12(3)^{n-2} + 18(-2)^{n-2} + 6n^2 - 24n + 24, && n \geq 2. \end{aligned}$$

Adding the sum of these two equations to $-6n^2 + 26n - 25$ gives

$$\begin{aligned} 18(3)^{n-2} + 12(-2)^{n-2} + n^2 &= 2(3)^n + 3(-2)^n + n^2 \\ &= a_n. \end{aligned}$$

Therefore, Equation (4.85) solves Sequence (4.83). □

4.5.12 Example. Consider the sequence defined by $a_0 = 9$, $a_1 = 17$, $a_2 = 24$, and

$$a_n = 4a_{n-1} - 5a_{n-2} + 2a_{n-3} + 6n - 20, \qquad n \geq 3. \tag{4.86}$$

The characteristic polynomial of the homogeneous part is

$$x^3 - 4x^2 + 5x - 2 = (x-1)^2(x-2), \tag{4.87}$$

which suggests guessing a solution of the form

$$a_n = r2^n + (sn + t)1^n + an^2 + bn + c.$$

Because $1^n = 1$, $n \geq 0$, we may as well combine $sn + t$ with $bn + c$ and guess a solution of the form

$$a_n = r2^n + an^2 + bn + c. \tag{4.88}$$

After using the initial conditions and Equation (4.86) to compute $a_3 = 27$, we are led to the following system of four equations in four unknowns:

$$\begin{array}{rrrrrrr} r & & & + & c & = & 9 \\ 2r & + & a & + & b & + & c & = & 17 \\ 4r & + & 4a & + & 2b & + & c & = & 24 \\ 8r & + & 9a & + & 3b & + & c & = & 27, \end{array}$$

the solution to which is $r = -3$, $a = 1$, $b = 10$, and $c = 12$. (Check it.) So, if the sequence has a solution of the form given in Equation (4.88), that solution is

$$a_n = -3(2^n) + n^2 + 10n + 12. \tag{4.89}$$

As confirmed by the first three of our four equations, the sequence defined by Equation (4.89) satisfies the right initial conditions. However, computations show that this sequence satisfies

$$\begin{aligned} a_n - 4a_{n-1} + 5a_{n-2} - 2a_{n-3} &= -2 \\ &\neq 6n - 20. \end{aligned}$$

In other words, Sequence (4.89) fails to satisfy Recurrence (4.86), i.e., the (original) sequence is not solved by Equation (4.88). The *correct* solution turns out to be

$$a_n = 3(2^n) - n^3 + n^2 + 5n + 6, \qquad n \geq 0. \tag{4.90}$$

(Confirm that the first few terms of the sequence given by this formula are $9, 17, 24, 27, 26, \ldots$.) □

What went wrong in Example 4.5.12? In one sense, *nothing*! There is, after all, no *a priori* guarantee that guesses always check. In this particular case, a better guess would evidently have been $a_n = r2^n + an^3 + bn^2 + cn + d$, i.e., $r2^n$ plus a polynomial of degree *three*. Hold that thought.

4.5.13 Example. Let $\{b_n\}$ be the sequence defined by $b_0 = 9$, $b_1 = 17$, $b_2 = 24$, $b_3 = 27$, $b_4 = 26$, and

$$b_n = 6b_{n-1} - 14b_{n-2} + 16b_{n-3} - 9b_{n-4} + 2b_{n-5}, \qquad n \geq 5. \tag{4.91}$$

The characteristic polynomial of this homogeneous linear recurrence is

$$x^5 - 6x^4 + 14x^3 - 16x^2 + 9x - 2 = (x-1)^4(x-2),$$

which, by Theorem 4.5.6, means a solution of the form

$$\begin{aligned} b_n &= r2^n + (an^3 + bn^2 + cn + d)1^n \\ &= r2^n + an^3 + bn^2 + cn + d. \end{aligned} \tag{4.92}$$

Solving for the undetermined coefficients yields

$$b_n = 3(2^n) - n^3 + n^2 + 5n + 6. \tag{4.93}$$

□

Despite the fact that Recurrences (4.86) and (4.91) are dramatically different, Equations (4.90) and (4.93) show that $\{a_n\} = \{b_n\}$, i.e., the sequences themselves are identical! This coincidence bears on why our guesses were successful

in Examples 4.5.10 and 4.5.11 but not in Example 4.5.12. The difficulty can be traced to the multiplicity of $x = 1$ as a zero of the characteristic polynomial. The way to overcome this difficulty is to adjust our guesses, not by combining polynomial contributions as in Example 4.5.12, but by adding their degrees.

4.5.14 Rule. Let $\{a_n\}$ be a sequence determined by the initial values $a_0, a_1, \ldots, a_{k-1}$ and linear recurrence $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + w(n)$, $n \geq k$, where $w(n)$ is a polynomial in n of degree d. If the distinct roots $1 = r_0$, $r_1, r_2, \ldots, r_s$ of the corresponding characteristic polynomial $u(x) = x^k - c_1 x^{k-1} - c_2 x^{k-2} - \cdots - c_k$ have multiplicities $m_0, m_1, m_2, \ldots, m_s$, respectively, then there exist polynomials p_i of degree at most $m_i - 1$, $1 \leq i \leq s$, such that

$$a_n = p_1(n) r_1^n + p_2(n) r_2^n + \cdots + p_s r_s^n + p(n), \qquad n \geq 0,$$

where $p(n)$ is a polynomial of degree at most $d + m_0$.

Before going on to the next idea, check to see that the solutions in Examples 4.5.10–4.5.13 are consistent with Rule 4.5.14.

4.5.15 Example. Consider the sequence $\{a_n\}$ defined by $a_0 = 3$ and $a_n = 3a_{n-1} + 2(5^{n-1})$, $n \geq 1$. This time $w(n) = 2(5^{n-1})$ is not a polynomial in n. What do we do now? Why not try guess and check? The general solution to the homogeneous part, namely, $a_n = 3a_{n-1}$, is $a_n = c3^n$. Might the solution have the form $a_n = c3^n + b5^{n-1}$, $n \geq 0$? We might just as well take $d = b/5$ and look for a solution of the form

$$a_n = c3^n + d5^n. \tag{4.94}$$

Because there are two unknowns, we should look for two equations. The initial condition $a_0 = 3$ gives one, and setting $n = 1$ in the recurrence yields $a_1 = 3a_0 + 2(5^0) = 11$. It follows from

$$\begin{aligned} c + d &= 3 \\ 3c + 5d &= 11 \end{aligned}$$

that $c = 2$ and $d = 1$.

Once again, *if* there is a solution of the form given in Equation (4.94), then it must be

$$a_n = 2(3^n) + 5^n, \qquad n \geq 0. \tag{4.95}$$

Let's check it out. First, the sequence defined by Equation (4.95) satisfies the initial condition $a_0 = 3$; after all, that is where the equation $c + d = 3$ came from. Thus, it remains to verify that Sequence (4.95) satisfies the recurrence $a_n = 3a_{n-1} + 2(5^{n-1})$, $n \geq 1$. But, $a_{n-1} = 2(3^{n-1}) + 5^{n-1}$ implies that $3a_{n-1} + 2(5^{n-1}) = 6(3^{n-1}) + 5(5^{n-1}) = 2(3^n) + 5^n = a_n$. □

4.5.16 Example. Consider the sequence

$$5, 17, 57, 189, 621, \ldots$$

defined by $a_0 = 5$ and $a_n = 3a_{n-1} + 2(3^{n-1})$, $n \geq 1$. Following the approach of Example 4.5.15 would lead to a guess of the form $a_n = c3^n + d3^n$, $n \geq 0$, which can be expressed more simply as $a_n = b3^n$, $n \geq 0$. From the initial condition, $5 = a_0 = b3^0$, we see that $b = 5$. Thus, our guess becomes $a_n = 5(3^n)$, $n \geq 0$. Since $a_1 = 3 \times 5 + 2 \times 3^0 = 17 \neq 15 = 5 \times 3^1$, this guess fails to check out. The solution we seek is *not* of the form $a_n = b3^n$.

As in the discussion leading to Rule 4.5.14, the difficulty arises from an overlap between $w(n)$ and the general solution to the homogeneous part. Let's try to mimic Example 4.5.13 and design a sequence $\{b_n\}$ with initial conditions $b_0 = 5$, $b_1 = 17$, and a homogeneous recurrence with characteristic polynomial $u(x) = (x-3)^2 = x^2 - 6x + 9$, i.e., $b_n = 6b_{n-1} - 9b_{n-2}$. Then, from Theorem 4.5.6, $b_n = (cn + d)3^n$, $n \geq 0$. Together with the initial conditions, this leads to the simultaneous equations

$$\begin{aligned} d &= 5 \\ 3c + 3d &= 17, \end{aligned}$$

the solution to which is $c = \frac{2}{3}$ and $d = 5$, i.e., $b_n = 2n(3^{n-1}) + 5(3^n)$, $n \geq 0$. The confirmation that $\{a_n\} = \{b_n\}$ is left to the reader. □

4.5. EXERCISES

1 Consider the Lucas sequence $\{L_n\}$ defined on p. 320.

- **(a)** Compute $|L_n^2 - L_{n-1}L_{n+1}|$ for several values of n.
- **(b)** Make a conjecture about the sequence whose nth term is $|L_n^2 - L_{n-1}\, L_{n+1}|$, $n \geq 1$.
- **(c)** Does the Fibonacci sequence exhibit a similar property?
- **(d)** Can you prove your conjecture in part (b)?
- **(e)** Ratios of successive Fibonacci numbers were the subject of Exercise 6(d), Section 4.2. What can be said about the ratio of successive Lucas numbers, L_{n+1}/L_n, as n increases?

2 Find a closed formula for a_n if

- **(a)** $a_0 = 0$ and $a_n = a_{n-1} + n$, $n \geq 1$.
- **(b)** $a_0 = 0$ and $a_n = a_{n-1} + n^2$, $n \geq 1$.
- **(c)** $a_0 = 0$ and $a_n = a_{n-1} + n^3$, $n \geq 1$.
- **(d)** $a_0 = 0$ and $a_n = na_{n-1}$, $n \geq 1$.

3 Find a closed formula for a_n if

(a) $a_0 = 0$, $a_1 = 1$, and $a_n = 5a_{n-1} - 6a_{n-2}$, $n \geq 2$.

(b) $a_0 = 2$, $a_1 = 5$, and $a_n = 5a_{n-1} - 6a_{n-2}$, $n \geq 2$.

(c) $a_0 = 2$, $a_1 = 9$, and $a_n = 5a_{n-1} - 6a_{n-2}$, $n \geq 2$.

4 Find a closed formula for a_n if

(a) $a_0 = 1$, $a_1 = 2$, $a_2 = 6$, and $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$, $n \geq 3$.

(b) $a_0 = 1$, $a_1 = 0$, $a_2 = 6$, and $a_n = 4a_{n-1} - a_{n-2} - 6a_{n-3}$, $n \geq 3$.

(c) $a_0 = 3$, $a_1 = 4$, $a_2 = 14$, and $a_n = 4a_{n-1} - a_{n-2} - 6a_{n-3}$, $n \geq 3$.

5 Find a closed formula for a_n if

(a) $a_0 = 3$, $a_1 = 9$, $a_2 = 16$, and $a_n = 4a_{n-1} - 5a_{n-2} + 2a_{n-3}$, $n \geq 3$.

(b) $a_0 = 1$, $a_1 = 6$, $a_2 = 28$, and $a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3}$, $n \geq 3$.

(c) $a_0 = 1$, $a_1 = 8$, $a_2 = 36$, and $a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3}$, $n \geq 3$.

6 Confirm that $a_n = 3(2^n) - n^3 + n^2 + 5n + 6$, $n \geq 0$, solves the sequence in Example 4.5.12.

7 Find a closed formula for a_n if

(a) $a_0 = 3$, and $a_n = a_{n-1} + 3n - 2$.

(b) $a_0 = 1$, and $a_n = a_{n-1} + 2n - 3$.

(c) $a_0 = 2$, and $a_n = a_{n-1} + n^2 + 1$.

8 Find a closed formula for a_n if

(a) $a_0 = 3$, and $a_n = 3a_{n-1} + 4^n/2$.

(b) $a_0 = 1$, and $a_n = 2a_{n-1} + 4^{n-1}$.

(c) $a_0 = 2$, and $a_n = 3a_{n-1} - 4n + 3(2^n)$.

9 Find a closed formula for a_n if

(a) $a_0 = 2$, $a_1 = 9$, and $a_n = 6a_{n-1} - 9a_{n-2}$.

(b) $a_0 = 2$, and $a_n = 3a_{n-1} + 3^n$.

10 Finish Example 4.5.16 by confirming that the sequence $\{a_n\}$ defined by $a_0 = 5$ and $a_n = 3a_{n-1} + 2(3^{n-1})$, $n \geq 1$, is solved by $a_n = 3^{n-1}(2n + 15)$, $n \geq 0$.

11 Solve the sequence $\{a_n\}$ defined by

(a) $a_0 = 6$, $a_1 = 4$, and $a_n = a_{n-1} + 6a_{n-2} + 2^n$, $n \geq 2$.

(b) $a_0 = 4$, $a_1 = 7$, and $a_n = -a_{n-1} + 6a_{n-2} + 5(2^n)$, $n \geq 2$.

(c) $a_0 = 4$, $a_1 = 7$, $a_2 = 37$, and $a_n = a_{n-1} + 8a_{n-2} - 12a_{n-3}$, $n \geq 3$.

12 The *Tower of Hanoi* puzzle was introduced by Professor *Claus* in 1983. It consists of three vertical rods of the same diameter and n circular disks of

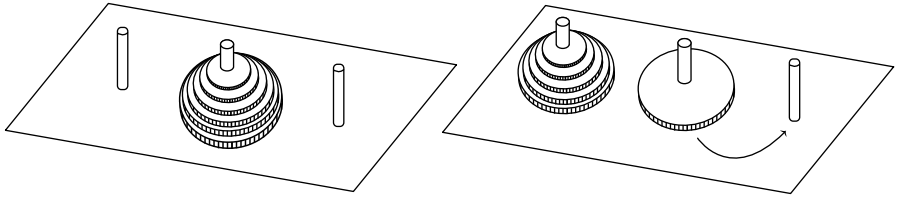


Figure 4.5.1. Tower of Hanoi.

different diameters with holes punched from their centers so that they can be slipped over the rods. In their initial position, the disks are arranged on one of the rods in the shape of a tower. (See Fig. 4.5.1.) A *move* consists of removing the top disk from one rod and transferring it to the top position on another, subject to the condition that no disk can ever sit on top of a smaller one. The object of these moves is to transfer the entire tower from the initial rod to one of the other two rods, one move at a time.*

Denote by T_n the *minimum* number of moves required to transfer an n-disk tower from one rod to another.

(a) Prove that the sequence $\{T_n\}$ satisfies the conditions $T_0 = 0$ and $T_n = 2T_{n-1} + 1$, $n \geq 1$.

(b) Find a closed formula for T_n.

(c) If one disk is moved each second, 24 hours a day, seven days a week, without making any mistakes, approximately how many centuries will it take to transfer a 64–disk tower? (*Hint*: $2^{10} \doteq 10^3$.)

13 Find a closed formula for L_n, the nth Lucas Number.

14 Suppose the monks in some monastery undertake the task of tossing a gold coin, believing that the monastery will vanish into hyperspace the moment two successive tails are tossed. Let $P(n) = a_n/b_n$ be the probability that successive tails occur for the first time on the $(n-1)$ st and nth tosses of the coin.

(a) Explain why we may take $b_n = 2^n$.

(b) Explain why $a_0 = a_1 = 0$.

(c) Prove that $a_{n+2} = F_n$, the nth Fibonacci number, $n \geq 0$.

(d) If $f(x) = \sum_{n\geq 0} a_{n+2}x^n$, prove that $f(x) = 1/(1 - x - x^2)$.

(e) Prove that $\sum_{n\geq 0} P(n) = 1$. (*Hint*:† Show that the sum is $\frac{1}{4} f\left(\frac{1}{2}\right)$, where $f(x)$ is the generating function from part (d). What implications does this probabilistic result have for the monks?)

*In 1884, de Parville published a two-page paper in *La Nature*, revealing that *Claus* is the anagrammatic pen name of (Edouard) Lucas. According to de Parville, a group of Tibetan monks is presently working in a secret monastery to transfer a tower of 64 golden disks. As de Parville tells the tale, the world will end in a thunderclap the moment the monks finish their task.

†S. Kennedy and M. Stafford, *Math. Mag.* 67 (1994), 380–382.

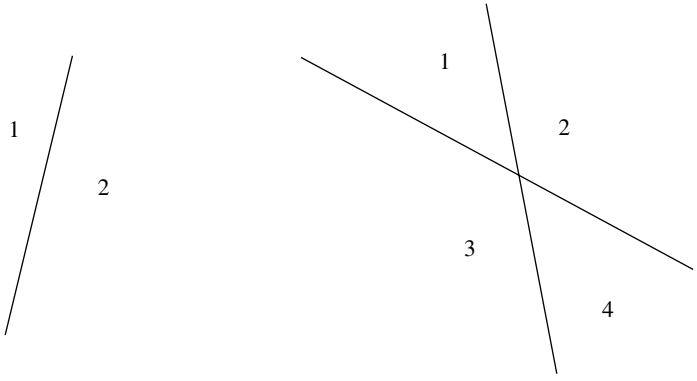


Figure 4.5.2

15 If two sequences satisfy the same linear recurrence, show that they differ by a solution to the corresponding homogeneous recurrence.

16 Let $\{c_n\}$ be the sequence defined by $c_0 = 1$ and $c_{n+1} = \sum_{r=0}^{n} c_r c_{n-r}$, $n \geq 1$.

(a) If $f(x) = \sum_{n\geq 0} c_n x^n$ is the generating function for $\{c_n\}$, prove that $xf(x)^2 = f(x) - 1$.

(b) Deduce from part (a) that $f(x) = [1 - (1 - 4x)^{1/2}]/2x$.

(c) Prove that $c_n = C(2n, n)/(n + 1)$, the nth *Catalan number* from Exercise 13, Section 1.2. (*Hint*: Newton's binomial theorem. Compare and contrast with Exercise 16, Section 1.2.)

17 Say that n lines in the plane are in *general position* if no two of them are parallel and no three of them are concurrent (incident with a single point). Apart from the lines themselves, n lines in general position partition the plane into some number r_n of *regions*. It is clear, e.g., from Fig. 4.5.2, that $r_0 = 1$, $r_1 = 2$, and $r_2 = 4$.

(a) Show that $r_3 = 7$.

(b) Prove that the sequence $\{r_n\}$ satisfies the linear recurrence $r_n = r_{n-1} + n$, $n \geq 1$.

(c) Find a closed formula for r_n.

18 Prove the converse of Theorem 4.5.3.

19 Consider a sequence $\{a_n\}$, with fixed but arbitrary initial conditions, a_0, $a_1, \ldots, a_{k-1}$, and homogeneous linear recurrence $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$, $n \geq k$. Let v_j be the $k \times 1$ column vector whose ith entry is a_{j+i-1}, i.e.,

$$v_j = (a_j, a_{j+1}, \ldots, a_{j+k-1})^t, \qquad j \geq 0.$$

Finally, let M be the $k \times k$ *companion matrix*

$$M = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \dots & & \\ 0 & 0 & 0 & \dots & 1 \\ c_k & c_{k-1} & c_{k-2} & \dots & c_1 \end{pmatrix}.$$

(a) Show that $Mv_j = v_{j+1}$, $j \geq 0$.

(b) Show that the characteristic polynomial of M is $u(x) = x^k - c_1 x^{k-1} - c_2 x^{k-2} - \ldots - c_{k-1} x - c_k$, the characteristic polynomial of the sequence.

(c) Suppose $a_n = r^n$, $0 \leq n < k$, where r is a real root of $u(x)$. Using parts (a) and (b), prove that $a_n = r^n$ for all $n \geq 0$.

5

Enumeration in Graphs

By convention there is color ... but in reality there are atoms and space.

— Democritus

The material in Chapter 5 has been selected from those topics in graph theory that afford an opportunity to discuss a combinatorical technique, like the pigeonhole principle; that exhibit an important combinatorial application, such as using Ferrers diagrams to characterize graphic sequences; or that involve a particularly nice example of combinatorial enumeration, e.g., the theory of chromatic polynomials.

Apart from the pigeonhole principle, Section 5.1 introduces graph isomorphism and illustrates the notion of an invariant using degree sequence and number of connected components as examples. The theme of edge colorings is used in Section 5.2, first to introduce the basic elements of Ramsey Theory and then to count nonisomorphic graphs. Readers who omitted Section 3.7 should either skip all of Section 5.2 or just the material beyond Theorem 5.2.5.

Stirling numbers of the first kind are seen, in Section 5.3, to be coefficients in chromatic polynomials of complete graphs. The notion of a proper coloring leads to bipartite graphs and trees.

In Section 5.4, counting things in planar graphs leads to Euler's formula relating numbers of vertices, edges, regions, and components. By using this discussion as a pretext to prove the five-color theorem, the text strays a bit from those topics in graph theory strictly related to combinatorial enumeration. Discipline is restored in Section 5.5, but only by choosing from the extensive theory of matchings just those topics related to the matching polynomial.

Oriented graphs, Laplacian matrices, and the matrix-tree theorem are discussed in Section 5.6. The focus of the final section is on necessary and sufficient conditions for a partition of $2m$ to be the degree sequence of some graph, finishing with the connection between Laplacian matrices and *threshold* graphs, i.e., graphs whose degree sequences are maximal with respect to *majorization*. Techniques from elementary linear algebra are used extensively in Section 5.6.

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

Apart from some vocabulary on p. 348, Sections 5.2 and 5.4 are optional. Later sections do not depend on either of them. Except for the second half of Section 5.2 (where the cycle index polynomial of the pair group is used to count nonisomorphic graphs), Chapter 5 is independent of Chapter 3. Despite the fact that the words *generating function* are used twice (once each in Sections 5.2 and 5.7), Chapter 5 is independent of Chapter 4. Finally, one might reasonably exit Chapter 5 either from the middle of Section 5.2 or at the end of any section.

5.1. THE PIGEONHOLE PRINCIPLE

Either through a sense of curiosity or to break up the tedium of a long flight, most air travel passengers eventually become acquainted with the contents of the seat pocket in front of them. Among the more interesting items to be found there is the airline's route map. On the typical map, a nonstop flight connecting cities u and v is illustrated by a line segment or arc joining the cities. Let's give a name to the number of segments/arcs that touch at u. Call it the *degree* of u. Would it surprise you to learn that, on *any* route map, there are *always* two cities that have exactly the same degree? This coincidence is a consequence of the following self-evident fact.

5.1.1 Pigeonhole Principle. If n pigeonholes are occupied by more than n pigeons, then some pigeonhole contains more than one pigeon.

Let's see what the pigeonhole principle has to do with airline route maps. We may assume that a total of $k > 1$ cities are represented on the map. It may happen that some city appears on the map even though it is not served by the airline; any such city has degree 0. At the other extreme, it might happen that a city is connected to every other city on the map. Any such *hub* will have degree $k - 1$. Notice, however, that these two extreme cases cannot occur simultaneously. (If some city is connected to every other city, then there can be no city of degree 0.) So, among the k cities on any given map, at most $k - 1$ degrees are possible. In particular, there are always more cities (pigeons) than degrees (pigeonholes).

Airline route maps afford just one illustration of the mathematical abstraction called a graph. Roughly speaking, a graph is a set of points some pairs of which are joined by arcs. To give a precise mathematical definition, let V be a set. Denote the family of its two-element subsets by $V^{(2)}$. Then, for example, $\{u, v, w\}^{(2)} = \{\{u, v\}, \{u, w\}, \{v, w\}\}$; $\{1, 2, 3, 4\}^{(2)} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$ and $\{x, y\}^{(2)} = \{\{x, y\}\}$. If $o(V) = n$, then $o(V^{(2)}) = C(n, 2)$.

5.1.2 Definition. A *graph* consists of two things, a nonempty finite set V and a (possibly empty) subset E of $V^{(2)}$. If $G = (V, E)$ is a graph, the elements of V are its *vertices* and the elements of E its *edges*. When more than one graph is under consideration, it may be useful to write $V(G)$ and $E(G)$, respectively, for the sets of vertices and edges. If $e = \{u, v\} \in E(G)$, the vertices u and v are said to be *adjacent* (to each other) and *incident* with e. Two edges are *adjacent* if they are

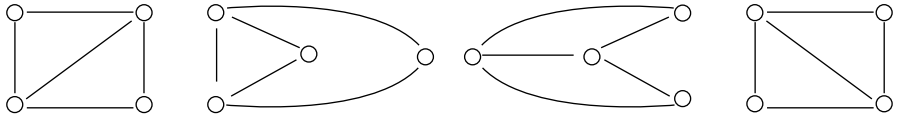


Figure 5.1.1

both incident with the same vertex, i.e., if their set-theoretic intersection consists of a single vertex.

5.1.3 Example. If $V = \{1,2,3,4\}$, then $V^{(2)}$ has 6 elements and 2^6 subsets. Hence, there are 64 different graphs with vertex set $V = \{1,2,3,4\}$.

It is common to draw pictures of graphs in which vertices are represented by points, and points representing adjacent vertices are joined by segments (or arcs). If $E = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\}\} = V^{(2)} \setminus \{\{3,4\}\}$, then each of the four pictures in Fig. 5.1.1 illustrates $G_1 = (V,E)$. □

An airline route map consists of a graph superimposed on a geometric representation of part of the Earth's surface. In such maps, the length of an arc is a rough indication of distance. This metric property makes a route map more than a graph. The length of an arc representing an edge of G has no graph-theoretic significance. An edge of a graph is a subset consisting of exactly two of its vertices.

5.1.4 Example. Not only can one graph be illustrated by different pictures, but one picture can represent different graphs! If $V_2 = \{a,b,c,d\}$ and $E_2 = \{\{a,b\}, \{a,c\},\{b,c\},\{b,d\},\{c,d\}\}$, then each picture in Fig. 5.1.1 (also) illustrates $G_2 = (V_2,E_2)$. □

We are not so much interested in "different" graphs as in "nonisomorphic" graphs.

5.1.5 Definition. Let $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ be graphs. Then G_1 is *isomorphic* to G_2 if there is a one-to-one function f from V_1 onto V_2 such that u and v are adjacent in G_1 if and only if $f(u)$ and $f(v)$ are adjacent in G_2, i.e., such that

$$\{u,v\} \in E_1 \qquad \text{if and only if} \quad \{f(u),f(v)\} \in E_2. \tag{5.1}$$

The function f is called an *isomorphism* from G_1 onto G_2.

5.1.6 Example. If G_1 and G_2 are the graphs in Examples 5.1.3 and 5.1.4, respectively, then G_1 and G_2 are isomorphic. If $f : V_1 \to V_2$ is the function (b,c,a,d), i.e., if $f(1) = b$, $f(2) = c$, $f(3) = a$, and $f(4) = d$, then f is one of four isomorphisms from G_1 onto G_2. □

If G_1 and G_2 can be illustrated by the same picture, they are isomorphic, because to each point of the picture there corresponds a unique vertex v_1 of G_1 and a unique

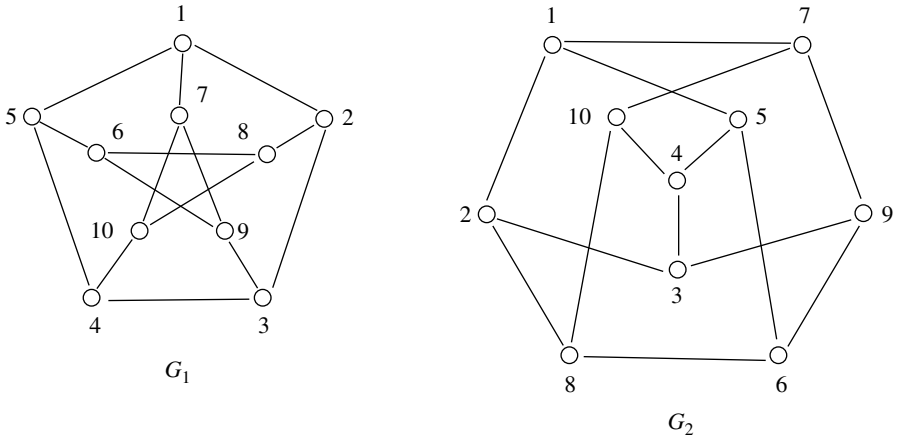


Figure 5.1.2. Two illustrations of the Petersen graph.

vertex v_2 of G_2. The function that sends v_1 to v_2 (for every point of the picture) is an isomorphism. It is much more challenging to tell when graphs illustrated by different pictures are isomorphic.

5.1.7 Example. Consider the so-called *Petersen graph* G_1, illustrated in Fig. 5.1.2. It is isomorphic to the graph G_2, pictured in the same figure. The proof that G_1 and G_2 are isomorphic is *by the numbers*. If $V(G_1) = \{1, 2, \ldots, 10\} = V(G_2)$, then $f(i) = i$, $1 \leq i \leq 10$, is an isomorphism. (Check it out. Confirm that i and j are adjacent in G_1 if and only if i and j are adjacent in G_2.) Such a pair of labeled figures may be considered a proof of isomorphism. (Provided, of course, that they check out.) □

One problem with picturing graphs by means of points and lines is that a line segment contains infinitely many geometric points, whereas an edge of a graph consistes of just two vertices.

5.1.8 Example. Take another look at the illustration of graph G_2 in Fig. 5.1.2. Note that, in the picture, edge $\{3, 9\}$ appears to *cross* edge $\{5, 6\}$, yet these two edges have no vertex in common. □

It follows from the definition that isomorphic graphs have the same numbers of vertices and edges. Consequently, if G_1 and G_2 do not share these properties, they cannot be isomorphic. Properties like these, that isomorphic graphs must share, are called *invariants*.

If G_1 and G_2 have the same number n of vertices, and the same number m of edges, then, in principle at least, the *isomorphism problem* involves sifting through $n!$ functions, looking for one that satisfies Condition (5.1). If $n = 10$, as in Example 5.1.7, this involves $10! \doteq 3.6$ million functions! It is one thing to verify,

by the numbers, that some given function is an isomorphism. It is something else entirely to identify an isomorphism among so many condidates! This troublesome prospect helps motivate the search for invariants. The more invariants we have, the better our chances of finding one for which G_1 and G_2 differ, giving a *back-door* proof that the graphs are not isomorphic. One important invariant is the multiset of vertex degrees, a useful discussion of which depends on a proper definition.

5.1.9 Definition. Let $G = (V, E)$ be a graph. Suppose $v \in V$. The *degree* of v, denoted $d_G(v)$, is the number of edges of G that are incident wth v, i.e., $d_G(v)$ is the number of vertices of G that are adjacent to v.

When its meaning is clear, we will typically write $d(v)$ in place of $d_G(v)$. Given a graph on n vertices, it is convenient to arrange the vertex degrees $d(v_1)$, $d(v_2), \ldots, d(v_n)$ in a sequence. Define

$$d(G) = (d_1, d_2, \ldots, d_n),$$

where $d_1 \geq d_2 \geq \cdots \geq d_n$ are the degrees of the vertices of G arranged in non-increasing order. (It need not be the case that $d_i = d(v_i)$.)

5.1.10 Theorem. *The degree sequence $d(G)$ is an invariant.*

Proof. Let $f : V_1 \to V_2$ be an isomorphism from $G_1 = (V_1, E_1)$ onto $G_2 = (V_2, E_2)$. Since f is one-to-one, it suffices to show that $d(f(v)) = d(v)$ for all $v \in V_1$. Because $\{u, v\} \in E_1$ if and only if $\{f(u), f(v)\} \in E_2$,

$$\begin{aligned} d(v) &= o(\{u \in V_1 \,:\, \{u, v\} \in E_1\}) \\ &= o(\{f(u) \in V_2 \,:\, \{f(u), f(v)\} \in E_2\}) \\ &= d(f(v)). \end{aligned}$$

■

From $d(G)$, we can determine both n, the number of vertices of G, and m, the number of its edges: n is just the length of the sequence $d(G)$, and m is given by the so-called *first theorem of graph theory*:

5.1.11 Theorem. *Let $G = (V, E)$ be a graph with vertex set $V = \{v_1, v_2, \ldots, v_n\}$. If $o(E) = m$, then*

$$\sum_{i=1}^{n} d(v_i) = 2m.$$

Proof. By definition, $d(v)$ is the number of edges incident with vertex v. Thus, in summing $d(v)$, each edge is counted twice, once at each of its vertices. ■

It is not uncommon in medieval literature for some character to be involved in a *quest*. If graph theorists had a quest, it would most likely be a short list of easily

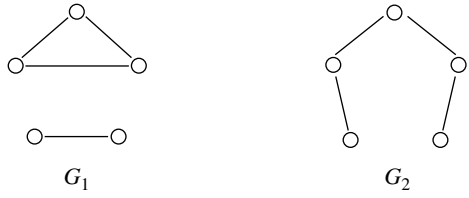


Figure 5.1.3

computed invariants, sufficient to distinguish nonisomorphic graphs.* For the moment let's observe that, by itself, $d(G)$ can fail to distinguish nonisomorphic graphs.

5.1.12 Example. The nonisomorphic graphs G_1 and G_2 of Fig. 5.1.3 share the degree sequence (2,2,2,1,1). □

5.1.13 Definition. Let $G = (V, E)$ be a graph. Suppose $u, w \in V$. A *path* in G of *length* r, from u to w, is a sequence of distinct vertices $[v_0, v_1, \ldots, v_r]$ such that $v_0 = u$, $v_r = w$, and $\{v_{i-1}, v_i\} \in E$, $1 \leq i \leq r$. Vertices u and w are in the same *component* of G if $u = w$ or if $u \neq w$ and there is a path in G from u to w. A graph with just one component is said to be *connected*.

5.1.14 Example. In Fig. 5.1.3, G_2 is connected but G_1 is not. A little care should be taken with this notion. If G_3 is the graph illustrated in Fig. 5.1.4, then G_3 is *not* connected. In fact, G_3 is isomorphic to G_1. □

5.1.15 Theorem. *Isomorphic graphs have the same number of components.*

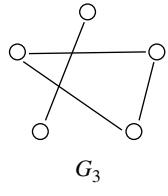


Figure 5.1.4

*Discussions of intractability frequently involve the class NP of decision problems that can be solved in polynomial time by a "nondeterministic" computer (a hypothetical device able to work on an unbounded number of independent computational sequences in parallel). In 1971, S. A. Cook proved that every problem in NP can be reduced to the "satisfiability" problem, making it the first NP-*complete* problem. As of this writing, whether the graph isomorphism problem is NP-complete remains an open question. Among the best introductions to NP-completeness is (still) M. Garey and D. Johnson, *Computers and Intractability: A guide to the Theory of* NP-*Completeness*, W. H. Freeman, San Francisco, 1979.

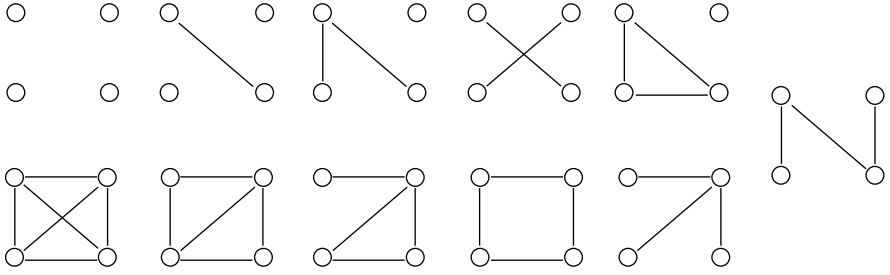


Figure 5.1.5

Proof. Let $f : V(G_1) \to V(G_2)$ be an isomorphism from G_1 onto G_2. Then $[v_0, v_1, \ldots, v_r]$ is a path in G_1 if and only if $[f(v_0), f(v_1), \ldots, f(v_r)]$ is a path in G_2. Thus, f maps the vertices of a component of G_1 onto the vertices of a component of G_2. ■

Suppose $V = \{v_1, v_2, \ldots, v_n\}$ and $W = \{w_1, w_2, \ldots, w_n\}$. Let S be the set of all graphs with vertex set V and T the set of all graphs with vertex set W. Define a function $h : S \to T$ by $h((V, E)) = (W, F)$, where $F = \{\{w_i, w_j\} : \{v_i, v_j\} \in E\}$. Then, h affords a one-to-one correspondence between S and T in which corresponding graphs are isomorphic. Thus, as far as the mathematics of graph theory goes, the nature of the vertices is immaterial. It doesn't matter whether they are cities on an airline route map, carbon atoms in a chemical molecule, or microprocessors in a parallel computer. In particular, it makes sense to talk about "the nonisomorphic graphs on n vertices". It doesn't matter *which* n vertices, just that there are n of them.

5.1.16 Example. There are 11 nonisomorphic graphs among the $2^{C(4,2)} = 64$ different graphs on four vertices. They are illustrated in Fig. 5.1.5. □

A useful short-cut when making lists of nonisomorphic graphs involves the notion of a "complement".

5.1.17 Definition. The *complement* of $G = (V, E)$ is the graph $G^c = (V, V^{(2)} \setminus E)$. So, G and G^c share the same vertex set, but $\{u, v\}$ is an edge of G if and only if it is *not* an edge of G^c.

With one exception, the graphs in Fig. 5.1.5 are illustrated in complementary pairs. This is possible because G and H are isomorphic if and only if G^c and H^c are isomorphic.

5.1.18 Example. The graphs illustrated in Fig. 5.1.6 are both complementary *and* isomorphic. □

If $V = \{v_1, v_2, \ldots, v_n\}$ then $K_n = (V, V^{(2)})$, the graph with all $C(n, 2)$ possible edges, is the *complete graph* on n vertices. Its complement is the graph with n

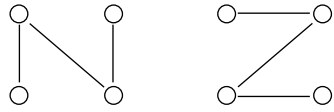


Figure 5.1.6

vertices but no edges at all. Thus, K_n^c is the graph having n components each consisting of a single *isolated* vertex.

5.1. EXERCISES

1 Suppose n is a positive integer. If S is a set of n integers, show that some subset of S sums to a multiple of n.

2 Suppose 100 balls are distributed among 15 urns. Prove that some two urns contain the same number of balls.

3 If both x and y are integers, the point $P = (x, y)$ is a *lattice point* of the plane. Suppose P_i, $1 \leq i \leq 5$, are five (different) lattice points. Each of the $C(5, 2) = 10$ *pairs* of these points determines a unique line segment. Show that the midpoint of (at least) one of these segments is a lattice point.

4 Suppose k pigeonholes are occupied by r pigeons. Show that some pigeonhole contains at least $\lceil r/k \rceil$ pigeons, where $\lceil x \rceil$ is the smallest integer not less than x.

5 Consider n objects each of which weighs a (positive) integer number of grams. Suppose, taken all together, the objects weigh a total of $2n$ grams. If the objects do not all weigh the same, and none of them weighs more than n grams, prove that they can be partitioned into two piles of equal weight.

6 Prove that, in any group of 40 people, some 4 of them have birthdays in the same month.

7 (P. Erdös) Let S be an $(n + 1)$-element subset of $\{1, 2, \ldots, 2n\}$. Prove that there exist two (different) integers in S, one of which exactly divides the other.

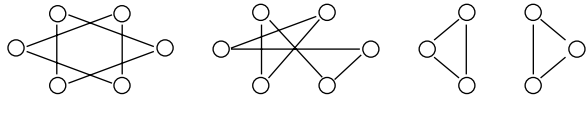
8 Consider an equilateral triangle 2 units on a side. Prove that it is not possible to place five points in the interior of the triangle so that each of them is more than 1 unit away from all the others.

9 Consider the graphs G_1 and G_2 in Examples 5.1.3 and 5.1.4

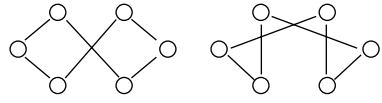
(a) Prove that the function f described in Example 5.1.6 is an isomorphism.

(b) Explicitly describe the other three isomorphisms from G_1 onto G_2.

10 Find all pairs of isomorphic graphs from the following:



(i) (ii) (iii)



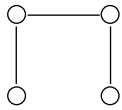
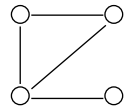
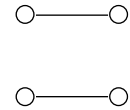
(iv) (v)

11 Prove that two graphs on three vertices are isomorphic if and only if they have the same numbers of vertices and edges.

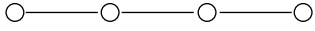
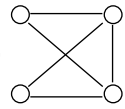
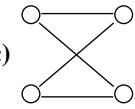
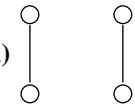
12 Use Example 5.1.16 to show that two graphs on four vertices are isomorphic if and only if they have the same degree sequence.

13 Let $G = (V, E)$ be a graph having k odd vertices, i.e., $k = o(\{v \in V : d(v)$ is odd$\})$. Prove that k is even.

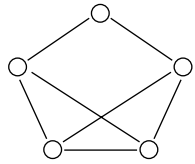
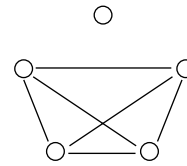
14 Let $V = \{1, 2, 3, 4\}$. Find a set E so that $G = (V, E)$ is illustrated by the picture

(a)  **(b)**  **(c)** 

15 Among those graphs pictured in Fig. 5.1.5, find one isomorphic to

(a)  **(b)**  **(c)**  **(d)** 

16 Illustrate the complement of

(a)  **(b)** 

17 Evidently (Example 5.1.18) it is possible for a graph to be isomorphic to its complement.

(a) Find a graph on five vertices that is ismorphic to its complement.

(b) Prove that no graph on six vertices is isomorphic to its complement.

(c) Prove that no graph on seven vertices is isomorphic to its complement.

18 Prove that

(a) $(G^c)^c = G$.

(b) G^c is isomorphic to H^c if and only if G is isomorphic to H.

19 Let $G = (V, E)$ be a graph with n vertices. For each $v \in V$, let $d^c(v)$ be the degree of v in the graph G^c. Explain why $d(v) + d^c(v) = n - 1$.

20 A graph with more than one component is said to be *disconnected*.

(a) How many of the graphs in Fig. 5.1.5 are disconnected?

(b) Show that the complement of a disconnected graph is connected.

(c) Which graph(s) G on four vertices have the property that both G and G^c are connected?

(d) Illustrate a connected graph G whose complement is connected, but not isomorphic to G.

(e) Illustrate two nonisomorphic, connected graphs that have the same degree sequence.

21 Prove that the relation "isomorphic to" is an equivalence relation on the set of graphs.

22 Two of the graphs in Fig. 5.1.5 are drawn in such a way that edges appear to *cross*, yet their would-be intersection is not a vertex of the graph. Redraw these two graphs in such a way that the segments (arcs) representing edges do not cross, i.e., do not meet except at vertices.

23 Explain why no graph can have degree sequence

(a) $(3, 3, 3, 3, 3, 3)$. **(b)** $(5, 4, 2, 2, 1)$.

24 Let G be the graph illustrated in Fig. 5.1.7. Prove, by the numbers, that G is isomorphic to the graph whose vertices and edges are the 8 vertices and 12 edges of a cube, respectively.

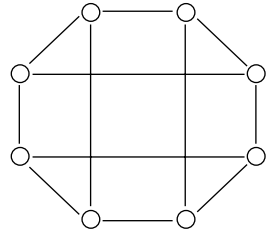


Figure 5.1.7

25 Illustrate six nonisomorphic graphs, each having five vertices and five edges.

26 Prove, "by the numbers", that the graph illustrated in Fig. 5.1.8 is isomorphic to the Petersen graph (shown twice in Fig. 5.1.2).

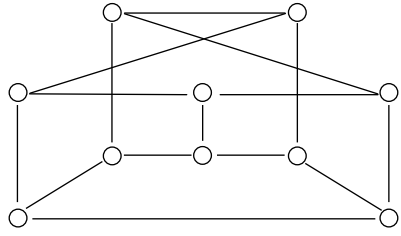


Figure 5.1.8

27 A *multigraph* consists of two things, a nonempty set V, and a multiset E satisfying the property that every element of E is an element of $V^{(2)}$. So, a multigraph is like a graph except that more than one edge can be incident to the same pair of vertices.

(a) Illustrate the multigraph $M = (V, E)$, where $V = \{1, 2, 3, 4\}$ and $E = \{\{1, 2\}, \{1, 2\}, \{1, 4\}, \{2, 3\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$.

(b) Show that Theorem 5.1.11 is valid for multigraphs.

(c) Define "isomorphism" for multigraphs.

28 Let $G = (V, E)$ and $H = (W, F)$ be graphs. Then H is a *subgraph* of G if $W \subset V$ and $F \subset E$. Illustrate the seven nonisomorphic subgraphs of the complete graph K_3.

29 A *planar* graph is one that can be drawn in the plane in such a way that segments (arcs) representing edges do not meet except at vertices.

(a) Show that K_3 and K_4 are planar.

(b) Is K_5 planar?

(c) Show that the graph illustrated in Fig. 5.1.7 is planar.

*5.2. EDGE COLORINGS AND RAMSEY THEORY

Minds are like parachutes. They only function when they are open.

— James Dewar

Let's say that two people are *acquainted* if they have met before (whether they remember it or not). *Strangers* are people who are not acquainted. Would it surprise you to learn that, among the first six guests to arrive at a random Hollywood

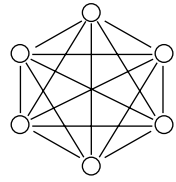


Figure 5.2.1. The complete graph K_6.

cocktail party, there will *always* be three mutual acquaintances or three mutual strangers? To see why this is so, suppose Alan is the first guest to arrive. The next five guests fall into one of two categories according to whether they are acquainted with Alan or not, and one of these categories (pigeonholes) must contain (at least) three people.

Suppose Bev, Connie, and Donna are all acquaintances of Alan. If the ladies are mutual strangers, we are finished. Otherwise, some two of them are acquainted. These two, together with Alan, comprise three mutual acquaintances. It may be, on the other hand, that none of the three ladies are acquainted with Alan. If they happen to be mutually acquainted, we are finished. Otherwise, some two of them are strangers and these two, together with Alan, comprise three mutual strangers.

Let's transcribe our observation to graphs. Identify the six guests with the vertices of K_6 (Fig. 5.2.1). If guests X and Y are acquainted, color edge $\{X, Y\}$ black. Otherwise, color it white. Our conclusion is that the resulting figure contains a black triangle, a white triangle, or both.

What about n guests? Imagine a picture of $K_n = (V, V^{(2)})$ drawn using a black pen. Select a (possibly empty) subset $E \subset V^{(2)}$ and *white-out* the edges of K_n that do not belong to E. The resulting black–white edge coloring of K_n could easily be mistaken for an illustration of the graph $G = (V, E)$. These two ways of looking at the same picture reveal a natural one-to-one correspondence between the $2^{C(n,2)}$ different black–white colorings of the edges of K_n and the $2^{C(n,2)}$ different graphs on n vertices. Exploiting this correspondence requires some new definitions.

5.2.1 Definition. Let $G = (V, E)$ and $H = (W, F)$ be graphs. If $W \subset V$ and $F \subset E$, then H is a *subgraph* of G. If $F = E \cap W^{(2)}$, then H is the subgraph of G *induced* by W, written $H = G[W]$.

If $H = (W, F)$ is a subgraph of $G = (V, E)$ then, because H is a graph, $F \subset W^{(2)}$. Therefore, $F \subset E \cap W^{(2)}$, with equality if and only if $H = G[W]$. It follows that, $H = (W, F)$ is a subgraph of G if and only if H is a subgraph of $G[W]$, where $W = V(H)$. In particular, $G[W] = (W, E \cap W^{(2)})$ is the unique maximal subgraph of G with vertex set W.

A *clique* is a nonempty set of mutually adjacent vertices. So, a nonempty subset W of $V(G)$ is a clique if and only if $W^{(2)} \subset E(G)$, if and only if $G[W] = (W, W^{(2)})$ is a complete graph. An *independent set* is a nonempty set of mutually *non*adjacent vertices. So, a nonempty subset W of $V(G)$ is an independent set if and only if no

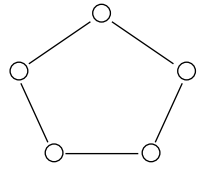


Figure 5.2.2

two of its vertices comprise an edge of G, if and only if $G[W] = (W, \varnothing)$, if and only if W is a clique in G^c.

Consider some fixed black–white edge coloring of K_6. Let G be the six-vertex subgraph whose edge set consists of the black-colored edges. Then a black triangle in K_6 is a clique in G, and a white triangle in K_6 is an independent set in G. This identification yields another way to state our party guest observation: Any graph G with six vertices contains a three-vertex clique or a three-vertex independent set, i.e., G contains an induced subgraph isomorphic to K_3 or one isomorphic to K_3^c.

It is a consequence of Theorem 5.2.3 (below) that, for any positive integers s and t, there exists an integer N such that every graph on N vertices contains an induced subgraph isomorphic to K_s or one isomorphic to K_t^c. If G is a graph on $n > N$ vertices, then G has a total of $C(n, N)$ induced subgraphs each having N vertices. If H is one of them then, since H has an induced subgraph isomorphic to K_s or to K_t^c, so does G. We are led to the following:

5.2.2 Definition. Let s and t be positive integers. The *Ramsey number*[*] $N(s, t)$ is the smallest value of n such that every graph on n vertices contains an induced subgraph isomorphic to K_s or an induced subgraph isomorphic to K_t^c.

Our cocktail party discussion proves that $N(3, 3) \leq 6$. Because the *pentagon graph* (illustrated in Fig. 5.2.2) contains neither K_3 nor K_3^c as an induced subgraph, $N(3, 3)$ is not less than 6. Therefore, $N(3, 3) = 6$.

It is not difficult to show that $N(1, t) = 1$ and $N(2, t) = t$ for all $t \geq 1$. Moreover, the Ramsey numbers are symmetric, i.e., $N(s, t) = N(t, s)$ for all s and t. The easy proofs of these elementary observations obscure the difficulty of obtaining exact values for Ramsey numbers in general.[†] In fact, every known Ramsey number can be obtained by combining these elementary observations with the information contained in Fig. 5.2.3.

s \ t	3	4	5	6	7	8	9
3	6	9	14	18	23	28	36
4	9	18	25	?	?	?	?

Figure 5.2.3. Ramsey Numbers $N(s, t)$.

[*] After Frank Ramsey (1902–1930).

[†] See the lively and colorful article, "Ramsey Theory", by Ron Graham and Joel Spencer, in the July 1990 issue of *Scientific American* (pp 112–117).

Because exact values of Ramsey numbers are so hard to determine, there is a good deal of interest in bounding them.

5.2.3 Theorem. *If* $s, t \geq 2$, *then* $N(s,t)$ *exists and* $N(s,t) \leq N(s,t-1) + N(s-1,t)$.

The proof that every graph on $N(s,t-1) + N(s-1,t)$ vertices satisfies the Ramsey property for s and t is left to the exercises.

5.2.4 Corollary. *If* s *and* t *are positive integes, then* $N(s,t) \leq C(s+t-2, s-1)$.

Proof. The proof is by induction on $k = s + t$. It follows from the "elementary observations" that $N(s,t) = C(s+t-2, s-1)$ if either s or t is at most 2. So, we may proceed under the assumptions that $s, t \geq 3$, and that the result is true for all values of $k < s + t$. Together with Theorem 5.2.3, these assumptions yield

$$\begin{aligned} N(s,t) &\leq N(s,t-1) + N(s-1,t) \\ &\leq C(s+t-3, s-1) + C(s+t-3, s-2) \\ &= C(s+t-2, s-1). \end{aligned}$$

■

What about lower bounds?

5.2.5 Theorem. *Ramsey number* $N(s,t) \geq (s-1)(t-1) + 1$.

Proof. Let $n = (s-1)(t-1)$. It suffices to exhibit a black–white coloring of the edges of K_n in which there is no black K_s and no white K_t. Imagine the vertices of K_n arranged in a rectangular array of $s-1$ rows and $t-1$ columns. If vertices u and v lie in the same row of the array, color edge $\{u, v\}$ white. Otherwise, color it black. By the pigeonhole principle, in any collection of s vertices, some two of them must come from the same row. Hence, this coloring of K_n can contain no black K_s. If all the black edges are deleted, then the connected components of what's left correspond to the rows. Since each of these holds $t-1$ vertices, K_n can contain no white K_t. ■

It follows from Corollary 5.2.4 and Theorem 5.2.5, e.g., that $10 \geq N(3,4) \geq 7$. In fact (see Fig. 5.2.3), $N(3,4) = 9$.

Let's move on to another application* of the correspondence between the different graphs on n vertices and the different black–white edge colorings of K_n. Denote

*The application discussed from this point to the end of the section involves counting nonisomorphic graphs using the techniques developed in Sections 3.6 and 3.7. Readers who omitted those sections should either skip the remainder of Section 5.2 or just skim it for the flavor and conclusion.

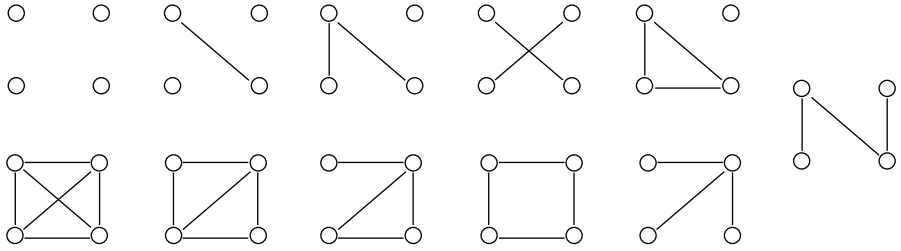


Figure 5.2.4

by $g(n, m)$ the number of nonisomorphic graphs having n vertices and m edges. Then

$$f_n(x) = \sum_{m=0}^{C(n,2)} g(n, m)x^m \tag{5.2}$$

is a *generating function* for the nonisomorphic graphs on n vertices.

5.2.6 Example. The 11 nonisomorphic graphs on four vertices from Fig. 5.1.5 have been reproduced in Fig. 5.2.4. Using these pictures, it is easy to see that

$$f_4(x) = 1 + x + 2x^2 + 3x^3 + 2x^4 + x^5 + x^6. \tag{5.3}$$

(Confirm that $f_4(1) = 11$.) □

Because K_n is the unique graph having n vertices and $m = C(n, 2)$ edges, $g(n, C(n, 2)) = 1$, i.e., $f_n(x)$ is a monic polynomial of degree $C(n, 2)$. Since G_1 and G_2 are isomorphic if and only if G_1^c and G_2^c are isomorphic, $f_n(x)$ is symmetrical in the sense that $g(n, m) = g(n, C(n, 2) - m)$, $0 \le m \le C(n, 2)$. It follows that $f_n(x)$ is a *reciprocal polynomial*, i.e.,

$$x^{C(n,2)} f_n(x^{-1}) = f_n(x).$$

(Confirm that $x^6 f_4(x^{-1}) = f_4(x)$.)

If we had a picture comparable to Fig. 5.2.4 for the 34 nonisomorphic graphs on five vertices, it would be a simple matter to produce

$$f_5(x) = x^{10} + x^9 + 2x^8 + 4x^7 + 6x^6 + 6x^5 + 6x^4 + 4x^3 + 2x^2 + x + 1. \tag{5.4}$$

On the other hand, if it were *your* assignment to produce such a picture, it would surely be useful to know, for eample, that the coefficient of x^4 in $f_5(x)$ is 6, i.e., that there are exactly six nonisomorphic graphs having five vertices and four edges. Okay, so how does one go about generating $f_5(x)$ without a picture?

Let's begin by taking $V = \{1, 2, \ldots, n\}$. Then $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ are isomorphic if and only if there is a permutation $p : V \to V$ such that

$$\{i,j\} \in E_1 \qquad \text{if and only if} \quad \{p(i), p(j)\} \in E_2. \tag{5.5}$$

Recall (Definition 3.7.11) that the natural action of $p \in S_n$ on $V^{(2)}$ is denoted $\tilde{p}$, where $\tilde{p} : V^{(2)} \to V^{(2)}$ is defined by

$$\tilde{p}(\{i,j\}) = \{p(i), p(j)\}. \tag{5.6}$$

Expressed in terms of this induced action, Condition (5.5) becomes

$$e \in E_1 \qquad \text{if and only if} \quad \tilde{p}(e) \in E_2. \tag{5.7}$$

In other words, G_1 is isomorphic to G_2 if and only if there is a permutation $\tilde{p}$ in the pair group $S_n^{(2)}$ (see Definition 3.7.11) such that

$$\tilde{p}(E_1) = E_2. \tag{5.8}$$

As a geometric object, the symmetry group of $K_n = (V, V^{(2)})$ is S_n, when it is expressed as permutations of $V = \{1, 2, \ldots, n\}$. As permutations of the edge set $V^{(2)}$, it is $S_n^{(2)}$. Viewing $G = (V, E)$ as a 2-coloring of the edges of K_n, Condition (5.8) implies that two graphs on n vertices are isomorphic if and only if the corresponding 2-colorings of K_n are equivalent modulo $S_n^{(2)}$. This yields the following.

5.2.7 Theorem. *In terms of the cycle index polynomial for $S_n^{(2)}$, the generating function for the nonisomorphic graphs on n vertices is*

$$\begin{aligned} f_n(x) &= W_{S_n^{(2)}}(1, x) \\ &= Z_{S_n^{(2)}}(1 + x, 1 + x^2, 1 + x^3, \ldots, 1 + x^{C(n,2)}). \end{aligned}$$

Proof. If $V = \{1, 2, \ldots, n\}$ then, modulo $S_n^{(2)}$, the number of inequivalent black–white colorings of $V^{(2)}$, in which exactly m edges are colored black, is equal to $g(n, m)$, the number of nonisomorphic graphs having n vertices and m edges. Thus, it remains to substitute $w = 1$ and $b = x$ in the pattern inventory $W_{S_n^{(2)}}(w, b)$ and use Pólya's theorem. ■

5.2.8 Example. If $n = 4$ then, from Equation (3.60),

$$Z_{S_4^{(2)}}(s_1, s_2, \ldots, s_6) = \tfrac{1}{24}(s_1^6 + 9s_1^2 s_2^2 + 8s_3^2 + 6s_2 s_4). \tag{5.9}$$

The substitution $s_r = 1 + x^r$, $r \geq 1$, produces

$$\begin{aligned} f_4(x) &= \tfrac{1}{24}\left[(1+x)^6 + 9(1+x)^2(1+x^2)^2 + 8(1+x^3)^2 + 6(1+x^2)(1+x^4)\right] \\ &= \tfrac{1}{24}\left[(1 + 6x + 15x^2 + 20x^3 + 15x^4 + 6x^5 + x^6)\right. \\ &\quad + 9(1 + 2x + 3x^2 + 4x^3 + 3x^4 + 2x^5 + x^6) \\ &\quad \left. + 8(1 + 2x^3 + x^6) + 6(1 + x^2 + x^4 + x^6)\right] \\ &= 1 + x + 2x^2 + 3x^3 + 2x^4 + x^5 + x^6, \end{aligned}$$

which is exactly Equation (5.3). □

5.2.9 Example. From Example 3.7.16, the cycle index polynomial for $S_5^{(2)}$ is

$$\begin{aligned} Z_{S_5^{(2)}}(s_1, s_2, \ldots, s_{10}) = \tfrac{1}{120}\left[s_1^{10} + 10s_1^4 s_2^3 + 20s_1 s_3^3 + 15s_1^2 s_2^4\right. \\ \left. + 30s_2 s_4^2 + 20s_1 s_3 s_6 + 24s_5^2\right] \end{aligned}$$

Let's use this formula (and Theorem 5.2.7) to compute $g(5, 6)$, the coefficient of x^6 in $f_5(x)$. Because $C(10, 6) = 210$,

$$(1+x)^{10} = 1 + \cdots + 210x^6 + \cdots + x^{10}.$$

Similarly,

$$\begin{aligned} &10(1+x)^4(1+x^2)^3 \\ &\quad = 10(1 + 4x + 6x^2 + 4x^3 + x^4)(1 + 3x^2 + 3x^4 + x^6) \\ &\quad = 10(1 + \cdots + [(1)(x^6) + (6x^2)(3x^4) + (x^4)(3x^2)] + \cdots + x^{10}) \\ &\quad = 10 + \cdots + 220x^6 + \cdots + 10x^{10}. \end{aligned}$$

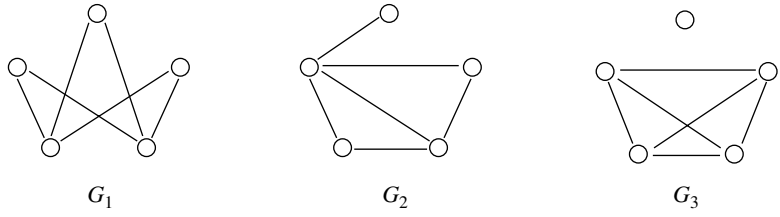
The coefficient of x^6 in $20(1+x)(1+x^3)^3$ is $20(1)(3) = 60$. In

$$\begin{aligned} &15(1+x)^2(1+x^2)^4 \\ &\quad = 15(1 + 2x + x^2)(1 + 4x^2 + 6x^4 + 4x^6 + x^8) \\ &\quad = 15(1 + \cdots + [(1)(4x^6) + (x^2)(6x^4)] + \cdots + x^{10}) \\ &\quad = 15 + \cdots + 150x^6 + \cdots + 15x^{10}, \end{aligned}$$

it is 150. It is $30(1)(2) = 60$ in $30(1+x^2)(1+x^4)^2$, 20 in $20(1+x)(1+x^3)(1+x^6)$, and 0 in $24(1+x^5)^2$. Summing up, the coefficient of x^6 in $f_5(x)$ is

$$\begin{aligned} \tfrac{1}{120}(210 + 220 + 60 + 150 + 60 + 20 + 0) &= \tfrac{720}{120} \\ &= 6. \end{aligned}$$

The $g(5, 6) = 6$ nonisomorphic graphs having five vertices and six edges are illustrated in Fig. 5.2.5. The first few values of $g(n, m)$ are tabulated in Fig. 5.2.6. □



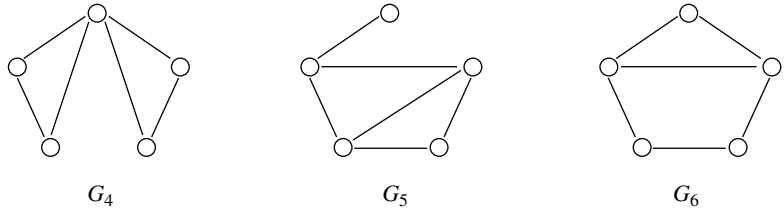


Figure 5.2.5

5.2.10 Corollary. *The number of nonisomorphic graphs on n vertices is given by the formula*

$$\sum_{m=1}^{C(n,2)} g(n,m) = \frac{1}{n!}\sum_{p\in S_n} 2^{c(\bar{p})}.$$

Proof. The result follows from setting $x = 1$ in Theorem 5.2.7. ■

5.2. EXERCISES

1 Let H be an induced subgraph of G. If K is an induced subgraph of H, prove that K is an induced subgraph of G.

2 Prove the "elementary observations" about Ramsey numbers, i.e., that

n \ m	0	1	2	3	4	5	6	7	8	9	10
1	1										
2	1	1									
3	1	1	1	1							
4	1	1	2	3	2	1	1				
5	1	1	2	4	6	6	6	4	2	1	1
6	1	1	2	5	9	15	21	24	24	21	15
7	1	1	2	5	10	21	41	65	97	131	148

Figure 5.2.6 The number $g(n,m)$ of graphs with n vertices and m edges.

(a) $N(s,t) = N(t,s)$ for all $s,t \geq 1$.

(b) $N(1,t) = 1$ for all $t \geq 1$.

(c) $N(2,t) = t$ for all $t \geq 1$.

3 Prove from scratch (i.e., without using Theorem 5.2.3) that

(a) $N(3,4) \leq 10$.

(b) $N(4,4) \leq 20$.

4 Prove Theorem 5.2.3. (*Hint*: Exercise 3.)

5 How many nonisomorphic graphs are there

(a) on six vertices? **(b)** on seven vertices?

6 Explain how the graph in Fig. 5.2.7 proves that Ramsey number $N(3,4) > 8$.

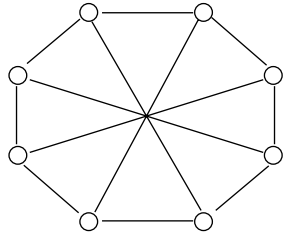


Figure 5.2.7

7 Of the six graphs in Fig. 5.2.5, only G_1 and G_6 share the same degree sequence. Prove that G_1 and G_6 are not isomorphic

(a) by counting components in their complements.

(b) by an argument based on the fact that the two vertices of degree 3 are adjacent in G_6 but not adjacent in G_1.

8 Illustrate the nonisomorphic graphs having five vertices and four edges.

9 Compute $f_3(x)$

(a) from an illustration of the nonisomorphic graphs on three vertices.

(b) using Theorem 5.2.7.

10 Illustrate the nonisomorphic graphs having five vertices and

(a) seven edges. **(b)** three edges.

11 Suppose $n \geq 4$. Independently of Theorem 5.2.7, give an intuitive explanation why there should be exactly two nonisomorphic graphs having n vertices and two edges.

12 Independently of Theorem 5.2.7, give an intuitive explanation why there should be exactly two nonisomorphic graphs having

(a) five vertices and eight edges.

(b) six vertices and 13 edges.

13 Compute $g(6, 3)$

(a) without appealing to Theorem 5.2.7.

(b) using Theorem 5.2.7 in the manner of Example 5.2.9.

14 Prove that $g(n, 3) = g(6, 3)$ for all $n > 6$.

15 Verify the value for $g(6, m)$ tabulated in Fig. 5.2.6 when

(a) $m = 4$. **(b)** $m = 5$. **(c)** $m = 6$. **(d)** $m = 7$.

16 Prove that $g(n, m) = g(2m, m)$ for all $n > 2m$.

17 Illustrate the nine nonisomorphic graphs having six vertices and

(a) 4 edges. **(b)** 11 edges.

18 How many of the nonisomorphic graphs on five vertices are connected?

19 Prove that the graphs illustrated in Fig. 5.2.8 are *not* isomorphic.

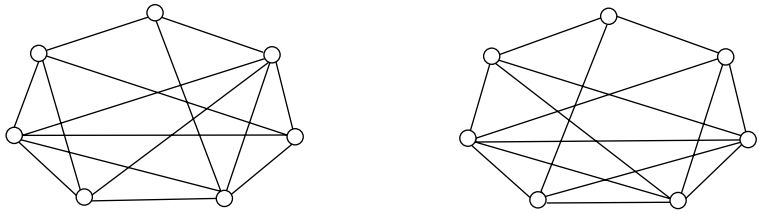


Figure 5.2.8

20 Let Γ_n be the set of all $2^{C(n,2)}$ graphs on n vertices, and let $\Gamma_{n,k}$ be the subset of Γ_n consisting of those graphs that contain a k-vertex clique.

(a) Prove that $o(\Gamma_{n,k}) \leq C(n, k)2^{C(n,2)-C(k,2)}$.

(b) Prove that $o(\Gamma_{n,k})/o(\Gamma_n) < n^k/[k!2^{C(k,2)}]$.

(c) Prove that $o(\Gamma_{n,k})/o(\Gamma_n) < \frac{1}{2}$ when $n < 2^{k/2}$.

(d) Prove Erdös's theorem: $N(k, k) \geq 2^{k/2}$.

21 A *proper* coloring of the edges of (an arbitrary graph) G is one in which adjacent edges are colored differently. The *edge chromatic number* $k(G)$ is the smallest number of colors that suffice to properly color the edges of G. Evidently, $k(G) \geq d_1$, the largest vertex degree in G. In 1964, Russian mathematician V. G. Vizing proved that $k(G) \leq d_1 + 1$.

(a) Prove that $k(G) = d_1$ for every connected graph G on four vertices.

(b) If $G = K_3$, prove that $k(G) = d_1 + 1$.

(c) Exhibit a connected graph $G \neq K_3$ for which $k(G) = d_1 + 1$.

5.3. CHROMATIC POLYNOMIALS

The intellect of man is forced to choose.

— William Butler Yeats

In Section 5.2, we discussed edge colorings of the complete graph K_n. In this section, we are interested in coloring *vertices*, not only of K_n, but of any graph. An *r-coloring* of G is a function from $V(G)$ into some set of r colors.

5.3.1 Definition. A *proper* coloring of G is one in which adjacent vertices are colored differently. The *number of proper r-colorings* of G is denoted $p(G, r)$.

5.3.2 Example. If $G = K_n^c$, then the criterion that adjacent vertices be colored differently is no restriction at all:

$$p(K_n^c, r) = r^n. \qquad \square$$

5.3.3 Example. Since every vertex of the complete graph is adjacent to every other vertex, the only proper colorings of K_n are those for which all the vertices are colored differently. By the fundamental counting principle,

$$\begin{aligned} p(K_n, r) &= r(r-1)(r-2)\cdots(r-n+1) \\ &= r^{(n)}, \end{aligned}$$

the falling factorial function. In particular (Equations (2.33) and (2.34)),

$$p(K_n, r) = r^n - s(n, n-1)r^{n-1} + s(n, n-2)r^{n-2} - \cdots + (-1)^{n-1}s(n, 1)r,$$

where $s(n, k)$ is a Stirling number of the first kind, $1 \le k < n$. $\square$

These examples turn out to be typical in the sense that, for any graph G on n vertices, $p(G, r)$ is a monic polynomial of degree n in r. One way to establish this fact makes use of a recursive algorithm for computing "chromatic polynomials".

5.3.4 Definition. Suppose $e = \{u, v\}$ is an edge of $G = (V, E)$. The *edge subgraph* $G - e = (V, E \setminus \{e\})$ is the graph obtained from G by deleting edge e.

Let G be the graph illustrated in Fig. 5.3.1*a*, with $e = \{u, v\}$. Then $G - e$ is pictured in Fig. 5.3.1*b*.

Note that every proper coloring of G is a proper coloring of $G - e$. The difference $p(G - e, r) - p(G, r)$ is the number of proper colorings of $G - e$ in which u and v are colored the same. To evaluate this difference, consider the *multigraph*

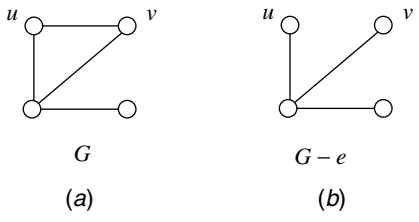


Figure 5.3.1

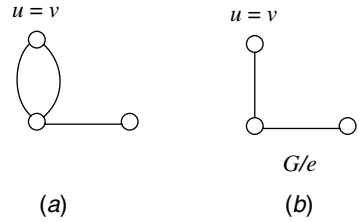


Figure 5.3.2

obtained from $G - e$ by identifying vertices u and v, i.e., by *coalescing* u and v into a single vertex. This multigraph is illustrated in Fig. 5.3.2*a*. Observe that there is a one-to-one correspondence between proper colorings of the multigraph and those colorings of $G - e$ in which u and v are colored the same.

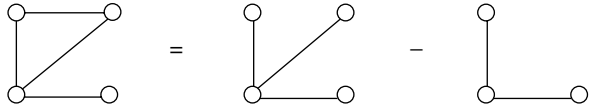
From the perspective of proper (vertex) colorings, extra edges are immaterial. There is a one-to-one correspondence between proper colorings of the multigraph in Fig. 5.3.2*a* and proper colorings of its underlying graph G/e, pictured in Fig. 5.3.2*b*. In particular, the difference $p(G - e, r) - p(G, r) = p(G/e, r)$. Rearranging terms in this equation proves the following fundamental result.

5.3.5 Theorem (Chromatic Reduction). *Let G be a graph. If $e = \{u, v\}$ is an edge of G, then*

$$p(G, r) = p(G - e, r) - p(G/e, r), \tag{5.10}$$

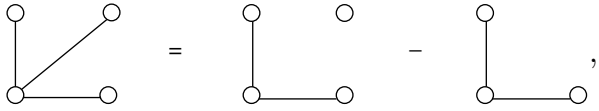
where $G - e$ is the graph obtained from G by deleting edge e, and G/e is the graph obtained from $G - e$ by identifying vertices u and v, and deleting any multiple edges that may arise in the process.

5.3.6 Example. Let's use chromatic reduction to work out $p(G, r)$ for the graph shown in Fig. 5.3.1*a*. With respect to the edge $e = \{u, v\}$, Equation (5.10) may be written in the picturesque form

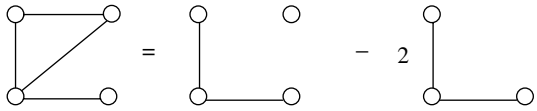


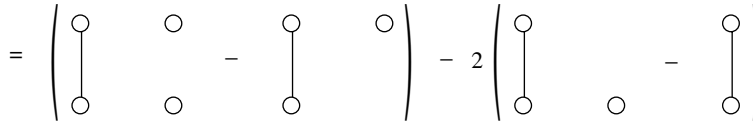
(5.11)

In Equation (5.11), a picture of H has been used to represent $p(H, r)$. Another picturesque application of Theorem 5.3.5 yields

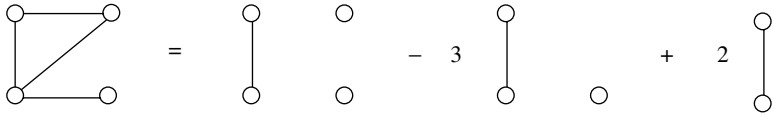


so

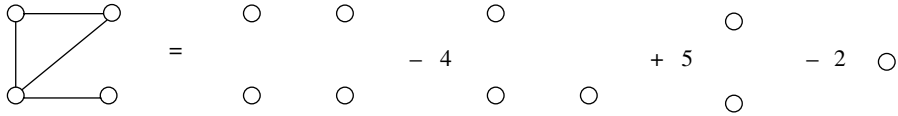




After consolidating isomorphic graphs, this last equation becomes



Another step (consolidation included) produces



$$= p(K_4^c, r) - 4p(K_3^c, r) + 5p(K_2^c, r) - 2p(K_1^c, r).$$

Because $p(K_n^c, r) = r^n$, this last equation is equivalent to

$$p(G, r) = r^4 - 4r^3 + 5r^2 - 2r. \tag{5.12}$$

□

If G is any graph with n vertices and m edges then, after m steps, chromatic reduction results in an expression of the form

$$\begin{aligned} p(G, r) &= p(K_n^c, r) - b_1 p(K_{n-1}^c, r) + b_2 p(K_{n-2}^c, r) - \cdots \\ &= r^n - b_1 r^{n-1} + b_2 r^{n-2} - \cdots, \end{aligned}$$

where $b_1, b_2, \ldots$ are integers. This proves the following:

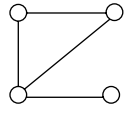
5.3.7 Corollary. *Let G be a graph on n vertices. Then $p(G, r)$ is a monic polynomial of degree n in the variable r.*

Now that we know $p(G, r)$ is a polynomial, we may as well replace r with a more customary variable.

5.3.8 Definition. The *chromatic polynomial*[*] of G is

$$p(G, x) = x^n - b_1 x^{n-1} + b_2 x^{n-2} - \cdots + (-1)^{n-1} b_{n-1} x.$$

From Equation (5.12), $f(x) = p(G, x) = x^4 - 4x^3 + 5x^2 - 2x$ is the chromatic polynomial of

G =  (5.13)

meaning that $f(r)$ is the number of proper colorings of G using (at most) r colors. Because it contains a three-vertex clique, G cannot be properly colored with fewer than three colors. Therefore, $f(0) = f(1) = f(2) = 0$, which implies that $x(x-1)(x-2)$ is a factor of $f(x)$. Indeed,

$$\begin{aligned} f(x) &= p(G, x) \\ &= x(x-1)^2(x-2). \end{aligned} \tag{5.14}$$

An important open problem in graph theory is to determine when a given polynomial is the chromatic polynomial of some graph. Consider, for example, $p(x) = x(x-1)(x-3)^2$. If $p(x) = p(G, x)$ for some graph G then, because $p(3) = 0$, G could not be properly colored with three (or fewer!) colors. But, $p(2) = 2 > 0$ implies that G is properly 2-colorable! This contradiction proves that $p(x)$ is not the chromatic polynomial of any graph. It also suggests something more. For any graph G, there is some minimum positive integer k (depending on G) such that $p(G, r) = 0$ whenever $r < k$, but $p(G, r) > 0$ for every integer $r \geq k$.

5.3.9 Definition. The *chromatic number* $\chi(G)$ is the minimum number of colors that suffice to color G properly.[†]

The chromatic number of the graph in Equation (5.13) is 3, the first positive integer that is *not* a root of its chromatic polynomial (Equation (5.14)).

5.3.10 Definition. If $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are graphs on disjoint sets of vertices, their *union* is the graph $G_1 + G_2 = (V_1 \cup V_2, E_1 \cup E_2)$.

[*]The chromatic polynomial of a *planar* graph was introduced in 1912 by G. Birkhoff as part of his effort to prove the four-color theorem.

[†]Computing $\chi(G)$ is an NP-complete problem.

If G_1 and G_2 are connected, then $G_1 + G_2$ is a graph with two components, one isomorphic to G_1 and the other isomorphic to G_2.

5.3.11 Theorem. *If $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are graphs on disjoint sets of vertices, then*

$$p(G_1 + G_2, x) = p(G_1, x)p(G_2, x).$$

Proof. The result is an immediate consequence of the definition of $p(G, r)$ and the fundamental counting principle. ■

If G is not connected then, from Theorem 5.3.11,

$$\chi(G) = \max\ \chi(C),$$

where the maximum is over the components C of G.

Since every graph has at least one vertex, no graph can be properly colored with zero colors. The only graphs that can be properly colored with just one color are the graphs with no edges. Thus, $\chi(G) \geq 2$ for any graph with an edge.

5.3.12 Definition. If $\chi(G) \leq 2$, then G is *bipartite*[*].

Suppose G is a bipartite graph with at least one edge. Consider some proper blue–green coloring of G. Let V_b and V_g be the vertices of G that are colored blue and green, respectively. Then $V(G) = V_b \cup V_g$, is the disjoint union of two *parts* such that every edge of G has one vertex in each part. Conversely, if $V(G)$ is the disjoint union of two independent sets of vertices, then G can be properly 2-colored. This explains the name "bipartite". (There may be more than one way to *bipartition* the vertex set of a bipartite graph.)

5.3.13 Definition. Let s and t be positive integers. Suppose X and Y are disjoint sets of s and t elements, respectively. Let $V = X \cup Y$. Then the *complete bipartite graph* $K_{s,t} = (V, E)$, where $E = \{\{x, y\} : x \in X \text{ and } y \in Y\}$.

The complete bipartite graph $K_{2,3}$ is illustrated in Fig. 5.3.3. Observe that $K_{2,3}$ is "maximally bipartite" in the sense that $\chi(G) = 3$ for any graph G that can be obtained from $K_{2,3}$ by adding an edge.

5.3.14 Definition. If G_1 and G_2 are graphs on disjoint sets of vertices, their *join* $G_1 \vee G_2 = (G_1^c + G_2^c)^c$ is the graph obtained from $G_1 + G_2$ by adding new edges from each vertex of G_1 to every vertex of G_2.

[*]In chemical applications of graph theory, bipartite graphs correspond to so-called *alternant* hydrocarbons.

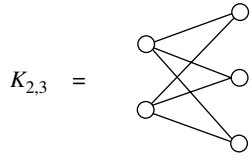


Figure 5.3.3

Observe that the complete bipartite graph $K_{s,t} = K_s^c \vee K_t^c$.
More important than complete bipartite graphs are the "trees".

5.3.15 Definition. Suppose $k \geq 3$. A *cycle* in G of *length* k is a sequence of distinct vertices $\langle v_1, v_2, \ldots, v_k \rangle$ such that $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{k-1}, v_k\}$, and $\{v_k, v_1\}$ are all edges of G. A *tree* is a connected graph that does not have any cycles.

The nonisomorphic trees on six vertices are illustrated in Fig. 5.3.4.

5.3.16 Theorem. *If T is a tree on n vertices, then $p(T, x) = x(x-1)^{n-1}$.*

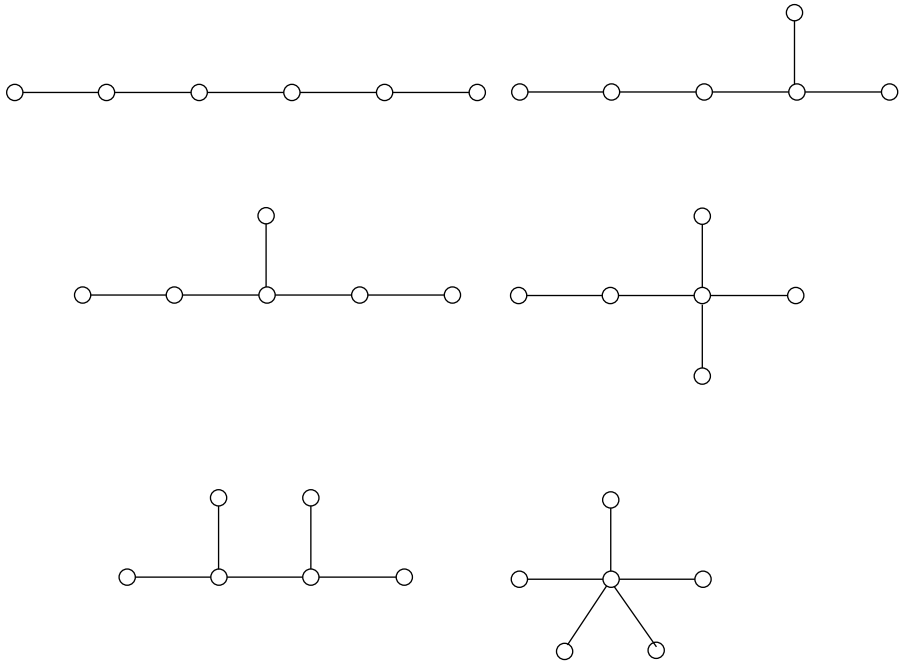
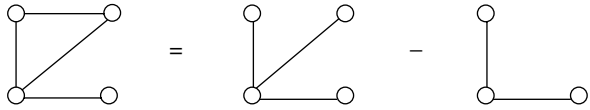


Figure 5.3.4

The first step of Example 5.3.6 resulted in the picturesque equation



Because the graphs on the right-hand side of this equation are both trees, it follows from Theorem 5.3.16 that

$$\begin{aligned} p(G,x) &= x(x-1)^3 - x(x-1)^2 \\ &= x(x-1)^2[(x-1)-1] \\ &= x(x-1)^2(x-2), \end{aligned} \tag{5.15}$$

confirming Equation (5.14) for the graph G of Equation (5.13).

The following will be useful in the proof of Theorem 5.3.16.

5.3.17 Lemma. *Let T be a tree on $n > 1$ vertices. Then T has (at least) two vertices of degree 1.*

Proof. Among all the paths in T there is one of greatest length, say from vertex u to vertex v. If either u or v had degree greater than 1 then, because there are no cycles in T, the path from u to v could be extended. ■

Proof of Theorem 5.3.16. The proof is by induction on n. If $n = 1$, then $p(T,x) = x$ and the proof is complete. So, suppose $n > 1$. Let u be a vertex of T of degree 1 and let e be the unique edge incident with u. Then $T - e$ is a disconnected graph having two components, one the isolated vertex u and the other isomorphic to the tree T/e. By Theorem 5.3.11, $p(T-e,x) = xp(T/e,x)$. Hence, by chromatic reduction (Theorem 5.3.5),

$$\begin{aligned} p(T,x) &= p(T-e,x) - p(T/e,x) \\ &= xp(T/e,x) - p(T/e,x) \\ &= (x-1)p(T/e,x). \end{aligned}$$

Because T/e is a tree on $n-1$ vertices, the induction hypothesis gives $p(T/e,x) = x(x-1)^{n-2}$, and the proof is complete. ■

5.3.18 Corollary. *If T is a tree on $n > 1$ vertices then $\chi(T) = 2$. So, every tree is a bipartite graph.*

Proof. While the corollary is an immediate consequence of Theorem 5.3.16, a direct proof affords some additional insight. Let u be a fixed but arbitrary vertex of T. Let v be some other vertex. Since all trees are connected, there is a path in T from u to v. Indeed, this path must be unique. Otherwise, there would be a cycle in T. Define the distance (in T) from u to v to be the length of this unique path. Color vertex u blue. Color vertex v blue if the distance from u to v is even, and color it green if the distance is odd.

If this scheme results in adjacent vertices v_1 and v_2 being colored the same, then the path from u that determines the color of v_2 could not pass through v_1. But, that means there are two paths from u to v_2, one that passes through v_1, and one that does not. Hence, v_1 and v_2 lie on a cycle of T, contradicting the definition of a tree. ■

The notion of distance used in the proof of Corollary 5.3.18 can be extended.

5.3.19 Definition. Let $G = (V, E)$ be a connected graph. Suppose $u, w \in V$. If $u = w$, the *distance* $d(u, w) = 0$. If $u \neq w$, then $d(u, w)$ is the length of a shortest path in G from u to w. The *diameter* of G is

$$\max_{u,w \in V} d(u, w).$$

Using this notion of distance, the parity proof of Corollary 5.3.18 can be extended to obtain the following characterization of bipartite graphs.

5.3.20 Theorem. *Let G be a graph. Then G is bipartite if and only if it contains no cycles of odd length.*

Proof. It is easy to see that a cycle of odd length cannot be colored using two colors. Conversely, because of Theorem 5.3.11, it suffices to prove the theorem when G is connected. Let u be a fixed but arbitrary vertex of G. Color u blue. If $v \in V(G)$, color v blue if $d(u, v)$ is even and color it green if $d(u, v)$ is odd. Because G has no cycles of odd length, the result is a proper 2-coloring. ■

We now return to the general study of chromatic polynomials.

5.3.21 Definition. Let $G_1 = (V, E)$ and $G_2 = (W, F)$ be graphs on disjoint sets of vertices. Suppose $\{u_1, u_2, \ldots, u_t\}$ and $\{w_1, w_2, \ldots, w_t\}$ induce (t-vertex) cliques in G_1 and G_2, respectively. Let G be the graph obtained from $G_1 + G_2$ by identifying u_i with w_i, $1 \leq i \leq t$. Then G is an *overlap of G_1 and G_2 in K_t*.

5.3.22 Example. Graphs G and H in Figure 5.3.5 are two (nonisomorphic) overlaps of G_1 and G_2 in K_4. They can also be viewed as overlaps of G_1 and K_3 in K_2. □

5.3.23 Theorem. *If G is an overlap of G_1 and G_2 in K_t, then $p(G, x) = p(G_1, x)p(G_2, x)/x^{(t)}$.*

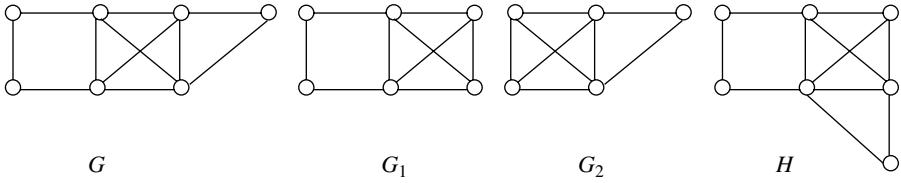


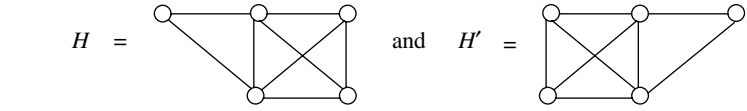
Figure 5.3.5

Proof. If r colors are available, the vertices of the overlapping clique can be colored properly in $r^{(t)}$ ways. Evidently, the remaining vertices of G_1 can then be colored properly in $p(G_1, r)/r^{(t)}$ ways. Similarly (and independently), the remaining vertices of G_2 can then be colored properly in $p(G_2, r)/r^{(t)}$ ways. So, by the fundamental counting principle,

$$p(G, r) = r^{(t)} \times \frac{p(G_1, r)}{r^{(t)}} \times \frac{p(G_2, r)}{r^{(t)}}.$$

The result now follows from the fact that the polynomial identity $r^{(t)}p(G, r) = p(G_1, r)p(G_2, r)$ holds for infinitely many positive integers r. ■

5.3.24 Example. The graph G illustrated in Fig. 5.3.6 is an overlap of



in K_4. Because H and H' are isomorphic, they have the same chromatic polynomial. Therefore, from Theorem 5.3.23,

$$p(G, x) = \frac{p(H, x)^2}{x^{(4)}}. \tag{5.16}$$

Because H is the overlap of K_3 and K_4 in K_2, $p(H, x) = x^{(3)}x^{(4)}/x^{(2)} = (x - 2)x^{(4)}$. Substituting this into Equation (5.16) yields

$$\begin{aligned} p(G, x) &= \frac{(x-2)^2 x^{(4)} x^{(4)}}{x^{(4)}} \\ &= x(x-1)(x-2)^3(x-3). \end{aligned}$$

□

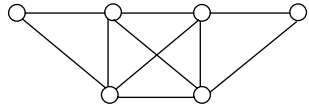
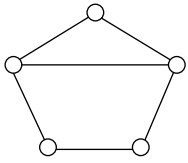
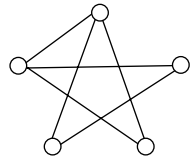


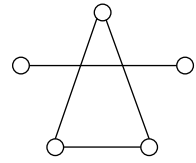
Figure 5.3.6

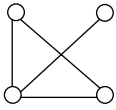
5.3. EXERCISES

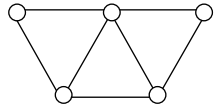
1 Compute the chromatic polynomial of

(a) 

(b) 

(c) 

(d) 

(e) 

2 Compute the chromatic polynomials for the 11 nonisomorphic graphs on four vertices.

3 Let G be the *wheel* illustrated in Fig. 5.3.7. Compute the

(a) chromatic number of G.

(b) chromatic polynomial of G.

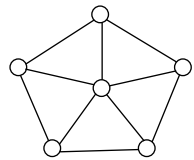


Figure 5.3.7

4 The coefficients of $p(G,x)$ are known to alternate in sign. (See Exercise 28, below.) Confirm this fact

(a) when $G = K_n$. **(b)** when G is a tree.

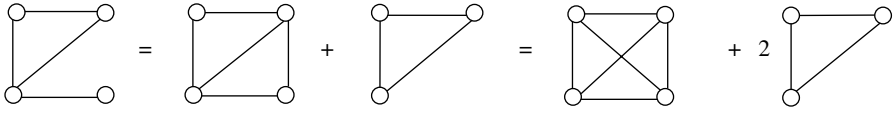
5 Among the most famous open problems for chromatic polynomials is the following conjecture of R. C. Read: If $p(G,x) = x^n - b_1x^{n-1} + b_2x^{n-2} - \cdots$, then the sequence $b_1, b_2, \ldots$ is *unimodal*, i.e., there is an integer k, depending on G, such that $b_1 \leq b_2 \leq \cdots \leq b_k$ and $b_k \geq b_{k+1} \geq \cdots$. Confirm Read's conjecture

(a) if G is a tree. **(b)** for $p(K_n,x)$, $3 \leq n \leq 8$.

6 In modern telecasts of National Football League games, one frequently has an opportunity to examine important plays from "the reverse angle". Let's look at chromatic reduction from the reverse angle, i.e., expressed in the

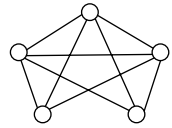
form $p(H,x) = p(H+e,x) + p(H/e,x)$, where $H+e$ is obtained from H by adding in a new edge $e = \{u,v\}$ that was not there before, and H/e is obtained from H by identifying vertices u and v (and deleting superfluous edges).

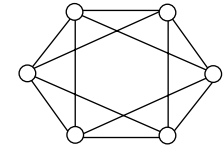
(a) Show that the followign picturesque example of this reverse-angle approach produces the same answer as Example 5.3.6:



(b) If G is a graph on n vertices, prove that $p(G,x)$ is a linear combination of the falling factorial functions $x^{(k)}$, $k \le n$, with nonnegative integer coefficients.

7 Use the reverse-angle technique of Exercise 6 to compute the chromatic polynomial of

(a) 

(b) 

8 Prove that x^2 is a factor of $p(G,x)$ whenever G is disconnected. (The converse turns out to be true as well.)

9 Denote by C_n the graph with n vertices, n edges, and a single cycle of length n. Then $C_3 = K_3$, C_4 is the square, C_5 is the pentagon, etc.

(a) Draw suitable pictures, using dark and light vertices, to show that C_4 and C_6 are bipartite.

(b) Use the chromatic polynomials of C_4 and C_6 to prove that they are bipartite.

(c) Prove that $p(C_n,x) = (x-1)^n + (-1)^n(x-1)$.

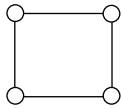
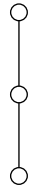
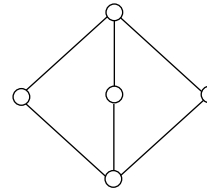
(d) Use part (c) to prove that C_n is bipartite if and only if n is even.

10 The *path* P_n is the unique tree on n vertices with diameter $n-1$. The *clique number* $\omega(G)$ is the maximum value of t such that K_t is an induced subgraph of G. Evidently, $\chi(G) \ge \omega(G)$. Curiously enough, if G does not contain an induced subgraph isomorphic to P_4, then $\chi(G) = \omega(G)$.

(a) Show that $\chi(C_5) > \omega(C_5)$. (*Hint*: Exercise 9.)

(b) Show that $\chi(P_4) = \omega(P_4)$.

11 Consider the graphs

C_4 =  , P_3 =  , and G =  .

(a) Explain how G might be viewed as an "overlap of two copies of C_4 in P_3."

(b) *Without* computing $p(G,x)$, show that it could not possible equal $f(x) = p(C_4,x)^2/p(P_3,x)$.

12 In 1941, R. L. Brooks proved that if G is neither an odd cycle nor a complete graph, then $\chi(G) \leq d_1$, the largest vertex degree of G. Confirm that the

(a) inequality fails for C_5. (See Exercise 9.)

(b) inequality fails for K_4.

(c) theorem is valid for C_4.

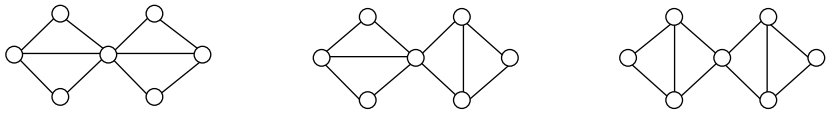
(d) theorem is valid for any tree on $n \geq 3$ vertices.

13 Let G be a graph with n vertices, m edges, and chromatic polynomial $p(G,x) = x^n - b_1x^{n-1} + \cdots$. Prove that $b_1 = m$.

14 Let G_1 and G_2 be graphs on disjoint sets of n_1 and n_2 vertices, respectively. A *coalescence* of G_1 and G_2 is any graph on $n_1 + n_2 - 1$ vertices that can be obtained from $G_1 + G_2$ by identifying (coalescing into a single vertex) some vertex of G_1 with any vertex of G_2. Let $G_1 * G_2$ be one of the n_1n_2 different coalescences of G_1 and G_2.

(a) Prove that $p(G_1 * G_2,x) = p(G_1,x)p(G_2,x)/x$.

(b) Without actually computing them, prove that the chromatic polynomials of the three graphs in Fig. 5.3.8 are all the same.



G_1 G_2 G_3

Figure 5.3.8

15 Prove that the chromatic polynomials of the four graphs in Fig. 5.3.9 are all the same.

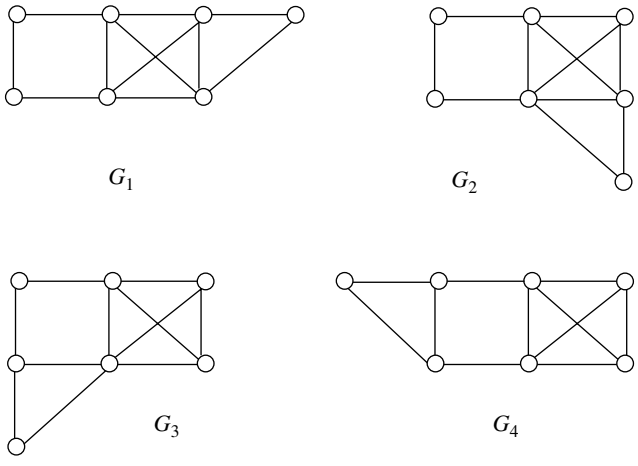


Figure 5.3.9

16 Suppose $f(x)$ and $g(x)$ are defined in terms of falling factorial functions by

$$f(x) = \sum_{i=0}^{r} a_i x^{(i)} \quad \text{and} \quad g(x) = \sum_{j=0}^{s} b_j x^{(j)}.$$

Define the *join-product* of $f(x)$ and $g(x)$ by

$$f(x) \vee g(x) = \sum_{k=0}^{r+s} \left(\sum_{t=0}^{k} a_t b_{k-t} \right) x^{(k)}.$$

Then, e.g., $(x^{(3)} + x^{(2)}) \vee (x^{(4)} + 2x^{(3)} + x^{(2)}) = x^{(7)} + 3x^{(6)} + 3x^{(5)} + x^{(4)}$. So, the join-product of linear combinations of falling factorial functions $x^{(k)}$ behaves like an ordinary product of linear combinations of ordinary powers of x. It turns out that the chromatic polynomial of a join of two graphs is just the join-product of their chromatic polynomial, i.e., $p(G_1 \vee G_2, x) = p(G_1, x) \vee p(G_2, x)$. This is, of course, a useful observation only if $p(G_1, x)$ and $p(G_2, x)$ are expressed in terms of falling factorial functions, as in Exercise 6(b).

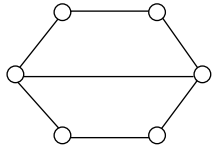
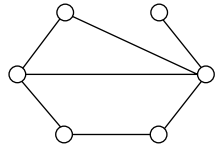
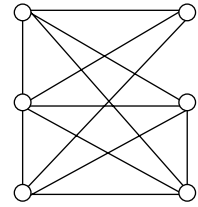
(a) Use the join-product approach to show that $p(K_{1,2} \vee C_4, x) = x(x-1) \times (x-2)(x-3)(x^3 - 12x^2 + 50x - 71)$. (*Hint:* The complete bipartite graph $K_{1,2}$ is a tree on three vertices, and C_4 is a square.)

(b) Prove the formula $p(G_1 \vee G_2, x) = p(G_1, x) \vee p(G_2, x)$. (*Hint:* Use the reverse-angle approach of Exercise 6 on the part of $G_1 \vee G_2$ that used to be G_2; note that $K_r \vee K_s = K_{r+s}$.)

17 Use the join-product formula of Exercise 16 to express the chromatic polynomial of the following graph as a linear combination of falling factorial functions:

(a) $K_{1,3}$. **(b)** $K_{2,3}$. **(c)** $K_{3,3}$. **(d)** $K_{4,3}$.

18 Compute the chromatic polynomial of

(a)  **(b)**  **(c)** 

19 Let G be a graph. Prove or disprove that

(a) all roots of $p(G,x)$ are real.

(b) all positive roots of $p(G,x)$ are integers.

(c) all real roots of $p(G,x)$ are positive.

20 Suppose $T = (V,E)$ is a tree on n vertices. Prove that T has $n-1$ edges.

21 Prove that $f(x) = x^6 - 12x^5 + 54x^4 - 112x^3 + 105x^2 - 36x$ is not the chromatic polynomial of a graph.

22 Let $G = (V,E)$ be a graph with n vertices and m edges. Suppose $e = \{u,v\} \in E$. To *subdivide* e means, informally, to put a new vertex in the middle of e. Of course, adding a vertex changes the graph. Let $H = (W,F)$ be the new graph. Then $W = V \cup \{w\}$, where $w \notin V$; and $F = (E \setminus \{e\}) \cup \{\{u,w\},\{w,v\}\}$ is the set obtained from E by replacing $\{u,v\}$ with new edges $\{u,w\}$ and $\{w,v\}$. (Note, e.g., that $d_H(w) = 2$.) If every edge of G is subdivided, the resulting graph $S(G)$ has $n+m$ vertices and $2m$ edges. Prove, for any graph G, that $S(G)$ is bipartite.

23 Let t_n be the number of nonisomorphic trees on n vertices.

(a) Prove that $t_4 = 2$.

(b) Illustrate three nonisomorphic trees on five vertices, explaining how you can be sure that they are nonisomorphic.

(c) Illustrate the $t_7 = 11$ nonisomorphic trees on seven vertices.

24 A cycle of length n in a graph on n vertices is called a *Hamiltonian cycle*. A graph is *Hamiltonian* if it has a Hamiltonian cycle.

(a) Illustrate the three nonisomorphic Hamiltonian graphs on four vertices.

(b) Illustrate the two nonisomorphic Hamiltonian graphs having five vertices and no more than six edges.

(c) Illustrate the two nonisomorphic Hamiltonian graphs having five vertices and seven edges.

(d) Prove that the existence of a Hamiltonian cycle is an invariant.

(e) Find two Hamiltonian cycles in K_5 that, between them, contain all 10 edges of K_5.

(f) Find three Hamiltonian cycles in K_7 that, between them, contain all 21 edges of K_7.

25 In how many ways can the faces of a cube be colored, using r colors, so that any two faces that share an edge are colored differently?

26 If $p(G,x) = x^n - b_1x^{n-1} + \cdots + (-1)^{n-1}b_{n-1}x$, then G is both connected and bipartite if and only if b_{n-1} is odd. Use this criterion to prove that

(a) every tree is bipartite.

(b) C_n is bipartite if and only if n is even. (*Hint*: Exercise 9(c).)

27 Consider the following recursive construction of a family of graphs called 2-*trees*: (1) The smallest 2-tree is K_2; (2) if $e = \{u, v\}$ is an edge of a 2-tree G, on n vertices, then the graph obtained from G by adding a new vertex w and two new edges $\{u, w\}$ and $\{v, w\}$ is a 2-tree on $n+1$ vertices. (Up to isomorphism, K_3 is the only 2-tree on three vertices, and $K_4 - e$ is the unique 2-tree on four vertices.)

(a) Find the two nonisomorphic 2-trees on five vertices.

(b) Find the five nonisomorphic 2-trees on six vertices.

(c) If G is a 2-tree on n vertices, prove that its chromatic polynomial is $p(G,x) = x(x-1)(x-2)^{n-2}$. (E. G. Whitehead has proved the converse, i.e., if $p(G,x) = x(x-1)(x-2)^{n-2}$, then G is a 2-tree.)

28 Let G be a graph with n vertices and c connected components. Prove that

(a) $p(G,x) = x^n - b_1x^{n-1} + b_2x^{n-2} - \cdots + (-1)^{n-c}b_{n-c}x^c$, i.e., prove that $b_k = 0$ for all $k > n - c$.

(b) $b_1, b_2, \ldots, b_{n-c}$ are positive integers, i.e., the coefficients of $p(G,x)$ alternate in sign. (*Hint*: Induction on the number of edges.)

29 Prove that $p(G,t) = 0$ for all $t \in (0,1)$.

30 Let $G = (V,E)$ be a connected graph. If $u, v, w \in V$, show that the distance from u to w satisfies

(a) $d(u,w)$ is a nonnegative integer.

(b) $d(u,w) \geq 0$, with equality if and only if $u = w$.

(c) $d(u,w) = d(w,u)$.

(d) $d(u,w) \leq d(u,v) + d(v,w)$.

31 Let $s \geq 2$ be an integer. Suppose T is a fixed but arbitrary three on $t \geq 2$ vertices. Let N be the smallest integer such that any graph G on N vertices contains an s-vertex clique or a subgraph isomorphic to T.

(a) Prove that $N \geq (s-1)(t-1)+1$.

(b) Prove that $N \leq (s-1)(t-1)+1$.

32 Let $G=(V,E)$ be a graph with vertex set $V=\{v_1, v_2 \ldots, v_n\}$. Suppose the set of colors is $C=\{x_1, x_2, \ldots, x_r\}$. The *Stanley polynomial* $\mathscr{S}(G,r) = \sum x_{f(v_1)}x_{f(v_2)}\cdots x_{f(v_r)}$, where the sum is over all proper colorings $f : V \to C$.

(a) Show that $\mathscr{S}(P_3,3) = M_{[2,1]}(x_1,x_2,x_3) + 6M_{[1^3]}(x_1,x_2,x_3)$, where P_3 is the unique three-vertex tree.

(b) Show that substituting $x_1 = x_2 = \cdots = x_r = 1$ in $\mathscr{S}(G,r)$ produces $p(G,r)$.

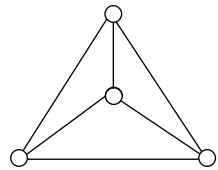
*5.4. PLANAR GRAPHS

> What you call Solid things are really superficial; what you call Space is really nothing but a great Plane.
>
> — The Stranger (from E. A. Abbott's *Flatland*)

As we have seen, illustrating graphs by points and lines can be misleading. An arc representing an edge consists of infinitely many geometric points but only two vertics. In depictions of graphs, it is not unusual for arcs representing nonadjacent edges to cross. While the edges, themselves, do not intersect, their representing arcs do. This raises the question of whether it is possible to draw pictures of graphs with no edge crossings. Evidently (see Fig. 5.4.1), it is possible to draw K_4 with no edge crossings, but what about K_5?

Provided there is enough space, it is always possible to draw a graph, any graph, without edge crossings. Represent the n vertices of G by the points $1, 2, \ldots, n$ along the x-axis in three-dimensional Euclidean space. Take m different planes that intersect in the x-axis, and draw one edge of G in each of them.

What about two-dimensional space? Which graphs can be drawn in the plane with no edge crossings? This is a much more interesting question, not because the answer has any great significance, but because the search for answers has led to some good mathematics.



K_4

Figure 5.4.1

5.4.1 Definition. A graph is *planar* if it can be illustrated in the plane in such a way that arcs representing edges do not meet except in points representing vertices.

Less formally, G is planar if it can be drawn in the plane with no edge crossings. We will refer to such a drawing as a *plane graph*. So, the phrase "plane graph" means a specific plane illustration of some (necessarily planar) graph.

Any discussion of plane graphs leads, sooner or later, to the notion of a "region". Imagine a plane graph as if it were a network of fences viewed from above. The vertices of the graph correspond to posts and its edges to fencing. From this perspective, a typical plane graph divides two-dimensional space into pastures, or regions, all but one of which is bounded.* It is natural to wonder how the number r of regions might vary among different plane illustrations of the same planar graph G. Somewhat surprisingly, $r = r(G)$ is the same for *all* plane representations of G.

5.4.2 Theorem (Euler's Formula). *If G is a plane graph with n vertices, m edges, c components, and r regions, then $r = c + m - n + 1$.*

Proof. The proof is by induction on m. If $m = 0$, then $G = K_n^c$ is a disconnected graph consisting of $c = n$ components each of which is an isolated vertex. In this case, $c + m - n + 1 = n + 0 - n + 1 = 1$. Since there is just one (unbounded) region, the $m = 0$ case is established.

Assume the theorem is true for every plane graph having $k \geq 0$ edges. Let G be a plane graph with $k + 1$ edges, and suppose e is one of them. Now, it may happen that e is part of the boundary separating two different regions. If so, then e lies on a cycle of G, in which case $G - e$ is a plane graph having the same numbers of vertices and components as G, but one fewer edge and one fewer region. Applying the induction hypothesis to $G - e$, we obtain $r - 1 = c + (m - 1) - n + 1$, and the proof is finished.

If the same region lies on both sides of e, then $G - e$ is a plane graph having the same numbers of vertices and regions as G, but one fewer edge and one more component. Applying the induction hypothesis to $G - e$ produces $r = (c + 1) + (m - 1) - n + 1 = c + m - n + 1$. ■

In the special case that G is a *connected* plane graph, Euler's formula is equivalent to

$$r + n = m + 2. \tag{5.17}$$

The Flemish cartographer Gerhard Mercator (1512–1594) is generally credited with inventing the technique of map making in which the meridians (lines of longitude) are drawn parallel to each other; perpendicular to these, the parallels of

*The regions might also be described as the connected components of what is left of the plane after the drawing of the graph has been etched away, i.e., the components of the complement of the plane graph.

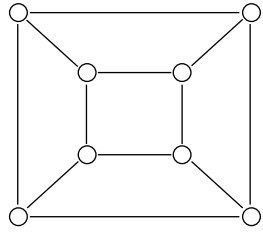


Figure 5.4.2. Plane map of a cube.

latitude are represented by straight lines whose distance from each other increases with the distance from the equator. Regardless of the exact details, a *Mercator projection* produces a plane map of the spherical Earth. The same sort of thing can be done with any convex polyhedron. Figure 5.4.2 illustrates a plane map of a cube. Note that, just as Greenland appears comparable in size to South America on a typical plane map of the world, our plane map of the cube distorts the square faces. Indeed, one of the six faces actually becomes unbounded.

In a similar way, any convex polyhedron can be represented by a plane graph in which the vertices, edges, and faces of the polyhedron correspond, respectively, to the vertices, edges, and regions of the graph. It follows from Equation (5.17) that there is a relationship between the numbers F of faces, V of vertices, and E of edges of any convex polyhedron, namely,

$$F + V = E + 2. \tag{5.18}$$

5.4.3 Corollary. *Let G be a planar graph with m edges and n vertices. Then*

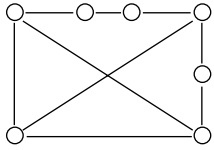
$$m \leq 3n - 6. \tag{5.19}$$

Proof. If G is a plane graph, it may happen that some nonadjacent pair of vertices of G can be joined by a new edge e that does not cross any of the existing edges of G, i.e., maybe $G + e$ is still a plane graph. Assume that a maximum of k such edges can be added to G. Call the resulting plane graph H. Then H has n vertices and $m + k$ edges. The proof will be completed by showing that $m + k = 3n - 6$.

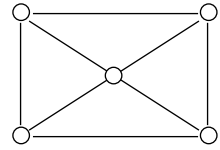
Clearly, H is connected, otherwise more edges could be added without destroying planarity. If the cycle bounding some region of H contained four or more edges, then another edge could be added to H. Thus, the boundary cycles of the regions of H all have length 3. Let $r(H)$ be the number of regions of H. Then, counting the edges that bound each region, we obtain the formula $2(m + k) = 3r(H)$. Substituting in Euler's formula (applied to H) yields $\frac{2}{3}(m + k) = (m + k) - n + 2$. ■

The complete graph K_5 has $n = 5$ vertices and $m = 10$ edges; if K_5 were planar, it would follow from Corollary 5.4.3 that $10 \leq 15 - 6$.

Not surprisingly, strengthening the hypothesis of Corollary 5.4.3 also strengthens its conclusion.



(*a*)



(*b*)

Figure 5.4.3

5.4.4 Corollary. *Let G be a bipartite planar graph with m edges and $n > 2$ vertices. Then*

$$m \leq 2n - 4. \tag{5.20}$$

The proof is similar. By Theorem 5.3.20, G has no odd cycles. So, this time, the minimal cycle length is 4, and it follows that $2m \geq 4r$. Together with Euler's formula, this implies that $\frac{1}{2}m \geq m - n + 2$. ■

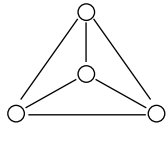
Because the complete bipartite graph $K_{3,3}$ has $n = 6$ vertices and $m = 9$ edges, if $K_{3,3}$ were planar, it would follow from Corollary 5.4.4 that $9 \leq 12 - 4$.

If G contains a nonplanar subgraph then G, itself, cannot be planar. Thus, any graph that contains a subgraph isomorphic to K_5 or to $K_{3,3}$ cannot be planar. In 1930, Kasimir Kuratowski proved a kind of converse, the statement of which involves a new idea.

Let $G = (V, E)$ be a graph with n vertices and m edges, of which $e = \{u, v\}$ is one. To *subdivide e* means, informally, to put a new vertex of degree 2 in the middle of e. If H is the new graph, then $V(H) = V \cup \{w\}$, where $w \notin V$, and $E(H) = (E \backslash \{e\}) \cup \{\{u, w\}, \{w, v\}\}$. A *subdivision* of G is any graph that can be "constructed" from G by subdividing edges. The graph in Fig. 5.4.3*a*, for example, is a subdivision of K_4; the graph in Fig. 5.4.3*b* is not.

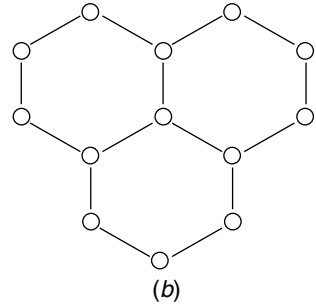
5.4.5 Definition. Graphs G_1 and G_2 are *homeomorphic* if they have isomorphic subdivisions.

Informally, "homeomorphic" might be thought of as "isomorphic to within vertices of degree 2". In particular, any graph is homeomorphic to all of its subdivisions. The graph in Fig. 5.4.4*b* is homeomorphic to the complete graph K_4 illustrated in Fig. 5.4.4*a*.



K_4

(*a*)



(*b*)

Figure 5.4.4

5.4.6 Kuratowski's Theorem. *If G is not planar, then G has a subgraph homeomorphic to K_5 or to $K_{3,3}$.*

The proof of Kuratowski's theorem is beyond the scope of this text.

Almost from its inception, the study of planar graphs has been associated with coloring problems. The following technical result is useful in this regard.

5.4.7 Lemma. *Let G be a planar graph with m edges, n vertices, and minimum vertex degree d_n. Then $d_n \leq 5$.*

Proof. If $d_n \geq 6$, then $2m = \sum d(v) \geq 6n$, contradicting Inequality (5.19). ■

5.4.8 Five-Color Theorem. *If G is a planar graph, then $\chi(G) \leq 5$.*

Proof. The proof is by induction on the number of vertices of G. Since five colors suffice to properly color any graph on $n \leq 5$ vertices, planar or not, the induction is off to a good start. Let us take as our induction hypothesis that $\chi(H) \leq 5$ for every plane graph H on k vertices. Let G be a plane graph on $n = k + 1$ vertices. By Lemma 5.4.7, G has a vertex u of degree at most 5. Let H be the (plane) subgraph of G obtained by deleting vertex u and all the edges incident with it. By the induction hypothesis, $\chi(H) \leq 5$. If $\chi(H) < 5$, then we can "lift" a four-coloring of H to G and have a fifth color left over for u. So, we may assume $\chi(H) = 5$.

Suppose H to be properly 5-colored. If $d_G(u) < 5$ then, lifting the 5-coloring of H to G leaves a color available for u, i.e., the 5-coloring of H can be extended to a 5-coloring of G. Thus, we proceed under the assumption that $d_G(u) = 5$.

Figure 5.4.5 illustrates u and its five neighbors in the plane graph G. If it happens that some two of $v_1, v_2, \ldots, v_5$ are colored the same in H, then the 5-coloring of H can be extended to G. So, we come at last to the hard case in which vertex v_i is colored c_i, $1 \leq i \leq 5$, and these colors are all different.

Suppose there is a path in H from v_1 to v_3, the vertices of which are alternately colored c_1 and c_3. Adjoining the path $[v_3, u, v_1]$ results in a cycle. Either v_2 is inside this cycle (as shown in Fig. 5.4.6), or v_2 is outside and v_4 and v_5 are inside. Either

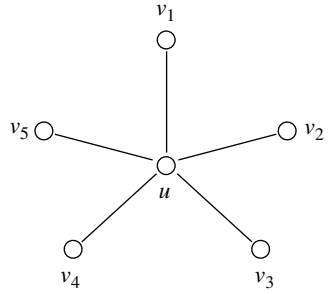


Figure 5.4.5

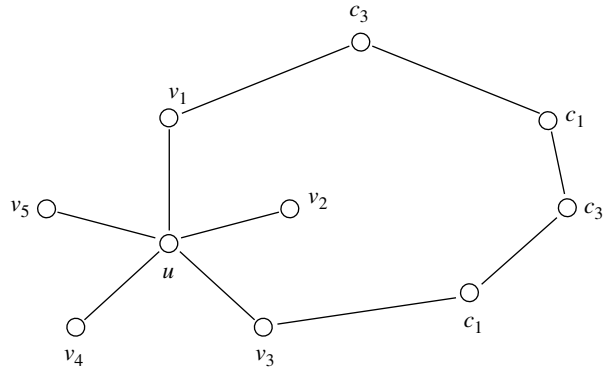


Figure 5.4.6

way, there could not exist a path in H from v_2 to v_4, the vertices of which are alternately colored c_2 and c_4. (A path in H from v_2 to v_4 is a path in the plane graph G, so it cannot cross any of the edges of our cycle. Because the colors are wrong, neither can it pass through a vertex of the cycle.) We deduce that there does not exist an alternating c_1–c_3 path in H from v_1 to v_3, or there does not exist an alternating c_2–c_4 path in H from v_2 to v_4. As these two cases are equivalent, we may as well assume there does not exist an alternating c_1–c_3 path in H from v_1 to v_3.

Perhaps no vertex of H is both adjacent to v_1 and colored c_3. If so, we can change the color of v_1 from c_1 to c_3, freeing up color c_1 for u. The rest of the proof is an extension of this idea.

Let W be the set of all those vertices $w \in V(H)$ such that there is an alternating c_1–c_3 path in H from v_1 to w. (We are working under the assumption that $v_3 \notin W$.) Observe that if $v \in V(H)$ is colored either c_1 or c_3, and if v is adjacent to a vertex of W, then $v \in W$. Put another way, if $v \notin W$, but v is adjacent to some vertex in W, then v is not colored c_1 or c_3. Consequently, if we interchange the colors of the vertices in W, the result is a new proper 5-coloring of H, one in which both v_1 and v_3 are colored c_3. This frees up c_1 for u. ■

Reviewing the proof of the five-color theorem, one cannot help but be struck by the uselessness of v_5. It seems there ought to be a way to eliminate v_5 and prove the following.

5.4.9 Four-Color Theorem. *If G is a planar graph, then $\chi(G) \leq 4$.*

The earliest surviving reference to the *four-color problem* dates to the 1850s when Francis Guthrie mentioned it to his brother, Frederick, who happened to be a student of Augustus de Morgan. In an 1852 letter, de Morgan shared the problem with William Rowan Hamilton (who is known for many things, among them the Cayley–Hamilton theorem of linear algebra). By 1879, the problem had been widely circulated. In that year, the journal *Nature* announced that the four-color

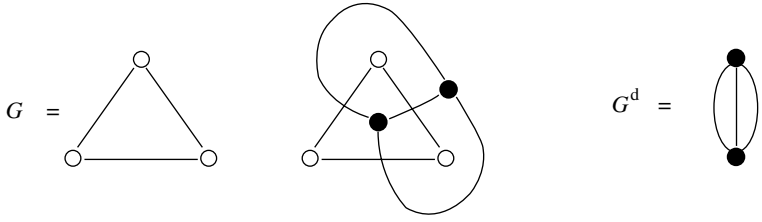


Figure 5.4.7

theorem had been proved by Alfred Kempe. It wans't until 1890 that Percy Heawood discovered an error in Kempe's proof. While he could not fix the mistake, Heawood was able to prove Theorem 5.4.8. Finally, in 1976, the four-color theorem was established by Kenneth Appel and Wolfgang Haken. Appel and Haken used more than 1000 hours of computer time to sort through a large number of cases. Their work is frequently cited in philosophical discussions about the nature of mathematical proof.

The original four-color problem was stated in terms of properly coloring the *regions* of a plane graph. The connection between coloring regions and coloring vertices is via the notion of a geometric dual. If G is a plane graph with vertex set $V(G) = \{v_1, v_2, \ldots, v_n\}$, edge set $E(G) = \{e_1, e_2, \ldots, e_m\}$, and "region set" $R(G) = \{f_1, f_2, \ldots, f_r\}$, then $R(G) = V(G^{\mathrm{d}})$ is the vertex set of its *dual*, G^{d}. Vertices f_i and f_j are adjacent in G^{d} if and only if regions f_i and f_j share an edge in G. Thus, there is a natural one-to-one correspondence between the edges of G^{d}; and the edges of G. If $e \in E(G)$, then e bounds two (not necessarily different) regions of G, say f_i and f_j. The edge of G^{d} corresponding to e is $\{f_i, f_j\}$.

5.4.10 Example. It is frequently convenient to draw G^{d} right on top of G. In such illustrations, a vertex of G^{d} is placed in every region of G, and every edge of G is crossed by exactly one edge of G^{d}. The situation for $G = K_3$ is illustrated in Fig. 5.4.7. The bad news is that G^{d} can be a multigraph. In fact, there is more bad news. As illustrated in Fig. 5.4.8, the dual may even be a *pseudograph*, containing *loops* as well as multiple edges. (A loop is an "edge" from a vertex to itself.)

□

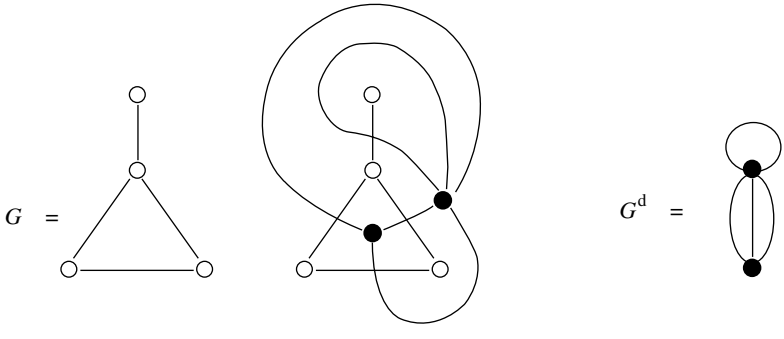


Figure 5.4.8

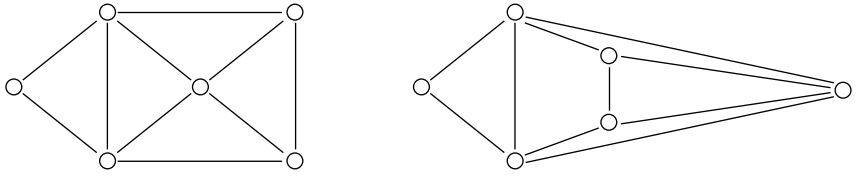


Figure 5.4.9. Isomorphic plane graphs with nonisomorphic duals.

5.4.11 Example. There is even more bad news. The plane graphs in Fig. 5.4.9 are isomorphic, but their dual multigraphs are not! □

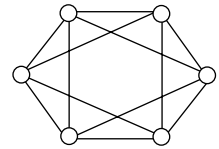
Despite these complications, every dual pseudograph G^{d} has a unique underlying graph G_{d} and $\chi(G^{\mathrm{d}}) = \chi(G_{\mathrm{d}})$. Thus, coloring regions of G is the same as coloring vertices of G_{d}. Because G_{d} is also planar, Theorem 5.4.9 solves the original four-color problem.

5.4. EXERCISES

1 Prove that every tree is a planar graph.

2 Use Equation (5.17) and Exercise 1 to prove that every tree on n vertices has $m = n - 1$ edges. (Compare with Exercise 20, Section 5.3.)

3 In 1936, K. Wagner proved that every planar graph has a plane illustration in which each edge is represented by a *straight* line segment.* Draw such a plane illustration of

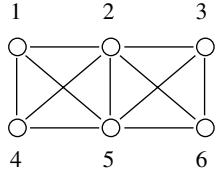
(a) $K_5 - e$. **(b)** $K_{3,3} - e$. **(c)** G =  .

4 In 1990, chemists synthesized the first *fullerene*, a molecule C_{60} consisting of 60 carbon atoms—and nothing else. This third form of carbon (the first two begin graphite and diamond) had been predicted by R. Buckminster Fuller. Less expected were C_{70}, C_{76}, C_{84}, C_{90}, and C_{94}, all of which had been produced by 1992. Every one of these higher fullerenes takes the shape of a convex polyhedron each of whose faces is either a pentagon or a hexagon. Prove that, for any such structure, the number of pentagonal faces is exactly 12 (*Hint*: Each vertex has degree 3.)

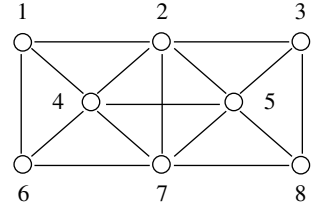
*Wagner's paper, "Bemerkungen zum Vierfarbenproblem," appeared in *Jahresberichte D. M. V.* 46 (1936), 26–32. The result was also discovered by I. Fary, On straight line representation of planar graphs, *Acta. Sci. Math. Szeged Univ.* 11 (1948), 229–233.

5 Redraw each of the following as a plane graph. (Number the vertices of your drawings to exhibit an isomorphism with the original graph.)

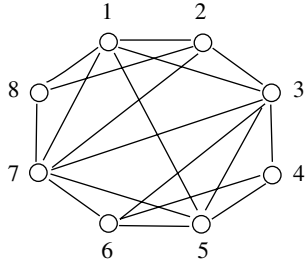
(a)



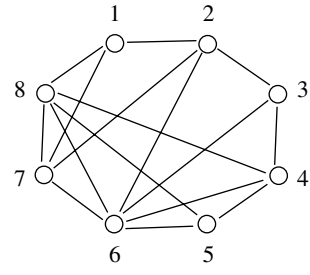
(b)



(c)



(d)



6 Let G be the graph in Fig. 5.4.10.

(a) Prove directly, without using the four-color theorem, that $\chi(G) = 4$.

(b) Prove that G is planar by redrawing it as a plane graph. (Number the vertices of your drawing so as to exhibit an isomorphism with G.)

(c) Prove that Lemma 5.4.7 cannot be strengthened to the following: If G is a planar graph on n vertices, then $d_n \leq 4$.

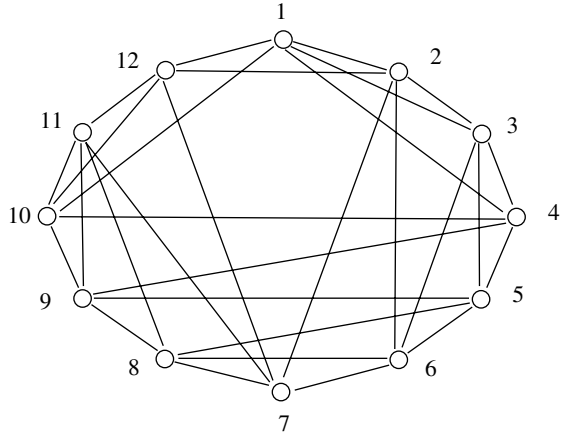


Figure 5.4.10

7 Prove or disprove the converse of the four-color theorem.

8 What is the smallest number of edges among planar graphs of chromatic number 4?

9 Let $G = C_4 \vee P_3$, the join of the square and the tree of Fig. 5.4.11. Is G planar? Justify your answer.

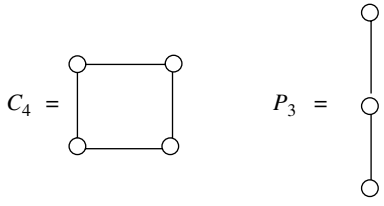


Figure 5.4.11

10 The graph G in Fig. 5.4.12 is the Petersen graph from Example 5.1.7. Prove that it is not planar by illustrating a subgraph of G that is homeomorphic to $K_{3,3}$. (*Hint*: G will not be an induced subgraph.)

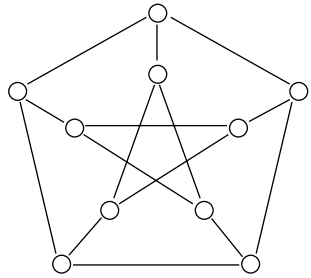


Figure 5.4.12

11 Prove that any planar graph on $n \geq 2$ vertices has *two* vertices of degree at most 5.

12 Let G be a graph on $n > 10$ vertices. Prove that G and G^c cannot both be planar.

13 Let G be a plane projection of a cube (illustrated in Fig. 5.4.2).

(a) Show that $G^d = G_d$. (In other words, show that the dual pseudograph of G is, in fact, a graph.)

(b) It turns out that G^d can be drawn so that it is a plane projection of another regular polyhedron. Which one?

14 Let G be a plane graph and consider G^{dd} the dual of G^d.

(a) If G is connected, prove that G^{dd} is isomorphic to G.

(b) Illustrate G^{dd} for the graph G having two components each of which is isomorphic to K_3.

15 Let G and H be the plane graphs in Fig. 5.4.9.

(a) Prove that G and H are isomorphic.

(b) Show that G^{d} and H^{d} are not isomorphic.

(c) Prove that G_{d} and H_{d} are isomorphic.

16 Let G be the plane graph obtained by projecting a regular tetrahedron (pyramid with a triangular base) onto the plane of its base.

(a) Prove that G is isomorphic to K_4.

(b) Prove that G is isomorphic to G^{d}.

17 Illustrate a graph G that contains a subgraph homeomorphic to K_3 but that satisfies $\chi(G) < 3$.

18 Because K_5 is not planar, it cannot be drawn in the plane without any edge crossings. However, if an over/underpass is erected on the plane, it is then possible to draw K_5 with no edge crossings. (See Fig. 5.4.13.) The minimum number of over/underpasses that are needed to draw a graph with no edge crossings is its *genus*. Thus, planar graphs have genus 0 and K_5 has genus 1.

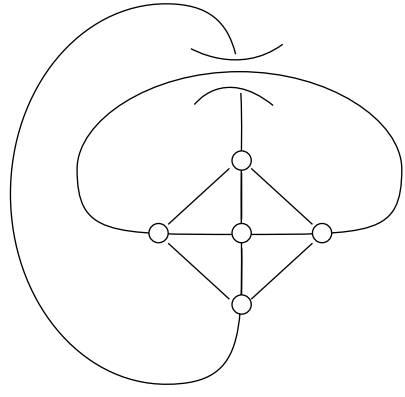


Figure 5.4.13. K_5 with an over/underpass.

(a) Prove that K_6 has genus 1 by drawing it (with no edge crossings) on a plane with one over/underpass.

(b) Prove that $K_{3,3}$ has genus 1.

(c) Prove that $K_{4,4}$ has genus 1.

(d) In 1968, G. Ringel and J. W. Youngs proved that the genus of K_n is $\lceil (n-3)(n-4)/12 \rceil$, where $\lceil x \rceil$ is the smallest integer not less than x. Use this formula to show that K_7 has genus 1.

19 Given a plane graph H, explain why there exists a plane graph G such that $G_{\mathrm{d}} = H$.

20 What does it mean to say that two plane graphs are isomorphic? Give a mathematical definition of *plane graph isomorphism*.

5.5. MATCHING POLYNOMIALS

I find that the harder I work, the more luck I seem to have.

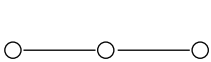
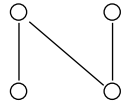
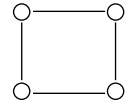
— Thomas Jefferson

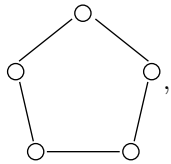
Let's begin by giving formal definitions to two families of graphs that have been encountered several times already.

5.5.1 Definition. Let $V = \{v_1, v_2, \ldots, v_n\}$. The *path* $P_n = (V, E)$, where $E = \{\{v_i, v_{i+1}\} : 1 \le i < n\}$. The *cycle* $C_n = (V, F)$, where $F = E \cup \{\{v_n, v_1\}\}$.

So, P_n is a path of length $n - 1$, and C_n is a cycle of length n.

5.5.2 Example. $P_1 = K_1$, $P_2 = K_2$, $C_3 = K_3$,

P_3 =  , P_4 =  , C_4 =  ,

C_5 =  , and so on. □

Recall that a subset of $V(G)$ is independent if no two of its vertices are incident with the same edge of G. One might naturally suppose that a subset of $E(G)$ is independent if no two of its edges are incident with the same vertex. For historical reasons, independent sets of edges are called matchings.

5.5.3 Definition. Let G be a graph. A *matching* of G is a set of edges, no two of which share a vertex. If $M \subset E(G)$ is a matching, and if $e = \{u, v\} \in M$, then u and v are said to be *matched* vertices, *covered* by M. An *r-matching* is a matching consisting of r edges. The *matching number* $\mu(G)$ is the largest number of edges in any matching of G, i.e., the maximum value of r in any r-matching of G.

A 1-matching is a set consisting of a single edge covering two vertices. A 2-matching is a set of two (nonadjacent) edges covering four vertices. The edges in a 3-matching cover six vertices, and so on. In particular, $\mu(G) \le \frac{1}{2}n$.

5.5.4 Definition. Let G be a graph on n vertices. A *perfect matching*[*] is a $\frac{1}{2}n$-matching, i.e., an r-matching where $2r = n$.

[*]Perfect matchings are sometimes called *Kekulé structures*, after August Kekulé, the chemist who showed that the carbon atoms of a benzene molecule arrange themselves at the vertices of a hexagon.

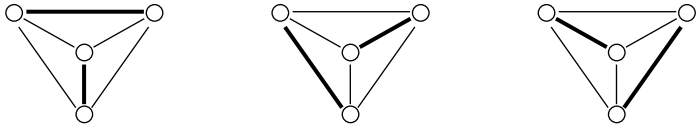


Figure 5.5.1

5.5.5 Example. The three perfect matchings of K_4 are illustrated in Fig. 5.5.1.

With its edges numbered 1–6, as illustrated in Fig. 5.5.2, the 1-matchings of C_6 are $\{e_1\}, \{e_2\}, \ldots, \{e_6\}$. There are nine 2-matchings, namely, $\{e_1, e_3\}$, $\{e_1, e_4\}$, $\{e_1, e_5\}$, $\{e_2, e_4\}$, $\{e_2, e_5\}$, $\{e_2, e_6\}$, $\{e_3, e_5\}$, $\{e_3, e_6\}$, and $\{e_4, e_6\}$. The two perfect matchings of C_6 are $\{e_1, e_3, e_5\}$ and $\{e_2, e_4, e_6\}$. (In particular $\mu(C_6) = 3$.) □

5.5.6 Definition. Suppose G is a graph on n vertices. Let $q(G, r)$ be the number of r-matchings of G, $r > 0$, and define $q(G, 0) = 1$. The *matching polynomial*[*] of G is

$$M(G, x) = \sum_{r \geq 0} (-1)^r q(G, r) x^{n-2r}. \tag{5.21}$$

Let $G = (V, E)$ be a fixed but arbitrary graph with n vertices and m edges. Because M is a 1-matching of G if and only if $M = \{e\}$ for some $e \in E$, $q(G, 1) = m$. Thus,

$$M(G, x) = x^n - mx^{n-2} + \cdots \tag{5.22}$$

Equation (5.22) bears a striking resemblance to the chromatic polynomial $p(G, x) = x^n - mx^{n-1} + \cdots$. One of the most striking differences is that $q(G, r)$, the number of r-matchings of G, is a *coefficient* of $M(G, x)$, whereas $p(G, r)$, the number of proper colorings of G, is a *value* of $p(G, x)$.

5.5.7 Example. From Example 5.5.5, the matching polynomial $M(C_6, x) = x^6 - 6x^4 + 9x^2 - 2$. □

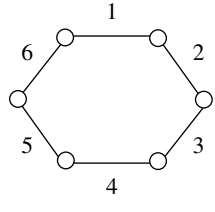


Figure 5.5.2

[*]First introduced by H. Hosoya in a paper on chemical thermodynamics [*Bull. Chem. Soc. Japan* 44 (1971), 2332–2339], chemists still refer to $M(G, x)$ as the *acyclic polynomial*. At roughly the same time, O. J. Heilmann and E. H. Lieb used the same notion in a paper in statistical mechanics [*Commun. Math. Phys.* 25 (1972), 190–232].

What's missing from the discussion so far is a convenient way to produce $M(G,x)$, one that does not involve having to count, much less list, all the matchings of G. What's needed is an analogue of chromatic reduction.

5.5.8 Definition. Suppose $u \in V$, where $G = (V,E)$ is a graph with at least two vertices. Denote by $G-u$ the subgraph of G induced on $W = V\backslash\{u\}$, i.e., $G-u = (W,F)$ where $F = E \cap W^{(2)}$.

Informally, $G-u$ is the graph obtained from G by deleting vertex *u and all the edges incident with it*. Note that extracting a vertex from G involves a more invasive kind of surgery than removing an edge. When edges are removed, the vertices are left undisturbed, $V(G-e) = V(G)$.

If $H = G-u$ and $w \in W = V(H)$, then $H-w = (G-u)-w$ is denoted $G-u-w$, which brings us to the matching analogue of chromatic reduction.

5.5.9 Theorem. *Let $G = (V,E)$ be a graph with $n > 2$ vertices. Suppose $e = \{u,w\} \in E$. Then*

$$M(G,x) = M(G-e,x) - M(G-u-w,x). \tag{5.23}$$

Proof. The number of r-matchings of G that do not contain edge e is $q(G-e,r)$ The r-matchings that do contain e are in one-to-one correspondence with the $(r-1)$-matchings of $G-u-w$. Thus,

$$q(G,r) = q(G-e,r) + q(G-u-w,r-1), \qquad r \geq 1. \tag{5.24}$$

Now, $q(G,r)$ is the coefficient of $(-1)^r x^{n-2r}$ in $M(G,x)$ and $q(G-e,r)$ is the coefficient of $(-1)^r x^{n-2r}$ in $M(G-e,x)$. But, $q(G-u-w,r-1)$ is the coefficient of $(-1)^{r-1}x^{(n-2)-2(r-1)} = -(-1)^r x^{n-2r}$ in $M(G-u-w,r-1)$, i.e., it is the coefficient of $(-1)^r x^{n-2r}$ in $-M(G-u-w,r-1)$. In other words, Equation (5.23) is the polynomial equivalent of Equation (5.24). ■

5.5.10 Corollary. *Suppose $G = (V,E)$ is a graph on n vertices. Let u be a vertex of G of degree $d(u) = k \leq n-2$. Suppose w_i, $1 \leq i \leq k$, are the vertices of G adjacent to u. Then*

$$M(G,x) = xM(G-u,x) - \sum_{i=1}^{k} M(G-u-w_i,x). \tag{5.25}$$

Proof. The proof is by induction on k. If $k = 0$, then u is an isolated vertex. In that case, $q(G,r) = q(G-u,r)$ for all r, and

$$\begin{aligned} M(G,x) &= x^n - q(G,1)x^{n-2} + q(G,2)x^{n-4} - \cdots \\ &= x^n - q(G-u,1)x^{n-2} + q(G-u,2)x^{n-4} - \cdots \\ &= x\left[x^{n-1} - q(G-u,1)x^{n-3} + q(G-u,2)x^{n-5} - \cdots\right] \\ &= xM(G-u,x). \end{aligned} \tag{5.26}$$

If $k > 0$, let $e = \{u, w_k\}$. If $H = G - e$ then, from Equation (5.23),

$$M(G,x) = M(H,x) - M(G - u - w_k, x).$$

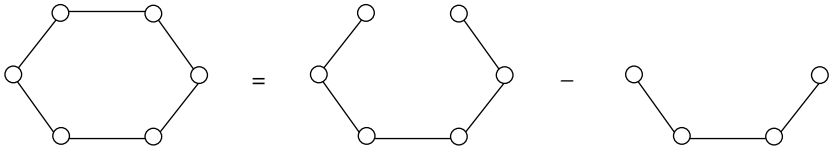
Because $d_H(u) = k - 1$ and $H - u = G - u$ it remains to apply the induction hypothesis to $M(H,x)$. ■

5.5.11 Example. Equation (5.22) suffices to determine that $M(P_1,x) = x$, $M(P_2,x) = x^2 - 1$, and $M(P_3,x) = x^3 - 2x$. If $n \geq 1$, then P_{n+1} has a vertex u of degree 1 and, by Equation (5.25),

$$M(P_{n+1},x) = xM(P_n,x) - M(P_{n-1},x). \tag{5.27}$$

So, $M(P_4,x) = x(x^3 - 2x) - (x^2 - 1) = x^4 - 3x^2 + 1$. Similarly, $M(P_5,x) = x^5 - 4x^3 + 3x$, $M(P_6,x) = x^6 - 5x^4 + 6x^2 - 1$, and so on. □

5.5.12 Example. Theorem 5.5.9 lends itself to the same kind of picturesque usage as chromatic reduction. If $G = C_6$, for example, Equation (5.23) can be expressed as



(In the matching analogue of chromatic reduction, vertices are not coalesced; they are removed.) This picturesque equation is equivalent to $M(C_6,x) = M(P_6,x) - M(P_4,x)$. From Example 5.5.11, $M(P_6,x) = x^6 - 5x^4 + 6x^2 - 1$ and $M(P_4,x) = x^4 - 3x^2 + 1$. Hence, $M(C_6,x) = x^6 - 6x^4 + 9x^2 - 2$, confirming Example 5.5.7. □

5.5.13 Example. Let's compute the matching polynomial of K_n. From Equation (5.22), $M(K_1,x) = x$, $M(K_2,x) = x^2 - 1$, and $M(K_3,x) = x^3 - 3x$. From Fig. 5.5.1, $M(K_4,x) = x^4 - 6x^2 + 3$. If $n > 1$, then $K_{n+1} - u = K_n$ and $K_{n+1} - u - w = K_{n-1}$. So, from Equation (5.25),

$$M(K_{n+1},x) = xM(K_n,x) - nM(K_{n-1},x), \qquad n \geq 2, \tag{5.28}$$

Thus, e.g.,

$$\begin{aligned} M(K_5,x) &= xM(K_4,x) - 4M(K_3,x) \\ &= x(x^4 - 6x^2 + 3) - 4(x^3 - 3x) \\ &= x^5 - 10x^3 + 15x. \end{aligned} \tag{5.29}$$

□

The so-called *Hermite polynomials*[*] are recursively defined by $h_1(x) = x$, $h_2(x) = x^2 - 1$, and $h_{n+1}(x) = xh_n(x) - nh_{n-1}(x)$. These polynomials first appeared as solutions to the second-order, linear differential equation

$$y'' - xy' + ny = 0.$$

It follows from Example 5.5.13 that $M(K_n, x) = h_n(x)$, $n \geq 1$. (It turns out that the polynomials $M(P_n, 2x)$ are also well known. They are *Chebyshev polynomials of the second kind.*[†])

What about doing some of these calculations by computer? One way to enter a graph into a computer is by means of a matrix.

5.5.14 Definition. Let $G = (V, E)$ be a graph with vertex set $V = \{1, 2, \ldots, n\}$. The $n \times n$ *adjacency* matrix $A(G) = (a_{ij})$ is defined by

$$a_{ij} = \begin{cases} 1 & \text{if } \{i,j\} \in E, \\ 0 & \text{otherwise.} \end{cases} \tag{5.30}$$

It is clear from the definition that $A(G)$ is a symmetric, (0, 1)-matrix whose main diagonal consists entirely of 0's, and that the number of 1's in row i of $A(G)$ is $d_G(i)$, the degree of vertex i. What about the other way around? Suppose you are given an arbitrary $n \times n$, symmetric, (0, 1)-matrix $A = (a_{ij})$ with zeros on the diagonal. Must it be the adjacency matrix of some graph? Yes, and it is easy to see how to illustrate the graph. Draw n vertices in the plane, number them from 1 to n, and draw an arc from vertex i to vertex j precisely when $a_{ij} = 1$.

Obscured by the notation is the fact that $A(G)$ depends, not only on G, but on the numbering of its vertices. If G_1 and G_2 are the (isomorphic) graphs of Fig. 5.5.3, then

$$A(G_1) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad A(G_2) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

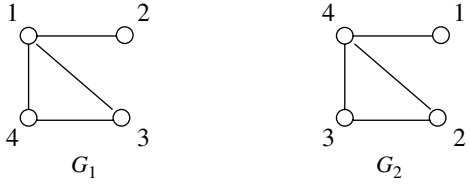


Figure 5.5.3

[*]After Charles Hermite (1822–1901). Among Hermite's students was the eminent mathematician Jules Henri Poincaré (1854–1912).

[†]After Pafnuti Chebyshev (1821–1894).

are different matrices. How different? To answer this question, let f be the permutation $(1432) \in S_4$. Then $f : V(G_1) \to V(G_2)$ is an isomorphism of G_1 onto G_2. Corresponding to f is a *permutation matrix* $P(f) = (\delta_{if(j)})$, i.e.,

$$P(f) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{5.31}$$

is the matrix obtained by permuting the columns of the identity matrix I_4 according to the permutation f (an elementary column operation). The connection between $A(G_1)$ and $A(G_2)$ is given by

$$A(G_2) = P(f)A(G_1)P(f)^{-1}. \tag{5.32}$$

(Because $P(f)$ is a permutation matrix, its inverse is equal to its *transpose*, i.e., $P(f)^{-1} = P(f)^t$.)

Conversely, if $A(G_2) = PA(G_1)P^{-1}$ for some permutation matrix P, then there is a permutation $f \in S_n$ such that $P = P(f)$. Moreover, $f : V(G_1) \to V(G_2)$ is an isomorphism. Let's summarize these observations.

5.5.15 Theorem. *Graphs G_1 and G_2 are isomorphic if and only if their adjacency matrices are permutation similar, i.e., if and only if there is a permutation matrix P such that $A(G_2) = PA(G_1)P^{-1}$.*

Theorem 5.5.15 opens a window on a new class of invariants.

5.5.16 Corollary. *Graphs G_1 and G_2 are isomorphic only if $A(G_1)$ and $A(G_2)$ have the same characteristic polynomial, i.e., only if $det(xI_n - A(G_1)) = det(xI_n - A(G_2))$.*

Proof. From linear algebra, two real symmetric matrices are similar if and only if they have the same characteristic polynomial. ■

Another perspective from which to view Corollary 5.5.16 is this: If nineteenth-century linear algebraists had a *quest*, it was to solve the *similarity problem* by finding a short list of easily computed (similarity) invariants sufficient to determine when two matrices are similar. That quest was successfully completed long ago, at least for matrices over the real numbers. For real *symmetric* matrices, one such list has a single entry, the characteristic polynomial. This raises some interesting questions. For starters, might the adjacency characteristic polynomial solve the graph isomorphism problem? An equivalent formulation of the question is this: Can two symmetric (0, 1)-matrices be similar without being permutation similar? That the answer to the reformulated question is *yes* will be confirmed momentarily.

While $\det(xI_n - A(G))$ does not solve the graph isomorphism problem all by itself, neither do any of the other invariants we have studied. Our situation is not

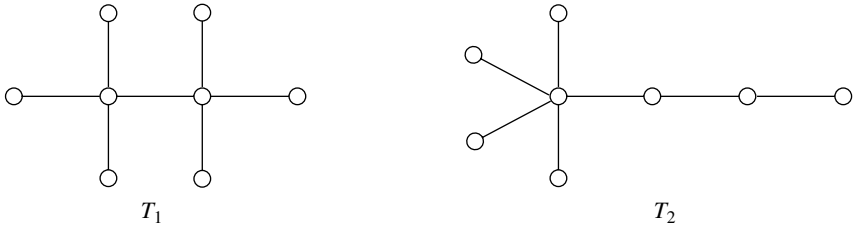


Figure 5.5.4

unlike that of a physician trying to treat a patient suffering from some particularly stubborn disease. If no single drug cures the patient, why not try a combination of drugs? In medicine, mixing drugs can have fatal consequences. While the graph-theoretic analogue may be less vital, it is no less interesting: To what extent is the new invariant, in this case $\det(xI_n - A(G))$, independent of other invariants? To address this question, define a *forest* to be an acyclic graph, i.e., a graph without any cycles. Then G is a forest if and only if each of its connected components is a tree.

5.5.17 Theorem. *Let G be a graph on n vertices. Then G is a forest if and only if $\det(xI_n - A(G)) = M(G,x)$.*

Proof Sketch. If $V(G) = \{1, 2, \ldots, n\}$, then $\det(xI_n - A(G))$ is an alternating sum of $n!$ products, one for each permutation of $\{1, 2, \ldots, n\}$. The product corresponding to $p \in S_n$ is nonzero if and only if $\{i, p(i)\} \in E(G)$ for all $i \neq p(i)$. In particular, there is a one-to-one correspondence between the r-matchings of G and the nonzero products arising from permutations of cycle type $[2^r, 1^{n-2r}]$. This correspondence yields $\det(xI_n - A(G)) = M(G,x) +$ terms involving cycles of G. If G is acyclic, the proof is complete. Otherwise, one must show that the added terms make a nonzero contribution. ■

5.5.18 Example. Let T_1 and T_2 be the trees illustrated in Fig. 5.5.4. Then $M(T_1,x) = x^8 - 7x^6 + 9x^4 = M(T_2,x)$. (Confirm it.) It follows from Theorem 5.5.17 that $\det(xI_8 - A(T_1)) = \det(xI_8 - A(T_2))$, so $A(T_1)$ and $A(T_2)$ are similar. Because T_1 and T_2 are not isomorphic, $A(T_1)$ and $A(T_2)$ cannot be permutation similar. □

5.5.19 Example. If $G = K_3 = C_3$, then

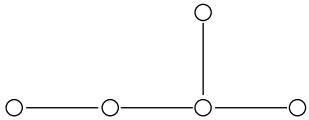
$$A(G) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

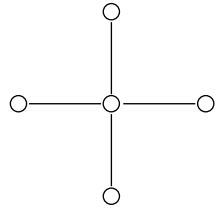
Because G is not a forest, it follows from Theorem 5.5.17 that $\det(xI_3 - A(G)) \neq M(G,x)$. Indeed, $\det(xI_3 - A(C_3)) = x^3 - 3x - 2$, whereas $M(C_3,x) = x^3 - 3x$. (Check it.) □

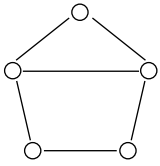
5.5. EXERCISES

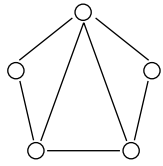
1 Use Definition 5.5.6 to confirm directly that $M(P_6, x) = x^6 - 5x^4 + 6x^2 - 1$. (Make a list of all six 2-matchings.)

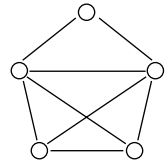
2 Compute the matching polynomial of

(a) 

(b) 

(c) 

(d) 

(e) 

3 Compute

(a) $M(K_6, x)$. **(b)** $M(K_7, x)$. **(c)** $M(P_7, x)$.

(d) $M(P_8, x)$. **(e)** $M(C_7, x)$. **(f)** $M(C_8, x)$.

4 Let k_n be the number of perfect matchings in the complete graph K_n, $n \geq 2$.

(a) Compute k_3.

(b) Compute k_4.

(c) Compute k_6.

(d) Prove that $k_{n+2} = (n+1)k_n$, $n \geq 2$.

(e) Prove that k_{2r} is odd, $r \geq 1$.

5 Prove that $M(G, x)$ is an invariant.

6 Prove that $M(G_1 + G_2, x) = M(G_1, x)M(G_2, x)$. (See Definition 5.3.10 for the definition of graph union.)

7 Let $G = (V, E)$ be a graph. An r-matching of G is *maximal* if it is not properly contained in another matching of G. An r-matching is *maximum* if $r = \mu(G)$.

(a) Explain why every maximum matching is a maximal matching.

(b) Give an example of a graph G with a matching M that is maximal but not maximum.

8 Let G be a graph on three or more vertices. Suppose u and w are nonadjacent vertices of G. If $G + e$ is the graph obtained from G by adding a new

edge $e = \{u, w\}$, then Equation (5.23) can be written, in "reverse-angle" form, as

$$M(G, x) = M(G + e, x) + M(G - u - w, x).$$

Use this formula, along with Example 5.5.13, to compute

(a) $M(K_5 - e, x)$. **(b)** $M(K_6 - e, x)$.

9 Let $G = (V, E)$ be a graph on n vertices. A subset $K \subset V$ is a *covering* of G if, for all $e \in E$, there is a $v \in K$ such that $v \in e$. (Note that the word "cover" is being used a little differently here than in Definition 5.5.3.) The *covering number* $\beta(G) = \min o(K)$, where the minimum is over all coverings of G. The *independence number* $\alpha(G) = \max o(S)$, where the maximum is over all independent sets $S \subset V$.

(a) Find a connected graph G such that $\alpha(G) < \beta(G)$.

(b) Find a connected graph G such that $\alpha(G) > \beta(G)$.

(c) Show that $\chi(G) \leq 1 + \beta(G)$.

(d) Show that $\alpha(G) + \beta(G) = n$.

(e) Show that $\chi(G) + \beta(G^c) \geq n$.

(f) Show that $\mu(G) \leq \beta(G)$.

(g) D. König proved that $\mu(G) = \beta(G)$ for any bipartite graph G. Find a nonbipartite graph G for which $\mu(G) = \beta(G)$.

10 It can be shown that the *derivative* of the matching polynomial is given by the equation

$$D_x M(G, x) = \sum_{u \in V} M(G - u, x).$$

(a) Use this result to prove that the Hermite polynomials satisfy the identity $D_x h_n(x) = n h_{n-1}(x), \quad n \geq 2$.

(b) Use Exercise 4(c) and part (a) of this exercise to obtain $M(K_6, x)$ by antidifferentiating Equation (5.29).

11 It can be shown that

$$M(G^c, x) = \sum_{r \geq 0} q(G, r) M(K_{n-2r}, x),$$

where $M(K_0, x) = 1$. Confirm this formula for the self-complementary graph

(a) P_4. **(b)** C_5.

12 Consider the matrices

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(a) Prove that they are not similar.

(b) Show that they have the same characteristic polynomial, namely, $(x-1)^2$.

13 For each graph in Fig. 5.5.5, compute

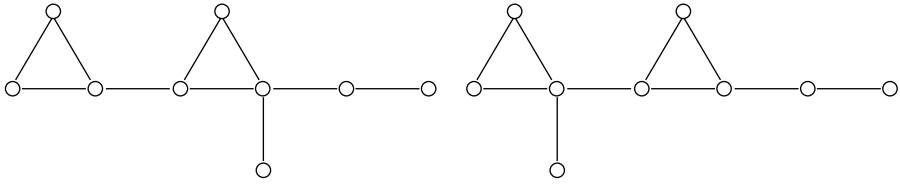


Figure 5.5.5

(a) its degree sequence.

(b) its chromatic polynomial.

(c) its matching polynomial.

14 If A is a real symmetric matrix, then its characteristic roots are all real. It follows that $A(G)$ has n real eigenvalues $\gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G)$. Compute these (graph) invariants for

(a) $G = K_3$. **(b)** $G = P_3$. **(c)** $G = K_4$.

(d) $G = C_4$. **(e)** $G = K_{1,3}$. **(f)** $G = K_2 \vee K_3^c$.

15 If $\gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G)$ are the eigenvalues of $A(G)$, show that $\gamma_1(G) + \gamma_2(G) + \cdots + \gamma_n(G) = 0$.

16 Prove that the eigenvalues of $A(K_n)$ (see Exericse 14) are $n-1$ with multiplicity 1, and -1 with multiplicity $n-1$.

17 It follows from Theorem 5.5.17 (and Exericse 14) that the roots of $M(G,x)$ are all real whenever G is a forest. In fact, the roots of $M(G,x)$ are all real for any graph G. Moreover, if $a_1 \geq a_2 \geq \cdots \geq a_n$ are the roots of $M(G,x)$ and $b_1 \geq b_2 \geq \cdots \geq b_{n-1}$ are the roots of $M(G-u,x)$, then the b's *interlace* the a's, i.e., $a_i \geq b_i \geq a_{i+1}$, $1 \leq i < n$. Confirm that the roots of $M(K_4,x)$ interlace the roots of $M(K_5,x)$.

18 Confirm that the number of *different* roots of $M(G,x)$ is greater than the length of a longest path in G when

(a) $G = P_3$. **(b)** $G = P_4$.

(c) $G = C_3$ **(d)** $G = C_4$.

19 Let G be a connected graph. The *edge connectivity* $\varepsilon(G)$ is the smallest number k for which there exist edges $e_1, e_2, \ldots, e_k \in E(G)$ such that $G - e_1 - e_2 - \cdots - e_k$ is disconnected. If $G = K_n$, the *vertex connectivity* $\kappa(G) = n-1$. Otherwise, $\kappa(G)$ is the smallest number k for which there exist vertices $u_1, u_2, \ldots, u_k \in V(G)$ such that $G - u_1 - u_2 - \cdots - u_k$ is disconnected.

(a) Prove that $\varepsilon(G) \leq d_n(G)$, the minimum vertex degree.

(b) Prove that $\kappa(G) \leq \varepsilon(G)$.

(c) Suppose $G \neq K_n$. If $\kappa(G) = 1$, then there is some vertex $u \in V(G)$ such that $G - u$ is disconnected. Such a vertex is called a *cut vertex*. A *block* of G is a maximal subgraph that doesn't have a cut vertex. Prove that the chromatic polynomial of a graph is uniquely determined by the chromatic polynomials of its blocks.

20 Let $\det(xI_n - A(G)) = x^n + c_1x^{n-1} + \cdots + c_n$ be the characteristic polynomial of $A(G)$. In 1963, H. Sachs proved that

$$c_i = \sum_H (-1)^{c(H)} 2^{k(H)},$$

where the summation extends over all i-vertex subgraphs H of G whose connected components are either single edges or cycles, and where $c(H)$ and $k(H)$ are the numbers of components and cycles, respectively. Use Sach's theorem to compute $\det(xI_n - A(G))$ for the graph

(a) K_3. **(b)** P_3. **(c)** K_4.

(d) C_4. **(e)** $G = K_{1,3}$. **(f)** $G = K_2 \vee K_3^c$.

(*Hint*: Your answer(s) should be consistent with Exercise 14.)

21 Use Sachs's theorem (Exericse 20) to prove Theorem 5.5.17.

22 Prove Sach's theorem (Exercise 20).

23 Recall (Exercise 19, Section 3.5) that the permanent of an $n \times n$ matrix $A = (a_{ij})$ is defined by

$$\text{per}(A) = \sum_{p \in S_n} \prod_{t=1}^{n} a_{tp(t)}.$$

If G is a *bipartite* graph, then the number of perfect matchings in G is the square root of the permanent of $A(G)$. Confirm this formula if

(a) $G = K_{1,3}$. **(b)** $G = P_4$. **(c)** $G = C_4$.

24 Show that $\text{per}(A(G))$ is a (graph) invariant. (See Exercise 23.)

25 Important to the theory of matchings is the concept of adjacent edges. This notion arises in other contexts as well. Associated with graph G is its *line graph*, $G^{\#}$. The vertex set of $G^{\#}$ is $V(G^{\#}) = E(G)$, i.e., the vertices of $G^{\#}$ are the edges of G. The edges of $G^{\#}$ are those pairs of its vertices that are adjacent edges in G.

(a) Show that the line graph of K_4 is isomorphic to $K_6 - M$, where M is a perfect matching.

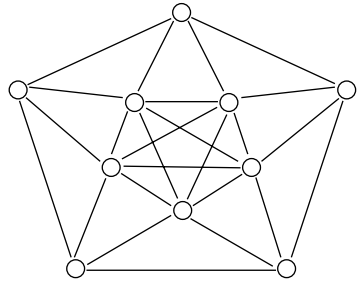


Figure 5.5.6

(b) Show that the line graph of the *wheel*, $W = K_1 \vee C_5$, is isomorphic to the graph in Fig. 5.5.6.

26 A *walk* in G of *length* r is a sequence of vertices $u_0, u_1, \ldots, u_r$ in which $\{u_{i-1}, u_i\} \in E(G)$, $1 \leq i \leq r$. (A path is a walk consisting of distinct vertices.) If $V(G) = \{1, 2, \ldots, n\}$,

(a) prove that the number of walks in G of length r, from vertex i to vertex j, is the (i,j)-entry of $A(G)^r$.

(b) prove that the distance from vertex i to vertex j is the smallest value of k such that the (i,j)-entry of $A(G)^k$ is not zero.

27 Give a formal proof of Theorem 5.5.15.

28 Let G be a graph on n vertices. The *Hosoya topological index* of G is

$$H(G) = \sum_{r=0}^{\lfloor n/2 \rfloor} q(G, r).$$

(a) Show that $H(P_1) = 1$ and $H(P_2) = 2$.

(b) Show that $H(P_{n+1}) = H(P_n) + H(P_{n-1}), \quad n \geq 2$.

(c) Show that $H(P_n) = F_n$, the nth Fibonacci number, $n \geq 1$. (See Section 1.2, Exericse 19.)

(d) Show that $H(C_n) = F_n + F_{n-2}$, $n \geq 3$.

5.6. ORIENTED GRAPHS

Destiny is not a matter of chance, it is a matter of choice.

— William Jennings Bryan

If $G = (V, E)$ is a graph with n vertices and m edges then, by definition, E is an m-element subset of $V^{(2)}$. Not to be confused with the *cartesian product*

$V \times V = \{(u, v) : u, v \in V\}$, whose elements are ordered pairs of vertices, the elements of $V^{(2)}$ are *unordered*.

5.6.1 Definition. An *orientation* of $G = (V, E)$ is a function $f : E \to V \times V$ such that, for all $e = \{u, v\} \in E$, the *oriented edge* $f(e)$ is one of (u, v) or (v, u).

By the fundamental counting principle, a graph with m edges has 2^m orientations. By convention, the number of orientations of the edgeless graph K_n^c is $2^0 = 1$.

An *oriented graph*[*] is a graph with a nonempty set of edges and some prescribed orientation. The situation in which G is oriented by f, and $f(e) = (u, v)$ for some $e = \{u, v\} \in E(G)$, is summarized by referring to $e = (u, v)$ as an *oriented edge* of G.

If $e = (u, v)$ is an *oriented edge* of G, then vertex v is the *head* of e, and vertex u is its *tail*. Consistent with this language, e is typically illustrated by a *directed arc*, or *arrow*, from u to v.

5.6.2 Example. Suppose four ultimate frisbee teams enter a round-robin tournament in which they are seeded (ranked) 1–4. The outcome of such a tournament can be illustrated by an orientation of K_4 in which oriented edge $e = (u, v)$ indicates that team u won its match with team v[†]. In the outcome illustrated by Fig. 5.6.1*a*, e.g., team 1 fulfilled the expectations of the organizers by beating every other team in the tournament. On the other hand, having lost all of its games, team 2 seems to have underperformed.

The notorious intransitivity of athletic competitions is illustrated in Fig. 5.6.1*b*. Represented here is a tournament in which team 1 beat team 3 and team 3 beat team 2, but team 1 lost to team 2. (Unlike the first outcome, some sort of tie-breaking procedure will be required to determine the championship team in the second tournament.) □

5.6.3 Definition. A *directed path* of length r in the oriented graph G is a path $[w_0, w_1, \ldots, w_r]$ in which (w_{i-1}, w_i) is an oriented edge of G, $1 \le i \le r$. A *directed*

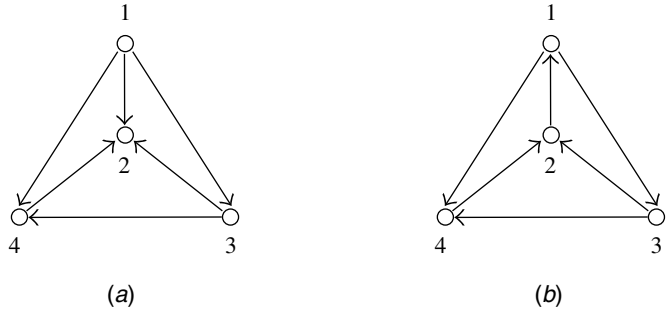


Figure 5.6.1

*An oriented graph is a special kind of *directed* graph in which at most one of (u, v) and (v, u) can be an edge.

†This has become such a widely accepted model for round-robin tournaments that oriented complete graphs have come, themselves, to be known as *tournments*.

cycle of length r in G is a cycle $\langle w_1, w_2, \ldots, w_r \rangle$ in which (w_r, w_1) and (w_{i-1}, w_i), $1 < i \leq r$, are oriented edges.

5.6.4 Example. The oriented graph illustrated in Fig. 5.6.1*b* contains three directed cycles: $\langle 1, 3, 2 \rangle$, $\langle 1, 4, 2 \rangle$, and $\langle 1, 3, 4, 2 \rangle$. The oriented graph in Fig. 5.6.1*a* has none. □

5.6.5 Definition. An orientation of G is *acyclic* if it contains no directed cycles.

Because a tree has no cycles at all, each of its orientations is acyclic. What about some arbitrary graph having m edges? Of its 2^m orientations, how many are acyclic?

5.6.6 Stanley's Theorem.* *If G is a graph with n vertices, m edges, and chromatic polynomial $p(G, x)$, then the number of acyclic orientations of G is $(-1)^n p(G, -1)$.*

Proof Sketch. Let $c(G)$ be the number of acyclic orientations of G and set $\rho(G) = p(G, -1)$. The heart of the proof lies in showing that $c(G) - \rho(G) = c(G - e) - \rho(G - e)$, $e \in E(G)$. Because $c(K_n^c) = \rho(K_n^c) = 1$, this yields a proof by induction on m. Details are omitted. ■

5.6.7 Example. Given that $p(K_4, x) = x(x-1)(x-2)(x-3)$, we can use Stanley's theorem to determine that, of the 64 orientations of K_4, $(-1)^4 \times p(K_4, -1) = 4! = 24$ are acyclic.

If $G = C_n$, then G has n edges and 2^n orientations. According to Exercise 9(c) of Section 5.3,

$$p(C_n, x) = (x-1)^n + (-1)^n (x-1).$$

So, by Stanley's theorem, C_n has $2^n - 2$ acyclic orientations. Indeed, the two remaining orientations might well be labeled *clockwise* and *counterclockwise*.

If T is a tree on $n \geq 2$ vertices then, by Theorem 5.3.16, $p(T, x) = x(x-1)^{n-1}$. So, T has $(-1)^n p(T, -1) = 2^{n-1}$ acyclic orientations. Because T has $m = n - 1$ edges, it has a total of 2^{n-1} orientations, confirming that every orientation of every (nontrivial) tree is ayclic. □

5.6.8 Definition. Suppose $G = (V, E)$ is an oriented graph with vertex set $V = \{1, 2, \ldots, n\}$ and edge set $E = \{e_1, e_2, \ldots, e_m\}$. Let $Q(G) = (q_{ij})$ be the $n \times m$ matrix defined by $q_{ij} = 1$ if vertex i is the head of edge e_j, -1 if i is the tail of e_j, and 0 otherwise. Then $Q(G)$ is an *oriented vertex–edge incidence matrix* for G.

*R. P. Stanley, Acyclic orientations of graphs, *Discrete Math.* 5 (1973), 171–178.

It can be useful to think of $Q(G)$ as a vertex-by-edge matrix. If oriented edge $e = (u, v)$, then column e of $Q(G)$ contains precisely two nonzero entries: -1 in row u and $+1$ in row v. The number of nonzero entries in row w of $Q(G)$ is $d_G(w)$, the degree of vertex w.

5.6.9 Example. Let $G = K_4$, numbered and oriented as in Fig. 5.6.1*a*, following. If the edges of G are numbered in dictionary order, i.e., if $e_1 = \{1,2\}$, $e_2 = \{1,3\}$, $e_3 = \{1,4\}$, $e_4 = \{2,3\}$, $e_5 = \{2,4\}$, and $e_6 = \{3,4\}$, then

$$Q(G) = \begin{pmatrix} -1 & -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 1 \end{pmatrix}.$$

If $H = K_4$, with the same numbering of vertices and edges, but with the orientation illustrated in Fig. 5.6.1*b*, then $Q(H)$ differs from $Q(G)$ by the signs of the entries in its first column. □

As usual, denote by Q^{t} the *transpose* of $Q = Q(G) = (q_{ij})$, i.e., the $m \times n$ matrix whose (i,j)-entry is q_{ji}.

5.6.10 Theorem. *Let G be a graph with vertex set $V(G) = \{1, 2, \ldots, n\}$. If $Q = Q(G)$ is an oriented vertex–edge incidence matrix corresponding to some orientation of G and some numbering of its edges, then the (i,j)-entry of QQ^{t} is*

$$(QQ^{\mathrm{t}})_{ij} = \begin{cases} d_G(i) & \text{if } j = i, \\ -1 & \text{if } i \neq j \text{ and } \{i,j\} \in E(G), \\ 0 & \text{otherwise.} \end{cases}$$

While $Q = Q(G)$ depends both on the orientation and the numbering of the edges of G, it follows from Theorem 5.6.10 that QQ^{t} depends on neither.

Proof of Theorem 5.6.10. From the definitions of transpose and matrix multiplication, the (i,j)-entry of QQ^{t} is

$$\sum_{r=1}^{m} (Q)_{ir} (Q^{\mathrm{t}})_{rj} = \sum_{r=1}^{m} q_{ir} q_{jr}. \tag{5.33}$$

If $i = j$, then $q_{ir} q_{jr} = q_{ir}^2$, and Equation (5.33) is the sum of the squares of the entries in row i of $Q(G)$. Since q_{ir} is ± 1 when vertex i is incident with edge e_r, and 0 otherwise, the sum of q_{ir}^2 is precisely $d_G(i)$.

If $i \neq j$, then $q_{ir} q_{jr} \neq 0$ if and only if $q_{ir} \neq 0 \neq q_{jr}$, if and only if $\{i,j\} = e_r \in E(G)$, if and only if $q_{ir} q_{jr} = -1$. Hence, the (i,j)-entry of QQ^{t} is -1 when $\{i,j\} \in E(G)$, and 0 otherwise. ■

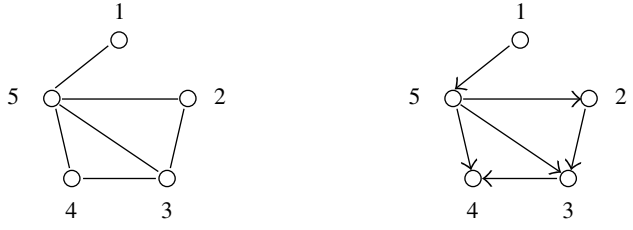


Figure 5.6.2

5.6.11 Definition. If G is a graph with vertex set $\{1, 2, \ldots, n\}$, let $D(G) = \operatorname{diag}(d_G(1), d_G(2), \ldots, d_G(n))$ be the $n \times n$ diagonal matrix of vertex degrees. The *Laplacian matrix* $L(G) = D(G) - A(G)$, where $A(G)$ is the adjacency matrix of G.

5.6.12 Corollary. *Let G be a graph with vertex set $V = \{1, 2, \ldots, n\}$. If $Q = Q(G)$ is an oriented vertex–edge incidence matrix with respect to some fixed but arbitrary numbering of the edges of G, then $QQ^t = L(G)$.*

Proof. Immediate from Theorem 5.6.10 and Definition 5.6.11. ■

5.6.13 Example. If H is the graph in Fig. 5.6.2*a*, then

$$L(H) = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 \\ 0 & 2 & -1 & 0 & -1 \\ 0 & -1 & 3 & -1 & -1 \\ 0 & 0 & -1 & 2 & -1 \\ -1 & -1 & -1 & -1 & 4 \end{pmatrix}.$$

With respect to the orientation exhibited in Fig. 5.6.2*b* and the edge numbering $e_1 = (1, 5)$, $e_2 = (2, 3)$, $e_3 = (5, 2)$, $e_4 = (3, 4)$, $e_5 = (5, 3)$, and $e_6 = (5, 4)$,

$$Q(H) = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 & -1 & -1 \end{pmatrix}.$$

It is left to the reader to confirm that $Q(H)Q(H)^{\mathrm{t}} = L(H)$. □

Let A be a generic $n \times n$ matrix and denote by A_{ij} the $(n-1)$-square submatrix of A obtained by deleting its ith row and jth column. Recall from linear algebra that the *classical adjoint* (or *adjugate*) of A, call it $A^{\dagger}$, is the $n \times n$ matrix whose

(i,j)-entry is $(-1)^{i+j}\det(A_{ji})$. The result which makes classical adjoints worth knowing about is this:

$$AA^{\dagger} = \det(A)I_n. \tag{5.34}$$

It is from Equation (5.34) that one obtains the formula $A^{-1} = [\det(A)]^{-1}A^{\dagger}$ whenever $\det(A) \neq 0$.

If G is a fixed but arbitrary graph on n vertices then $L(G)Y_n = 0$, where (in this section) Y_n is the $n \times 1$ column vector each of whose entries is 1. This is because the number of 1's in row i of $A(G)$ is equal to $d_G(i)$, the (i,i)-entry of $D(G)$. It follows that rank $L(G) < n$, so

$$\det(L(G)) = 0.$$

Setting $A = L(G)$ in Equation (5.34) gives $L(G)L(G)^{\dagger} = 0$, from which it follows that $L(G)C = 0$ for every column C of $L(G)^{\dagger}$. If rank $L(G) \leq n-2$, this is perfectly understandable because, in that case, $C = 0$. On the other hand, if rank $L(G) = n-1$, then $L(G)C = 0$ if and only if C is a multiple of Y_n. In either case,

$$L(G)^{\dagger} = \begin{pmatrix} a & b & c & \cdots & d \\ a & b & c & \cdots & d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a & b & c & \cdots & d \end{pmatrix}, \tag{5.35}$$

where $a, b, c, \ldots,$ and d are constants. Since $\det(A) = \det(A^{\mathrm{t}})$, the classical adjoint of a symmetric matrix is symmetric. Thus, the numbers in the first column of $L(G)^{\dagger}$ equal the numbers in its first row. From Equation (5.35), this means *all the entries of* $L(G)^{\dagger}$ *are equal*, and it proves the following.

5.6.14 Theorem. *If G is a graph on n vertices, then there exists an integer $t(G)$ depending only on G such that*

$$t(G) = (-1)^{i+j}\det(L(G)_{ij}), \qquad 1 \leq i,j \leq n.$$

Moreover, $t(G) = 0$ if and only if rank $L(G) \leq n-2$.

When an integer emerges in a combinatorial setting, it is natural to expect that it counts something.

5.6.15 Definition. Let $H = (W,F)$ be a subgraph of $G = (V,E)$. If $W = V$, then H is a *spanning* subgraph of G. A *spanning tree* is a spanning subgraph that is a tree.

A spanning subgraph is one that uses all of the vertices and some of the edges. In particular, graph G has only one *induced* spanning subgraph, namely, G itself.

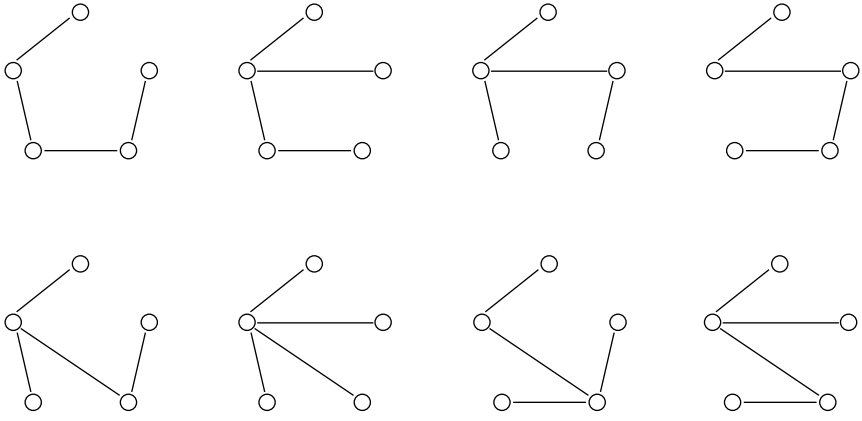


Figure 5.6.3

5.6.16 Example. The graph in Fig. 5.6.2*a* has the eight spanning trees illustrated in Fig. 5.6.3. □

5.6.17 Matrix-Tree Theorem. If G is a graph, then $t(G)$ is the number of different spanning trees in G.

Proof Sketch. By Theorem 5.6.14, it suffices to compute, say, the (1, 1)-entry of $L(G)^{\dagger}$. Because $L(G) = Q(G)Q(G)^{t}$, this computation can be done using a classical (nineteenth-century) result known as the Cauchy–Binet determinant theorem. The effect of this computation is to express $t(G)$ as a sum of squares of $(n-1)\times(n-1)$ subdeterminants of Q. Finally, by an old result of Poincaré, these subdeterminants have absolute value 1 or 0, depending on whether they correspond to edges in a spanning tree or not. The details are beyond the scope of this book. ■

5.6.18 Example. If H is the graph in Fig. 5.6.2*a*, then, by Example 5.6.16, the *spanning tree number* $t(H) = 8$.* Let's use Theorem 5.6.14 to compute $t(H)$. From Example 5.6.13,

$$L(H) = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 \\ 0 & 2 & -1 & 0 & -1 \\ 0 & -1 & 3 & -1 & -1 \\ 0 & 0 & -1 & 2 & -1 \\ -1 & -1 & -1 & -1 & 4 \end{pmatrix}.$$

*Theorem 5.6.17 concerns the number of *different* spanning trees. The fact that there are numerous isomorphisms among the trees in Fig. 5.6.3 is irrelevant to the computation of $t(H)$.

To compute, say, the (5, 3)-entry of $L(H)^{\dagger}$, take the product of $(-1)^{5+3}$ and the determinant of the matrix obtained from $L(H)$ by deleting its third row and fifth column, i.e.,

$$t(H) = (-1)^8 \det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 \\ 0 & 0 & -1 & 2 \\ -1 & -1 & -1 & -1 \end{pmatrix}.$$

Expanding this determinant along the first row yields

$$\begin{aligned} t(H) &= \det \begin{pmatrix} 2 & -1 & 0 \\ 0 & -1 & 2 \\ -1 & -1 & -1 \end{pmatrix} \\ &= 2 \det \begin{pmatrix} -1 & 2 \\ -1 & -1 \end{pmatrix} + \det \begin{pmatrix} 0 & 2 \\ -1 & -1 \end{pmatrix} \\ &= 2(3) + 2 = 8. \end{aligned}$$

□

Because it is a symmetric matrix, the eigenvalues of $L(G)$ are all real. Indeed, because $L(G) = Q(G)Q(G)^{\mathrm{t}}$, its eigenvalues are all nonnegative!

5.6.19 Definition. If G is a graph on n vertices, the *spectrum* of $L(G)$ is denoted $s(G) = (\lambda_1(G), \lambda_2(G), \ldots, \lambda_n(G))$, where

$$\lambda_1(G) \geq \lambda_2(G) \geq \cdots \geq \lambda_n(G) \geq 0 \tag{5.36}$$

are the eigenvalues of $L(G)$ arranged in nonincreasing order.

5.6.20 Example. Computations show that the (Laplacian) characteristic polynomial of the graph H in Fig. 5.6.2*a* is

$$\begin{aligned} \det(xI_5 - L(H)) &= x^5 - 12x^4 + 49x^3 - 78x^2 + 40x \\ &= x(x-1)(x-2)(x-4)(x-5), \end{aligned}$$

so $s(H) = (5, 4, 2, 1, 0)$. □

Recall that

$$(x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n) = x^n - E_1 x^{n-1} + \cdots + (-1)^n E_n,$$

where $E_r = E_r(\lambda_1, \lambda_2, \ldots, \lambda_n)$ is the rth elementary symmetric function. In particular, the coefficient of x in the characteristic polynomial $\det(xI_n - L(G))$ is

$$E_{n-1}(s(G)) = E_{n-1}(\lambda_1(G), \lambda_2(G), \ldots, \lambda_n(G)).$$

Because $L(G)$ is singular, $\lambda_n(G) = 0$. Therefore,

$$E_{n-1}(s(G)) = \prod_{i=1}^{n-1} \lambda_i(G). \tag{5.37}$$

On the other hand, the coefficient of x in $\det(xI_n - L(G))$ is

$$\sum_{i=1}^{n} \det(L(G)_{ii}) = nt(G). \tag{5.38}$$

5.6.21 Corollary. *If G is a graph with Laplacian spectrum $s(G) = (\lambda_1(G), \lambda_2(G), \ldots, \lambda_n(G))$ and spanning tree number $t(G)$, then*

$$nt(G) = \prod_{i=1}^{n-1} \lambda_i(G).$$

In particular, $\lambda_{n-1}(G) > 0$ if and only if G is connected.

Proof. The first statement follows from Equations (5.37) and (5.38). The second is a consequence of the fact that G has a spanning tree if and only if it is connected. ■

Corollary 5.6.21 suggests that $\lambda_{n-1}(G)$ might be viewed as a quantitative measure of connectivity.

5.6.22 Definition. If G is a graph, its *algebraic connectivity* is $a(G) = \lambda_{n-1}(G)$, the second smallest eigenvalue of $L(G)$.*

What about the other eigenvalues? Using an argument similar to the one that established Equation (5.32) in Section 5.5, one can show that G_1 and G_2 are isomorphic if and only if $L(G_1)$ and $L(G_2)$ are permutation similar. Because symmetric matrices are similar if and only if they have the same eigenvalues, it follows that $s(G)$ is an invariant of G. But, what do the eigenvalues of $L(G)$ mean graph theoretically? To a large extent, that is still an open question. One thing that *is* known follows from an old result of I. Schur.

5.6.23 Definition. Suppose $(a) = (a_1, a_2, \ldots, a_s)$ and $(b) = (b_1, b_2, \ldots, b_t)$ are two nonincreasing sequences of real numbers that satisfy $a_1 + a_2 + \cdots + a_s = b_1 + b_2 + \cdots + b_t$. Then (a) *majorizes* (b), written $(a) \succ (b)$, if $s \leq t$ and

$$\sum_{i=1}^{r} a_i \geq \sum_{i=1}^{r} b_i, \qquad 1 \leq r \leq s. \tag{5.39}$$

*The algebraic connectivity was introduced by Miroslav Fiedler.

5.6.24 Example. The degree sequence for the graph H in Fig. 5.6.2*a* is $d(H) = (4, 3, 2, 2, 1)$, a partition of $12 = 2m$. From Example 5.6.20, $s(H) = (5, 4, 2, 1, 0)$. To see that $s(H)$ majorizes $d(H)$, observe that

$$\begin{aligned} 5 &\geq 4, \\ 5 + 4 &\geq 4 + 3, \\ 5 + 4 + 2 &\geq 4 + 3 + 2, \\ 5 + 4 + 2 + 1 &\geq 4 + 3 + 2 + 2, \end{aligned}$$

and

$$5 + 4 + 2 + 1 + 0 = 4 + 3 + 2 + 2 + 1. \qquad \square$$

In fact, Example 5.6.24 is typical.

5.6.25 (Schur's Majorization) Theorem.[*] *If G is a graph with degree sequence $d(G)$ and (Laplacian) spectrum $s(G)$, then $s(G)$ majorizes $d(G)$.*

The proof of Theorem 5.6.25 is beyond the scope of this book.

Returning to the issue of invariants, graphs G_1 and G_2 are isomorphic only if they have the same chromatic polynomial, the same matching polynomial, the same adjacency characteristic polynomial, and the same Laplacian characteristic polynomial. While no single one of these polynomials characterizes graphs up to isomorphism, might all four, taken in combination, do the job? As shown by Allen Schwenk[†] and Brendan McKay,[‡] the answer is an emphatic negative.

5.6.26 Theorem. *Let $P(n)$ be the probability that given a randomly chosen tree T_1 on n vertices, there is a nonisomorphic tree T_2 such that, simultaneously,*

(a) $p(T_1, x) = p(T_2, x)$,
(b) $M(T_1, x) = M(T_2, x)$,
(c) $\det(xI_n - A(T_1)) = \det(xI_n - A(T_2))$, *and*
(d) $\det(xI_n - L(T_1)) = \det(xI_n - L(T_2))$.

Then $\lim_{n\to\infty} P(n) = 1$.

[*]Theorem 5.6.25 is a special case of a more general theorem published by Issai Schur in 1923. An improvement of Theorem 5.6.25 can be found in the article: R. D. Grone, Eigenvalues and the degree sequence of graphs, *Linear & Multilinear Algebra* 39 (1995), 133–136.

[†]A. J. Schwenk, Almost all trees are cospectral, in *New Directions in the Theory of Graphs*, Academic Press, New York, 1973, pp. 275–307.

[‡]B. D. McKay, On the spectral characteristics of trees, *Ars Combinatoria* 3 (1977), 219–232.

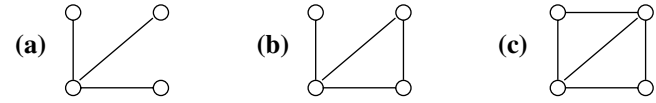
Proof Sketch. From Theorem 5.3.16, any two trees on n vertices have the same chromatic polynomial, namely, $x(x-1)^{n-1}$. By Theorem 5.5.17, parts (b) and (c) are equivalent. Thus, it suffices to obtain the conclusion for trees that simultaneously satisfy parts (c) and (d).

The proof is in two parts. The first is to find a pair of trees, L_1 and L_2, with vertices $u \in V(L_1)$ and $w \in V(L_2)$, such that the following property holds: For any tree T, and any vertex v of T, if T_1 is the tree obtained by identifying vertex u of L_1 with vertex v, and T_2 the tree obtained from T by identifying vertex w of L_2 with vertex v, then parts (c) and (d) hold for T_1 and T_2. Informally, T_1 and T_2 might be thought of as the trees obtained from T by grafting on, at vertex v, *limbs* isomorphic to L_1 (at vertex u) and L_2 (at vertex w), respectively.

The second part is to prove that the probability of finding a limb isomorphic to L_1 (at vertex u), on a randomly chosen n-vertex tree T_1, goes to 1 as n goes to infinity. It then remains to show that if T_2 is the tree obtained from T_1 by pruning off limb L_1 and grafting limb L_2 in its place, then T_2 is not isomorphic to T_1. ■

5.6. EXERCISES

1 Compute both the number of orientations and the number of acyclic orientations of the graph



2 Compute the number of acyclic orientations for the graph G in Fig. 5.6.4.

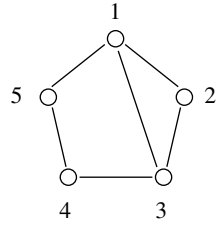


Figure 5.6.4

3 Exhibit the oriented vertex–edge incidence matrix $Q = Q(G)$ for the graph G in Fig. 5.6.4 with orientation given by

(a) $e_1 = (1,2)$, $e_2 = (3,2)$, $e_3 = (3,4)$, $e_4 = (4,5)$, $e_5 = (5,1)$, and $e_6 = (1,3)$.

(b) $e_1 = (1,2)$, $e_2 = (2,3)$, $e_3 = (3,4)$, $e_4 = (4,5)$, $e_5 = (1,5)$, and $e_6 = (3,1)$.

(c) $e_1 = (2,3)$, $e_2 = (1,2)$, $e_3 = (1,5)$, $e_4 = (3,1)$, $e_5 = (3,4)$, and $e_6 = (4,5)$.

4 Confirm that $QQ^{t} = L(G)$, where G is the graph in Fig. 5.6.4 and $Q = Q(G)$ is the oriented vertex–edge incidence matrix from the corresponding part of Exercise 3.

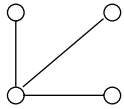
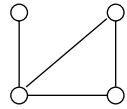
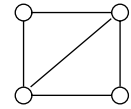
5 Let G be the graph in Fig. 5.6.4.

(a) Exhibit the Laplacian matrix $L(G)$.

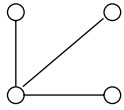
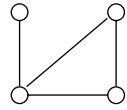
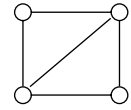
(b) Compute two different entries of $L(G)^{\dagger}$.

(c) Illustrate all $t(G)$ spanning tress of G.

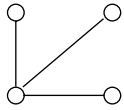
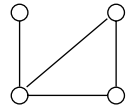
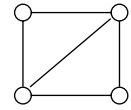
6 Compute the classical adjoint $L(G)^{\dagger}$ if G is the graph

(a)  **(b)**  **(c)** 

7 Compute the Laplacian spectrum $s(G)$ if G is the graph

(a)  **(b)**  **(c)** 

8 M. Fiedler proved that the algebraic connectivity $a(G)$ is at most the vertex connectivity $\kappa(G)$ of Section 5.5, Exercise 19. Confirm Fiedler's result for the graph

(a)  **(b)**  **(c)** 

9 Show that the algebraic connectivity $a(T) \leq 1$ for any tree T on $n \geq 2$ vertices.

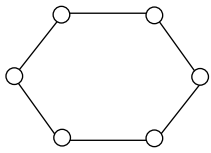
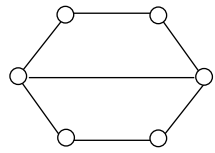
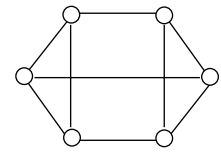
10 Determine whether

(a) (7, 7, 3, 2, 1) majorizes (5, 5, 5, 5). (Justify your answer.)

(b) (5, 5, 4, 2) majorizes (4, 4, 4, 4). (Justify your answer.)

(c) (6) majorizes (2, 2, 2). (Justify your answer.)

11 Confirm that $s(G)$ majorizes $d(G)$ for the graph

(a)  **(b)**  **(c)** 

12 Let G be a bipartite graph with m edges. Show that G can be oriented so that $Q(G)^{\mathrm{t}}Q(G) = I_m + A(G^{\#})$, where $G^{\#}$ is the line graph of G discussed in Section 5.5, Exercise 25.

13 If G is a graph on n vertices, prove that $\lambda_i(G^{\mathrm{c}}) + \lambda_{n-i}(G) = n$, $1 \leq i < n$, i.e., prove that the Laplacian spectrum

$$s(G^{\mathrm{c}}) = (n - \lambda_{n-1}(G), n - \lambda_{n-2}(G), \ldots, n - \lambda_1(G), 0).$$

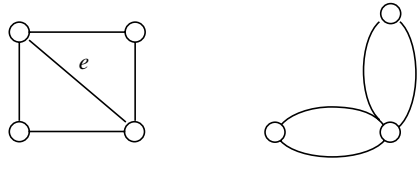
14 Let G be a graph with vertex set $V(G) = \{1, 2, \ldots, n\}$. Prove that

$$XL(G)X^{\mathrm{t}} = \sum_{\{i,j\} \in E(G)} (x_i - x_j)^2,$$

where X is the row vector $(x_1, x_2, \ldots, x_n)$.

15 If G is a graph on n vertices, prove that $\lambda_1(G) \leq n$, with equality if and only if G^{c} is disconnected.

16 Suppose $e = \{u, v\}$ is an edge of the graph $G = (V, E)$. Recall that $G - e = (V, E \setminus \{e\})$ is the graph obtained from G by deleting edge e, and G/e is the graph obtained from $G - e$ by identifying vertices u and v, and deleting any multiple edges that may have arisen in the process. Denote by $G|e$ the multigraph obtained from $G - e$ by identifying vertices u and v, and deleting loops but *not* multiple edges. If, e.g., G is the graph in Fig. 5.6.5*a*, then $G|e$ is the multigraph in Fig. 5.6.5*b*.



(*a*) (*b*)

Figure 5.6.5

(a) Prove that the spanning tree number $t(G) = t(G - e) + t(G|e)$.

(b) Use repeated applications of part (a) to evaluate $t(G)$ for the graph in Fig. 5.6.2*a*.

(c) Use repeated applications of part (a) to evaluate $t(G)$ for the graph in Fig. 5.6.4.

17 If G_1 and G_2 are graphs on disjoint sets of n_1 and n_2 vertices, respectively, prove that the eigenvalues of $L(G_1 \vee G_2)$ are $n_1 + n_2$; $n_2 + \lambda_i(G_1)$, $1 \leq i < n_1$; $n_1 + \lambda_i(G_2)$, $1 \leq i < n_2$; and 0.

18 Compute the eigenvalues of $L(G)$ for

(a) $G = K_{2,2}$. **(b)** $G = K_{2,3}$. **(c)** $G = K_{1,4}$.

(*Hint*: $K_{s,t} = K_s^{\mathrm{c}} \vee K_t^{\mathrm{c}}$. Use Exercise 17.)

19 Confirm Corollary 5.6.21 for

(a) $G = K_{2,2}$. **(b)** $G = K_{2,3}$. **(c)** $G = K_{1,4}$.

20 Prove that the Laplacian spectrum $s(K_n) = (n, n, \ldots, n, 0)$.

21 Let $H = P_4$.

(a) Compute $s(H)$.

(b) Confirm Corollary 5.6.21 for H.

(c) Prove or disprove that, for any graph G, the Laplacian spectrum $s(G)$ consists entirely of integers.

22 Let G and H be the graphs in Fig. 5.6.6. Show that

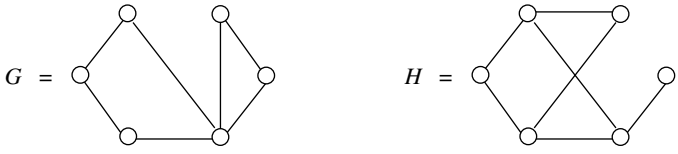


Figure 5.6.6

(a) G and H are not isomorphic.

(b) $\det(xI_6 - L(G)) = x(x-2)(x-3)^2(x^2-6x+4)$.

(c) $\det(xI_6 - L(H)) = x(x-2)(x-3)^2(x^2-6x+4)$.

23 Let G and H be the graphs in Fig. 5.6.7.

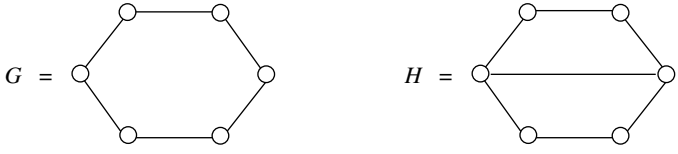


Figure 5.6.7

(a) Compute the Laplacian spectrum $s(G)$.

(b) Compute $s(G^c)$.

(c) Compute $s(H)$.

(d) Compute $s(H^c)$.

(e) Show that the union $G + G^c$ is not isomorphic to $H + H^c$.

(f) Show that the join $G \vee G^c$ is not isomorphic to $H \vee H^c$.

(g) Compute $s(G + G^c)$.

(h) Show that $s(H + H^c) = s(G + G^c)$.

(i) Show that $s(H \vee H^c) = s(G \vee G^c)$.

5.7. GRAPHIC PARTITIONS

Luck is the residue of design.

— Branch Rickey

Suppose $\pi = [\pi_1, \pi_2, \ldots, \pi_\ell] \vdash k$. Under what conditions will π be the degree sequence of some graph?

5.7.1 Definition. Partition π is *graphic* if there exists a graph G with degree sequence $d(G) = \pi$.

Because the parts of a partition must be positive, but graphs can have isolated vertices of degree 0, not every degree sequence is a graphic partition. However, the degree sequence of any graph can be obtained from some graphic partition by appending finitely many zeros.

An obvious necessary condition for $\pi \vdash k$ to be graphic emerges from the first theorem of graph theory, namely, k must be even. Almost as obvious is the necessary condition that $\ell = \pi_1^* \geq \pi_1 + 1$, where $\pi^* = [\pi_1^*, \pi_2^*, \ldots]$ is the partition conjugate to π. In a graph with π_1^* vertices of positive degree, π_1 (the maximum vertex degree) can be no more than $\pi_1^* - 1$. In fact, this second criterion can be extended. To see how, suppose G is the graph illustrated in Fig. 5.7.1, with vertex set $V(G) = \{1, 2, \ldots, 6\}$ and degree sequence $d(G) = \pi = (5, 3^2, 2^2, 1)$.

A *Young tableau*[*] is a variation on a Ferrers diagram in which the boxes contain numbers. In Fig. 5.7.2*a*, e.g., every box in row i of $F(\pi)$ contains vertex number i, $1 \leq i \leq 6$. In Fig. 7.6.2*b*, the boxes in row i of $F(\pi)$ contain, in increasing order, the numbers of the vertices adjacent in G to vertex i, $1 \leq i \leq 6$. Note that, in addition to having the same shape, the two tableaux contain the same integers with the same multiplicities. While it is framed in the context of this example, the discussion that follows remains valid for any graphic partition.

Consider the tableau in Fig. 5.7.2*b*. Because the numbers in each row are arranged in increasing order, the first *column* contains all the 1's. Moreover, because vertex 1 is not adjacent to itself, the top entry of column 1 contains a number larger than 1. Thus, we recover the second criterion for π to be graphic, namely, $\pi_1^* \geq \pi_1 + 1$.

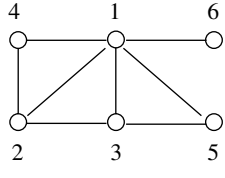


Figure 5.7.1

[*]Named for Alfred Young (1873–1940).

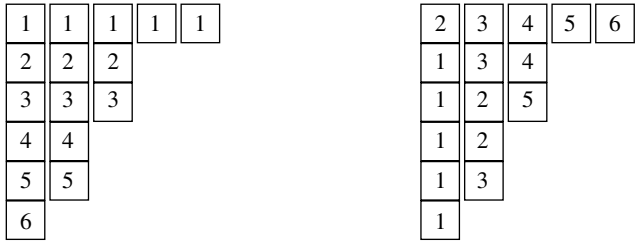


Figure 5.7.2

Continuing with the tableau in Fig. 5.7.2*b*, all the 2's must lie in the first two columns. Moreover, because the first number in row 1 is at least 2, the second number in row 1 (i.e., the top number in column 2) must be at least 3. Indeed, since it cannot be 2, the second number in the second row (i.e., the second number in column 2) also cannot be less than 3. In addition to all the 1's and all the 2's, the first two columns of the second tableau must contain (at least) two numbers larger than 2. Hence, $\pi_1^* + \pi_2^* \geq \pi_1 + \pi_2 + 2$.

As long as $\pi_r \geq r$, this same approach proves that

$$\begin{aligned} \pi_1^* + \pi_2^* + \cdots + \pi_r^* &\geq \pi_1 + \pi_2 + \cdots + \pi_r + r \\ &= (\pi_1 + 1) + (\pi_2 + 1) + \cdots + (\pi_r + 1). \end{aligned} \tag{5.40}$$

Let's give a name to the number of parts of π that satisfy $\pi_r \geq r$.

5.7.2 Definition. If $\pi \vdash k$, the *trace* of π is $f(\pi) = o(\{r : \pi_r \geq r\})$.

Geometrically, $f(\pi)$ is the length of the *diagonal* of $F(\pi)$. To make them easier to recognize, the diagonal boxes of the Ferrers diagram for $\tau = [5, 4, 3^2, 2, 1]$ have been darkened in Fig. 5.7.3. Note, in particular, that $F(\tau)$ is completely determined by its first $f(\tau)$ rows and columns.

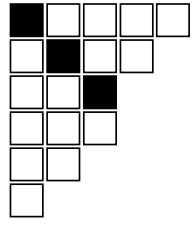


Figure 5.7.3

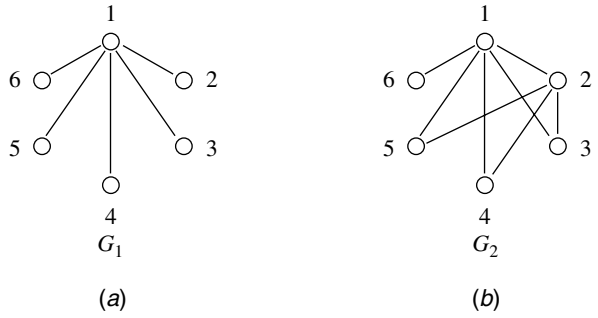


Figure 5.7.4

5.7.3 (Ruch–Gutman) Theorem.[*] *Let* $\pi = [\pi_1, \pi_2, \ldots, \pi_\ell]$ *be a partition of* $2m$ *for some positive integer* m*. Then* π *is graphic if and only if*

$$\sum_{j=1}^{r} \pi_j^* \geq \sum_{j=1}^{r} (\pi_j + 1), \qquad 1 \leq r \leq f(\pi). \tag{5.41}$$

While they may seem complicated and technical, Inequalities (5.41) are the same necessary conditions for π to be graphic as those expressed by Inequalities (5.40). Before addressing sufficiency, we will give some examples and discuss an alternative presentation, due to Tom Roby,[†] that may be more appealing.

5.7.4 Example. Consider the partition $\tau = [5, 4, 3, 3, 2, 1]$. Because $\tau \vdash 18$, the first condition of Theorem 5.7.3 is satisfied $(m = 9)$. From Fig. 5.7.3, it is easy to see that $\tau^* = [6, 5, 4, 2, 1]$. Because $\tau_j^* = \tau_j + 1$, $1 \leq j \leq 3 = f(\tau)$, equality holds in each of Inequalities (5.41).

In this case, it is easy to *construct* a graph having degree sequence τ. Draw six points in the plane and label them $1, 2, \ldots, 6$. Drawing arcs from vertex 1 to each of vertices 2–6 results in the graph G_1, illustrated in Fig. 5.7.4*a*, whose largest vertex degree is $\tau_1 = 5$.

Joining vertex 2 to vertices 3, 4, and 5 results in the graph G_2 shown in Fig. 5.7.4*b*. Note that the first two components of $d(G_2) = (5, 4, 2, 2, 2, 1)$ are $\tau_1 = 5$ and $\tau_2 = 4$. So far, so good. To obtain a graph that *realizes* τ i.e., a graph G with degree sequence $d(G) = \tau$, it remains to add an arc between vertices 3 and 4 of G_2.

What about taking this same *greedy* approach with, say, $\gamma = [3^6]$? With $f(\gamma) = 3$ and $\gamma^* = [6^3]$, it is easy to see that Inequalities (5.41) are satisfied. So, as before, label six points in the plane with the numbers 1–6. Joining vertex 1 to vertices 2–4

[*]Theorem 5.7.3 seems first to have been published by E. Ruch and I. Gutman, The branching extent of graphs, *J. Combin. Inform. System Sci.* 4 (1979), 285–295. Also see W. Hässelbarth, Die Verzweigtheit von Graphen, *Commun. Math. Computer Chem.* (MATCH) 16 (1984), 3–17.

[†]Tom Roby is a professor at California State University, Hayward.

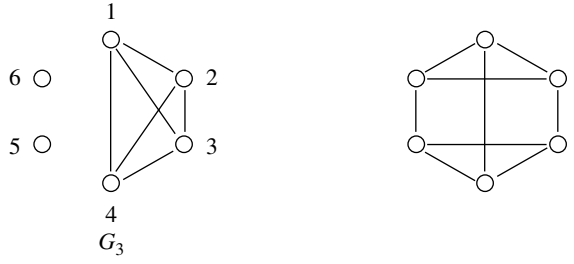


Figure 5.7.5

results in a graph G_1 having degree sequence $d(G_1) = (3, 1, 1, 1, 0, 0)$, the first coordinate of which is $3 = \gamma_1$. Graph G_2 with degree sequence $d(G_2) = (3, 3, 2, 2, 0, 0)$ is obtained from G_1 by adding arcs from vertex 2 to vertices 3 and 4. Finally, adding an arc between vertices 3 and 4 results in the graph G_3, illustrated in Fig. 5.7.5*a*, with degree sequence $d(G_3) = (3, 3, 3, 3, 0, 0)$. So far, so good. However, as a moment's reflection shows, no graph realizing γ can be obtained from G_3 by adding more arcs![*] (A graph that *does* realize γ can be found in Fig. 5.7.5*b*.) □

5.7.5 Definition. Suppose $\tau \vdash 2m$. If $\tau_j^* = \tau_j + 1,\ 1 \le j \le f(\tau)$, then τ is a *threshold partition*.

Coming to the promised alternative presentation of the Ruch–Gutman criteria, suppose $\pi \vdash k$. Denote that portion of $F(\pi)$ consisting of the boxes on or to the *right* of its diagonal by $R(\pi)$. Let $B(\pi)$ be what's left, i.e., the boxes *below* the diagonal. If $\pi = [4, 3^2, 2^2, 1^2]$, e.g., this division of $F(\pi)$ is illustrated in Fig. 5.7.6 (where diagonal boxes have again been darkened to facilitate their easy recognition).

5.7.6 Definition. Suppose $\pi \vdash k$. Let $\rho(\pi)$ be the partition whose parts are the lengths of the *rows* of the *shifted shape* $R(\pi)$. Denote by $\beta(\pi)$ the partition whose parts are the lengths of the *columns* of $B(\pi)$.

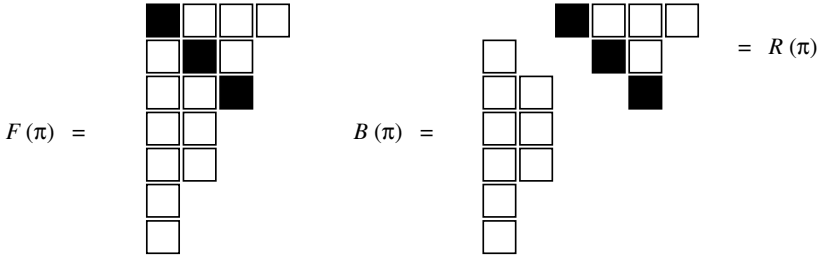


Figure 5.7.6

[*] While the greedy approach does not work in all cases, it does work whenever $\pi \vdash 2m$ satisfies $\pi_j^* = \pi_j + 1$, $1 \le j \le f(\pi)$. See Exercise 11 (below).

If $\pi = [4, 3^2, 2^2, 1^2]$ then, from Fig. 5.7.6, $\rho(\pi) = [4, 2, 1]$ and $\beta(\pi) = [6, 3]$. Observe, in general, that shifted shapes $R(\pi)$ and $B(\pi)$ can be the pieces of such a division of $F(\pi)$, only if $f(\pi) - 1 \leq \ell(\beta(\pi)) \leq f(\pi) = \ell(\rho(\pi))$.

5.7.7 Definition. If $(a) = (a_1, a_2, \ldots, a_s)$ and $(b) = (b_1, b_2, \ldots, b_t)$ are two nonincreasing sequences of real numbers, then (a) *weakly majorizes* (b), written $(a) \succcurlyeq_w (b)$, if $t \geq s$,

$$\sum_{i=1}^{r} a_i \geq \sum_{i=1}^{r} b_i, \qquad 1 \leq r \leq s, \tag{5.42}$$

and

$$\sum_{i=1}^{s} a_i \geq \sum_{i=1}^{t} b_i. \tag{5.43}$$

Evidently, (a) majorizes (b) if and only if $(a) \succcurlyeq_w (b)$, with equality in Inequality (5.43). With the appearance of Definition 5.7.7 we finally have the vocabulary we needed to state Roby's elegant variation on the Ruch–Gutman criteria.

5.7.8 Theorem. *If $\pi \vdash 2m$, then π is graphic if and only if $\beta(\pi)$ weakly majorizes $\rho(\pi)$.*

To see that Theorems 5.7.3 and 5.7.8 are equivalent, observe that $\beta_1 \geq \rho_1$ if and only if $\pi_1^* - 1 \geq \pi_1$, if and only if $\pi_1^* \geq \pi_1 + 1$; $\beta_1 + \beta_2 \geq \rho_1 + \rho_2$ if and only if $(\pi_1^* - 1) + (\pi_2^* - 2) \geq \pi_1 + (\pi_2 - 1)$, if and only if $\pi_1^* + \pi_2^* \geq (\pi_1 + 1) + (\pi_2 + 1)$; and so on. Notice that equality holds throughout Inequalities (5.41), if and only if π is a threshold partition, if and only if $\pi_i^* = \pi_i + 1$, $1 \leq i \leq f(\pi)$, if and only if $\beta(\pi) = \rho(\pi)$. Let's formalize this observation for future reference.

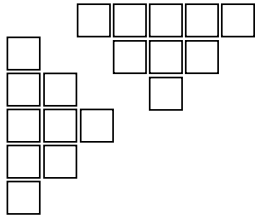
5.7.9 Corollary. *Partition π is a threshold partition if and only if $\beta(\pi) = \rho(\pi)$.*

However they may be stated, the proof that the Ruch-Gutman criteria are sufficient for $\pi \vdash 2m$ to be graphic begins with the following.

5.7.10 Lemma. *If $\tau \vdash 2m$ is a threshold partition, then τ is a graphic partition.*

5.7.11 Example. Consider the partition $\tau = [5, 4, 3^2, 2, 1]$ in Example 5.7.4. From the division of $F(\tau)$ illustrated in Fig. 5.7.7*a* (with no boxes darkened), it is easy to see that $B(\tau)$ is the transpose of $R(\tau)$, so $\beta(\tau) = \rho(\tau)$, i.e., τ is a threshold partition.

Observe that the symmetric, $\ell(\tau) \times \ell(\tau), (0, 1)$-matrix $A(\tau)$ in Fig. 5.7.7*b*, obtained from Fig. 5.7.7*a* by replacing boxes with 1's and spaces with 0's, is the adjacency matrix of a graph with degree sequence τ. □



$F(\tau)$

(*a*)

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$A(\tau)$

(*b*)

Figure 5.7.7

Proof of Lemma 5.7.10. As in Example 5.7.11, let $A(\tau) = (a_{ij})$ be the $\ell(\tau)$-square matrix defined by $a_{ij} = 0$ if $i = j$ or if $i < j$ and $\tau_i + 1 < j$; $a_{ij} = 1$ if $i < j \leq \tau_i + 1$; and $a_{ij} = a_{ji}$ if $i > j$. Then $A(\tau)$ is the adjacency matrix of a graph realizing τ. ■

Sufficiency of the Ruch–Gutman criteria: The proof of sufficiency can be reduced to Lemma 5.7.10 in two steps. The first is to show that if π is majorized (that's right, not *weakly* majorized, but majorized) by a graphic partition, then π is graphic. The second is to show that any partition that satisfies Inequalities (5.41) is majorized by a threshold partition. Details are omitted.

5.7.12 Example. While any two partitions of k are majorization comparable when $k \leq 5$, neither $[3^2]$ nor $[4, 1^2]$ majorizes the other. The majorization *partial order* for the 11 partitions of 6 is illustrated by the so-called *Hasse diagram* in Fig. 5.7.8, where the graphic partitions have been darkened. Observe that the threshold partitions $[2^3]$ and $[3, 1^3]$ are *maximal* among the graphic partitions. □

5.7.13 Definition. A *threshold graph* is one whose degree sequence is, apart from 0's, a threshold partition.

Many interesting things are known about threshold graphs, a few of which are listed below.*

5.7.14 Theorem. *A threshold graph is uniquely determined by its degree sequence, i.e., two threshold graphs are isomorphic if and only if they have the same degree sequence.*

It follows from Theorem 5.7.14 that there is a one-to-one correspondence between the threshold graphs with m edges and no isolated vertices, and the

* Further details can be found, e.g., in R. Merris, *Graph Theory*, Wiley-Interscience, New York, 2001.

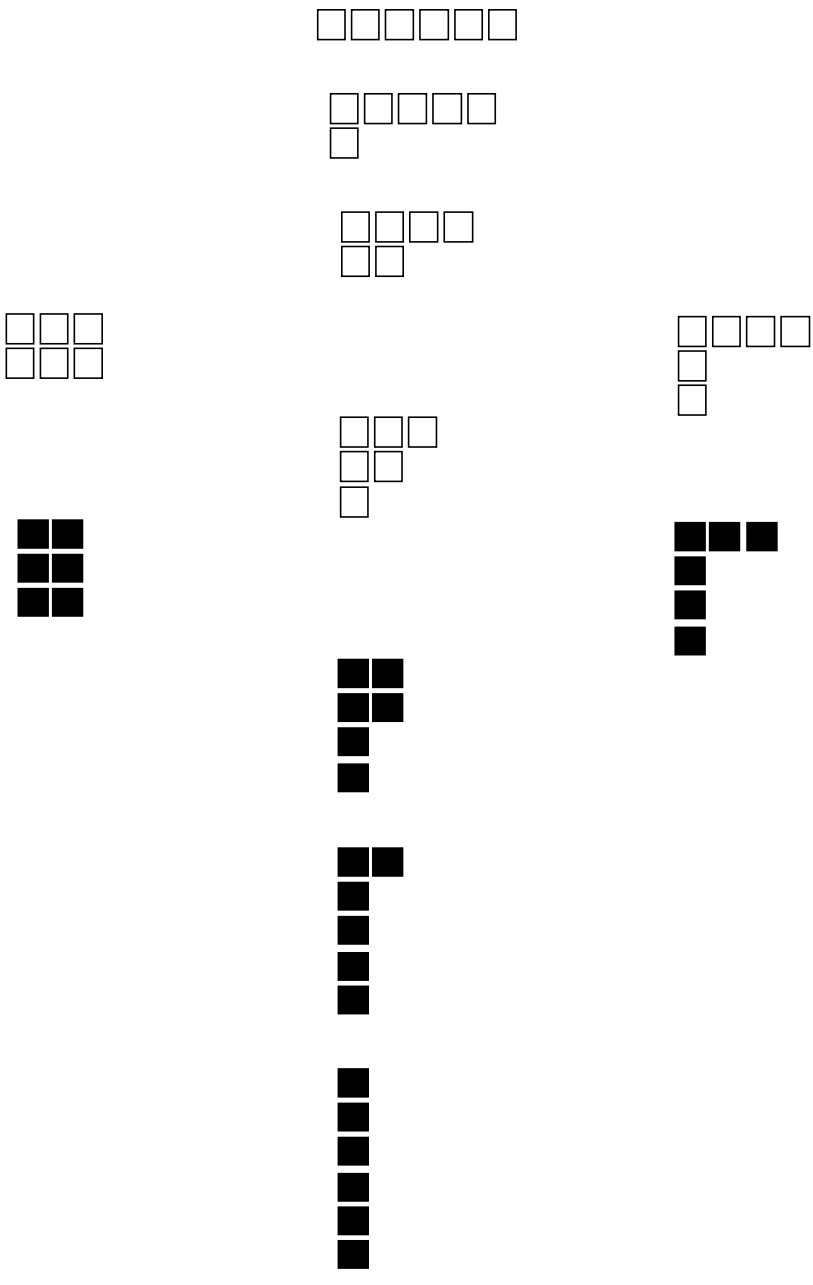


Figure 5.7.8. Partitions of 6 partially ordered by majorization.

partitions $\tau \vdash 2m$ that satisfy $\rho(\tau) = \beta(\tau)$, i.e., that satisfy $R(\tau) = B(\tau)^t$. In other words, there is a one-to-one correspondence between the threshold graphs with m edges and no isolated vertices, and the shifted shape partitions of m. But the shifted shape partitions are precisely the partitions having distinct parts. In view of Example 4.3.10, this proves the following.

5.7.15 Corollary. *The number of nonisomorphic threshold graphs with m edges and no isolated vertices is the coefficient of x^m in the generating function*

$$\prod_{j\geq 1}(1+x^j) = 1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + 4x^6 + \cdots$$

5.7.16 Example. The 12 nonisomorphic connected threshold graphs with $2 \leq m \leq 6$ edges are illustrated in Fig. 5.7.9. □

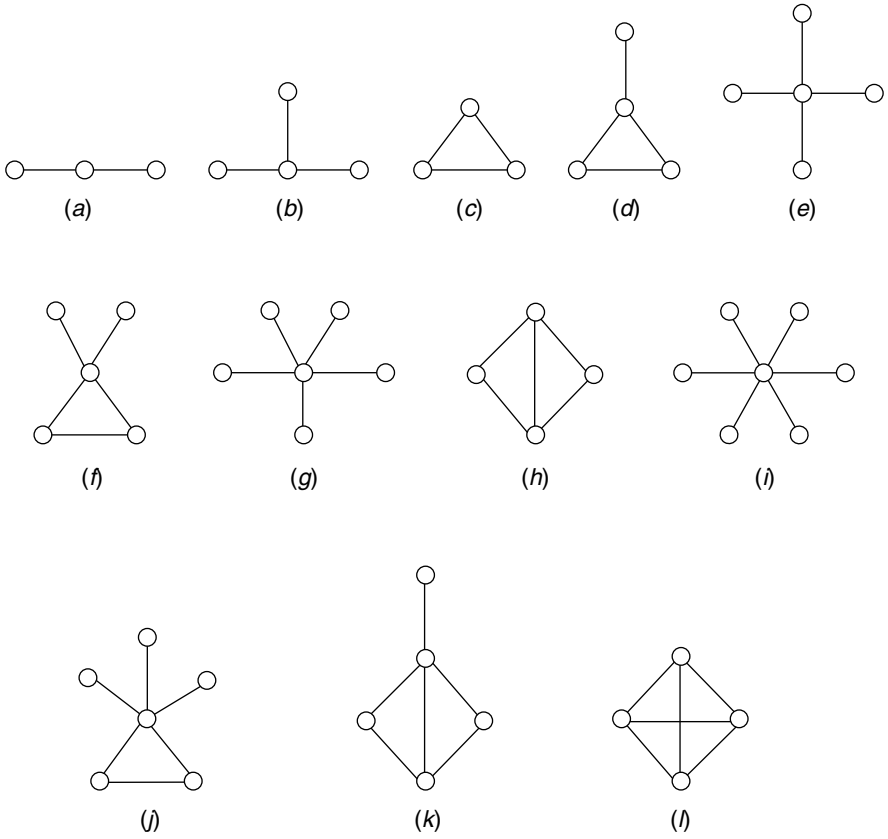


Figure 5.7.9

Finally, there is an interesting characterization of threshold graphs by means of Laplacian spectra.

5.7.17 (Merris's) Theorem.[*] *Let G be a graph on n vertices, none of which is isolated (of degree 0). Then G is a threshold graph if and only if the conjugate of its degree sequence is equal to $[\lambda_1(G), \lambda_2(G), \ldots, \lambda_{n-1}(G)]$, where $s(G) = (\lambda_1(G), \lambda_2(G), \ldots, \lambda_n(G))$ is the Laplacian spectrum of G.*

While not especially difficult, the proof of Theorem 5.7.17 is beyond the scope of this text.

5.7. EXERCISES

1 Which of the following sequences weakly majorizes (2.5, 1.5, 1)? Justify your answer.

(a) (3, 1). **(b)** (3, 2). **(c)** (3, 3).

(d) (4, 1). **(e)** (5, 1). **(f)** (6, 1).

2 Exhibit $F(\pi)$, $R(\pi)$, $B(\pi)$, and $f(\pi)$ for the partition

(a) $\pi = [6^2, 2^2]$. **(b)** $\pi = [6^2, 3^4, 2]$.

(c) $\pi = [7, 6, 5^2, 4^2, 2, 1]$. **(d)** $\pi = [4^5]$.

(e) $\pi = [5^4]$. **(f)** $\pi = [2^6]$.

(g) $\pi = [3, 2^2, 1^2]$. **(h)** $\pi = [2, 1^5]$.

3 Which of the partitions in Exercise 2

(a) is graphic? **(b)** is threshold?

(Justify your answers.)

4 Exhibit a graph with degree sequence

(a) $(4, 4, 3, 2, 2, 1)$. **(b)** $(5, 5, 3, 3, 3, 3)$.

5 Exhibit two nonisomorphic graphs, both having degree sequence

(a) $(2, 2, 2, 2, 2, 2)$. **(b)** $(3, 3, 3, 3, 3, 3)$.

6 Graph G is *r-regular* if $d_G(v) = r$ for all $v \in V(G)$. Prove that

(a) $\pi = [r^n]$ is graphic if $1 \leq r < n$ and the product $r \times n$ is even.

(b) $\pi = [r^n]$ is threshold if and only if $r = n - 1$.

[*] R. Merris, Degree maximal graphs are Laplacian integral, *Linear Algebra Appl.* 199 (1994), 381–389.

7 Exhibit graphs whose degree sequences match the five graphic partitions of Fig. 5.7.8.

8 A graph on n vertices is *antiregular* if its multiset of vertex degrees contains $n-1$ different numbers. (See, e.g., Example 5.7.4.)

(a) Illustrate the nonisomorphic antiregular graphs on five vertices.

(b) If G is a connected antiregular graph on n vertices, show that there exist two vertices $u, w \in V(G)$ such that $d_G(u) = d_G(w)$.

(c) Show that the common value of $d_G(u)$ and $d_G(w)$ in part (a) is $\lceil (n-1)/2 \rceil$, the integer obtained from $(n-1)/2$ by rounding up.

(d) Prove that every connected antiregular graph is a threshold graph.

9 Prove that π^* majorizes π for every graphic partition π.

10 Confirm Theorem 5.7.14 by proving independently that, up to isomorphism, there is just one graph with degree sequence

(a) $[5^2, 2^4]$. **(b)** $[5^2, 3^2, 2^2]$. **(c)** $[5, 4, 3^2, 2, 1]$.

11 Design an algorithm to input a threshold partition τ, and return a (threshold) graph G satisfying $d(G) = \tau$.

12 Let $\pi = [5^2, 3^4]$. Show that

(a) π is a graphic partition.

(b) π is not a threshold partition.

(c) up to isomorphism, there is a unique graph having degree sequence π.

13 Confirm Theorem 5.7.17 for the graph G in

(a) Fig. 5.7.9*d*. **(b)** Fig. 5.7.9*e*.

(c) Fig. 5.7.9*h*. **(d)** Fig. 5.7.9*f*.

14 If G is a threshold graph, then the chromatic number $\chi(G) = \omega(G)$, the size of a largest clique. Confirm this result for the graph in

(a) Fig. 5.7.9*d*. **(b)** Fig. 5.7.9*e*.

(c) Fig. 5.7.9*h*. **(d)** Fig. 5.7.9*f*.

15 If $G = (V, E)$ is a threshold graph, there exists an integer t and an integer-valued function f of V such that $\{u, v\} \in E$ if and only if $f(u) + f(v) > t$. Confirm this result by finding f and t for the graph in

(a) Fig. 5.7.9*d*. **(b)** Fig. 5.7.9*e*.

(c) Fig. 5.7.9*h*. **(d)** Fig. 5.7.9*f*.

16 If $G = (V, E)$ is a threshold graph, there exists an integer t and a *positive* integer-valued function f of V such that $X \subset V$ is an independent set of

vertices if and only if $\sum_{u \in x} f(u) \leq t$. Confirm this result by finding f and t for the graph in

(a) Fig. 5.7.9*d*. **(b)** Fig. 5.7.9*e*.

(c) Fig. 5.7.9*h*. **(d)** Fig. 5.7.9*f*.

17 The function f in Exercise 16 is called a *threshold labeling*. In many cases, labeling vertices by their degrees produces a threshold labeling.

(a) Show that labeling the vertices of the graph in Fig. 5.7.9*j* by its vertex degrees is not a threshold labeling.

(b) Find a threshold labeling for the graph in Fig. 5.7.9*j*.

18 It is known that G is a threshold graph if and only if it does not contain an induced subgraph isomorphic to one of the three *forbidden* graphs P_4, C_4, or $K_2 + K_2$. Show that none of these forbidden graphs is a threshold graph.

19 A *split graph* is one whose vertex set can be partitioned into a clique and an independent set. It is known that G is a split graph if and only if it does not have an induced subgraph isomorphic to one of the three graphs C_4, C_5, or $K_2 + K_2$. Prove that every threshold graph is a split graph.

20 Prove that the Laplacian spectrum of a threshold graph consists entirely of integers.

21 Find a connected, nonthreshold graph G whose Laplacian spectrum consists entirely of integers.

22 Let G be a threshold graph on n vertices. Prove that G either has a vertex of degree 0 or a vertex of degree $n - 1$.

23 Confirm the result you obtained in Exercise 19 for the graph in

(a) Fig. 5.7.9*d*. **(b)** Fig. 5.7.9*e*.

(c) Fig. 5.7.9*h*. **(d)** Fig. 5.7.9*f*.

24 Let G be a threshold graph. Suppose $\{u, v\} \in E(G)$. If $x, y \in V(G)$ satisfy $d(x) \geq d(u)$ and $d(y) \geq d(v)$, prove that $\{x, y\} \in E$.

25 It is known that there are exactly 2^{n-2} nonisomorphic connected threshold graphs on n vertices. When $n = 5$, three of the eight are exhibited in Fig. 5.7.9. Illustrate the other five.

26 Graph G is an *interval* graph if there is a one-to-one function f from $V(G)$ into the family of open intervals of the real line such that $\{u, v\} \in E(G)$ if and only if $f(u) \cap f(v) \neq \varnothing$. It is known that every threshold graph is an interval graph. Confirm this for the graph G *in*

(a) Fig. 5.7.9*d*. **(b)** Fig. 5.7.9*e*.

(c) Fig. 5.7.9*h*. **(d)** Fig. 5.7.9*f*.

27 Let G be a graph with vertex set $V = \{v_1, v_2, \ldots, v_n\}$ and edge set $E = \{e_1, e_2, \ldots, e_m\}$. The $n \times m$ *incidence matrix* $T(G) = (t_{ij})$ is defined by $t_{ij} = 1$ if v_i is incident with e_j, and t_{ij} otherwise.

(a) Show that $t_{ij} = |q_{ij}|$, $1 \leq i \leq n$, $1 \leq j \leq m$, where $Q(G) = (q_{ij})$ is the oriented vertex–edge incidence matrix afforded by some arbitrary orientation of G.

(b) If G is r-regular (Exercise 6), show that $n = 2m/r$.

(c) If G is r-regular, $r > 1$, show that the triple of parameters for the binary code $\mathscr{C}$ comprised of the rows of $T(G)$ is $(m, 2m/r, 2r - 2)$.

6

Codes and Designs

While this chapter is independent of Chapters 3–5, Section 1.4 is an essential prerequisite for Sections 6.1, 6.2, and 6.4.

In 1455, Johann Gutenberg printed what is commonly believed to have been the first book set in movable type. By making information widely accessible, this technical innovation profoundly influenced the development of human civilization for the next 500 years. Indeed, the next leap of comparable magnitude did not take place until 1946, when civilian scientists began to think of information as strings of 0's and 1's.

Launched March 2, 1972, *Pioneer* 10 was the first spacecraft to travel through the asteroid belt. After a rendezvous with Jupiter in December, 1973, *Pioneer* continued downstream through the heliomagnetosphere, passing the orbit of Pluto in 1983. On March 2, 2002, 30 years after its launch, 5 years after its scientific mission ended, and 22 hours after a message was beamed to it from a NASA facility in the Mojave Desert, a 10^{-20}-watt signal was received from the spacecraft by a radio telescope in Spain. The fact that an identifiable signal could be detected at all is an engineering triumph of the first magnitude. The fact that the *message* carried by the signal was decipherable, despite distance* and background noise, is a triumph for the mathematical theory of error-correcting codes, the defining topic of this chapter.

Apart from the pictures themselves, one of the most dramatic things about photographs from the early *Pioneer*, *Voyager*, and *Mariner* missions was their emergence, one pixel at a time, on the big screen of the Jet Propulsion Laboratory as the transmissions from space were decoded in real time. This achievement was made possible by a combination of the fastest digital computers then available and a fast algorithm for decoding messages, the topic of Sections 6.1 and 6.2.

Applications of error-correcting codes in telecommunications have driven renewed interest in a beautiful areas of combinatorics that deals with relationships between numerical constraints and geometric configurations. Mutually orthogonal

**Pioneer* 10 had, by then, ceased to be the most distant man-made object. On February 17, 1998, it was surpassed by *Voyager* 1, headed in the opposite direction, upstream toward the nose of the heliomagnetosphere.

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

Latin squares and their connection with finite projective planes are the subject of Section 6.3. this section is independent of Sections 6.1 and 6.2 and may be used, all by itself, as an optional excursion at any point during the course. On the other hand, some readers may wish to exit from Chapter 6, either immediately after Example 6.2.9, or at the end of Section 6.2.

Applications of finite projective planes is through their (0,1)-incidence matrices, motivating the generalization to balanced incomplete block designs (BIBDs). Section 6.4 is a brief introduction to the existence of BIBDs.

6.1. LINEAR CODES

Recall from Section 1.4 that an (n, M, d) code $\mathscr{C}$ is a nonempty set of M binary words of length n, the minimum distance between any pair of which is d. *Nearest-neighbor decoding* refers to a process by which an erroneous binary word b is corrected to a legitimate codeword c such that

$$d(b, c) = \min_{w \in \mathscr{C}} d(b, w).$$

An (n, M, d) code can reliably detect as many as $d - 1$ errors. Using nearest-neighbor decoding, it can reliably correct as many as $r = \lfloor (d - 1)/2 \rfloor$.

So far, so good, but what about a practical *process*? Given a binary word b, how, exactly, does one go about finding a codeword w that minimizes $d(b,w)$? When $\mathscr{C} = \{00000, 11111\}$, that isn't much of a problem. When M is large, however, it may not be easy to find the smallest number in the M-element set $\{d(b, w) \ : \ w \in \mathscr{C}\}$, much less compute $d(b, w)$ for every $w \in \mathscr{C}$, much less do these things for every word in a long message, much less do it in real time! Among the many virtues of *linear codes* is a fast, efficient process for nearest-neighbor decoding.

Our discussion of linear codes begins with the notion of Boolean arithmetic.* Recall that a binary code is a subset of F^n, i.e., a set of n-bit words assembled from the alphabet $F = \{0, 1\}$. In these statements, 0 and 1 are viewed as letters. However, it can be useful to view them as numbers. The distinction involves arithmetic—of a sort. *Boolean addition* and *multiplication* are defined for the elements of F by means of the tables in Fig. 6.1.1.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Figure 6.1.1. Boolean arithmetic.†

*Named for George Boole (1815–1864).

†Boolean arithmetic makes $F = \{0, 1\}$ a "field of characteristic 2." Having no need for the theory behind these words, we will avoid using them.

While Boolean multiplication is identical to ordinary multiplication, Boolean addition differs from ordinary addition in one important way, namely, $1 + 1 = 0$. In effect, this makes $+1$ and -1 the same, which makes addition the same as subtraction! Boolean addition is extended to F^n, bit by bit.

6.1.1 Example. In F^3, e.g., $101 + 011 = 110$, $010 + 111 = 101$, $110 + 111 = 001$, and $110 + 110 = 000$. Indeed, $w + w = 000$ for all $w \in F^3$. Boolean addition of words from F^n is both commutative and associative. □

The first important application of Boolean arithmetic requires the following idea.

6.1.2 Definition. The *weight* of a binary word u, denoted $\mathrm{wt}(u)$, is the number of 1's in u.

For example, $\mathrm{wt}(01011000) = 3$ and $\mathrm{wt}(10111001) = 5$.

6.1.3 Theorem. *The distance between binary words $u, v \in F^n$ is the weight of their sum, i.e., $d(u, v) = wt(u + v)$.*

Proof. If $u = u_1u_2 \cdots u_n$ and $v = v_1v_2 \cdots v_n$ then w_i, the ith bit of $u + v = w_1w_2 \cdots w_n$, is 1 if and only if $u_i \neq v_i$. (See the addition table in Fig. 6.1.1.) Thus, $\mathrm{wt}(u + v)$ counts the number of places in which u and v differ. ■

6.1.4 Definition. A binary code $\mathscr{C}$ is *linear* if the sum of any two codewords is another codeword, i.e., if $u + v \in \mathscr{C}$ for all $u, v \in \mathscr{C}$.

6.1.5 Example. Among the linear codes is F^n, the set of all 2^n binary words of length n. The code $\mathscr{C}_1 = \{000, 100, 001, 101\}$ is linear, but the code $S = \{101, 010, 111\}$ is not. While it is true that the sums $101 + 010 = 111$, $101 + 111 = 010$, and $010 + 111 = 101$ are all elements of S, $101 + 101 = 000$ is not. The smallest linear code containing S is $\mathscr{C}_2 = \{000, 101, 010, 111\}$. □

It is clear from Example 6.1.5 that every linear code contains the binary word each of whose bits is 0. When n is understood, the *zero word* $00\ldots0 \in F^n$ is denoted 0. This usage introduces an obvious ambiguity. Whether the symbol 0 is to be understood as a single bit or as a binary word of length n will have to be discerned from the context.

Why introduce deliberate ambiguities? Why not use, e.g., z to denote the zero word? It is because the zero word *plays the role* of zero in the sense that $b + 0 = b$ for every binary word $b \in F^n$. Indeed, with respect to the "scalar multiplication" of binary words defined by

$$1b = b \quad \text{and} \quad 0b = 0, \tag{6.1}$$

F^n is a *vector space*, with binary words playing the role of vectors, and $F = \{0, 1\}$ playing the role of the "scalar field" (where the arithmetic is Boolean). While binary codes are subsets of F^n, linear codes are sub*spaces* of F^n, i.e., $\mathscr{C}$ is a linear code if and only if it is a (Boolean) vector space!

6.1.6 Definition. If S is a nonempty subset of F^n, the subspace *generated* (or *spanned*) by S is the linear code $\mathscr{L}(S)$ consisting of all (Boolean) linear combinations of binary words from S.

As in "ordinary" linear algebra,* $\mathscr{L}(S)$ is the intersection of all the linear codes (subspaces of F^n) that contain S. In particular (when $\varnothing \neq S \subset F^n$), $S \subset \mathscr{L}(S)$ with equality if and only if S is a linear code.

Recall that a minimal generating set is a *basis*.† (Evidently, S contains a basis of $\mathscr{L}(S)$.) If $B = \{u_1, u_2, \cdots, u_k\}$‡ is a basis of $\mathscr{C}$, then every codeword $w \in \mathscr{C}$ is uniquely expressible as a linear combination

$$w = a_1u_1 + a_2u_2 + \cdots + a_ku_k, \tag{6.2}$$

where $a_i \in F$, $1 \leq i \leq k$. since each a_i is either 0 or 1, each codeword w is a simple sum of basis vectors. Selecting a codeword w by specifying the coefficients in equation (6.2) is equivalent to making a sequence of k decisions, each having two choices, i.e., $o(\mathscr{C}) = 2^k$, so $\mathscr{C}$ is a $(n, 2^k, d)$ code.§

6.1.7 Corollary. *If $\mathscr{C}$ is an $(n, 2^k, d)$ linear code, then d is the minimum of the weights of the nonzero codewords of $\mathscr{C}$, i.e.,*

$$d = \min_{0 \neq w \in \mathscr{C}} \mathrm{wt}(w).$$

To determine d for an M-word code generally requires computing and comparing $C(M, 2)$ distances. For *linear* codes, Corollary 6.1.7 reduces the chore by a factor of $2/M$.

Proof of Corollary 6.1.7. Since $u + v = 0$ if and only if $u = v$, it follows from Theorem 6.1.3 that

$$d = \min_{\substack{u,v \in \mathscr{C} \\ u \neq v}} d(u, v) \geq \min_{\substack{w \in \mathscr{C} \\ w \neq 0}} \mathrm{wt}(w).$$

The reverse inequality is a consequence of the fact that $d \leq d(w, 0) = \mathrm{wt}(w + 0) = \mathrm{wt}(w)$ whenever $0 \neq w \in \mathscr{C}$. ■

While the notion of a *scalar* ("dot") *product* has the obvious Boolean analog, its interpretation is a little different. If $u = u_1u_2 \cdots u_n$ and $v = v_1v_2 \cdots v_n$ are binary words of length n then

$$u \cdot v = u_1v_1 + u_2v_2 + \cdots + u_nv_n. \tag{6.3}$$

*For example, where the scalars come from the real number field $\mathbb{R}$.

†A basis of $\mathscr{C}$ is a linearly independent set B of vectors such that $\mathscr{C} = \mathscr{L}(\mathrm{B})$.

‡Here $u_i \in \mathscr{C}$ is a codeword of length n, *not* the ith bit of some binary word u.

§Some authors use (n, k, d) to denote the parameters of a linear code. The original $(n, 2^k, d)$ notation will be retained in this book.

Whereas in ordinary linear algebra, $u \cdot u = \|u\|^2$ is the square of the *magnitude* of u, in Boolean linear algebra, $u \cdot u$ is the "parity" of u.

6.1.8 Definition. The *parity* of a binary word w is 1 if the weight of w is odd, and 0 if wt(w) is even.

6.1.9 Example. Consider the (3,4,1) linear code $\mathscr{C} = \{000, 001, 100, 101\}$. With minimum distance $d = 1, \mathscr{C}$ cannot (realiably) detect, much less correct, even a single transmission error. One way to "fix" this deficiency is by repetition, e.g., by sending each message twice. This can be done in two rather different ways. If, e.g., the message is 000-100, repetition could take the form 000-100-000-100, where the message is followed by a duplicate message. An alternative would be to duplicate each word of the message as it is sent, resulting in 000-000-100-100. This alternative is equivalent to sending 000000-100100, i.e., to sending each word once, using a different code. The "repetition" code $\mathscr{C}^{(2)} = \{000000, 001001, 100100, 101101\}$ is obtained by replacing each codeword $xyz \in \mathscr{C}$ with the concatenated word $xyzxyz \in \mathscr{C}^{(2)}$.

Because addition of binary words is bitwise, the linearity of $\mathscr{C}^{(2)}$ is an immediate consequence of the linearity of $\mathscr{C}$. In particular, Corollary 6.1.7 may be used to determine that the minimum distance between any two codewords of $\mathscr{C}^{(2)}$ is $d = 2$. Thus, $\mathscr{C}^{(2)}$ a (6,4,2) code capable of detecting (single) errors, thus "fixing" the deficiency of the original code $\mathscr{C}$.

Here is an alternative to $\mathscr{C}^{(2)}$. Denote by $\mathscr{C}^+ = \{0000, 0011, 1001, 1010\}$ the code obtained from $\mathscr{C}$ by adding a single *parity check* bit to the end of each word, i.e., by replacing $xyz \in \mathscr{C}$ with $xyzp \in \mathscr{C}^+$, where p is the parity of xyz. Because $\mathscr{C}^+$ is a linear code (The proof is left to the exercises, but why wait?), Corollary 6.1.7 can be used to deduce that $\mathscr{C}^+$ is a (4,4,2) code capable of detecting (single) errors. Thus, $\mathscr{C}^+$ also fixes $\mathscr{C}$'s deficiency.

Because its codewords are shorter, $\mathscr{C}^+$ has an obvious advantage over $\mathscr{C}^{(2)}$ in efficiency (and speed). The concatenation idea, on the other hand, seems to have an advantage over the parity check bit idea because it can be extended to obtain, e.g., a (9,4,3) (linear) code $\mathscr{C}^{(3)}$. Because every codeword in $\mathscr{C}^+$ has even weight (parity 0), passing to $\mathscr{C}^{++}$ increases the length of the code without increasing the minimum distance between codewords. The *obvious* extension of the idea that led to $\mathscr{C}^+$ is useless. There are, however, more subtle extensions of the parity check bit idea that hold enormous power. While these extensions will not be fully developed until Section 6.2, they *begin* with the innocent observation that

$$xyzp \cdot 1111 = 0 \tag{6.4}$$

for all $xyzp \in \mathscr{C}^+$. □

In ordinary linear algebra, the scalar product $u \cdot v = 0$, if and only if u and v are orthogonal. It is convenient to use this same terminology in Boolean linear algebra.

6.1.10 Definition. Binary words $u, v \in F^n$ are *orthogonal* if $u \cdot v = 0$.

Equation (6.4) gives a necessary condition for a binary word w to belong to the parity check bit code $\mathscr{C}^+$ of Example 6.1.9, namely, $w \cdot 1111 = 0$. Because, e.g., $w = 0110$ is orthogonal to 1111 but $w \notin \mathscr{C}^+$, this necessary condition is not sufficient. The key to the subtle but powerful extensions of the parity check bit idea entails orthogonality conditions that are both necessary and sufficient. (In the case of Example 6.1.9, $w \in \mathscr{C}^+$ if and only if $w \cdot 1111 = 0$ *and* $w \cdot 0100 = 0$.)

6.1.11 Definition. The *orthogonal complement* of a nonempty subset $S \subset F^n$ is the set $S^\perp = \{w \in F^n \ : \ u \cdot w = 0 \text{ for all } u \in S\}$.

6.1.12 Example. Because orthogonality has more to do with parity than perpendicularity, care should be taken with this concept, e.g., if $S = \{000, 101, 010\}$, then $S^\perp = \{000, 101\} \subset S$. □

6.1.13 Theorem. *If S is a nonempty subset of F^n, then $S^\perp$ is a linear code.*

Proof. Because $u \cdot 0 = 0$ for $u \in S$, $0 \in S^\perp$. If v, $w \in S^\perp$ then, for all $u \in S$, $u \cdot (v + w) = u \cdot v + u \cdot w = 0 + 0 = 0$, so $v + w \in S^\perp$. ■

Since $u \cdot w = w \cdot u$, $S \subset S^{\perp\perp}$. Because $S^{\perp\perp}$ is a linear code and $\mathscr{L}(S)$ is the intersection of all linear codes containing S, it is evidently the case that $\mathscr{L}(S) \subset S^{\perp\perp}$.

6.1.14 Theorem. *If $\varnothing \neq S \subset F^n$, then $\mathscr{L}(S) = S^{\perp\perp}$.*

The proof of Theorem 6.1.14 will occupy us for the rest of this section. Before getting to the details, let's discuss some implications.

6.1.15 Corollary. *If $\mathscr{C}$ is a linear code, then $\mathscr{C} = \mathscr{C}^{\perp\perp}$.*

Proof. If $\mathscr{C}$ is a linear code, then $\mathscr{C} = \mathscr{L}(\mathscr{C}) = \mathscr{C}^{\perp\perp}$. ■

6.1.16 Definition. The *dual* of a linear code $\mathscr{C}$ is the linear code $\mathscr{C}^\perp$.

By Corollary 6.1.15, $(\mathscr{C}^\perp)^\perp = \mathscr{C}^{\perp\perp} = \mathscr{C}$, i.e., the dual of $\mathscr{C}^\perp$ is $\mathscr{C}$. It seems that every linear code is paired with a unique (linear) dual.

Every bit as interesting is the case in which $\mathscr{C} = S^\perp$ for some *nonlinear* code S. By Theorem 6.1.13, $\mathscr{C}$ is a linear code. By Theorem 6.1.14 and the definitions, the dual of $\mathscr{C}$ is $S^{\perp\perp} = \mathscr{L}(S)$. Finally, the dual of $\mathscr{L}(S)$ is $\mathscr{C} = S^\perp$, i.e.,

$$\mathscr{L}(S)^\perp = S^\perp. \tag{6.5}$$

6.1.17 Example. Let's return to Example 6.1.12, where $S = \{000, 101, 010\} \subset F^3$. Because $B = \{101, 010\}$ is linearly independent, it is a basis of $\mathscr{L}(S)$. So, any

codeword in $\mathscr{L}(S)$ is uniquely expressible in the form $a_1\,101 + a_2\,010$, where $a_1, a_2 \in F = \{0, 1\}$. It follows, as in Equation (6.2), that $\mathscr{L}(S)$ contains $2 \times 2 = 4$ codewords, three of which are already in S. The "missing" word is 111, corresponding to $a_1 = a_2 = 1$, i.e.,

$$\mathscr{L}(S) = \{000, 101, 010, 111\}.$$

From Equation (6.5) and Example 6.1.12, $\mathscr{L}(S)^\perp = S^\perp = \{000, 101\}$. Now, despite the fact that $\mathscr{L}(S)^\perp \subset \mathscr{L}(S)$, it is nevertheless the case (as in ordinary linear algebra) that $\dim(\mathscr{L}(S)) + \dim(\mathscr{L}(S)^\perp) = 2 + 1 = 3 = \dim(F^3)$. □

The key to proving Theorem 6.1.14 is the following extension of the last observation from Example 6.1.17.

6.1.18 Lemma. *If $\mathscr{C} \subset F^n$ is a linear code, then*

$$\dim(\mathscr{C}) + \dim(\mathscr{C}^\perp) = n. \tag{6.6}$$

Before embarking on the somewhat technical proof of Lemma 6.1.18, let's see another example.

6.1.19 Example. Let $B = \{11010, 01101, 01110\}$. We claim that B is linearly independent. To prove it, observe that the (vector) equation

$$x\ 11010 + y\ 01101 + z\ 01110 = 00000$$

is equivalent to five linear equations, the first and fifth of which are $x = 0$ and $y = 0$. Together with any of the remaining three equations, these yield $z = 0$.

Let $\mathscr{C} = \mathscr{L}(B)$, the linear code with basis B. From Definition 6.1.11, $w \in \mathscr{C}^\perp$ if and only if $u \cdot w = 0$ for all $u \in \mathscr{C}$ if and only if $u \cdot w = 0$ for all $u \in B$. If $w = x_1x_2x_3x_4x_5$, then $11010 \cdot w = x_1 + x_2 + x_4$, $01101 \cdot w = x_2 + x_3 + x_5$, and $01110 \cdot w = x_2 + x_3 + x_4$, i.e., $w \in \mathscr{C}^\perp$ if and only if

$$x_1 + x_2 + x_4 = 0, \tag{6.7a}$$
$$x_2 + x_3 + x_5 = 0, \tag{6.7b}$$
$$x_2 + x_3 + x_4 = 0. \tag{6.7c}$$

This homogeneous system of linear equations is equivalent to the single matrix equation $Gw^t = 0$, where 0 is the 3×1 column vector of zeros, w^t is the *transpose* of w (the 5×1 column vector whose ith component is x_i), and

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

is the 3×5 matrix whose rows are the basis vectors of $\mathscr{C}$. In other words, $w \in \mathscr{C}^{\perp}$ if and only if w^{t} belongs to the *kernel* of G. Thus, it appears that Equation (6.6) is a consequence of the well-known theorem from (ordinary) linear algebra that the sum of the *rank* and *nullity* of a $k \times n$ matrix is equal to n. To confirm that this result is still valid in Boolean linear algebra, let's walk through the proof for this example.

Because its rows are a basis of $\mathscr{C}$, matrix G has rank $k = 3$, and $\mathscr{C}$ is equal to the row space of G. Recall that the row space of a matrix is unchanged by elementary row operations (a fact that remains valid in the context of Boolean arithmetic). Adding the second row of G to its first and third row produces (because Boolean addition and subtraction are the same) the row equivalent marix

$$G' = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Adding the third row of G' to the first row yields the *Hermite normal form* (or *reduced row echelon form*)* of G, namely,

$$G'' = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Because $Gx = 0$ and $G''x = 0$ have the same solution set, the linear system in Equations (6.7a)–(6.7c) is equivalent to

$$x_1 + x_3 = 0, \tag{6.8a}$$
$$x_2 + x_3 + x_5 = 0, \tag{6.8b}$$
$$x_4 + x_5 = 0. \tag{6.8c}$$

Solving for the leading, *pivot* variables, we obtain

$$\begin{aligned} x_1 &= x_3, \\ x_2 &= x_3 + x_5, \\ x_4 &= x_5, \end{aligned}$$

where the dependent (pivot) variables have been expressed as (linear) functions of the independent (nonpivot) variables x_3 and x_5. These last three equations can be expressed as the single vector equation

$$x_1x_2x_3x_4x_5 = x_3 11100 + x_5 01011. \tag{6.9}$$

*See Appendix 3.

In other words, $w = x_1x_2x_3x_4x_5 \in \mathscr{C}^\perp$ if and only if w is a (Boolean) linear combination of the linearly independent vectors 11100 and 01011, i.e., $\{11100, 01011\}$ is a basis for $\mathscr{C}^\perp$. In particular, $\dim(\mathscr{C}^\perp) = 2$. Thus, $\dim(\mathscr{C}) + \dim(\mathscr{C}^\perp) = 3 + 2 = 5$, the length of the codewords.

It is interesting to observe the dominant role played by bits x_3 and x_5 in Equation (6.9). Once the binary words (vectors) 11100 and 01011 have been indentified, $\mathscr{C}^\perp$ is completely determined by x_3 and x_5. What is the use of x_1, x_2, and x_4? The answer is clear from Equations (6.8a)–(6.8c), where these pivot bits can be seen to play the role of parity check digits! This is the sense in which the idea leading to $\mathscr{C}^+$ in Example 6.1.9 can be generalized to obtain error-correcting codes that are vastly superior to repetition codes.

Finally, interpreting Equations (6.8a)–(6.8c) to mean that $w \in \mathscr{C}^\perp$ if and only if $w \cdot 10100 = 0$, $w \cdot 01101 = 0$, and $w \cdot 00011 = 0$ reminds us that the word "orthogonality" has been borrowed from another context. In Boolean linear algebra, *orthogonality* should be interpreted in terms of *parity*. □

Proof of Lemma 6.1.18 (i.e., $dim(\mathscr{C}) + dim(\mathscr{C}^\perp) = n$). Suppose B is a basis of the $(n, 2^k, d)$ linear code $\mathscr{C}$. Let G be the $k \times n$ matrix whose rows are the vectors in B. Then $\dim(\mathscr{C}) = k = \text{rank}(G)$, the number of pivot variables in the Hermite normal form of G. Because of the ientification of $\mathscr{C}^\perp$ with the kernel of G, $\dim(\mathscr{C}^\perp) = \text{nullity}(G)$ is the number of nonpivot variables of G. It remains to observe that the total number of variables is equal the number of columns of G. ■

Proof of Theorem 6.1.14 (i.e., $\mathscr{L}(S) = S^{\perp\perp}$). Suppose $\varnothing \neq S \subset F^n$. Let $B \subset S$ be a basis of $\mathscr{L}(S)$, and G the $k \times n$ matrix whose rows are the vectors in B. Then $S^\perp = \{v \in F^n \ : \ Gv^t = 0\} = \mathscr{L}(S)^\perp$. Therefore, $\dim(S^\perp) = \dim(\mathscr{L}(S)^\perp)$.

It follows from Lemma 6.1.18 (and Theorem 6.1.13) that

$$\dim(S^\perp) + \dim(S^{\perp\perp}) = n = \dim(\mathscr{L}(S)) + \dim(\mathscr{L}(S)^\perp).$$

Subtracting $\dim(S^\perp)$ from the left-hand side and $\dim(\mathscr{L}(S)^\perp)$ from the right leaves $\dim(S^{\perp\perp}) = \dim(\mathscr{L}(S))$. Since it was established in the discussion leading up to the statement of Theorem 6.1.14 that $\mathscr{L}(S) \subset S^{\perp\perp}$, the proof is complete. ■

The notions that emerged in Example 6.1.19 have implications far beyond the proofs of Lemma 6.1.18 and Theorem 6.1.14. Let's summarize their most striking features.

6.1.20 Definition. Let B be a fixed but arbitrary basis of the linear $(n, 2^k, \text{d})$ code $\mathscr{C}$. The $k \times n$ matrix G whose rows are the vectors of B is a *generating matrix* for $\mathscr{C}$.

6.1.21 Theorem. *If G is a generating matrix for the linear code $\mathscr{C}$, then $w \in \mathscr{C}^\perp$ if and only if $Gw^t = 0$, if and only if $w^t \in \ker(G)$, the kernel of G.*

6.1. EXERCISES

1 Compute

(a) $\mathrm{wt}(110100010)$.

(b) $\mathrm{wt}(001011101)$.

2 Compute the Boolean sum

(a) $110100010 + 001011101$.

(b) $110100010 + 110100010$.

3 Find a basis for $\mathscr{L}(S)$ when

(a) $S = \{1100, 0011\}$.

(b) $S = \{1110, 0111\}$.

(c) $S = \{1100, 1010, 1001, 0110, 0101, 0011\}$.

(d) $S = \{11000, 10100, 10010, 10001, 01100, 01010, 01001, 00110, 00101, 00011\}$.

4 If $\mathscr{C}_1$ and $\mathscr{C}_2$ are linear codes, define $\mathscr{C}_1 + \mathscr{C}_2 = \{u + v : u \in \mathscr{C}_1 \text{ and } v \in \mathscr{C}_2\}$.

(a) Show that $\mathscr{C}_1 + \mathscr{C}_2$ is a linear code.

(b) Show that $(\mathscr{C}_1 + \mathscr{C}_2)^\perp = \mathscr{C}_1^\perp \cap \mathscr{C}_2^\perp$.

5 Let S be the (nonlinear) binary code in Exercise 3(c). Exhibit all the binary words in $\mathscr{L}(S) \backslash S$, the complement of S in $\mathscr{L}(S)$.

6 Let B be a basis of the linear $(n, 2^k, d)$ code $\mathscr{C}$. Prove or disprove that $d = \min_{b \in B} \mathrm{wt}(b)$.

7 A nonempty set $S \subset F^n$ is *orthogonal* if $u \cdot v = 0$ for all $u, v \in S$, $u \neq v$. Prove or disprove that an orthogonal set is linearly independent.

8 Prove that $\mathrm{wt}(u + v) \leq \mathrm{wt}(u) + \mathrm{wt}(v)$ for all $u, v \in F^n$.

9 Let $S = \{u \in F^n : \mathrm{wt}(u) \text{ is odd}\}$. Prove that $\mathscr{L}(S)$ is an $(n, 2^n, 1)$ code.

10 Let $S = \{u \in F^n : \mathrm{wt}(u) \text{ is even}\}$. If $n \geq 2$,

(a) prove that $\mathscr{L}(S) = S$.

(b) prove that S is an $(n, 2^{n-1}, 2)$ linear code.

11 Let $\mathscr{C} = \{0000, 1100, 0011, 1111\}$.

(a) Prove that $\mathscr{C}$ is a linear code.

(b) Prove that $\mathscr{C}$ is *self-dual*, i.e., that $\mathscr{C}^\perp = \mathscr{C}$.

12 Suppose $\mathscr{C}$ is an $(n, 2^k, d)$ linear code. As in Example 6.1.9, let $\mathscr{C}^+$ be the corresponding parity check code obtained from $\mathscr{C}$ by appending a single parity

check bit to the end of each codeword, i.e., by replacing $xy\ldots z \in \mathscr{C}$ with $xy\ldots zp \in \mathscr{C}^+$, where p is the parity of $xy\ldots z$.

(a) Prove that $\mathscr{C}^+$ is a linear code.

(b) Prove that $\mathscr{C}$ and $\mathscr{C}^+$ have the same dimension.

(c) If d is odd, show that $\mathscr{C}^+$ is an $(n+1, 2^k, d+1)$ code.

(d) If d is even, show that $\mathscr{C}^+$ is an $(n+1, 2^k, d)$ code.

13 A linear code $\mathscr{C}$ is *self-dual* if $\mathscr{C}^\perp = \mathscr{C}$.

(a) Prove that a self-dual $(n, 2^k, d)$ linear code has dimension $k = n/2$.

(b) Construct a self-dual linear code of length 8.

14 Prove or disprove that a linear code of dimension k has (exactly)

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i)$$

different (unordered) bases.

15 Find a basis for the dual code $\mathscr{C}^\perp$, where $\mathscr{C} = \mathscr{L}(B)$ is the linear code with basis

(a) $B = \{10000, 01000, 00100\}$.

(b) $B = \{110111, 111101, 110011\}$.

16 Let $\mathscr{C}$ be a (not necessarily linear) (*n*,*M*,*d*) binary code. The *weight enumerator* of $\mathscr{C}$ is the two-variable polynomial

$$W_{\mathscr{C}}(x, y) = \sum_{c\in\mathscr{C}} x^{\mathrm{wt}(c)}\ y^{n-\mathrm{wt}(c)}.$$

F. J. MacWilliams (1917–1990) discovered a relation between the weight enumerators of a linear code and its dual, namely,

$$W_{\mathscr{C}^\perp}(x, y) = \frac{W_{\mathscr{C}}(y - x, x + y)}{M}.$$

Confirm this identity for

(a) the code $\mathscr{C} = \mathscr{L}(S)$ in Example 6.1.17.

(b) the code $\mathscr{C} = \mathscr{L}(B)$ in Example 6.1.19.

(c) the code $\mathscr{C} = \mathscr{L}(S)$ in Exercise 3(c).

(d) the self-dual code $\mathscr{C}$ in Exercise 11.

(e) the code $\mathscr{C} = \mathscr{L}(B)$ in Exercise 15(a).

(f) the code $\mathscr{C} = \mathscr{L}(B)$ in Exercise 15(b).

17 Prove or disprove that the number of different

(a) $k \times n$ marices over $F = \{0, 1\}$ is 2^{nk}.

(b) $k \times n$ reduced row echelon form marices of rank k over F is

$$C_2(n,k) = \prod_{r=1}^{k} \frac{2^{n-r+1}-1}{2^r-1}.$$

(c) k-dimensional subspace of F^n is $C_2(n,k)$.

18 (L. Lovász) Let $A = (a_{ij})$ be an $n \times n$, symmetric $(0,1)$-matrix. Let $\mathscr{C}$ be the (Boolean) row space of A. Prove or disprove that $\text{diag}(A) \in \mathscr{C}$, where $\text{diag}(A)$ is the binary word $a_{11}a_{22}\ldots a_{nn}$.

19 Give a direct proof of Equation (6.5), i.e., one based on Definitions 6.1.6 and 6.1.11.

6.2. DECODING ALGORITHMS

Human history becomes more and more a race between education and catastrophe.

— H. G. Wells

Recall, from Theorem 6.1.21, that if G is a generating matrix for the linear code $\mathscr{C}$, then $u \in \mathscr{C}^\perp$ if and only if $Gu^t = 0$. Turning this around, $w \in \mathscr{C} = \mathscr{C}^{\perp\perp}$ if and only if $Hw^t = 0$, where H is a generating matrix for $\mathscr{C}^\perp$. Let's investigate this back-door way of defining $\mathscr{C}$.

It follows from Definition 6.1.20 that an $m \times n$, (0,1)-matrix H is a generating matrix for some linear code if and only if its rows are linearly independent. As a warm-up exercise, fix an arbitrary integer $m \geq 2$, let $n = 2^m - 1$, and define H_m to be the $m \times n$ matrix whose jth column is the (transposed) binary numeral for j, $1 \leq j \leq n$. Then

$$H_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \tag{6.10}$$

and

$$H_{m+1} = \begin{pmatrix} Z_m & 1 & U_m \\ H_m & O_m & H_m \end{pmatrix}, \qquad m \geq 2,$$

where Z_m and O_m are the $1 \times (2^m - 1)$ and $m \times 1$ zero matrices, respectively, and U_m is the $1 \times (2^m - 1)$ matrix each of whose entries is 1. (Confirm that $\text{rank}(H_{m+1}) = m + 1$, $m \geq 1$.)

Let $\mathscr{C}_m \in F^n$ be the m-dimensional linear code generated by H_m, and define $\mathscr{H}_m = \mathscr{C}_m^{\perp} = \{v \in F^n : H_m v^{\mathrm{t}} = 0\}$. Then, by Lemma 6.1.18, $\mathscr{H}_m$ is an $(n, 2^{n-m}, d)$ linear code, where $n = 2^m - 1$ and

$$d = \min_{0 \neq w \in \mathscr{H}_m} \mathrm{wt}(w).$$

Observe that $d = 1$ only if there is a codeword $w \in \mathscr{H}_m$ of weight 1. If the single nonzero bit of $w = 0 \ldots 0100$ is the jth, then $H_m w^{\mathrm{t}}$ is equal to column j of H_m. But, $w \in \mathscr{H}_m$ if and only if $H_m w^{\mathrm{t}} = 0$. Because no column of H_m is zero, no codeword of $\mathscr{H}_m$ can have weight 1. What about 2? If $w \in \mathscr{H}_m$ has exactly two nonzero bits, say bits i and j, then $H_m w^{\mathrm{t}}$ is the sum of column i and column j of H_m. But, the columns of H_m are just (transposed) binary words from F^m. If u, $u' \in F^m$, then the (Boolean) sum $u + u' = 0$ if and only if $u = u'$. Since no two distinct integers have identical numerals, no two columns of H_m are the same. Therefore, $d \geq 3$. Finally, for all $m \geq 2$, $H_m w^{\mathrm{t}} = 0$ when $w = 11100 \ldots 0$. (If $m = 2$, there are no zeros in w.) Thus $w \in \mathscr{H}_m$, so $d \leq 3$.

6.2.1 Definition. For a fixed but arbitrary integer $m \geq 2$, let $n = 2^m - 1$ and define H_m to be the $m \times n$ matrix whose jth column is the binary numeral for j. Then the mth *Hamming code* is the $(n, 2^{n-m}, 3)$ linear code $\mathscr{H}_m = \{w \in F^n : H_m w^{\mathrm{t}} = 0\}$.

Recall that a code of length n is perfect if F^n is the disjoint union of the "spheres of influence" of its codewords.

6.2.2 Theorem. *If $m \geq 2$, then $\mathscr{H}_m$ is a perfect, 1-error-correcting, linear code.*

Proof. Only the perfection of $\mathscr{H}_m$ remains to be proved, and that is an immediate consequence of Lemma 1.4.14. ■

6.2.3 Example Definition 6.2.1 gives an implicit (back-door) description of $\mathscr{H}_m$. Let's find an explicit description, e.g., of $\mathscr{H}_3$.

By definition, $\mathscr{H}_3 = \ker(H_3)$, the kernel of H_3, also known as the orthogonal complement of the row space of H_3. Since the row space of a matrix is left unchanged by elementary row operations, $\mathscr{H}_3$ could just as well be described as the orthogonal complement of the row space of the Hermite normal form of H_3. From Equation (6.10),

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Interchanging rows 1 and 3 produces its Hermite normal form

$$H' = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{6.11}$$

(with *pivot* columns 1, 2, and 4). So, $w = x_1x_2\cdots x_7 \in \mathscr{H}_3$ if and only if $H_3w^t = 0$; if and only if

$$x_1 + x_3 + x_5 + x_7 = 0, \tag{6.12a}$$
$$x_2 + x_3 + x_6 + x_7 = 0, \tag{6.12b}$$
$$x_4 + x_5 + x_6 + x_7 = 0; \tag{6.12c}$$

if and only if

$$x_1 = x_3 + x_5 + x_7,$$
$$x_2 = x_3 + x_6 + x_7,$$
$$x_4 = x_5 + x_6 + x_7;$$

if and only if

$$x_1x_2\cdots x_7 = x_3 1110000 + x_5 1001100 + x_6 0101010 + x_7 1101001. \tag{6.13}$$

Evidently, $B = \{1110000, 1001100, 0101010, 1101001\}$ is a basis for $\mathscr{H}_3$ and, therefore,

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{6.14}$$

is a generating matrix for $\mathscr{H}_3$. □

Suppose $w \in \mathscr{H}_m \subset F^n$ is sent and $v \in F^n$ is received. Because $\mathscr{H}_m$ is perfect, v lies in the sphere of influence, $S_1(c)$, of some (unique) codeword c.* Thus, c will be the output of any (valid) nearest-neighbor decoding algorithm. The missing piece is the algorithm.

Recall that $\mathscr{H}_m$ consists of $M = 2^{2^m-m-1}$ codewords. That "tower of exponents" indicates that M is likely to be BIG. While having a large vocabulary is good for composing messages, it means decoding algorithms based on computing $d(v, c)$, for all $c \in \mathscr{H}_m$ and all v in the message, are likely to be *slow*. Is there an alternative? Yes, that's the best part!

Let $u = H_m v^t$. If $u = 0$, then $v \in \mathscr{H}_m$ and $c = v$, i.e., no *correction* takes place. If $u \neq 0$, then v is not a codeword. In that case, c is the unique codeword that differs from v in a single bit. If we just knew which bit that was, changing it would yield c; if c differs from v in the jth bit, then $c = v + b$, where $b = 0\ldots010\ldots0$ is the binary word whose only nonzero bit is the jth. Here is the easy way to find j.

*Recall that $S_r(c) = \{y \in F^n \ : \ d(c, y) \leq r\}$, where $r = \lfloor (d-1)/2 \rfloor$.

In Boolean arithmetic, $c = v + b$ if and only if $c + b = v$. Together with the fact that $H_m c^{\mathrm{t}} = 0$, this yields

$$\begin{aligned} u &= H_m v^{\mathrm{t}} \\ &= H_m (c + b)^{\mathrm{t}} \\ &= H_m c^{\mathrm{t}} + H_m b^{\mathrm{t}} \\ &= H_m b^{\mathrm{t}}, \end{aligned} \tag{6.15}$$

the jth column of H_m. Evidently, all one needs do is scan the columns of H_m looking for u. Locating u in the jth column of H_m means that c differs from v in the jth bit!

The bad news is that H_m has $n = 2^m - 1$ columns. That's more than a million, even for m as small as 20. The good news is that j can be found without scanning *all* of the columns of H_m. In fact, it can be found without scanning *any* columns!

Recall that H_m is not just some random $m \times n$ matrix. It is the unique $m \times n$ matrix whose jth column is the binary numeral for j. Therefore, u is the jth column of H_m if and only if u is the binary numeral for j. From the perspective of the base 2 numeration system, $u = j$.

Let's summarize. When binary word v is received, it is decoded as

$$c = v + b, \tag{6.16}$$

where the binary word b is determined by $u = H_m v^{\mathrm{t}}$. If $u = 0$, then $b = 0$; if $u \neq 0$, then b has a single nonzero bit in the jth position, where j is determined by converting the binary numeral u to base 10.

6.2.4 Example. To find the codeword $c \in \mathscr{H}_3$ nearest to $v = 0101100$, observe that

$$u = H_3 v^{\mathrm{t}} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Because $u^{\mathrm{t}} = 011$ is the binary numeral for $j = 3$, $b = 0010000$ and

$$\begin{aligned} c &= 0101100 + 0010000 \\ &= 0111100. \end{aligned}$$

(Confirm that u is the third column of H_3.) □

A formal nearest-neighbor decoding algorithm for Hamming codes might look something like this:

6.2.5 Algorithm. *The codeword $c \in \mathscr{H}_m$ nearest to $v \in F^n$ is determined as follows:*

1. *Let $u = H_m v^t$.*
2. *If $u^t = 00\ldots0 \in F^m$ then $b = 00\ldots0 \in F^n$. Go to step 5.*
3. *Let j be the integer whose binary numeral is u^t.*
4. *Let $b = 0\cdots010\cdots0 \in F^n$ where the jth bit from the left is 1.*
5. *Return $c = v + b$.* □

If $w \in \mathscr{H}_m$ is sent and $v \in F^n$ is received, won't Algorithm 6.2.5 sometimes yield the wrong codeword? The answer depends on what is meant by *wrong*. If more than one bit of w is changed in transmission, no (valid) nearest-neighbor decoding algorithm will correct v to w. If the transmission channel is noisy enough for more than one error to occur with unacceptably high probability, a code that can correct more than one error should be chosen! If the code of choice is $\mathscr{H}_m$, then Algorithm 6.2.5 produces the *right* (nearest-neighbor) codeword!

In preparation for the more challenging problem of decoding general linear codes, it will be helpful to review the key steps that led to Algorithm 6.2.5. As in Example 6.1.19, Equations (6.12a)–(6.12c) show that the dependent pivot variables x_1, x_2, and x_4, can be viewed as *parity check digits*. This is the source of the following terminology.

6.2.6 Definition. Let $\mathscr{C}$ be a linear $(n, 2^k, d)$ code. A *parity check matrix* for $\mathscr{C}$ is a generating matrix for $\mathscr{C}^\perp$.

Evidently, H is a parity check matrix for $\mathscr{C}$ if and only if $\mathscr{C} = \{v \in F^n : Hv^t = 0\}$. Because the dimension of a linear $(n, 2^k, d)$ code is k, the dimension of its dual code is $n - k$. Therefore, H is a parity check matrix for *some* $(n, 2^k, d)$ linear code if and only if H is an $(n-k) \times n$, $(0,1)$-matrix of (Boolean) rank $n - k$.

6.2.7 Example. The $m \times n$ matrix H_m is the prototype parity check matrix. Its rows are a basis for $\mathscr{C}_m = \mathscr{H}_m^\perp$, i.e., $\mathscr{C}_m$ is the row space of H_m. An $m \times n$, (0,1)-matrix H is a parity check matrix for $\mathscr{H}_m$, if and only if H and H_m have the same row space, if and only if H and H_m are row equivalent. Indeed, the Hermite normal form of H_3 given in Equation (6.11) is the parity check matrix from which Equations (6.12a)–(6.12c) came. □

As the key to Algorithm 6.2.5 $u = H_m v^t$ also deserves a name. However, since row vectors are easier to typeset than column vectors, it is $u^t = vH_m^t$ that will receive the distinction.

6.2.8 Definition. Let H be a fixed but arbitrary parity check matrix for the linear $(n, 2^k, d)$ code $\mathscr{C}$. With respect to H, the *syndrome* of $v \in F^n$ is vH^t.

With respect to the $(n-k) \times n$ matrix H, the syndrome of $v \in F^n$ is the product of v (viewed as a $1 \times n$ matrix) and the $n \times (n-k)$ matrix H^t. In particular, the syndrome of v is a $1 \times (n-k)$ matrix (viewed as a binary word in F^{n-k}).

Are all these transposes really necessary?* After all, F^m and the space of column vectors $\{v^t : v \in F^m\}$ are isomorphic. It seems as if we could save ourselves a lot of grief by overlooking the distinction between "$\cong$" (isomorphic) and "$=$" (equal). That this approach may be too simplistic is suggested by the fact that $\mathscr{H}_3$ and F^4 are isomorphic vector spaces!

One thing we *can* do is substitute something like s for u^t in $u^t = vH^t$, writing, e.g., "the syndrome $s = vH^t$."

6.2.9 Example. From Example 6.2.4, with respect to H_3 the syndrome of $v = 0101100$ is $s = 011$. The reader may confirm that the syndrome of (the same) v with respect to the Hermite normal form of H_3 (Equation (6.11)) is $s' = vH'^t = 110 \neq s$. Evidently, as implied by Definition 6.2.8, the syndrome of a binary word $v \in F^n$ depends not only on the linear code but also on the parity check matrix used in its back-door definition.

While it may be the binary numeral for 6, $s' = 110$ is the transpose, not of column 6, but of column $j = 3$ of H'. This should not come as a surprise. After all, using H' in the back-door definition of $\mathscr{H}_3$ doesn't alter the fact that the codeword $c \in \mathscr{H}_3$, nearest to $v = 0101100$, is obtained by changing bit $j = 3$ of v. It is worth emphasizing that it is only the very special form of H_m that permits the elegant (base 2 numeral) alternative to having to scan $n = 2^m - 1$ columns in search of $u = H_m v^t$. □

So much for warming up. It's time to consider a general linear $(n, 2^k, d)$ code $\mathscr{C}$. Suppose, as usual, that $w \in \mathscr{C}$ is sent down a noisy transmission channel and $v \in F^n$ is received. Then $v = w + e$, where the 1's in e correspond to the places where v differs from w. Call $e = w + v$ an *error pattern*. If we knew the error pattern, we could recover $w = v + e$. But, that is asking too much. The best we can hope for is a fast way to find a binary word b such that $c = v + b$ is a codeword nearest to v.

If v is contained in the sphere of influence of some $c \in \mathscr{C}$, then c is the unique codeword nearest to v. But, each binary word in F^n belongs to the sphere of influence of some codeword, if and only if $\mathscr{C}$ is a perfect code.† While no binary word can ever belong to the sphere of influence of more than one codeword, v can fail to belong to the sphere of influence of any. In the worst case, there may be several nearest-neighbor codewords, each the same distance from v. It seems we should add to the specifications for a nearest-neighbor decoding algorithm some mechanism for resolving such ambiguities.

A necessary and sufficient condition for $v + b = c$ to be a codeword is that $Hc^t = 0$ for a fixed but arbitrary parity check matrix H. As in Equation (6.15), $Hc^t = 0$ if and only if $Hv^t = Hb^t$, if and only if $vH^t = bH^t$, i.e., if and only if v

*Some authors deal with the annoying transposes by defining, not H, but H^t to be the parity check marix. In this approach a generating matrix for $\mathscr{C}^\perp$ is the *transpose* of a parity check matrix for $\mathscr{C}$. In particular, some transposing is inevitable.

†In a perfect world, there might be a perfect code for every purpose. In the real world, if $\mathscr{C}$ is an r-error-correcting binary code, with more than two codewords and satisfying $r > 0$, then $\mathscr{C}$ is *equivalent* either to a Hamming code or to the [23,4096,7] *Golay code* $\mathscr{G}_{23}$ found in Exercise 29 (below).

and b have the same syndrome with respect to H. A necessary and sufficient condition for $v + b = c \in \mathscr{C}$ to be a *nearest* codeword to v is that the distance $d(c, v) = \mathrm{wt}(c + v) = \mathrm{wt}(b)$ be as small as possible. Thus, v should be decoded as $v + b = c$, where b is a binary word of minimum weight among those having the syndrome $s = vH^{\mathrm{t}}$.

Visualize a *code book* listing all 2^n binary words in F^n. Imagine the book organized into chapters, so that binary words v and b are in the same chapter if and only if $vH^{\mathrm{t}} = bH^{\mathrm{t}}$, i.e., if and only if v and b have the same syndrome. Because $vH^{\mathrm{t}} = 0 \in F^{n-k}$ if and only if $v \in \mathscr{C}$, one of the chapters consists of codewords. If the title of each chapter is the syndrome common to every word in it, then the chapter of codewords is Chapter 0. Finally, suppose the words in each chapter are organized into paragraphs, by weight, so that the first paragraph contains all the words of minimum weight. If $\mathscr{C}$ is a perfect code, then the first paragraph of every chapter will consist of a single word. For an arbitrary linear code, the first paragraph of Chapter 0 will contain only $0 \in F^n$. In general, however, some chapters will begin with paragraphs containing more than one word.

The following decoding strategy is an immediate consequence of having such a book. When binary word v is received, compute its syndrome $s = vH^{\mathrm{t}}$. Decode v as $v + b = c$, where b is the first word in Chapter s. (From the way in which the code book was assembled, b has minimum weight among those words with syndrome s. By our previous arguments, this means c is a nearest codeword to v. Note that the mechanism for resolving ambiguities is implicit in the arrangement of words that make up the first paragraph of Chapter s.)

This strategy can, in fact, be implemented *without the book!* All we need is a table of contents that lists the titles and first words of each chapter.

6.2.10 Definition. Let H be a fixed but arbitrary parity check matrix for the linear code $\mathscr{C}$. A *standard decoding array* for $\mathscr{C}$ is a table in which each syndrome s is matched with a minimum-weight binary word whose syndrome, with respect to H, is s.

Why should the first word in an arbitrarily arranged first paragraph be the right choice for b? Because *every* word in the first paragraph is a right choice for b! A more appropriate question is the extent to which a standard decoding array depends on the arbitrary parity check matrix H.

6.2.11 Theorem. *Suppose H and K are two parity check matrices for the same linear code $\mathscr{C}$. If binary words v and b have the same syndrome with respect to H, then they have the same syndrome with respect to K.*

As we saw in Example 6.2.9, the syndromes themselves may be different. In an H-based code book, the binary word $v = 0101100$ may belong to Chapter 011, while in a K-based book it belongs to Chapter 110. Theorem 6.2.11 guarantees, however, that the first paragraph of Chapter 011 in the H-based book contains precisely the same words as the first paragraph of Chapter 110 in the K-based book.

Proof of Theorem 6.2.11: H and K are parity check matrices for the same linear code $\mathscr{C}$ if and only if they have the same row space (namely, code $\mathscr{C}^{\perp}$), if and only if they are row equivalent, if and only if there is a (Boolean) invertible matrix E such that $K = EH$. Thus, $Hv^{\mathrm{t}} = Hb^{\mathrm{t}}$ if and only if $EHv^{\mathrm{t}} = EHb^{\mathrm{t}}$, if and only if $Kv^{\mathrm{t}} = Kb^{\mathrm{t}}$. ■

A formal algorithm based on the code book decoding strategy might look something like this.

6.2.12 **Algorithm.** *Let H be a fixed but arbitrary parity check matrix for the linear code $\mathscr{C}$. Given a standard decoding array based on H, a codeword $c \in \mathscr{C}$ nearest to $v \in F^n$ is obtained as follows:*

1. *Compute the syndrome $s = vH^t$.*
2. *Let b be the word corresponding to s in the array.*
3. *Return $v + b = c$.* □

6.2.13 Example. Suppose $S = \{11100, 01011, 01110, 11001\}$. Let $\mathscr{C} = \mathscr{L}(S)$. To implement Algorithm 6.2.12, we need a parity check matrix H. Because $c \in \mathscr{C}$ if and only if $cH^{\mathrm{t}} = 0$, it follows that $GH^{\mathrm{t}} = 0$ for any generating matrix G of $\mathscr{C}$. This identity also follows, of course, from the definition of H as a generating matrix for $\mathscr{C}^{\perp}$. Because $\mathscr{C}^{\perp} = \{w : w^{\mathrm{t}} \in \ker(G)\}$, the rows of H are a (transposed) basis of the kernel of G.

To find a generating matrix for $\mathscr{C} = \mathscr{L}(S)$, consider matrix

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

whose rows are the codewords in S. Because it is the row space of A, a basis for $\mathscr{C}$ is comprised of the nonzero rows in the Hermite normal form of A: Adding row 1 of A to row 4, and row 2 to rows 1 and 3, we obtain the row equivalent matrix

$$B = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Adding row 3 of B to rows 1 and 4 produces the Hermite normal form

$$C = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Therefore,

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{6.17}$$

is a generating matrix for $\mathscr{C}$. If $w = x_1x_2x_3x_4x_5$, then $w \in \mathscr{C}^\perp$ if and only if $w^t \in \ker(G)$, if and only if

$$\begin{aligned} x_1 + x_4 &= 0 \\ x_2 + x_4 + x_5 &= 0 \\ x_3 + x_5 &= 0, \end{aligned}$$

if and only if

$$x_1x_2x_3x_4x_5 = x_4\,11010 = x_5\,01101. \tag{6.18}$$

Therefore, $B = \{11010, 01101\}$ is a basis for $\mathscr{C}^\perp$, and

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \tag{6.19}$$

is a parity check matrix for $\mathscr{C}$.

If $u = Hv^t$ for some $v \in F^5$, then the corresponding syndrome $s = u^t = vH^t \in F^2$. Evidently, the available syndromes are 00, 01, 10, and 11. Because $00 = 00000H^t$, and every nonzero binary word in F^5 has positive weight, we see (again) that the only possible pairing for the syndrome $s = 00$ in a standard decoding array for $\mathscr{C}$ is $b = 00000$.

Let $e_j \in F^5$ be the word whose only nonzero bit is the jth, $1 \le j \le 5$. Then $1 = \mathrm{wt}(e_j) \le \mathrm{wt}(v)$ for every nonzero $v \in F^5$. Because $u_j = He_j^t$ is the jth column of H, it is easy to see, e.g., that $s = 01 = e_3H^t = e_5H^t \ne bH$, for any binary word b of weight 1 different from e_3 and e_5. It follows that 00100 and 00001 are the only possible pairings for syndrome $s = 01$ in a standard decoding array for $\mathscr{C}$. Which is correct? Either! These two words comprise the first paragraph of Chapter 01 of the code book for $\mathscr{C}$ based on H. Pick one of them at random, or pick one using some arbitrary criterion, e.g., the smaller base 2 numeral.

Similarly, one of 10000 or 00010 must correspond to $s = 10$. Finally, $b = 01000$ is the unique word of minimum weight corresponding to syndrome $s = 11$. Using the smaller binary word as a tie breaker, we obtain the standard decoding array exhibited in Fig. 6.2.1.

Syndrome s = vH^t	Minimum weight b
00	00000
01	00001
10	00010
11	01000

Figure 6.2.1. Standard decoding array for $\mathscr{L}(11100, 01011, 01110, 11001)$.

Suppose, e.g., binary word $v = 10101$ is received over a transmission channel employing the code $\mathscr{C}$. With respect to the same parity check matrix H just used in the construction of the standard decoding array, $vH^t = 10$. Because $s = 10$ is paired with the binary word $b = 00010$ in Fig. 6.2.1, v is decoded as $v + b = 10101 + 00010 = 10111$. (Confirm that $c = 10111 \in \mathscr{C}$.) □

The fact that the generating matrix in Equation (6.17) is of the form $G = (I_3|X)$ means that we worked harder than necessary in Example 6.2.13.

6.2.14 Theorem. *If $\mathscr{C}$ is an $(n, 2^k, d)$ linear code with a generating matrix of the form $G = (I_k|X)$, then $H = (X^t|I_{n-k})$ is a parity check matrix for $\mathscr{C}$.*

Proof. Because

$$\begin{aligned}(I_k|X)\begin{pmatrix} X \\ I_{n-k} \end{pmatrix} &= I_k X + X I_{n-k} \\ &= X + X \\ &= 0,\end{aligned}$$

the columns of H^t belong to the kernel of G, i.e., the rows of H belong to $\mathscr{C}^\perp$. Because it is an $(n-k) \times n$ matrix of rank $n-k$, H is a generating matrix for $\mathscr{C}^\perp$. ■

Note that the matrix H in Equation (6.19) is of the form $(X^t|I_2)$, where $G = (I_3|X)$ is the matrix in Equation (6.17).

6.2.15 Definition. A *systematic* linear code is one that has a generating matrix of the form $G = (I_k|X)$, where X is a $k \times (n-k)$, $(0, 1)$-matrix.

If G is an arbitrary generating matrix of an arbitrary $(n, 2^k, d)$ linear code $\mathscr{C}$, then $\mathscr{C}$ is a systematic linear code if and only if the (unique) Hermite normal form of G is $(I_k|X)$. If follows from Theorem 6.2.14 that a parity check matrix for a systematic linear code is easily obtained from the Hermite normal form (shared by all) of its generating matrices.

Consider the linear code $\mathscr{C}''$ generated by

$$G'' = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}. \tag{6.20}$$

Because G'' is already in Hermite normal form, $\mathscr{C}''$ is not systematic. However, $\mathscr{C}''$ is "equivalent" to the systematic code of Example 6.2.13.

6.2.16 Definition. Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be two (not necessarily linear) codes. If the codewords of $\mathscr{C}_2$ can be obtained from the codewords of $\mathscr{C}_1$ by some systematic permutation of their bits, then $\mathscr{C}_2$ is *equivalent* to $\mathscr{C}_1$.

Because the generating matrix G'' of Equation (6.20) can be obtained by switching columns 3 and 4 in the generating matrix G of Equation (6.17), the corresponding code $\mathscr{C}''$ is equivalent to the code $\mathscr{C}$ of Example 6.2.13. Thus, it should be possible to modify the table in Fig. 6.2.1 so as to obtain a standard decoding array for $\mathscr{C}''$. But how?

Switching columns 3 and 4 of G is an elementary column operation. It can be achieved by multiplying G on the right by a permutation matrix P. If $G'' = GP$, then $(GP)(P^{-1}H^{\mathrm{t}}) = GH^{\mathrm{t}} = 0$, i.e., $H''^{\mathrm{t}} = P^{-1}H^{\mathrm{t}}$. Since the inverse of a permutation matrix is its transpose, $H'' = HP$. In this case, a parity check matrix for G'' can be obtained from a parity check matrix for G simply by switching columns 3 and 4 of H, i.e.,

$$H'' = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Of course, finding a parity check matrix is only the first step in producing a standard decoding array.

6.2.17 Example. This section began with the construction of Hamming codes by means of generating matrices of their dual codes. Let's have a look at $\mathscr{C}_3 = \mathscr{H}_3^{\perp}$ in its own right. By definition,

$$G = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

is a generating matrix for the $(7, 8, 4)$ linear code $\mathscr{C}_3 = \{0000000, 0001111, 0110011, 1010101, 0111100, 1011010, 1100110, 1101001\}$. From the perspective of $\mathscr{H}_3$, the matrix G in Equation (6.14) is a generating matrix. From the perspective of $\mathscr{C}_3$, the same matrix is the parity check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{6.21}$$

j	0	1	2	3	4	5	6	7
s_j	0000	1101	1011	1000	0111	0100	0010	0001

Figure 6.2.2

Let's use H to construct a standard decoding array for $\mathscr{C}_3$. Because it has four rows, the syndromes with respect to H are elements of F^4. So, there are $2^4 = 16$ possible syndromes, of which $s_0 = 0000$ is the title of the chapter containing the codewords.

As in Example 6.2.13, let $e_j \in F^7$ be the binary word of weight 1 whose only nonzero bit is the jth, so that $u_j = He_j^t$ is the jth column of H. Because the columns of H are all different, and no nonzero word has weight less than e_j, we deduce that e_j is the unique minimum-weight binary word having syndrome $s_j = u_j^t = e_j H^t$. So, s_j must be paired with e_j, in any standard decoding array based on H. This takes care of the eight syndromes listed in Fig. 6.2.2. Moreover, any binary word associated with a syndrome not listed in Fig. 6.2.2 must have weight not less than 2.

The typical binary word of length 7 and weight 2 is of the form $e_i + e_j$, where $i \neq j$. Observe that $H(e_i + e_j)^t$ is the sum of columns i and j of H. Thus, e.g., the as-yet unlisted syndrome $0110 = (e_1 + e_2)H^t$, and we may associate 0110 with $e_1 + e_2 = 1100000$. (To construct a standard decoding array, we don't need to know every word in the first paragraph of each chapter; it suffices to know one of them!) Similarly, the transposed sum of columns 1 and 3 of H is 0101, the syndrome for $e_1 + e_3$. Because 0101 does not appear in Fig. 6.2.2, it is not the syndrome of any word of weight less than 2. So, we may as well pair 0101 with 1010000 in our growing standard decoding array.

Continuing in this way, it seems natural to pair 1010 with $e_1 + e_4 = 1001000$, 1001 with $e_1 + e_5 = 1000100$, 1111 with $e_1 + e_6 = 1000010$, 1100 with $e_1 + e_7 = 1000001$, and 0011 with $e_2 + e_3 = 0110000$. The only remaining unmatched syndrome is 1110. Because it is not the transposed sum of any two columns of H, there are two possibilities. Either 1110 is not the syndrome, with respect to this parity

Syndrome	Word	Syndrome	Word
0000	0000000	1000	0010000
0001	0000001	1001	1000100
0010	0000010	1010	1001000
0011	0110000	1011	0100000
0100	0000100	1100	1000001
0101	1010000	1101	1000000
0110	1100000	1110	0010110
0111	0001000	1111	1000010

Figure 6.2.3. A standard decoding array for $\mathscr{C}_3 = \mathscr{H}_3^{\perp}$.

check matrix, of any binary word (ruled out by Exercise 23, below) or, in the code book based on H, every binary word in Chapter 1110 has weight greater than 2. In fact, 1110 is the syndrome of $2^4 = 16$ words, of which $v = 0010110$ is one having weight 3. Pairing 0010110 with 1110 completes the standard decoding array for $\mathscr{C}_3 = \mathscr{H}_3^{\perp}$ exhibited in Fig. 6.2.3. □

There is nothing particularly fast about *constructing* a standard decoding array. Fortunately, it need be done only once. With a standard decoding array available, binary words can be decoded as fast as their syndromes can be identified.

6.2. EXERCISES

1 Using Boolean arithmetic, show that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

2 Confirm that the Hamming code of Example 1.4.15 is identical to the Hamming code of Example 6.2.3.

3 Let $\mathscr{C} = \mathscr{H}_2$.

(a) Compute the (n, M, d) parameters for $\mathscr{C}$.

(b) List (all) the codewords in $\mathscr{C}$.

(c) Exhibit a generating matrix for $\mathscr{C}$.

4 Let $\mathscr{C}_3$ be the linear code generated by H_3 (Equation (6.10)), so that $\mathscr{C}_3^{\perp} = \mathscr{H}_3$.

(a) Show that $\mathscr{C}$ is not perfect.

(b) Prove or disprove that $\mathscr{C}_3 \subset \mathscr{C}_3^{\perp}$.

5 Let $\mathscr{C}_m$ be the dual of the Hamming code $\mathscr{H}_m$.

(a) Show that $\mathscr{C}_m$ has a basis in which every codeword has weight 2^{m-1}.

(b) Does every nonzero codeword of $\mathscr{C}_m$ have weight 2^{m-1}? (Justify your answer.)

6 Find a systematic code equivalent to $\mathscr{C} = \mathscr{L}(S)$, when

(a) $S = \{10101, 10110, 00011\}$.

(b) $S = \{11100, 11110, 11111\}$.

7 Find the (Boolean) Hermite normal form of the matrix

(a) $\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$. **(b)** $\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$.

(c) $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$. **(d)** $\begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$.

8 Exhibit the parameters $(n, 2^k, d)$ for the linear code $\mathscr{C}$ defined to be the row space of the matrix in the corresponding part of Exercise 7.

9 Exhibit a parity check matrix for the linear code $\mathscr{C}$ defined to be the row space of the matrix in the corresponding part of Exercise 7.

10 Construct a standard decoding array for the linear code $\mathscr{C}$ defined to be the row space of the matrix in the corresponding part of Exercise 7.

11 Let $\mathscr{C} = \mathscr{L}(10010, 01011, 00101)$ be the code in Example 6.2.13. Use the standard decoding array of Fig. 6.2.1 to decode

(a) $v = 11001$. **(b)** $v = 01010$. **(c)** $v = 00110$.

12 Let $G = (I_k|X)$ be a generating matrix for the linear code $\mathscr{C}$. Prove that $\mathscr{C}$ is self-dual (i.e., $\mathscr{C}^\perp = \mathscr{C}$) if and only if $XX^{\mathrm{t}} = X^{\mathrm{t}}X = I_k$.

13 Let $\mathscr{C} = \mathscr{H}_3^\perp$ be the code in Example 6.2.17. Use the standard decoding array of Fig. 6.2.3 to find a nearest codeword to

(a) $v = 1101111$. **(b)** $v = 1001101$. **(c)** $v = 0101010$.

14 Let $\mathscr{C} = \mathscr{H}_3^\perp$ be the code in Example 6.2.17. Use the standard decoding array of Fig. 6.2.3 to find a nearest codeword to

(a) $v = 1000011$. **(b)** $v = 0100101$. **(c)** $v = 0010110$.

(d) $v = 1101010$. **(e)** $v = 1111111$. **(f)** $v = 1110001$.

15 Let G be the generating matrix for $\mathscr{H}_3$ given in Equation (6.14).

(a) Show that the Hermite normal form of G is of the form $G' = (I_4|X)$.

(b) Show that the Hermite normal form of the parity check matrix $H = (X^{\mathrm{t}}|I_3)$ is identical to the matrix H' given in Equation (6.11).

16 Let H be a parity check matrix for a linear $(n, 2^k, d)$ code $\mathscr{C}$. Suppose $v \in \mathscr{C}$ satisfies $\mathrm{wt}(v) = d$.

(a) Prove that the d columns of H corresponding to the positions of the 1's in v are linearly dependent.

(b) If $d > 1$, prove that every selection of $d - 1$ columns of H is linearly independent.

(c) Prove that $d \leq n - k + 1$.

17 Find the codeword $c \in \mathscr{H}_3$ nearest to

(a) $v = 1011110$. **(b)** $v = 1010110$. **(c)** $v = 0110110$.

(d) $v = 0001111$. **(e)** $v = 1110111$. **(f)** $v = 1101111$.

18 Let K be the 5×32 matrix obtained from H_5 by adding a new first column consisting entirely of 0's. Let G be the 6×32 matrix obtained from K by adding a new sixth row consisting entirely of 1's. Let $\mathscr{C}$ be the linear code generated by G. (This is the first-order Reed–Muller code used in the *Mariner* missions to Mars.)

(a) Show that $\mathscr{C}$ is a (32, 64, 16) code.

(b) Prove that $\mathscr{C}$ is not a perfect code.

19 Prove the statement in the text that, as vector spaces, $\mathscr{H}_3$ and F^4 are isomorphic.

20 Given that $\mathscr{H}_3$ and F^4 are isomorphic as vector spaces, would you say that $\mathscr{H}_3$ and F^4 are isomorphic as codes? Explain.

21 Let $\mathscr{C} = \mathscr{L}(10010, 01011, 00101)$ be the $(5, 8, d)$ code from Example 6.2.13.

(a) Find d.

(b) List all words $w \in F^5$ that have syndrome $s = 11 \in F^2$ with respect to the parity check matrix of Equation (6.19).

22 Let H be a fixed but arbitrary $(n-k) \times n$ parity check matrix for the $(n, 2^k, d)$ linear code $\mathscr{C}$. Suppose $s = vH^{\mathrm{t}}$ is the syndrome of $v \in F^n$. Let $X = \{w \in F^n : s = wH^{\mathrm{t}}\}$ be the set of binary words having the same syndrome as v. Prove that $X = \{v + c : c \in \mathscr{C}\}$.

23 Let $\mathscr{C}$ be an $(n, 2^k, d)$ linear code. Show that any code book for $\mathscr{C}$ must contain exactly 2^{n-k} chapters, so that every element of F^{n-k} is the syndrome of some binary word $v \in F^n$.

24 Suppose G is a $k \times n$ generating matrix for a linear $(n, 2^k, d)$ code $\mathscr{C}$. Define a function $T : F^k \to F^n$ by $T(v) = vG$. Prove that

(a) T is one-to-one.

(b) T is onto $\mathscr{C}$.

(c) T is linear.

(d) F^k and $\mathscr{C}$ are isomorphic as vector spaces.

25 A nonempty set $S \subset F^n$ is *orthogonal* if $u \cdot v = 0$ for all $u, v \in S$, $u \neq v$.

(a) Show that the rows of H_2 are not orthogonal.

(b) Show that the rows of H_3 are orthogonal.

(c) Prove or disprove that the rows of H_m are orthogonal for all $m \geq 3$.

26 Let G be the 4×7 matrix obtained from H_3 by adding a new fourth row consisting entirely of 1's. Let $\mathscr{C}$ be the linear code generated by G. Prove that $\mathscr{C} = \mathscr{H}_3$.

27 Let K be the 3×8 matrix obtained from H_3 by adding a new first column consisting entirely of 0's. Let G be the 4×8 matrix obtained from K by

$$X = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Figure 6.2.4

adding a new fourth row consisting entirely of 1's. Find the parameters of the linear code $\mathscr{C}$ generated by G.

28 The extended Golay code $\mathscr{G}_{24}$ used in the *Voyager* missions is the linear code generated by the matrix $G = (I_{12}|X)$, where X is the symmetric 12×12 matrix shown in Fig. 6.2.4.

(a) Show that $(X|I_{12})$ is also a generating matrix for $\mathscr{G}_{24}$.

(b) Show that $(X|I_{12})$ is a parity check matrix for $\mathscr{G}_{24}$.

(c) Prove that $\mathscr{G}_{24}$ is self-dual.

(d) Show that $\mathscr{G}_{24}$ is a $(24, 4096, 8)$ code.

29 The Golay code $\mathscr{G}_{23}$ is obtained from $\mathscr{G}_{24}$ (Exercise 28) by removing the last bit from every codeword.

(a) Find the parameters of $\mathscr{G}_{23}$.

(b) Prove that $\mathscr{G}_{23}$ is a perfect code.

(c) Prove or disprove that $\mathscr{G}_{23}$ is linear.

6.3. LATIN SQUARES

Growing tired of the debates, I was induced to amuse myself with making magic squares.

— Benjamin Franklin (*Autobiography*)

In the following two-person game, players G and B alternately choose numbers (without replacement) from $\{1, 2, \ldots, 9\}$. The first person to choose three numbers that sum to 15 is the winner. They need not be the first three numbers, or even some consecutive three numbers, but there must be three of them. The game is a draw if,

1	~~2~~	3	4	5	~~6~~	7	~~8~~	9
G:	2,	8		|	*B*:	6		

Figure 6.3.1

after all nine numbers have been chosen, neither player has three numbers that sum to 15.

Figure 6.3.1 shows a game in progress. Three numbers have been chosen, namely, $g_1 = 2$, $b_1 = 6$, and $g_2 = 8$. It is B's turn. The choice $b_2 = 9$ does not result in a win for B. While $6 + 9 = 15$, it is the sum of only two numbers. Since player B cannot hope to win on his second turn, the best he can do is block player G from winning by choosing $b_2 = 5$. Now it is G's turn, and she must choose g_3 from $\{1, 3, 4, 7, 9\}$. Since B has prevented her from winning on this turn, G's best strategy is to choose $g_3 = 4$, presenting B with the "board" exhibited in Fig. 6.3.2. Seeing that either 3 or 9 produces a winning triple for G, while he has no winning move himself, B resigns.

1	~~2~~	3	~~4~~	~~5~~	~~6~~	7	~~8~~	9
G:	2,	8,	4	|	*B*:	6,	5	

Figure 6.3.2

Is there a strategy that guarantees a win for the first player? Not only does s/he have the first opportunity to win (at the third turn), but if the point is reached where all nine numbers have been chosen, s/he will have $C(5, 3) = 10$ triples from which to find a winning combination, while the second player will have only $C(4, 3) = 4$.

Let's replay the game on the board illustrated in Fig. 6.3.3*a*. If we circle G's choices and cross out B's, then player B resigned at the point illustrated in Fig. 6.3.3*b*.

Convince yourself that there are exactly eight winning combinations in the 15-game, namely, $\{1, 5, 9\}$, $\{1, 6, 8\}$, $\{2, 4, 9\}$, $\{2, 5, 8\}$, $\{2, 6, 7\}$, $\{3, 4, 8\}$, $\{3, 5, 7\}$, and $\{4, 5, 6\}$. These correspond, via Fig. 6.3.3*a*, to the eight winning combinations in tic-tac-toe. Evidently, the 15-game is isomorphic to a game in which no strategy guarantees a win for the first player!

6.3.1 Definition. A *magic square* of *order n* is an $n \times n$ array in which the numbers $1, 2, \ldots, n^2$ are arranged so that each row and each column sums to the same (magic) number.

4	9	2		④	9	②
3	5	7		3	~~5~~	7
8	1	6		⑧	1	~~6~~
(*a*)				(*b*)		

Figure 6.3.3

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

Figure 6.3.4. Franklin's magic square.

The magic square of order 3 in Fig. 6.3.3*a* has some *extra* magic because the two diagonals also sum to 15. The magic square of order 8 in Fig. 6.3.4 (magic number 260) was discovered by Benjamin Franklin (1706–1790). It, too, has some extra magic. If it is partitioned into four 4×4 blocks, then each of them is a *pseudo* magic square. (While the rows and columns of each of these blocks sum to 130, none of them contains [just] the numbers $1, 2, \ldots, 16$.) when it comes to extra magic, however, the grand prize goes to Leonhard Euler, whose magic square of order 8 is simultaneously a *knight's tour* of the chess board (Fig. 6.3.5).

1	48	31	50	33	16	63	18
30	51	46	3	62	19	14	35
47	2	49	32	15	34	17	64
52	29	4	45	20	61	36	13
5	44	25	56	9	40	21	60
28	53	8	41	24	57	12	37
43	6	55	26	39	10	59	22
54	27	42	7	58	23	38	11

Figure 6.3.5. Euler's magic square.

For us, the significance of magic squares is that they illustrate an area of combinatorics concerned with the interplay between numerical constraints and geometric arrangements. Our study of more serious examples of this interplay begins with Latin squares.

6.3.2 Definition. Let V be an n-element set. A *Latin square* based on V is an $n \times n$ matrix, each of whose rows and columns contains every element of V. A Latin square of *order* n is a Latin square based on some n-element set.

6.3.3 Example. Matrices $A = (a_{ij})$ and $B = (b_{ij})$ in Fig. 6.3.6 are Latin squares of order 4 based on $V = \{0, 1, 2, 3\}$. Taken together, this pair has some magic of its own. There are $4^2 = 16$ ways to choose two elements from V, with replacement,

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

A B

Figure 6.3.6. Orthogonal Latin squares.

where order matters. The magic is that for every such ordered pair (s,t), there is a matrix location (i,j) such that $a_{ij} = s$ and $b_{ij} = t$. The 4×4 array comprised of these ordered pairs, (a_{ij}, b_{ij}), is exhibited in Fig. 6.3.7.

Euler used arrays like this to construct magic squares. Convert each ordered pair of Fig. 6.3.7 into a two-letter *word*, obtaining

$$C_4 = \begin{pmatrix} 00 & 11 & 22 & 33 \\ 12 & 03 & 30 & 21 \\ 23 & 32 & 01 & 10 \\ 31 & 20 & 13 & 02 \end{pmatrix}.$$

Now, forget that the elemens of C_4 are words and think of them as numbers. Then, because each row and column sums to 66, C_4 is a pseudo magic square. On the other hand, if we treat the elements of C_4, not as base 10 numerals, but as numerals in base 4 then, upon converting them to base 10, we obtain

$$C_{10} = \begin{pmatrix} 0 & 5 & 10 & 15 \\ 6 & 3 & 12 & 9 \\ 11 & 14 & 1 & 4 \\ 13 & 8 & 7 & 2 \end{pmatrix}.$$

Adding 1 to each entry of C_{10} produces the genuine magic square

$$\begin{matrix} 1 & 6 & 11 & 16 \\ 7 & 4 & 13 & 10 \\ 12 & 15 & 2 & 5 \\ 14 & 9 & 8 & 3 \end{matrix}.$$

□

6.3.4 Definition. Let $A = (a_{ij})$ and $B = (b_{ij})$ be Latin squares of order n based on the elements of V. Then A and B are *orthogonal*[*] if, for each ordered pair (s,t) of elements of V, there is a (unique) matrix location (i,j) such that $a_{ij} = s$ and $b_{ij} = t$.

[*]This use of "orthogonal" has no obvious connection either to perpendicularity or to parity.

(0,0)	(1,1)	(2,2)	(3,3)
(1,2)	(0,3)	(3,0)	(2,1)
(2,3)	(3,2)	(0,1)	(1,0)
(3,1)	(2,0)	(1,3)	(0,2)

Figure 6.3.7

6.3.5 Example. The Latin squares of order 4 exhibited in Fig. 6.3.6 are orthogonal. If $V = \{x, y, z\}$, the Latin squares

$$\begin{pmatrix} x & y & z \\ y & z & x \\ z & x & y \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix}$$

are orthogonal. (Confirm it.)

Can you find an orthogonal pair of Latin squares of order 2? (Resolve this question before proceeding any further.) □

Euler discovered an algorithm for generating an orthogonal pair of Latin squares of order n, provided n does not occur in the arithmetic sequence 2, 6, 10, 14, ... In 1782, defeated in his attempts to find an orthogonal pair of order 6, he conjectured not only that no such pair exists, but that there does not exist an orthogonal pair of Latin squares of order $n = 4k + 2$ for any $k \geq 1$.

It wasn't until 1900 that G. Tarry confirmed the $n = 6$ case of Euler's conjecture using the unrevealing strategy of comparing all possible pairs of Latin squares of order 6. So, Euler was right about $n = 6$. It turns out, however, that he was wrong about *every* number in the sequence beyond 6. In 1960, the combined efforts of Euler, R. C. Bose, E. T. Parker, and S. S. Shrikhande established the following.

6.3.6 Theorem. *For every n, except $n = 2$ and $n = 6$, there exists an orthogonal pair of Latin squares of order n.*

Might there be more than two? What about three mutually orthogonal Latin squares of order 5, say?

6.3.7 Theorem. *There exist at most $n - 1$ mutually orthogonal Latin squares of order n.*

Proof. Let $A_1, A_2, \ldots, A_k$ be a family of mutually orthogonal Latin squares based on $V = \{1, 2, \ldots, n\}$. Suppose the first row of A_1 is $x_1, x_2, \ldots, x_n$. Because A_1 is a Latin square, x_r occurs once in each of its rows and columns, $1 \leq r \leq n$. Construct an $n \times n$ matrix B_1, the (i,j)-entry of which is equal to r if and only if the (i,j)-entry of A_1 is equal to x_r, $1 \leq r \leq n$. Then B_1 is a Latin square whose first row is $1, 2, \ldots, n$. More remarkable is the fact that the family $B_1, A_2, A_3, \ldots, A_k$ is mutually orthogonal! To see why, suppose $m \in \{2, 3, \ldots, k\}$. Let $B_1 = (b_{ij})$ and

$A_m = (a_{ij})$. If $(a_{ij}, b_{ij}) = (s,t) = (a_{pq}, b_{pq})$, then $b_{ij} = t = b_{pq}$. So, x_t is both the (i,j)-entry and the (p,q)-entry of A_1. But then $(a_{ij}, x_t) = (a_{pq}, x_t)$, contradicting the orthogonality of A_m and A_1.

Suppose the first row of A_2 is $y_1, y_2, \ldots, y_n$. Let B_2 be the matrix whose (i,j)-entry is equal to r if and only if the corresponding entry of A_2 is y_r, $1 \le r \le n$. Then, B_2 is a Latin square whose first row is $1, 2, \ldots, n$ and, by the same argument, $B_1, B_2, A_3, A_4, \ldots, A_k$ is a family of mutually orthogonal Latin squares. Continuing in this way, we eventually obtain a family $B_1, B_2, \ldots, B_k$ of orthogonal Latin squares each of which has the same first row, namely, $1, 2, \ldots, n$.

Denote the $(2,1)$-entry of B_r by z_r, $1 \le r \le k$. Note that these z's are all different. If, for example, z_1 and z_2 were both equal to t, then t would be a common entry of B_1 and B_2 in positions $(1,t)$ and $(2,1)$, contradicting the orthogonality of B_1 and B_2. Moreover, if $z_r = 1$ for some r, then B_r would have two 1's in its first column. Hence, there are at most $n-1$ possible z's. ■

A family of $n-1$ mutually orthogonal Latin squares of order n is said to be *complete*. It follows from Example 6.3.5 that there exists a complete family of mutually orthogonal latin squares of order $n = 3$. However, from Tarry's computations, there are not even two, much less five, mutually orthogonal Latin squares of order 6. For the purposes of the next result, it is convenient to stipulate that a single Latin square constitutes a mutually orthogonal *family.*

6.3.8 Theorem. *For every prime p, there exists a (complete) family of $p-1$ mutually orthogonal Latin squares of order p.*

Proof. Define a family $A_1, A_2, \ldots, A_{p-1}$ of $p \times p$ matrices as follows: The (i,j)-entry of A_t is the remainder when $ti + j$ is divided by p. Evidently, the entries of A_t come from the set $V = \{0, 1, \ldots, p-1\}$.

Suppose $ti_1 + j = pq_1 + r_1$ and $ti_2 + j = pq_2 + r_2$, where $0 \le r_1, r_2 < p$. Then r_1 is the (i_1, j)-entry of A_t, and r_2 is its (i_2, j)-entry. If $r_1 = r_2$, then $t(i_1 - i_2) = p(q_1 - q_2)$, which implies that $p|t$ (i.e., p exactly divides t) or $p|(i_1 - i_2)$. Neither alternative is possible because both t and $|i_1 - i_2|$ are less than p. So, the entries in column j of A_t are all different. A similar argument for row i of A_t proves that A_t is a Latin square, $1 \le t \le p-1$.

To prove orthogonality, suppose x occurs in both the (i_1, j_1) and the (i_2, j_2) positions of A_t, and y occurs in both the (i_1, j_1) and the (i_2, j_2) positions of A_s. That is, suppose

$$\begin{aligned} ti_1 + j_1 &= pq_1 + x, \\ ti_2 + j_2 &= pq_2 + x, \\ si_1 + j_1 &= pq_3 + y, \\ si_2 + j_2 &= pq_4 + y. \end{aligned}$$

Then

$$t(i_1 - i_2) + (j_1 - j_2) = p(q_1 - q_2)$$

and

$$s(i_1 - i_2) + (j_1 - j_2) = p(q_3 - q_4),$$

from which it follows that $(t - s)(i_1 - i_2)$ is a multiple of p, contradicting the fact that both $|t - s|$ and $|i_1 - i_2|$ are positive and less than p. ■

Using the theory of finite fields, one can extend the proof of Theorem 6.3.8 and obtain the following stronger result.

6.3.9 Theorem. *Suppose p is a prime and a is a positive integer. If $n = p^a$, there exists a (complete) family of $n - 1$ mutually orthogonal Latin squares of order n.*

It follows from Theorem 6.3.9 that, apart from 6, there are complete families of mutually orthogonal Latin squares for $2 \leq n \leq 9$. The story for $n = 10$ takes us to the theory of finite projective planes, a topic that has no obvious connection to Latin squares.

6.3.10 Definition. A *projective plane* consists of three things, a set of *points*, a set of *lines*, and an *incidence relation*, that satisfy the following axioms.

1. For any pair of distinct points P and Q, there is a unique line L such that P and Q are both incident with L.
2. For any pair of distinct lines L and M, there is a unique point P such that L and M are both incident with P.
3. There exist four distinct points, no three of which are incident with the same line.

Suppose *A, B, C*, and *D* are four different points, no three of which are collinear (incident with the same line). From Axiom 1, there is a unique line determined by *A* and *B*; let's call it *AB*.

We claim that no three of the lines *AB*, *BC*, *CD*, and *AD* are concurrent (incident with the same point). Suppose, e.g., there were some point *P* incident with *AB*, *BC*, and *CD*. If $P = A$, then *A, B*, and *C* are all incident with line *BC*, contradicting the hypothesis. If $P = B$, then *B, C*, and *D* are all incident with *CD*, contradicting the hypothesis. If $A \neq P \neq B$ then, by the uniqueness part of Axiom 1, the line $AB = BP = BC$ is incident with *A, B*, and *C*, contradicting the hypothesis. So, *AB, BC*, and *CD* are not concurrent. Similar arguments work for the other three ways to select three lines from *AB, BC, CD*, and *AD*, proving the following.

6.3.11 Theorem. *There exist four distinct lines, no three of which are incident with the same point.*

It follows from Definition 6.3.10 and Theorem 6.3.11 that every theorem in the theory of projective planes has a "dual" in which the roles of points and lines are interchanged. This *duality principle* is of fundamental importance in the theory of projective planes.

6.3.12 Theorem. *Let P and Q be points, and L and M be lines in a projective plane. Then there is a one-to-one correspondence*

(a) between the points incident with L and the points incident with M.

(b) between the lines incident with P and the lines incident with Q.

(c) between the points incident with L and the lines incident with P.

Proof. The existence of a point O incident with neither L nor M is left to the exercises. For each point X incident with L, the distinct lines OX and M are incident with a unique point Y. This sets up a natural mapping f from the points of L to the points of M, namely $f(X) = Y$. If $f(X_1) = Y = f(X_2)$, then X_1 and X_2 are both incident with the line OY. If $X_1 \neq X_2$ then, by the uniqueness part of Axiom 1, $L = X_1X_2 = OY$, contradicting the fact that O is not incident with L. This proves that f is one-to-one. If Y is incident with M, then $Y \neq O$. If X is the unique point incident with both L and OY, then $f(X) = Y$, proving that f is onto. This completes the proof of part (a).

Part (b) follows from part (a) by the duality principle.

If K is a fixed but arbitrary line incident with O, there is a unique point X incident with both K and L. So, the function g, from the lines incident with O to the points incident with L, defined by $g(K) = X$, is one-to-one. Because line OX is incident with O for every point X of L, g is onto. Together with parts (a) and (b), this completes the proof of part (c). ■

6.3.13 Definition. A projective plane is *finite* if its set of points is finite. A finite projective plane has *order* n if there are exactly $n + 1$ points incident with every line.

6.3.14 Corollary. *A finite projective plane of order n has exactly $n^2 + n + 1$ points and $n^2 + n + 1$ lines.*

Proof. Let P be a point of a finite projective plane of order n. By Theorem 6.3.12(c) and Definition 6.3.13, there are exactly $n + 1$ lines incident with P. Apart from P, each of these lines is incident with exactly n other points. Since every point is incident with one of these $n + 1$ lines, the plane contains exactly $n(n + 1)$ points different from P, i.e., the total number of points is $n^2 + n + 1$. The corresponding enumeration of lines follows from the duality principle. ■

6.3.15 Example. Together with Axiom 3 of Definition 6.3.10, Corollary 6.3.14 precludes the existence of a finite projective plane of order 1. By itself, Corollary 6.3.14 requires that a finite projective plane of order 2 have a total of seven points.

Let $\{1, 2, \ldots, 7\}$ be the set of points and $\{L_1, L_2, \ldots, L_7\}$ the set of lines, where $L_1 = \{1, 2, 3\}$, $L_2 = \{1, 4, 7\}$, $L_3 = \{1, 5, 6\}$, $L_4 = \{2, 4, 6\}$, $L_5 = \{2, 5, 7\}$, $L_6 = \{3, 4, 5\}$, $L_7 = \{3, 6, 7\}$, and "P is incident with L" is interpreted to mean that $P \in L$. Perhaps the easiest way to confirm that Axioms 1–3 are valid for this

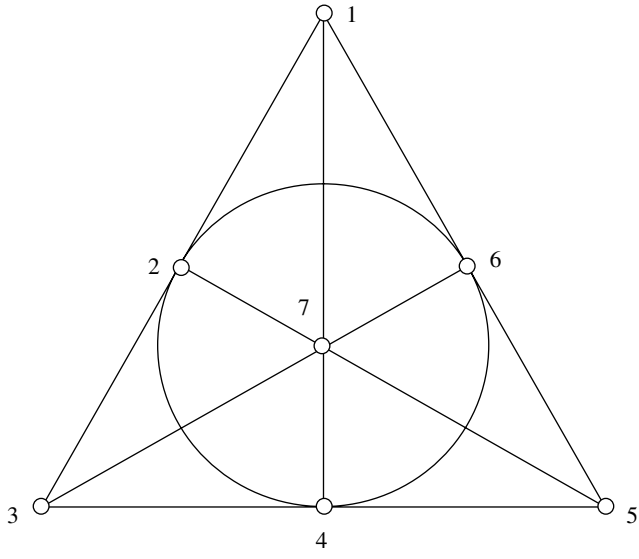


Figure 6.3.8. Finite projective plane of order 2.

model is by means of Fig. 6.3.8 (in which six of the lines are represented by segments and L_4 is represented by a circle). □

We come, at last, to the connection between finite projective planes and orthogonal Latin squares.

6.3.16 Theorem. *Suppose $n \geq 2$. Then there exists a finite projective plane of order n, if and only if there exists a (complete) family of $n-1$ mutually orthogonal Latin squares of order n.*

Proof. Let L be a fixed but arbitrary line in a finite projective plane of order n. Let $P_1, P_2, \ldots, P_{n+1}$ be the points that are incident with L and $Q_1, Q_2, \ldots, Q_{n^2}$ the points that are not. Apart from L, there are exactly n distinct lines that are incident with P_i, call them $M_{i1}, M_{i2}, \ldots, M_{in}$. The proof involves an $(n+1) \times n^2$ matrix C whose rows are indexed by $P_1, P_2, \ldots, P_{n+1}$ and whose columns are indexed by $Q_1, Q_2, \ldots, Q_{n^2}$. The (P_i, Q_j)-entry of C is $c_{ij} = t$, where t is uniquely determined by the identity $P_i Q_j = M_{it}$.

Consider, e.g., the model of the finite projective plane of order $n = 2$ discussed in Example 6.3.15 (and Fig. 6.3.8). Then $n + 1 = 3$ and $n^2 = 4$. If L is the line $L_1 = \{1, 2, 3\}$, then the points incident with L are $P_i = i$, $1 \leq i \leq 3$, and the points not incident with L are $Q_j = j + 3$, $1 \leq j \leq 4$. Let's find the (P_2, Q_3)-entry of the 3×4 matrix C corresponding to this scenario.

Apart from L, the $n = 2$ lines incident with $P_2 = 2$ are $L_4 = \{2, 4, 6\}$ and $L_5 = \{2, 5, 7\}$. Let $M_{21} = L_4$ and $M_{22} = L_5$ (an arbitrary choice). From

Example 6.3.15, the unique line determined by $P_2 = 2$ and $Q_3 = 6$ is $\{2, 4, 6\} = L_4 = M_{21}$, i.e., $P_2Q_3 = M_{21}$. Together with the definition of C, this yields $c_{23} = 1$.

The next step in the proof is to establish the following orthogonality property for the rows of this awkward matrix C.

Property O. If $1 \leq i < k \leq n+1$, then $S = \{(c_{ij}, c_{kj}) : 1 \leq j \leq n^2\}$ is the set of all n^2 ordered selections, with replacement, of two elements from $\{1, 2, \ldots, n\}$.

To confirm Property O, suppose $(c_{ir}, c_{kr}) = (c_{is}, c_{ks})$. If the common value of c_{ir} and c_{is} is t then, from the definition of C, $P_iQ_r = M_{it} = P_iQ_s$. In particular, $P_iQ_r = P_iQ_s$. Similarly, $P_kQ_r = P_kQ_s$. If $r \neq s$, this implies that P_i and P_k are both incident with line Q_rQ_s, i.e., $Q_rQ_s = P_iP_k = L$, contradicting the fact that neither Q_r nor Q_s is incident with L.

Note that permuting the *columns* of C is equivalent to renaming the points not incident with L. The effect on the set S is to rearrange its elements, leaving S itself unchanged. Thus, rearranging the columns of C has no effect on Property O. Indeed, one consequence of Property O is that the columns of C can be rearranged to obtain a matrix B the first two rows of which are

$$(1, 1, \ldots, 1, 2, 2, \ldots, 2, 3, 3, \ldots, 3, \ldots, n, n, \ldots, n), \tag{6.22}$$

and

$$(1, 2, \ldots, n, 1, 2, \ldots, n, 1, 2, \ldots, n, \ldots, 1, 2, \ldots, n). \tag{6.23}$$

Now, for each $r = 1, 2, \ldots, n-1$, form the $n \times n$ matrix A_r as follows: The first row of A_r consists of the first n entries in row $r+2$ of B. The second row of A_r consists of the entries in columns $n+1$ through $2n$ from row $r+2$ of B, and so on. In general, the (i,j)-entry of A_r is the entry in row $r+2$ and column $(i-1)n+j$ of B.

Applying Property O to rows 1 and $r+2$ of B yields that the entries in row i of A_r are all different, $1 \leq i \leq n$. (See Expression (6.22).) Applying Property O to rows 2 and $r+2$ of B yields that the entries in column j of A_r are all different, $1 \leq j \leq n$. (See Expression (6.23).) Therefore, A_r is a Latin square of order n based on $\{1, 2, \ldots, n\}$, $1 \leq r < n$. Finally, Property O guarantees that A_r and A_s are orthogonal whenever $r \neq s$.

The converse is proved by reversing these steps. Given $n-1$ mutually orthogonal Latin squares of order n, form an $(n+1) \times n^2$ matrix B whose first two rows are given by Expressions (6.22) and (6.23), respectively, and whose $(r+2)$nd row comes from the rows of A_r laid down one after another. For this part of the proof, no rearrangement of columns is necessary. One can (re)construct from matrix $C = B$ a finite projective plane of order n. The details are omitted, but see Example 6.3.18 (below). ■

6.3.17 Example. In the midst of the proof of Theorem 6.3.16, we evaluated c_{23} with respect to the choices $L = L_1 = \{1, 2, 3\}$, $P_i = i$, $1 \leq i \leq 3$, $Q_j = j + 3$,

$1 \le j \le 4$, $M_{21} = L_4 = \{2,4,6\} = \{P_2, Q_1, Q_3\}$, and $M_{22} = L_5 = \{2,5,7\} = \{P_2, Q_2, Q_4\}$ from the model of the finite projective plane of order $n = 2$ in Example 6.3.15. With the (arbitrary) choices $M_{11} = L_2 = \{P_1, Q_1, Q_4\}$, $M_{12} = L_3 = \{P_1, Q_2, Q_3\}$, $M_{31} = L_6 = \{P_3, Q_1, Q_2\}$, and $M_{32} = L_7 = \{P_3, Q_3, Q_4\}$, the entire matrix

$$C = \begin{pmatrix} 1 & 2 & 2 & 1 \\ 1 & 2 & 1 & 2 \\ 1 & 1 & 2 & 2 \end{pmatrix}.$$

Observe that the rows of C are, indeed, mutually orthogonal in the sense that $S = \{(c_{ij}, c_{kj}) : 1 \le j \le 4\}$ is the set of all four ordered selections, with replacement, of two elements from $\{1,2\}$, $1 \le i < k \le 3$. The matrix obtained from C by interchanging its second and fourth columns is

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

the first two rows of which have the form prescribed by Expressions (6.22) and (6.23), respectively. Finally, the Latin square emerging from the third row of B is

$$A_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$ □

6.3.18 Example. Let's use the mutually orthogonal Latin squares of order 3 from Example 6.3.5 to construct a finite projective plane of order $n = 3$. Replacing x, y, and z with 1, 2, and 3, respectively, yields

$$A_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}.$$

Laid out end to end, the rows of A_1 and A_2 generate rows 3 and 4, respectively, of

$$B = \begin{array}{c} \\ P_1 \\ P_2 \\ P_3 \\ P_4 \end{array} \begin{array}{c} \begin{array}{ccccccccc} Q_1 & Q_2 & Q_3 & Q_4 & Q_5 & Q_6 & Q_7 & Q_8 & Q_9 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 1 & 2 & 3 & 2 & 3 & 1 & 3 & 1 & 2 \\ 1 & 2 & 3 & 3 & 1 & 2 & 2 & 3 & 1 \end{pmatrix} \end{array},$$

the rows of which are indexed by P_i, $1 \le i \le n + 1 = 4$, and the colums by Q_j, $1 \le j \le n^2 = 9$. Together with the orthogonality of the pair A_1, A_2, the first two rows guarantee that B satisfies Property O.

The idea behind the proof of Theorem 6.3.16 is that $\{P_1, P_2, P_3, P_4\} \cup \{Q_1, Q_2, \ldots, Q_9\}$ comprises the $3^2 + 3 + 1 = 13$ points of a projective plane of order 3. Apart from $L = \{P_1, P_2, P_3, P_4\}$, the remaining 12 lines of this plane can be read off from matrix $C = B$:

$$
\begin{array}{lll}
M_{11} = \{P_1, Q_1, Q_2, Q_3\}, & M_{12} = \{P_1, Q_4, Q_5, Q_6\}, & M_{13} = \{P_1, Q_7, Q_8, Q_9\}, \\
M_{21} = \{P_2, Q_1, Q_4, Q_7\}, & M_{22} = \{P_2, Q_2, Q_5, Q_8\}, & M_{23} = \{P_2, Q_3, Q_6, Q_9\}, \\
M_{31} = \{P_3, Q_1, Q_6, Q_8\}, & M_{32} = \{P_3, Q_2, Q_4, Q_9\}, & M_{33} = \{P_3, Q_3, Q_5, Q_7\}, \\
M_{41} = \{P_4, Q_1, Q_5, Q_9\}, & M_{42} = \{P_4, Q_2, Q_6, Q_7\}, & M_{43} = \{P_4, Q_3, Q_4, Q_8\},
\end{array}
$$

where $P_i Q_j = M_{it}$ if and only if $c_{ij} = t$. Observe that each of these lines is incident with (contains) $n + 1 = 4$ points. Confirm that each point is incident with (contained in) exactly 4 lines.

To prove that this configuration satisfies Axioms 1–3 of Definition 6.3.10, observe that the unique line incident with two of the P's is L. The unique line incident with P_i and Q_j is M_{it}, where $t = c_{ij}$. The unique line incident with Q_r and Q_s is M_{it}, where i and t are uniquely determined by $c_{ir} = t = c_{is}$. (Property O implies that $c_{ir} = c_{is}$ and $c_{kr} = c_{ks}$ cannot both hold unless $i = k$.)

The unique point incident with L and M_{it} is P_i. The unique point incident with M_{it} and M_{kj} is P_i if $k = i$; otherwise, it is Q_r, where r is the column of C determined by $c_{ir} = t$ and $c_{kr} = j$. Finally, no three of the points P_1, P_2, Q_3, and Q_4 are incident with the same line. □

R. H. Bruck and H. J. Ryser independently discovered a necessary condition for the existence of a projective plane of order n. If d is the largest (perfect) square factor of n, then n/d is the *square-free* part of n.

6.3.19 Bruck–Ryser Theorem. *Suppose n is of the form $4k + 1$ or $4k + 2$. If the square-free part of n contains a prime factor of the form $4k + 3$, then there does not exist a finite projective plane of order n.*

6.3.20 Example. The square-free integer $6 = 4(1) + 2$ contains a prime factor $3 = 4(0) + 3$. So (as we already know from other considerations), there is no finite projective plane of order 6. While $10 = 4(2) + 2$ is also square-free, neither of its prime factors is of the form $4k + 3$. So, the Bruck–Ryser theorem is silent on planes of order 10, a topic *to be continued*. □

6.3. EXERCISES

1 Let m be the magic number for a magic square of order n. Find a formula that expresses m as a function of n. (Conclude that any two magic squares of the same order have the same magic number.)

2 Prove that there is no magic square of order 2.

3 Using the orthogonal Latin squares in Example 6.3.5, mimic the approach used in Example 6.3.3 to construct a magic square of order 3.

4 The 52 cards in a standard *bridge* deck come in four *suits* (clubs, diamonds, hearts, and spades) each headed by four *honors* (jack, queen, king, and ace).

(a) Show that the 16 honor cards can be arranged in a 4×4 array in such a way that every row and every column contains cards representing all four suits and all four honors.

(b) Explain how the arrangement in part (a) can be viewed as a model for two orthogonal Latin squares of order 4.

5 Exhibit a family of three mutually orthogonal Latin squares of order 4 each of which has the same first row.

6 Let $A = (a_{ij})$ be an $n \times n$ matrix. A (generalized) *diagonal* of A is a sequence $(a_{1p(1)}, a_{2p(2)}, \ldots, a_{np(n)})$, where $p \in S_n$. If A is a Latin square on V, a *transversal* of A is a diagonal that contains every element of V. If $B = (b_{ij})$ is another Latin square based on V, show that A and B are orthogonal if and only if, for all $x \in V$, the elements of $\{a_{ij} : b_{ij} = x\}$ are the terms of a transversal of A.

7 Prove that a Cayley table for a (finite) permutation group G is a Latin square based on $V = G$.

8 Construct a magic square of order 6. (This is not an easy exercise.)

9 Prove that magic squares of order n exist for every $n \neq 2$.

10 A Latin square is *self-orthogonal* if it is orthogonal to its transpose.

(a) Prove that there is no self-orthogonal Latin square of order 3.

(b) Exhibit a self-orthogonal Latin square of order 4.

11 Say that two Latin squares are *equivalent* if it is possible to obtain the second by permuting the rows and columns of the first. Exhibit two inequivalent Latin squares of order 4.

12 If a finite projective plane has 183 points, how many lines are incident with each one of them?

13 Explain why the Bruck–Ryser theorem does not supersede Tarry's theorem.

14 Use the Bruck–Ryser theorem to prove the nonexistence of a finite projective plane of order

(a) 14. **(b)** 21. **(c)** 22.

15 Construct a family of four mutually orthogonal Latin squares of order 5.

16 Let $C = (c_{ij})$ and $R = (r_{ij})$ be $n \times n$ matrices defined by $c_{ij} = i$, $1 \le j \le n$, and $r_{ij} = j$, $1 \le i \le n$.

(a) Show that C and R are *orthogonal*, i.e., for each ordered pair (s,t), $1 \le s,t \le n$, there is a (unique) matrix location (i,j) such that $c_{ij} = s$ and $r_{ij} = t$.

(b) Show that A is a Latin square based on $\{1,2,\ldots,n\}$ if and only if A is orthogonal to both C and R.

17 If $A = (a_{ij})$ and $B = (b_{ij})$ are $m \times m$ and $n \times n$ matrices, respectively, their *Kronecker product* is the $mn \times mn$ block partitioned matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{pmatrix},$$

where

$$a_{ij}B = \begin{pmatrix} a_{ij}b_{11} & a_{ij}b_{12} & \cdots & a_{ij}b_{1n} \\ a_{ij}b_{21} & a_{ij}b_{22} & \cdots & a_{ij}b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{ij}b_{n1} & a_{ij}b_{n2} & \cdots & a_{ij}b_{nn} \end{pmatrix}, \qquad 1 \le i,j \le m.$$

Compute $A \otimes B$ if

(a) $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix}$.

(b) $A = I_3$ and $B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$.

(c) $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ and $B = I_3$.

(d) $A = \begin{pmatrix} 1 & 0 & 2 \\ 1 & 1 & 1 \\ 0 & 2 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$.

18 Suppose A_1 and A_2 are a pair of orthogonal Latin squares of order m and L_1 and L_2 are a pair of order n. Prove that $A_1 \otimes L_1$ and $A_2 \otimes L_2$ are a pair of oder mn. (See Exercise 17.)

19 Suppose $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Let $k = \min\{p_i^{a_i} : 1 \le i \le r\}$. Prove that there exists a family of $k-1$ mutually orthogonal Latin squares of order n.

20 Use the following pair of orthogonal Latin squares of order 10 to generate a magic square of order 10:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 7 & 0 & 1 & 2 & 4 & 5 & 8 & 9 & 3 \\ 5 & 6 & 8 & 7 & 0 & 1 & 4 & 9 & 3 & 2 \\ 4 & 5 & 6 & 9 & 8 & 7 & 0 & 3 & 2 & 1 \\ 7 & 4 & 5 & 6 & 3 & 9 & 8 & 2 & 1 & 0 \\ 9 & 8 & 4 & 5 & 6 & 2 & 3 & 1 & 0 & 7 \\ 2 & 3 & 9 & 4 & 5 & 6 & 1 & 0 & 7 & 8 \\ 8 & 9 & 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\ 3 & 2 & 1 & 0 & 7 & 8 & 9 & 5 & 4 & 6 \\ 1 & 0 & 7 & 8 & 9 & 3 & 2 & 4 & 6 & 5 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 1 & 2 & 3 & 7 & 8 & 5 & 6 & 0 \\ 6 & 0 & 7 & 1 & 2 & 3 & 5 & 8 & 9 & 4 \\ 8 & 9 & 4 & 5 & 1 & 2 & 3 & 6 & 0 & 7 \\ 3 & 6 & 0 & 7 & 8 & 1 & 2 & 9 & 4 & 5 \\ 2 & 3 & 9 & 4 & 5 & 6 & 1 & 0 & 7 & 8 \\ 1 & 2 & 3 & 0 & 7 & 8 & 9 & 4 & 5 & 6 \\ 4 & 7 & 5 & 8 & 6 & 9 & 0 & 1 & 2 & 3 \\ 7 & 5 & 8 & 6 & 9 & 0 & 4 & 3 & 1 & 2 \\ 5 & 8 & 6 & 9 & 0 & 4 & 7 & 2 & 3 & 1 \end{pmatrix}$$

21 Let $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \\ 3 & 4 & 1 & 5 & 2 \\ 4 & 5 & 2 & 1 & 3 \\ 5 & 3 & 4 & 2 & 1 \end{pmatrix}$.

(a) Prove that A does not have an orthogonal mate, i.e., show that there is no Latin square B of order 5 such that A and B are orthogonal.

(b) Explain why this does not contradict Theorem 6.3.8.

(c) Find a Latin square of order 4 that does not have an orthogonal mate.

22 Prove the existence of the point O used in the proof of Theorem 6.3.12.

6.4. BALANCED INCOMPLETE BLOCK DESIGNS

> We feel *as if* we were free; consider Nature *as if* she were full of special designs; lay plans *as if* we were to be immortal; and we find then that these words do make a genuine difference in our moral life.
>
> — William James (*The Principles of Psychology*)

Perhaps the easiest way to describe a finite projective plane of order n is by means of $(0, 1)$-matrices.

6.4.1 Definition. Let $P_1, P_2, \ldots, P_m$ and $L_1, L_2, \ldots, L_m$ be the points and lines, respectively, of a finite projective plane of order n (so that $m = n^2 + n + 1$). Then the corresponding $m \times m$ *incidence matrix* $A = (a_{ij})$ is defined by

$$a_{ij} = \begin{cases} 1 & \text{if } P_i \text{ is incident with } L_j, \\ 0 & \text{otherwise.} \end{cases}$$

	M_{11}	M_{12}	M_{13}	M_{21}	M_{22}	M_{23}	M_{31}	M_{32}	M_{33}	M_{41}	M_{42}	M_{43}	L
P_1	1	1	1	0	0	0	0	0	0	0	0	0	1
P_2	0	0	0	1	1	1	0	0	0	0	0	0	1
P_3	0	0	0	0	0	0	1	1	1	0	0	0	1
P_4	0	0	0	0	0	0	0	0	0	1	1	1	1
Q_1	1	0	0	1	0	0	1	0	0	1	0	0	0
Q_2	1	0	0	0	1	0	0	1	0	0	1	0	0
Q_3	1	0	0	0	0	1	0	0	1	0	0	1	0
Q_4	0	1	0	1	0	0	0	1	0	0	0	1	0
Q_5	0	1	0	0	1	0	0	0	1	1	0	0	0
Q_6	0	1	0	0	0	1	1	0	0	0	1	0	0
Q_7	0	0	1	1	0	0	0	0	1	0	1	0	0
Q_8	0	0	1	0	1	0	1	0	0	0	0	1	0
Q_9	0	0	1	0	0	1	0	1	0	1	0	0	0

Figure 6.4.1. Incidence matrix for a projective plane of order 3.

6.4.2 Example. The incidence matrix for the plane of order 3 constructed in Example 6.3.18, with points $P_1, P_2, P_3, P_4, Q_1, Q_2, \ldots, Q_9$, and lines

$$\begin{array}{lll} M_{11} = \{P_1, Q_1, Q_2, Q_3\}, & M_{12} = \{P_1, Q_4, Q_5, Q_6\}, & M_{13} = \{P_1, Q_7, Q_8, Q_9\}, \\ M_{21} = \{P_2, Q_1, Q_4, Q_7\}, & M_{22} = \{P_2, Q_2, Q_5, Q_8\}, & M_{23} = \{P_2, Q_3, Q_6, Q_9\}, \\ M_{31} = \{P_3, Q_1, Q_6, Q_8\}, & M_{32} = \{P_3, Q_2, Q_4, Q_9\}, & M_{33} = \{P_3, Q_3, Q_5, Q_7\}, \\ M_{41} = \{P_4, Q_1, Q_5, Q_9\}, & M_{42} = \{P_4, Q_2, Q_6, Q_7\}, & M_{43} = \{P_4, Q_3, Q_4, Q_8\}, \end{array}$$

and $L = \{P_1, P_2, P_3, P_4\}$, is exhibited in Fig. 6.4.1. □

It is hard to took at this matrix and not see binary words! Consider the code $\mathscr{C} \subset F^{13}$, the codewords of which are the rows of this incidence matrix. While $\mathscr{C}$ may not be linear ($0 \notin \mathscr{C}$), it has other interesting properties. For example, because each point of the plane is incident with four lines, every codeword has weight 4. Since two points in the projective plane determine a unique line, the ones in two (different) rows of its incidence matrix overlap in exactly one place. Thus, if $c_1, c_2 \in \mathscr{C}$, $c_1 \neq c_2$, then the distance

$$\begin{aligned} d(c_1, c_2) &= [\mathrm{wt}(c_1) - 1] + [\mathrm{wt}(c_2) - 1] \\ &= 6, \end{aligned}$$

i.e., $\mathscr{C}$ is a $(13, 13, 6)$ code. These properties have the following obvious generalizations.

6.4.3 Theorem. *If A is an incidence matrix for a finite projective plane of order n, then the rows of A comprise an $(n^2 + n + 1, n^2 + n + 1, 2n)$ binary code in which every codeword has weight $n + 1$.*

Recall from Section 6.3 that there exists a finite projective plane of order n if and only if there exists a family of $n - 1$ mutually orthogonal Latin squares of order n.

Because such families are known to exist when n is a power of a prime, Theorem 6.4.3 establishes the existence, e.g., of codes with parameters $(73, 73, 16)$ and $(91, 91, 18)$, corresponding to $n = 8$ and $n = 9$, respectively. What about $n = 10$? The first *pair* of orthogonal Latin squares of order 10 was not discovered until 1959.* How does one go about finding nine of them? Computers?

That finite projective planes have applications to coding theory is already obvious from Theorem 6.4.3. Less obvious is that this is a two-way street. During the 1970s and 1980s it was shown that a code, exhibiting all of the interesting properties associated with a finite projective plane of order 10, could not exist! In fact, The *only* known proof of the nonexistence of a family of nine mutually orthogonal Latin squares of order 10 depends on the theory of error-correcting codes!†

The discussion leading up to Theorem 6.4.3 suggests that abstracting certain features of finite projective planes to a more general setting might be an easy way to produce binary codes with large error-correcting capabilities.

6.4.4 Definition. Let V be a set with v elements called *points*.‡ Suppose $\{B_1, B_2, \ldots, B_b\}$ is a family of k-element subsets of V called *blocks*. If each pair of distinct points of V occurs together in exactly λ blocks, then $\mathscr{D} = \{B_1, B_2, \ldots, B_b\}$ is a *balanced incomplete block design* (BIBD) with *parameters* (v, k, λ).

To avoid trivial cases, we will assume, throughout this section, that all designs satisfy $v > k > 1$. By a (v, k, λ)-design, we mean a BIBD with parameters (v, k, λ).

6.4.5 Example. Given a finite projective plane of order n, let V be its set of points and $\mathscr{D}$ its set of lines interpreted as subsets of V. Then $\mathscr{D}$ is a balanced incomplete block design with parameters $v = b = n^2 + n + 1$, $k = n + 1$, and $\lambda = 1$. A less exotic (and less interesting) example is the family of all k-element subsets of V, a BIBD in which $\lambda = C(v - 2, k - 2)$. □

In a finite projective plane, not only is each line incident with $n + 1$ points, but each point is incident with $n + 1$ lines. In a balanced incomplete block design, each block contains k points and, while it may not be the case that each point is contained in k blocks, each point *is* contained in the same number q of blocks.§

6.4.6 Theorem. *Each point of a (v, k, λ)-design belongs to exactly*

$$q = \lambda \frac{v - 1}{k - 1} \tag{6.24}$$

blocks.

*E. T. Parker, Orthogonal Latin squares, *Proc. Nat. Acad. Sci.* (USA) 45 (1959), 859–862.

†It is still an open problem to determine the size of a largest family of mutually orthogonal Latin squares of order 10.

‡Reflecting the origins of this notion in the design of statistical experiments, the elements of V are also known as *varieties*.

§The usual notation for this parameter is not q, but r, a letter made unavailable here by our focus on r-error-correcting codes.

Proof. Let $V = \{P_1, P_2, \ldots, P_v\}$ be the set of points. Suppose $P \in V$ is fixed but arbitrary. The theorem is proved by counting, in two different ways, the number of times P is paired with another point in some block of the design.

By renumbering the points, if necessary, we can assume $P = P_1$. By definition, P_1 and P_j occur together in exactly λ blocks, $2 \le j \le v$. Thus $\lambda(v-1)$ is one way to express the total number of pairings (multiplicities included) that involve P_1. On the other hand, P_1 is paired with the remaining $k-1$ points in each block to which it belongs. If P_1 is contained in (exactly) q blocks, then the number of pairings that involve P_1 is $q(k-1)$. Thus, $q(k-1) = \lambda(v-1)$. ■

Consider a BIBD $\mathscr{D} = \{B_1, B_2, \ldots, B_b\}$ with point set $V = \{P_1, P_2, \ldots, P_v\}$ and parameters (v, k, λ). Let $A = (a_{ij})$ be the $v \times b$ *incidence matrix* for the design, i.e.,

$$a_{ij} = \begin{cases} 1 & \text{if } P_i \in B_j, \\ 0 & \text{otherwise.} \end{cases}$$

Evidently, each row of A contains q ones, and there are k ones in each of its columns. Counting the total number of ones, first by columns and then by rows, yields the identity $bk = vq$, i.e.,

$$b = \frac{vq}{k}. \tag{6.25a}$$

Together, Equations (6.24) and (6.25a) imply that

$$b = \lambda \frac{v(v-1)}{k(k-1)}. \tag{6.25b}$$

Because they are functions of v, k, and λ, the numbers q and b will be referred to as *dependent parameters*.

6.4.7 Corollary. *Let A be the $v \times b$ incidence matrix of a (v, k, λ)-design. If $\mathscr{C}$ is the (n, M, d), r-error-correcting code comprised of the rows of A, then $n = b$, $M = v$, $d = 2(q - \lambda)$, $r = q - \lambda - 1$, and $wt(c) = q$ for all $c \in \mathscr{C}$.*

Proof. At this point, the only conclusion requiring proof is the value of d. If $1 \le i < j \le v$, then, by Definition 6.4.4, the q ones in row i of A overlap the q ones in row j of A in exactly λ places. Therefore, the distance between the corresponding codewords is $(q - \lambda) + (q - \lambda)$. ■

6.4.8 Example. Let $V = \{P_1, P_2, P_3\}$ be a set of points. If $B_1 = \{P_1, P_2\}$, $B_2 = \{P_2, P_3\}$, and $B_3 = \{P_1, P_3\}$, then $\mathscr{D}_1 = \{B_1, B_2, B_3\}$ is BIBD with parameters $(v, k, \lambda) = (3, 2, 1)$, and dependent parameters $b = 3$ and $q = \lambda(v-1)/(k-1) = 2$. Because $d = 2(q - \lambda) = 2$, the rows of the incidence matrix

$$A_1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9	B_{10}	B_{11}	B_{12}
1	1	1	1	1	0	0	0	0	0	0	0	0
2	1	0	0	0	1	1	1	0	0	0	0	0
3	1	0	0	0	0	0	0	1	1	1	0	0
4	0	1	0	0	1	0	0	1	0	0	1	0
5	0	0	1	0	0	1	0	0	1	0	1	0
6	0	0	0	1	0	0	1	0	0	1	1	0
7	0	1	0	0	0	0	1	0	1	0	0	1
8	0	0	0	1	0	1	0	1	0	0	0	1
9	0	0	1	0	1	0	0	0	0	1	0	1

Figure 6.4.2. Incidence matrix for a $(9, 3, 1)$-design.

comprise a $(3, 3, 2)$ binary code of constant weight 2. (Confirm the parameters of this code directly from the rows of A_1.) It is not a very useful code for a variety of reasons, not the least of which is that $r = q - \lambda - 1 = 0$. This code cannot correct even a single transmission error.

If $B_4 = B_1$, $B_5 = B_2$, and $B_6 = B_3$, then $\mathscr{D}_2 = \{B_1, B_2, \ldots, B_6\}$ is a BIBD with parameters $(v, k, \lambda) = (3, 2, 2)$. This time, $b = 6$, $q = 4$, $d = 4$, and $r = 1$. Thus, the rows of the incidence matrix

$$A_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

comprise a $(6, 3, 4)$, one-error-correcting (repetition) code of constant weight 4. (Confirm it.) □

6.4.9 Example. Let $V = \{1, 2, \ldots, 9\}$. If $B_1 = \{1, 2, 3\}$, $B_2 = \{1, 4, 7\}$, $B_3 = \{1, 5, 9\}$, $B_4 = \{1, 6, 8\}$, $B_5 = \{2, 4, 9\}$, $B_6 = \{2, 5, 8\}$, $B_7 = \{2, 6, 7\}$, $B_8 = \{3, 4, 8\}$, $B_9 = \{3, 5, 7\}$, $B_{10} = \{3, 6, 9\}$, $B_{11} = \{4, 5, 6\}$, and $B_{12} = \{7, 8, 9\}$, then $\mathscr{D} = \{B_1, B_2, \ldots, B_{12}\}$ is a balanced incomplete block design with parameters $(v, k, \lambda) = (9, 3, 1)$. The dependent parameters are $b = 12$ and $q = \lambda(v - 1)/(k - 1) = 4$. If A is the incidence matrix for this design (exhibited in Fig. 6.4.2), then the rows of A comprise a $(12, 9, 6)$, two-error-correcting code of constant weight 4.

Because $\lambda = 1$, any given pair of points is contained in exactly one block. Therefore, any pair of distinct blocks can intersect in at most one point. This implies that the 1's in two different *columns* of A can overlap in at most one place, i.e., the (Hamming) distance between columns is not less than $2(k - 1) = 4$. Hence, the columns of A comprise a $(9, 12, 4)$, one-error-correcting binary code of constant weight $k = 3$. □

6.4.10 Definition. A balanced incomplete block design is *symmetric* if $v = b$, i.e., if the number of points is equal to the number of blocks.

Note that every finite projective plane affords a symmetric BIBD. The design $\mathscr{D}_1$, from Example 6.4.8, is another. If $A = (a_{ij})$ is the incidence matrix of a symmetric BIBD, then A must be square, but it need not be symmetric. Despite the name, there is no requirement that a_{ij} be equal to a_{ji}.

If $b = v$ then, from Equation (6.25a), $q = k$, i.e., if $A = (a_{ij})$ is the $v \times v$ incidence matrix of a symmetric BIBD, then A has exactly k ones in each row and column. In particular, if $1 \leq s \leq t \leq v$, then the scalar (dot) product of rows s and t of A is

$$\sum_{j=1}^{v} a_{sj}a_{tj} = \begin{cases} k & \text{if } s = t, \\ \lambda & \text{if } s \neq t. \end{cases}$$

Because this is precisely the (s,t)-entry of the product of A and its transpose, the identity can be expressed more concisely as

$$AA^{\mathrm{t}} = (k - \lambda)I_v + \lambda J_v, \tag{6.26}$$

where J_v is the $v \times v$ matrix each of whose entries is 1. The marvelous thing about this necessary condition for A to be the incidence matrix of a symmetric BIBD is that it is also sufficient.

6.4.11 Lemma. *Let A be a $v \times v$ $(0,1)$-matrix. Then A satisfies Equation (6.26) if and only if it is the incidence matrix for a symmetric (v,k,λ)-design.*

The proof of sufficiency is left to the exercises.

Among the more surprising consequences of Equation (6.26) is the following:

6.4.12 Bruck–Ryser–Chowla Theorem (Part 1).[*] *Consider a symmetric balanced incomplete block design with parameters (v,k,λ). If v is even, then $k - \lambda$ is a perfect square.*

Proof. Let A be the $v \times v$ incidence matrix for the design. By Equation (6.26),

$$AA^{\mathrm{t}} = \begin{pmatrix} k & \lambda & \lambda & \cdots & \lambda \\ \lambda & k & \lambda & \cdots & \lambda \\ \lambda & \lambda & k & \cdots & \lambda \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \lambda & \cdots & k \end{pmatrix}.$$

Subtracting the first row of AA^{t} from each of its remaining rows gives

$$B = \begin{pmatrix} k & \lambda & \lambda & \lambda & \cdots & \lambda \\ \lambda - k & k - \lambda & 0 & 0 & \cdots & 0 \\ \lambda - k & 0 & k - \lambda & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda - k & 0 & 0 & 0 & \cdots & k - \lambda \end{pmatrix}.$$

[*]First proved for finite projective planes by R. H. Bruck and H. J. Ryser in 1949, the general theorem was published by S. Chowla and H. J. Ryser in 1950.

Adding columns 2 through v of matrix B to column 1 produces

$$C = \begin{pmatrix} x & \lambda & \lambda & \lambda & \cdots & \lambda \\ 0 & k-\lambda & 0 & 0 & \cdots & 0 \\ 0 & 0 & k-\lambda & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & k-\lambda \end{pmatrix}.$$

where $x = k + \lambda(v-1)$. Therefore,

$$\begin{aligned} (\det(A))^2 &= \det(AA^{\mathrm{t}}) \\ &= \det(B) \\ &= \det(C) \\ &= [k+\lambda(v-1)](k-\lambda)^{v-1}. \end{aligned} \tag{6.27}$$

Because $q = k$ we have, from Equation (6.24), that $k(k-1) = \lambda(v-1)$. Therefore, $k + \lambda(v-1) = k^2$. Together with Equation (6.27), this identity implies that one factor of $(\det(A))^2$ is a perfect square. Hence, the other factor, $(k-\lambda)^{v-1}$, must be a square as well. Because $v-1$ is odd, this is possible only if $k-\lambda$ is a square. ■

6.4.13 Example. Is there a symmetric BIBD with parameters $(46, 10, 2)$? When $b = v$ (so that $q = k$), Equation (6.24) becomes $k(k-1) = \lambda(v-1)$, a necessary condition that is satisfied for $k = 10$, $\lambda = 2$, and $v = 46$. On the other hand, because $v = 46$ is even, but $k - 2 = 8$ is not a perfect square, the existence of a symmetric $(46, 10, 2)$ design is precluded by Theorem 6.4.12. □

Let $\mathscr{C}$ be the r-error-correcting code comprised of the rows of the incidence matrix of a symmetric balanced incomplete block design. If $\mathscr{C}$ has an even number of codewords then, from Corollary 6.4.7 and Theorem 6.4.12, $r+1$ is a perfect square. How interesting is that? If, e.g., A is the incidence matrix for a finite projective plane of order n, then $v = n^2 + n + 1$ is odd. If $A = A_1$ in Example 6.4.8, then $v = 3$ is odd. Are there, in fact, *any* symmetric BIBDs for which v is even? For that matter, does a nontrivial* symmetric BIBD even exist?

6.4.14 Example. If A is the $(0,1)$-matrix exhibited in Fig. 6.4.3, then computations show (confirm them, at least for a few entries) that $AA^{\mathrm{t}} = 4I_{16} + 2J_{16}$. By Lemma 6.4.11, this means A is the incidence matrix for a symmetric BIBD with parameters $(16, 6, 2)$. If $\mathscr{C}$ is the (n, M, d) r-error-correcting code comprised of the rows of A then, by Corollary 6.4.7, $n = b = v = 16$, $M = v = 16$,

*For the purposes of this question, a symmetric BIBD is nontrivial if it has more than three points and does not correspond to a projective plane.

$$A = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

Figure 6.4.3

$d = 2(q - \lambda) = 8$, and $r = 3$. In particular, as guaranteed by Corollary 6.4.7 and Theorem 6.4.12, $r + 1 = 4$ is a perfect square. □

Okay. Example 6.4.14 establishes the existence of a nontrivial symmetric BIBD. Are there more? Yes. In fact, we can systematically produce as many as we like. Here's how.

6.4.15 Definition. Let H be an $n \times n$ matrix, each of whose entries is either $+1$ or -1. If

$$HH^{\mathrm{t}} = nI_n,$$

then H is a *Hadamard matrix* of *order n*.

Note that $HH^{\mathrm{t}} = nI_n$, if and only if $H^{-1} = (1/n)H^{\mathrm{t}}$, if and only if $H^{\mathrm{t}}H = nI_n$.

If all the entries in some row or column of a Hadamard matrix are multiplied by -1, the result is another Hadamard matrix. Thus, any Hadamard matrix can be transformed into a *normalized* Hadamard matrix, one whose first row and column consist entirely of $+1$'s.

6.4.16 Example. The unique normalized Hadamard matrices of orders 1 and 2 are

$$(1) \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

respectively. Before reading on, take a moment to convince yourself that there is no Hadamard matrix of order 3.

When $n = 4$, there are (at least) two normalized Hadamard matrices, namely,

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad \text{and} \quad H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Observe that H_2 can be obtained from H_1 by interchanging its second and third columns—an elementary column operation. In other words, $H_2 = H_1P$, where the permutation matrix

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

More generally, if P is a fixed but arbitrary permutation matrix of size n then, because $P^{-1} = P^{\mathrm{t}}$, the $n \times n$ $(+1, -1)$-matrix H is a Hadamard matrix if and only if $K = HP$ is a Hadamard matrix. □

The equation $HH^{\mathrm{t}} = nI_n$ implies that any two different rows of H are orthogonal, not in the sense of orthogonal Latin squares, but in the sense that their scalar product (over $\mathbb{R}$) is zero. In particular, if H is normalized, then every row but the first must contain the same number of $+1$'s and -1's. If H is a Hadamard matrix of order $n > 1$ then, evidently, n must be even. There is more.

If H_1 is a normalized Hadamard matrix of order $n > 2$ then, by permuting the columns of H_1, if necessary, we can obtain a normalized Hadamard matrix H_2 such that the first $n/2$ entries in the second row of H_2 all equal $+1$. (See, e.g., H_1 and H_2 in Example 6.4.16.) For a fixed but arbitrary row index $i > 2$, let t be the number of $+1$'s in the first $n/2$ columns of row i of H_2. If $s = (n/2) - t$, then, among the first $n/2$ columns of the ith row of H_2, there must be a total of s -1's. Moreover, by orthogonality with row 1, there must be s occurrences of $+1$ and t occurrences of -1 among the last $n/2$ entries of row i. In particular,

$$2s + 2t = n.$$

Finally, the orthogonality of rows 2 and i yields

$$2t - 2s = 0.$$

Therefore, $s = t$ and $4t = n$. Let's formalize this last observation.

6.4.17 Theorem. *If H is a Hadamard matrix of order $n > 2$, then n is an integer multiple of 4.*

What does any of this have to do with symmetric designs? Suppose H is a normalized Hadamard matrix of order $n = 4t \geq 8$. Delete its first row and column and replace the -1's in the resulting matrix with 0's. This produces a square $(0,1)$-matrix A, of order $v = 4t - 1$, with exactly $2t$ zeros in each row and column. Moreover, by the orthogonality of the rows of H,

$$AA^{\mathrm{t}} = tI_v + (t-1)J_v. \tag{6.28}$$

Thus (by Lemma 6.4.11), A is the incidence matrix of a symmetric balanced incomplete block design, the parameters of which are $v = 4t - 1$, $\lambda = t - 1$, and $k = t + \lambda = 2t - 1$.

Conversely, suppose A is a $v \times b$ incidence matrix for some BIBD $\mathscr{D}$ having parameters $(4t-1, 2t-1, t-1)$, where $t \geq 2$. Then, from Equation (6.25b),

$$\begin{aligned} b &= (t-1)\frac{(4t-1)(4t-2)}{(2t-1)(2t-2)} \\ &= 4t - 1 \\ &= v, \end{aligned}$$

so $\mathscr{D}$ is symmetric.

Let H be the matrix obtained from A by changing all of its zeros to -1's and adding a new first row and column consisting entirely of $+1$'s. Then H is a $4t \times 4t$ $(+1,-1)$-matrix, with exactly $2t$ ones in each row but the first. In particular, row 1 of H is orthogonal to each of rows 2 through $4t$.

Suppose i and m are fixed but arbitrary integers satisfying $1 < i < m \leq 4t$. Because $\mathscr{D}$ is symmetric, $b = k = 2t - 1$. Because $\mathscr{D}$ is a design, the $2t - 1$ ones in the $(i-1)$st row of A overlap the $2t - 1$ ones in its $(m-1)$st row in exactly $\lambda = t - 1$ places. Therefore, the $2t$ ones in row i of H overlap the $2t$ ones in row m of H in exactly t places. Because the remaining $2t$ entries in each of these rows of H all equal -1, it follows that the scalar product of rows i and m of H is 0. Because i and m were arbitrary, $HH^{\mathrm{t}} = 4tI_{4t}$, i.e., H is a Hadamard matrix of order $n = 4t$. Let's summarize.

6.4.18 Definition. Suppose $\mathscr{D}$ is a balanced incomplete block design with an incidence matrix that can be obtained from a normalized Hadamard matrix of order $n = 4t \geq 8$ by changing its -1's to 0's, and deleting its first row and column. Then $\mathscr{D}$ is a *Hadamard design* of order $4t - 1$.

6.4.19 Theorem. *A balanced incomplete block design is a Hadamard design if and only if its parameters are* $(4t-1, 2t-1, t-1)$ *for some* $t \geq 2$.

6.4.20 Example. When $t = 2$, the parameters from Theorem 6.4.19 are $(7, 3, 1)$. Evidently, the projective plane of order 2 affords a Hadamard design! Let's find the corresponding Hadamard matrix.

With respect to the model described in Example 6.3.15, with point set $V = \{1, 2, \ldots, 7\}$, the blocks are $B_1 = \{1, 2, 3\}$, $B_2 = \{1, 4, 7\}$, $B_3 = \{1, 5, 6\}$, $B_4 = \{2, 4, 6\}$, $B_5 = \{2, 5, 7\}$, $B_6 = \{3, 4, 5\}$, and $B_7 = \{3, 6, 7\}$. Therefore (check it), the incidence matrix is

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Thus (from the discussion leading up to Definition 6.4.18 and Theorem 6.4.19), the normalized Hadamard matrix yielding this design is (check it)

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \end{pmatrix}. \qquad \square$$

It has been conjectured that Hadamard matrices of order $4t$ exist for every integer $t \geq 1$. However, the fact that there are infinitely many Hadamard designs does not depend on the validity of this conjecture.

6.4.21 Theorem. *For any nonnegative integer k, there exists a Hadamard matrix of order 2^k.*

The proof is left to the exercises.

6.4. EXERCISES

1 Let $F_1, F_2, \cdots, F_6$ be the faces of a cube, and $B_1, B_2, \cdots, B_8$ its vertices, interpreted as three-element subsets of $V = \{F_1, F_2, \cdots, F_6\}$. Prove or disprove that $\mathscr{D} = \{B_1, B_2, \cdots, B_8\}$ is a BIBD.

2 Suppose P and Q are two (different) points of a (v, k, λ)-design.

(a) How many blocks of the design contain P or Q?

(b) How many blocks of the design contain P or Q but not both?

3 Prove that there is no BIBD with parameters

(a) $(9,4,2)$. **(b)** $(10,4,3)$. **(c)** $(22,7,2)$.

4 Prove that a BIBD whose parameters satisfy $\lambda = k(k-1)/(v-1)$ is necessarily symmetric.

5 If $\mathscr{D} = \{B_1, B_2, \ldots, B_b\}$ is a (v,k,λ)-design with point set V, its *complement* is $\mathscr{D}^c = \{V\backslash B_1, V\backslash B_2, \ldots, V\backslash B_b\}$.

(a) If $k < v-1$, prove that $\mathscr{D}^c$ is a BIBD.

(b) What are the parameters of $\mathscr{D}^c$?

(c) Describe how to obtain the incidence matrix for $\mathscr{D}^c$ from the incidence matrix for $\mathscr{D}$.

(d) Describe a $(7,4,2)$-design.

(e) Describe a $(9,6,5)$-design.

6 Prove that the dependent parameter $q \geq \lambda$ for any BIBD $\mathscr{D}$.

7 Let A be the incidence matrix of a (v,k,λ)-design $\mathscr{D}$.

(a) Show that $AA^t = (q-\lambda)I_v + \lambda J_v$.

(b) Show that $\det(AA^t) = qk(q-\lambda)^{v-1}$.

(c) Show that $\det(AA^t) > 0$.

(d) Prove that $b \geq v$.

(e) Prove that $k \leq q$.

8 Let A be the incidence matrix of a (v,k,λ)-design $\mathscr{D} = \{B_1, B_2, \ldots, B_b\}$.

(a) Show that $[A^tA]_{ij} = o(B_i \cap B_j)$.

(b) Show that A^tA need not equal $(k-\lambda)I_b + \lambda J_b$.

(c) Show that $A^tA = AA^t$ if and only if $\mathscr{D}$ is symmetric.

(d) Show that $\det(A^tA) \neq 0$ if and only if $\mathscr{D}$ is symmetric. (*Hint*: Exercise 7(d).)

(e) If $\mathscr{D}$ is symmetric, prove that A^t is the incidence matrix of a symmetric BIBD.*

(f) If $\mathscr{D}$ is symmetric, prove that any two blocks of $\mathscr{D}$ have exactly λ points in common.

9 Describe how you might construct a BIBD with parameters

(a) $(7,3,2)$. **(b)** $(9,3,2)$. **(c)** $(9,3,50)$.

10 A *Steiner sytem*† with parameters (t,k,v) is a set V with v elements called *points* and a family of distinct k-element subsets of V called *blocks*, with the

*The design $\mathscr{D}^d$, with incidence matrix A^t, is the *dual* of $\mathscr{D}$ in the sense that the points (blocks) of $\mathscr{D}^d$ correspond to the blocks (points) of $\mathscr{D}$.

†Named for Jakob Steiner, but previously studied by Thomas Kirkman [On a problem in combinations, *Cambridge & Dublin Math. J.* 2 (1847), 191–204], these objects are sometimes called *Steiner triple systems*.

$$X = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Figure 6.4.4

property that each t-element subset of V is contained in exactly one of the blocks.

(a) Exhibit a Steiner system with parameters $(2, 3, 7)$.

(b) Show that every finite projective plane in a Steiner system.

(c) Show that a Steiner system with parameters $(2, k, v)$ is a balanced incomplete block design.

(d) Let A be the incidence matrix for a Steiner system with parameters (t, k, v). Show that the columns of A comprise an (n, M, d) binary code where $n = v, M = C(v, t)/C(k, t)$, and $d > 2(k - t) + 1$.

11 From Exercise 28, Section 6.2, the extended Golay code $\mathscr{G}_{24}$ is a $(24, 4096, 8)$ linear code generated by the matrix $G = (I_{12}|X)$, where X is the symmetric 12×12 matrix in Fig. 6.4.4. Let A be the 11×11 matrix obtained from X by deleting its last row and column.

(a) Show that A is the incidence matrix for a symmetric $(11, 6, 3)$-design.

(b) Is the design in part (a) a Hadamard design? (Justify your answer.)

12 Prove the sufficiency part of Lemma 6.4.11.

13 Let J_n be the $n \times n$ matrix each of whose entries is 1. Then J_n is a rank 1 matrix whose only nonzero eigenvalue is equal to n.

(a) Use this observation to prove that the eigenvalues of $(k - \lambda)I_v + \lambda J_v$ are $k - \lambda$ with multiplicity $v - 1$, and $k + \lambda(v - 1)$ with multiplicity 1.

(b) Use part (a) to give an eigenvalue proof of Equation (6.27).

14 Let H be a Hadamard matrix of order n. Prove that

(a) $-H$ is a Hadamard matrix of order n.

(b) $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ is a Hadamard matrix of order $2n$.

15 Suppose H is a Hadamard matrix of order n. Prove that $|\det(H)| = n^{n/2}$.

16 Prove that the projective plane of order 3 does not afford a Hadamard design.

17 Explain why the symmetric design afforded by a projective plane of order n cannot be a Hadamard design for any $n > 2$.

18 If A_1 and A_2 are $m \times m$ matrices and B_1 and B_2 are $n \times n$ matrices, then the Kronecker product (described in Exercise 17, Section 6.3) satisfies $(A_1 \otimes B_1)(A_2 \otimes B_2) = (A_1A_2) \otimes (B_1B_2)$.

(a) Use this property to prove that the Kronecker product of two Hadamard matrices is a Hadamard matrix.

(b) Prove Theorem 6.4.21.

19 Describe how to construct a symmetric BIBD with parameters

(a) $(15, 7, 3)$. **(b)** $(31, 15, 7)$. **(c)** $(31, 16, 8)$.

20 Expanding on the Kronecker product technique of Exercise 18, J. Williamson proved the following: Let p be an odd prime. Suppose s is a positive integer such that $p^s - 1$ is a multiple of 4. If there is a Hadamard matrix of order $m > 1$, then there is a Hadamard matrix of order $m(p^s + 1)$. Use Williamson's theorem to prove the existence of a Hadamard matrix of order

(a) 12. **(b)** 24. **(c)** 28. **(d)** 52.

21 The normalized Hadamard matrices in Example 6.4.16 are all symmetric (i.e., $H^t = H$.)

(a) Find a nonsymmetric normalized Hadamard matrix of order 4.

(b) Prove that there exists a symmetric Hadamard matrix of order 2^k for every $k \geq 0$.

(c) Matrix A is said to be *skew symmetric* if $A^t = -A$. Prove that there are no skew-symmetric Hadamard matrices.

22 A Hadamard matrix H is said to be of *skew type*[*] if $H = I + S$, where S is skew symmetric, i.e., $S^t = -S$. Exhibit a skew-type Hadamard matrix

(a) of order 2? **(b)** of order 4?

23 Let $\mathscr{D}$ be a Hadamard design of order $4t - 1$. Let $\mathscr{C}$ be the binary code comprised of the rows of an incidence matrix for $\mathscr{D}$. Prove that $\mathscr{C}$ is a $(4t - 1, 4t - 1, 2t)$ code.

24 Confirm that $HH^t = 8I_8$ for the matrix H in Example 6.4.20.

[*]It is known that if there is a skew type Hadamard matrix of order n, then there exists a Hadamard matrix of order $n(n - 1)$; and if there is a skew type Hadamard matrix of order n and a symmetric Hadamard matrix of order $n + 4$, then there exists a Hadamard matrix of order $n(n + 3)$.

25 The complement of a binary word w is the word w^* obtained from w by changing all of its 0's to 1's and all of its 1's to 0's. For any binary code $\mathscr{C}$, define $\mathscr{C}^* = \{c^* : c \in \mathscr{C}\}$.

Suppose H is the Hadamard matrix constructed in Example 6.4.20. Let $\mathscr{C}$ be the (8,8,4) binary code obtained from the rows of H by replacing the -1's with 0's.

(a) Show that $\mathscr{C}^*$ is an (8,8,4) binary code.

(b) Show that $\mathscr{C} \cup \mathscr{C}^*$ is an (8,16,4) binary code.

26 Part 1 of the Bruck–Ryser–Chowla theorem (Theorem 6.4.12) gives a necessary condition for (v, k, λ) to be the triple of parameters for a symmetric BIBD when v is *even*. Part 2 gives a necessary condition when v is odd, namely, that there exist integers x, y, z, not all zero, such that

$$z^2 = (k - \lambda)x^2 + (-1)^{(v-1)/2}\lambda y^2.$$

(a) Show that the Bruck–Ryser–Chowla equation for a projective plane of order 10 is $y^2 + z^2 = 10x^2$.

(b) Find positive integers x,y, and z that solve the equation $y^2 + z^2 = 10x^2$.

(c) Show that the Bruck–Ryser–Chowla condition for the existence of a Hadamard matrix of order $4t \geq 8$ is that there is a solution in integers x,y,z, not all zero, of the equation $(t-1)y^2 + z^2 = tx^2$.

(d) Show that there exist positive integer solutions x,y,z of the equation $(t-1)y^2 + z^2 = tx^2, t \geq 2$.

27 Let H be a normalized Hadamard matrix of order n. Let K be the $(n-1)$-square submatrix of H obtained by deleting its first row and column, i.e.,

$$H = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & & & & \\ 1 & & K & & \\ \vdots & & & & \\ 1 & & & & \end{pmatrix}.$$

Let J_{n-1} be the $(n-1)$-square matrix each of whose entries is $+1$.

(a) Show that $K^{\mathrm{t}}K = KK^{\mathrm{t}} = nI_{n-1} - J_{n-1}$.

(b) Show that $K^{-1} = (1/n)(K^{\mathrm{t}} - J_{n-1})$.

(c) Prove Equation (6.28).

28 Prove or disprove that in every Hadamard matrix of order $n > 1$, half the entries are $+1$'s and half are -1's.

Appendix A1

Symmetric Polynomials

The purpose of this appendix is to prove two results from Section 1.9, beginning with the following.

1.9.14 Newton's Identities. For a fixed but arbitrary positive integer n, let $M_r = M_r(x_1, x_2, \ldots, x_n)$ and $E_r = E_r(x_1, x_2, \ldots, x_n)$. Then, for all $t \geq 1$,

$$M_t - M_{t-1}E_1 + M_{t-2}E_2 - \cdots + (-1)^{t-1}M_1E_{t-1} + (-1)^t tE_t = 0. \tag{A1}$$

If $t > n$, Equation (A1) has the simpler form

$$M_t - M_{t-1}E_1 + M_{t-2}E_2 - \cdots + (-1)^n M_{t-n}E_n = 0 \tag{A2}$$

(because, e.g., $E_t(x_1, x_2, \ldots, x_n) = 0$).

The mathematics behind the proof is relatively simple, involving the product rule for differentiation and the fact that if $p(x)$ is a polynomial of degree $n \geq 1$, and c is a constant, then there exists a unique polynomial $q(x)$ such that

$$p(x) = (x - c)q(x) + p(c). \tag{A3}$$

A1.1 Example. Suppose $p(x) = x^4 + x^3 - 6x^2 - 2x + 9$ and $c = -3$. Dividing $p(x)$ by $(x + 3)$ yields the *quotient* $q(x) = x^3 - 2x^2 - 2$, and the *remainder* $p(-3) = 15$. (Confirm that

$$x^4 + x^3 - 6x^2 - 2x + 9 = (x + 3)(x^3 - 2x^2 - 2) + 15.)$$

If $p(x) = x^4 + 3x^3 - 2x^2 - 4x + 6$ and $c = -3$, then $p(-3) = 0$. In this case, $(x + 3)$ is a factor of $p(x)$. The other factor is the quotient $q(x) = p(x)/(x + 3) = x^3 - 2x + 2$. (Confirm that $p(x) = (x + 3)(x^3 - 2x + 2)$.) □

Combinatorics, Second Edition, by Russell Merris.
ISBN 0-471-26296-X

Proof of Newton's Identities. As a polynomial identity, Equation (A1) can be proved by showing it to be valid for all possible substitutions for the variables. For fixed but arbitrary numbers $a_1, a_2, \ldots, a_n$, define $M_r = M_r(a_1, a_2, \ldots, a_n)$, $E_r = E_r(a_1, a_2, \ldots, a_n)$, and

$$\begin{aligned} p(x) &= (x - a_1)(x - a_2) \cdots (x - a_n) \\ &= x^n - E_1 x^{n-1} + E_2 x^{n-2} - \cdots + (-1)^n E_n. \end{aligned}$$

If c is a constant then, as in Equation (A3),

$$p(x) = (x - c)q(x) + p(c), \tag{A4}$$

where

$$p(c) = c^n - E_1 c^{n-1} + E_2 c^{n-2} - \cdots + (-1)^n E_n. \tag{A5}$$

Because $p(a_i) = 0$, substituting $c = a_i$ in Equation (A5) yields

$$0 = a_i^n - E_1 a_i^{n-1} + E_2 a_i^{n-2} - \cdots + (-1)^n E_n. \tag{A6}$$

Multiplying both sides of Equation (A6) by a_i^{t-n} and summing on i yields

$$0 = M_n - E_1 M_{n-1} + E_2 M_{n-2} - \cdots + (-1)^n n E_n$$

when $t = n$, and

$$0 = M_t - M_{t-1} E_1 + M_{t-2} E_2 - \cdots + (-1)^n M_{t-n} E_n$$

when $t > n$.

When $t < n$, things are a bit more complicated. Here, we need an explicit formula, not for $p(c)$, but for

$$\begin{aligned} q(x) = {} & x^{n-1} + (c - E_1)x^{n-2} + (c^2 - E_1 c + E_2)x^{n-3} + (c^3 - E_1 c^2 + E_2 c - E_3)x^{n-4} \\ & + \cdots + (c^{n-1} - E_1 c^{n-2} + \cdots + (-1)^{n-1} E_{n-1}). \end{aligned}$$

(Confirm that this is $q(x)$ in Equation (A4).)

Substituting $c = a_i$, not in Equation (A5), but in Equation (A4), we obtain, after canceling $(x - a_i)$ from both sides, that

$$\begin{aligned} & (x - a_1) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n) \\ & = x^{n-1} + (a_i - E_1)x^{n-2} + (a_i^2 - E_1 a_i + E_2)x^{n-3} \\ & \quad + (a_i^3 - E_1 a_i^2 + E_2 a_i - E_3)x^{n-4} + \cdots \\ & \quad + (a_i^{n-1} - E_1 a_i^{n-2} + \cdots + (-1)^{n-1} E_{n-1}). \end{aligned} \tag{A7}$$

Because $\sum_{i=1}^{n} a_i^r = M_r$, summing the right-hand side of Equation (A7) yields

$$\begin{aligned} &nx^{n-1} + (M_1 - nE_1)x^{n-2} + (M_2 - E_1M_1 + nE_2)x^{n-3} \\ &\quad + (M_3 - E_1M_2 + E_2M_1 - nE_3)x^{n-4} + \cdots \\ &\quad + (M_{n-1} - E_1M_{n-2} + \cdots + (-1)^{n-1}nE_{n-1}). \end{aligned} \tag{A8}$$

By the product rule from calculus, the sum on the left-hand side of Equation (A7) is the derivative

$$p'(x) = \sum_{i=1}^{n} (x - a_i) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n).$$

Another way to express the derivative of $p(x)$ is

$$\begin{aligned} &nx^{n-1} - (n-1)E_1x^{n-2} + (n-2)E_2x^{n-3} \\ &\quad - (n-3)E_3x^{n-4} + \cdots + (-1)^{n-1}E_{n-1}. \end{aligned} \tag{A9}$$

Comparing the coefficient of x^k in Expressions (A8) and (A9), $0 \le k \le n-1$, yields

$$\begin{aligned} -(n-1)E_1 &= M_1 - nE_1, && \text{or} \quad 0 = M_1 - E_1, \\ (n-2)E_2 &= M_2 - E_1M_1 + nE_2, && \text{or} \quad 0 = M_2 - E_1M_1 + 2E_2, \\ -(n-3)E_3 &= M_3 - E_1M_2 + E_2M_1 - nE_3, && \text{or} \quad 0 = M_3 - E_1M_2 + E_2M_1 - 3E_3, \end{aligned}$$

and so on until, finally,

$$0 = M_{n-1} - E_1M_{n-2} + \cdots + (-1)^{n-2}E_{n-2}M_1 + (-1)^{n-1}(n-1)E_{n-1},$$

precisely Newton's identities when $t < n$. ■

We now come to the second objective of this appendix, a proof of the following result from Section 1.9.

1.9.11 Theorem. *Any polynomial, symmetric in the variables $x_1, x_2, \ldots, x_n$ is a polynomial in the power sums*

$$M_t = M_t(x_1, x_2, \ldots, x_n), \qquad 1 \le t \le n.$$

Two proofs will be given. The first is a brute-force inductive proof. The second, while a little longer and subtler, is also more illuminating. Before giving either, we observe that Theorem 1.9.11 is equivalent to a classical result from nineteenth-century invariant theory.

A1.2 Fundamental Theorem of Symmetric Polynomials. *Any polynomial, symmetric in the variables $x_1, x_2, \ldots, x_n$, is a polynomial in the elementary symmetric functions $E_t = E_t(x_1, x_2, \ldots, x_n), 1 \leq t \leq n$.*

From Newton's identities,

$$M_t - M_{t-1}E_1 + M_{t-2}E_2 - \cdots + (-1)^{t-1}M_1E_{t-1} + (-1)^t tE_t = 0,$$

where $M_0 = E_0 = 1$. Solving recursively for the power sums, we obtain

$$\begin{aligned}
M_1 &= E_1, \\
M_2 &= E_1^2 - 2E_2, \\
M_3 &= E_1^3 - 3E_1E_2 + 3E_3, \\
M_4 &= E_1^4 - 4E_1^2E_2 + 4E_1E_3 + 2E_2^2 - 4E_4,
\end{aligned}$$

and so on. For each $t \geq 1$, M_t is a polynomial in $E_s, 1 \leq s \leq t$. Therefore, the fundamental theorem is a consequence of Theorem 1.9.11. To prove the converse, Newton's identities are solved recursively for the elementary symmetric functions:

$$\begin{aligned}
E_1 &= M_1, \\
E_2 &= \tfrac{1}{2}[M_1^2 - M_2], \\
E_3 &= \tfrac{1}{6}[M_1^3 - 3M_1M_2 + 2M_3], \\
E_4 &= \tfrac{1}{24}[M_1^4 - 6M_1^2M_2 + 8M_1M_3 + 3M_2^2 - 6M_4],
\end{aligned}$$

and so on. For each $t \geq 1$, E_t is a polynomial in $M_s, 1 \leq s \leq t$. Therefore, Theorem 1.9.11 is a consequence of the fundamental theorem.

Our first proof of Theorem 1.9.11 is achieved by proving the fundamental theorem. In order to do that, we need to introduce a natural ordering on the set of partitions of m.

A1.3 Definition. Suppose $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_\ell]$ and $\beta = [\beta_1, \beta_2, \ldots, \beta_s]$ are two partitions of m. Then α comes after β in *dictionary order*, written $\alpha > \beta$, if $\alpha_1 > \beta_1$, or if $\alpha_i = \beta_i, 1 \leq i < j$, and $\alpha_j > \beta_j$, for some positive integer $j \leq \ell$.

For example, $[6, 1^2] > [5, 3] > [5, 2, 1] > [4^2]$. A little less formally, $\alpha > \beta$ if α has the larger part in the first place where the partitions differ. If $\alpha, \beta \vdash m$, then $\alpha \geq \beta$ means $\alpha = \beta$ or $\alpha > \beta$.

Proof of the Fundamental Theorem of Symmetric Polynomials. Let $f = f(x_1, x_2, \ldots, x_n)$ be a symmetric polynomial. Write $f = f_0 + f_1 + \cdots + f_k$, where $f_i = f_i(x_1, x_2, \ldots, x_n)$ is the *homogeneous* part of f consisting of all terms of (total)

degree i. In particular, we are assuming that f, itself, is of degree k. Consider one of the monomial terms of f_k, say

$$cx_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}, \tag{A10}$$

where $r_1 + r_2 + \cdots + r_n = k$. Because f_k is symmetric, we may assume that $r_1 \geq r_2 \geq \cdots \geq r_\ell \geq 1 > r_{\ell+1} = \cdots = r_n = 0$. Let $\alpha = [r_1, r_2, \ldots, r_\ell] \vdash k$.

Among all partitions of k that occur as the sequence of exponents of some monomial term of f_k, suppose α is the largest (coming last) in dictionary order, meaning that r_1 is the largest exponent to occur in any monomial term of f_k; among all monomial terms of f_k that have r_1 as an exponent, r_2 is the maximum second largest exponent, and so on.

Consider the product

$$E_1^{s_1}E_2^{s_2}\cdots E_n^{s_n}, \tag{A11}$$

where $s_1 \geq s_2 \geq \cdots \geq s_n$. In dictionary order of the exponents, the last monomial term in Expression (A11) is

$$x_1^{s_1}(x_1x_2)^{s_2}\cdots(x_1x_2\cdots x_n)^{s_n}.$$

In order for this last term to equal $x_1^{r_1}x_2^{r_2}\cdots x_n^{r_n}$, we need

$$\begin{aligned} r_1 &= s_1 + s_2 + s_3 + \cdots + s_n, \\ r_2 &= \quad + s_2 + s_3 + \cdots + s_n, \\ r_3 &= \qquad\quad s_3 + \cdots + s_n, \end{aligned}$$

and so on, with $r_\ell = s_\ell + \cdots + s_n$. These equations are satisfied when $s_{\ell+1} = \cdots = s_n = 0$,

$$\begin{aligned} s_\ell &= r_\ell, \\ s_{\ell-1} &= r_{\ell-1} - r_\ell, \\ s_{\ell-2} &= r_{\ell-2} - r_{\ell-1}, \end{aligned}$$

and so on, finally setting $s_1 = r_1 - r_2$.

With these choices for $s_1, s_2, \ldots, s_n$, $f_k - cE_1^{s_1}E_2^{s_2}\cdots E_n^{s_n}$ is either zero, or a homogeneous symmetric polynomial of degree k, in which every partition occurring among the exponents of its monomial terms is less than α (in dictionary order). Because dictionary order is a total order and $p(k)$, the number of partitions of k, is finite, it follows by induction that the difference $f_k - cE_1^{s_1}E_2^{s_2}\cdots E_n^{s_n}$ is a polynomial in the elementary symmetric functions. Hence, f_k is a polynomial in the elementary symmetric functions and, by induction on k, so is f. ■

For the purposes of the second proof, it will be useful to modify our usual notation, replacing M_t with P_t. So, for the remainder of this appendix (only), $P_t = M_t(x_1, x_2, \ldots, x_n) = x_1^t + x_2^t + \cdots + x_n^t$. If $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_\ell] \vdash k$, define

$$P_\alpha = P_{\alpha_1} P_{\alpha_2} \cdots P_{\alpha_\ell}. \tag{A12}$$

Then, e.g., $P_{[3,1^2]} = P_3 P_1 P_1$. If $n = 3$, then

$$P_{[3,1^2]} = (x^3 + y^3 + z^3)(x + y + z)^2.$$

A product of symmetric polynomials, $P_\alpha = P_\alpha(x_1, x_2, \ldots, x_n)$ is a symmetric polynomial in the variables $x_1, x_2, \ldots, x_n$.

Before getting to the second proof, we need to introduce another ordering of the partitions of m.

A1.4 Definition. Suppose $\alpha = [\alpha_1, \alpha_2, \ldots, \alpha_\ell]$ and $\beta = [\beta_1, \beta_2, \ldots, \beta_s]$ are two partitions of m. Then α *majorizes* β, written $\alpha \succ \beta$, if $\ell \leq s$, and

$$\sum_{i=1}^{j} \alpha_i \geq \sum_{i=1}^{j} \beta_i, \qquad 1 \leq j \leq \ell.$$

If, e.g., $\alpha = [5, 3] \vdash 8$ and $\beta = [3^2, 2] \vdash 8$ then $\alpha \succ \beta$ because $5 \geq 3$ and $5 + 3 \geq 3 + 3$. On the other hand, neither $\alpha = [5, 3]$ nor $\beta = [6, 1^2]$ majorizes the other. Unlike dictionary order, in which every pair of partitions of m is comparable, majorization is a *partial order.*

A1.5 Lemma. *Suppose* $\alpha, \beta \vdash m$. *If* $\alpha \succ \beta$, *then* $\alpha \geq \beta$.

Proof. If $\alpha \succ \beta$ and $\alpha \neq \beta$, then α must be larger in the first part where they differ. ■

Direct Proof of Theorem 1.9.11. If $\beta \vdash m$ then, from Theorem 1.8.15, $P_\beta = P_\beta(x_1, x_2, \ldots, x_n)$ is a linear combination of minimal symmetric polynomials. In other words, there exist constants $c_{\alpha\beta}, \alpha \vdash m$, such that

$$P_\beta = \sum_{\alpha \vdash m} c_{\alpha\beta} M_\alpha, \tag{A13}$$

where $M_\alpha = M_\alpha(x_1, x_2, \ldots, x_n)$ is the minimal symmetric polynomial corresponding to α. (Together with Equation (A12), this explains why it was necessary to replace M_t with P_t.)

A1.6 Lemma. *In Equation* (A13)*, the constants* $c_{\alpha\beta}$ *satisfy*

(i) $c_{\alpha\alpha} \neq 0,\ \alpha \vdash m$; and
(ii) $c_{\alpha\beta} = 0$ unless $\alpha \succ \beta$.

Lemma A1.6 all but finishes the second proof of Theorem 1.9.11. To see why, consider the $p(m) \times p(m)$ *transition matrix* $C = (c_{\alpha\beta})$ whose rows and columns are indexed by the partitions of m arranged in dictionary order. It follows from Lemmas A1.5 and A1.6 that C is a lower triangular matrix, none of whose diagonal entries is zero. In particular, C is invertible. Therefore, the minimal symmetric polynomials $M_\alpha, \alpha \vdash m$, are linear combinations of the power sum products $P_\beta, \beta \vdash m$, i.e., M_α is a polynomial in the power sums $P_t, t \geq 1$.

In view of Theorem 1.8.15, this leaves us with the technical detail of showing, for a fixed but arbitrary $\beta \vdash m > n$, that $P_\beta(x_1, x_2, \ldots, x_n)$ is a polynomial in $P_t(x_1, x_2, \ldots, x_n),\ t \leq n$. This we prove by induction on $j = m - n$.

By Equation (A2), for any $m > n$,

$$P_m = P_{m-1}E_1 - P_{m-2}E_2 + \cdots - (-1)^n P_{m-n}E_n. \tag{A14}$$

Earlier in this appendix we used Newton's identities to show, for each $i \geq 1$, that E_i is a polynomial in $P_t,\ 1 \leq t \leq n$. Setting $m = n + 1$ in Equation (A14) establishes the basis $(j = 1)$ step of the induction. Setting $m = n + j$ finishes it.

Proof of Lemma A1.6. Suppose $\alpha, \beta \vdash m$. If the monomial $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_r^{\alpha_r}$ appears in

$$P_\beta = (x_1^{\beta_1} + x_2^{\beta_1} + \cdots + x_n^{\beta_1})(x_1^{\beta_2} + x_2^{\beta_2} + \cdots + x_n^{\beta_2})\cdots(x_1^{\beta_s} + x_2^{\beta_s} + \cdots + x_n^{\beta_s}),$$

then $\{\beta_1, \beta_2, \ldots, \beta_s\}$ can be expressed as the disjoint union $B_1 \cup B_2 \cup \cdots \cup B_l$ in such a way that α_i is the sum of the elements of $B_i,\ 1 \leq i \leq l$. Since $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_l$, and since β_1 belongs to some B_i, it must be that $\alpha_1 \geq \beta_1$. Because $\{\beta_1, \beta_2\}$ belongs to the union of some pair of the B's, $\alpha_1 + \alpha_2 \geq \beta_1 + \beta_2$, and so on. In other words, $\alpha \succ \beta$, establishing part (ii). Since $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_r^{\alpha_r}$ appears in P_α, part (i) is immediate. ■

Appendix A2

Sorting Algorithms

> There are two ways of constructing a software design; one way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies.
>
> — C. A. R. Hoare

The purpose of this appendix is to address the "sorting problem" raised in Section 1.10, i.e., to develop and discuss alogrithms to sort sets of numbers into numerical order and sets of words into dictionary order.

Suppose you had a well shuffled *deck* of 3×5 cards, each with a single number on it. Suppose you had the job of designing an algorithm to sort the cards into non-decreasing numerical order. The best way to begin is probably to try to articulate how you would do the chore yourself, and then consider alternative approaches that might yeild a better *step-by-step* pocess. One possibility is to scan the cards for a smallest number, move it up to the front (top) of the deck, scan the remaining cards for a smallest number, move it up to the second place, and so on. Another possibility is to start a new deck with some arbitrary card, choose another card from those that remain in the old deck and insert it in the new deck at an appropriate place, pick a third card from the old deck and insert it in its proper place in the new deck, etc. Might one of these approaches yield a *better* algorithm than the other? One way to find out would be to try them, say, on a set consisting of 1000 numbers.

This raises the tedious prospect of having to enter 1000 numbers into a computer. There is an alternative. Assuming the keyword RND returns a pseudo-random number from the interval (0,1), a subroutine to generate N pseudorandom integers from the interval $[0, 999]$ follows:

```
1. Input N.
2. For I = 1 to N.
3. R(I) = ⌊1000 × RND⌋.
4. Next I.
```

If a program implementing this subroutine were run several times, with the same N, many deskop computers would return the *same* N integers, in the *same* order!

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

That can be useful, e.g., when comparing different sorting algorithms. On the other hand, whenver it seems desirable, this default setting can be overridden by inserting (just once, at the beginning) a *Randomize* command.

Given N numbers to sort, let's try to implement the first approach and *scan* them for the smallest number. How, exactly, might that be done? One way is to let $X = R(1)$, then compare X with $R(2)$. If $R(2)$ is smaller than $R(1)$, change the value of X to $R(2)$. Otherwise keep its value equal to $R(1)$. Then compare X with $R(3)$, and so on. Eventually, after $N - 1$ comparisons, a smallest number is identified. Shifting the other numbers to make room for X at the front (top) of the deck requires knowledge, not only of the value of the smallest number, but also of its location in the deck. That's asking too much from a single memory location. We need one location, X, to keep track of the value of the number and another, J, to keep track of its location.

Imagine, in the middle of this process, having (re)arranged things so that, of the original N numbers, the smallest C are $R(1) \leq R(2) \leq \cdots \leq R(C)$. The next step would be to scan for the smallest of the remaining numbers. This process might start like this:

```
 5. C = C + 1.
 6. J = C.
 7. X = R(C).
```

If (the new) $C = N$, the task is complete, and it would be time to proceed to the check-out line:

```
 8. If C = N then go to step 20.

20. For I = 1 to N.
21. Write R(I).
22. Next I.
```

Otherwise, start scanning:

```
 9. For I = C + 1 to N.
10. If X ≤ R(I) then go to step 13.
11. J = I.
12. X = R(J).
13. Next I.
```

At the completion of the loop in steps 9–13, the next smallest number will have been located in position J. If J is still (the new) C, it is already in its proper palce and we can return to step 5:

```
14. If J = C then go to step 5.
```

Otherwise, we need to reorganize the list:

```
15. For I = J to C + 1.
16. R(I) = R(I - 1).
17. Next I.
```

```
18. R(C) = X.
19. Go to step 5.
```

Note, in step 15, that the value of I starts at J and works its way *backward* to $C + 1$.

There is a way to have the computer time itself as it sorts. Leaving out the time it takes to generate the numbers to be sorted, this timekeeping chore can be accomplished, symbolically, by adding the steps

```
4.1. Start = Time.
 23. Write Time – Start.
```

Finally, one might like to see the original list of unsorted numbers. This can be accomplished by adding step

```
3.1.  Write R(I).
```

Assembling these steps, in the proper order (and initializing C), we obtain the following:

A2.1 (Smallest First) Sorting Algorithm

```
  1. Input N and set C = 0.
  2. For I = 1 to N.
  3. R(I) = ⌊1000 × RND⌋.
3.1. Write R(I).
  4. Next I.
4.1. Start-Time.
  5. C = C + 1.
  6. J = C.
  7. X = R(C).
  8. If C = N then go to step 20.
  9. For I = C + 1 to N.
 10. If X ≤ R(I) then go to step 13.
 11. J = I.
 12. X = R(J).
 13. Next I.
 14. If J = C then go to step 5.
 15. For I = J to C + 1.
 16. R(I) = R(I – 1).
 17. Next I.
 18. R(C) = X.
 19. Go to step 5.
 20. For I = 1 to N.
 21. write R(I).
 22. Next I.
 23. Write Time – Start.
```

□

The other possibility we had in mind was to fashion a new deck, a card at a time, by insertion. If $A(1) \le A(2) \le \cdots \le A(C)$ are the numbers $R(1), R(2), \ldots, R(C)$

(re)arranged into nondecreasing order, then $R(C+1)$ can be inserted into its proper place among the A's using the following subroutine:

A2.2 Algorithm

```
 1. For J = 1 to C.
 2. If R(C+1) < A(J) then go to step 6.
 3. Next J.
 4. A(C+1) = R(C+1).
 5. Go to step 10.
 6. For I = C to J.
 7. A(I+1) = A(I).
 8. Next I.
 9. A(J) = R(C+1).
10. Return.
```
□

Embedding this subroutine into a For . . . Next loop yields the following alternative to Algorithm A2.1:

A2.3 (Insertion) Sorting Algorithm

```
  1. Input N.
  2. For I = 1 to N.
  3. R(I) = ⌊1000 × RND⌋.
3.1. Write R(I).
  4. Next I.
4.1. Start = Time.
  5. A(1) = R(1).
  6. For C = 1 to N − 1.
  7. Call Algorithm A2.2.
  8. Next C.
  9. For I = 1 to N.
 10. Write A(I).
 11. Next I.
 12. Write Time − Start.
```
□

A2.4 Example. How does *insertion sorting* compare with *smallest first* sorting? To some extent, what will depend on programming language and machine architecture. Experiments on a Pentium-based PC show that where, on average, Algorithm A2.1 requires 10 *units* of time to sort 1000 numbers, Algorithm A2.3 needs only 8 units.

Given that *insertion* needs 8 (standardized) units of time to sort 1000 numbers, how long would you expect it to take to sort 5000 numbers? Experiments with the same PC show that it takes, not 40, but 196 units. It takes, not 5, but nearly 25 times as long! And, it is easy to see why.

In discovering that $R(C+1) < A(J)$, the subroutine at the heart of Algorithm A2.3 needed to make J comparisons. Inserting $R(C+1)$ at the Jth place in the

sequence of A's required $C - J$ shifts, for a total of C *operations*. As C ranges from 1 to $N - 1$, the total number of operations is

$$1 + 2 + \cdots + (N - 1) = \tfrac{1}{2}N(N - 1).$$

Thus, the number of operations this algorithm uses to sort n numbers is on the order of n^2. Algorithm A2.3 is $O(n^2)$. □

A2.5 Definition. Suppose f and g are real-valued functions defined on the set of positive integers. Then $f(n)$ is $O(g(n))$ if there exists a positive real number c and a nonnegative integer m such that $|f(n)| \leq cg(n)$ for all $n \geq m$.

This *Big Oh* notation should not be confused with $o(S)$, which, in this book, denotes the cardinality of the set S.*

Assuming, for the sake of argument, that Example A2.4 is a convincing demonstration that *insertion* is faster than *smallest first* sorting when $N = 1000$, might some third alternative be even faster? With a little fine-tuning, *insertion* itself can be speeded up considerably.

Let's return to the point where $R(C + 1)$ is being inserted into the ordered list of A's. In the worst case it will have to be compared with C numbers, namely, $A(1), A(2), \ldots, A(C)$, before the correct insertion point is found. The same worst-case estimate applies if, instead of starting at $A(1)$ and working up, we first compare $R(C + 1)$ with $A(C)$, then with $A(C - 1)$, and so on, working down to $A(1)$. But, if the first comparison is with a *middle* A, we could determine, in a single stroke, to which *half* of the list of A's the new entry belongs. If the number of possible insertion points can be cut in half by each comparison, the worst case would go from C to $\log_2(C)$ comparisons.†

Using S for *start*, F for *finish*, M for *middle*, and T for *temporary*, here is a subroutine to find the correct insertion point for $R(C + 1)$:

1. $S = 1$ and $F = C$.
2. $T = F - S$.
3. [If T is too small, do something else.]
4. $M = \lfloor T/2 \rfloor$.
5. If $R(C+1) < A(S+M)$ then $F = S+M$.
6. If $R(C+1) \geq A(S+M)$ then $S = S+M$.
7. Go to step 2.

A complete algorithm based on this subroutine might look something like the following:

A2.6 (Fast Insertion) Sorting Algorithm

1. Input N.

*Elsewhere, *little oh* may be used in other ways.
†If $C = 1000$, then $\log_2(C) < 10$.

```
  2. For I = 1 to N.
  3. R(I) = ⌊1000 × RND⌋.
3.1. Write R(I).
  4. Next I
4.1. Start = Time.
  5. A(1) = R(1).
  6. If R(2) > R(1) then A(2) = R(2).
  7. If R(2) ≤ R(1) then A(1) = R(2) and A(2) = R(1).
  8. C = 2.
  9. If C = N then stop.
 10. S = 1 and F = C.
 11. T = F − S.
 12. If T < 4 then go to step 17.
 13. M = ⌊T/2⌋.
 14. If R(C + 1) < A(S + M) then F = S + M.
 15. If R(C + 1) ≥ A(S + M) then S = S + M.
 16. Go to step 11.
 17. For I = S to F.
 18. J = I.
 19. If R(C + 1) < A(I) then go to step 25.
 20. Next I.
 21. J = F.
 22. If F < C then go to step 25.
 23. A(C + 1) = R(C + 1).
 24. Go to step 29.
 25. For I = C to J.
 26. A(I + 1) = A(I).
 27. Next I.
 28. A(J) = R(C + 1).
 29. C = C + 1.
 30. Go to step 9.
 31. For I = 1 to N.
 32. Write A(I).
 33. Next I.
 34. Write Time − Start.                                    □
```

A2.7 Example. Nearly three times as long as *insertion* (Algorithm A2.3), *fast insertion* looks like something invented by a government bureaucrat! Nevertheless, in the language of Example A2.4, where *smallest first* requires, on average, 10 standardized units of time to sort 1000 numbers, and *insertion* takes 8 units, *fast insertion* does the job in 4 units. In the more demanding test of sorting 5000 numbers, *smallest first* needs 243 units, *insertion* 196 units, and fast *insertion* 92. □

Now that we know something about sorting numbers, what about sorting sets of words into dictionary order? Conceptually, all that's needed is a function f, from the

set of words to the positive integers, with the property that W_1 comes (strictly) before W_2 in dictionary order if and only if $f(W_1) < f(W_2)$. Given such a function, it is easy to outline a sorting algorithm:

1. Input the words.
2. Use f to assign a number to each word.
3. Sort the numbers.
4. Apply f^{-1} to the sorted numbers.
5. List the resulting words.

One way to define such a function begins by assigning the numbers 1–26 to the letters *A–Z*, respectively, and then extending the definition to arbitrary words by defining

$$f(W) = \sum_{i=1}^{m} f(L_i) \times 27^{m-i}, \tag{A15}$$

where $L_1, L_2, \ldots, L_m$ are the letters in $W = L_1 L_2 \cdots L_m$.*

It is not difficult to see that f is a one-to-one function and that $f(W_1) < f(W_2)$ if and only if W_1 comes before W_2 in dictionary order, *provided* W_1 and W_2 contain precisely the same number of letters. For words of different length, things can go wrong, e.g., *ABC* comes before *D* in dictionary order, but

$$\begin{aligned} f(ABC) &= 1 \times 27^2 + 2 \times 27 + 3 \\ &= 786 \\ &> 4 \\ &= f(D). \end{aligned}$$

This difficulty can be circumvented by the introduction of an artificial letter, say @, defining $f(@) = 0$, and appending enough copies of @ to the end of the shorter word so that it becomes so long as the longer word, e.g.,

$$\begin{aligned} f(D@@) &= 4 \times 27^2 + 0 \times 27 + 0 \\ &= 2916 \\ &> 786 \\ &= f(ABC). \end{aligned}$$

To invert f, suppose $N = f(W)$. Dividing N by 27 yields a quotient Q_1 and a remainder $R_1 = N - 27Q_1$. Because quotients and remainders are unique, it follows

*This approach is equivalent to viewing words as base 27 numerals.

from Equation (A15) that $R_1 = f(L_m)$. Dividing Q_1 by 27 produces a new quotient Q_2 and a new remainder $R_2 = f(L_{m-1})$, and so on. The numerical values of the letters comprising W are (reading from right to left) the remainders obtained when successive quotients are divided by 27. This reduces the problem of inverting f to finding $f^{-1}(N), 0 \leq N \leq 26$.

A2.8 (Successive Division by 27) Algorithm

1. $T = N$ and $I = 0$.
2. $I = I + 1$ and $Q = \lfloor T/27 \rfloor$.
3. $R = T - 27Q$.
4. $K_I = f^{-1}(R)$.
5. If $Q = 0$ then go to step 8.
6. $T = Q$.
7. Go to step 2.
8. $W = K_I \cdots K_2 K_1$.

A2.9 Example. Zircon is a mineral whose appearance can vary from colorless to brown. When heated, cut, and polished, zircon yields a brilliant blue-white gemstone. According to our scheme for assigning numbers to words, the numercial value of ZIRCON is

$$\begin{aligned} f(\text{ZIRCON}) &= 26 \times 27^5 + 9 \times 27^4 + 18 \times 27^3 + 3 \times 27^2 + 15 \times 27 + 14 \\ &= 378211451. \end{aligned}$$

when the successive-division-by-27 algorithm was executed on a (Pentium-based) desktop PC, it produced $f^{-1}(f(\text{ZIRCON})) = \text{ZIRCOS}$. Because ZIRCON $\neq$ ZIRCOS, there is obviously an error somewhere.

Unfortunately, ''obviously an error'' is not the same as ''an obvious error.'' In this case, however, the source of the error is well known. It is due to *round-off*. Employing only its default accuracy, this computer confused $f(\text{ZIRCOS}) = 378211456$ with $f(\text{ZIRCON}) = 378211451$. □

In principle, an algorithm to sort an arbitrary set of words into dictionary order is new at hand:

1. Input the number, N, of words to be ordered.
2. Input the maximum word-length, M.
3. Input N words.
4. Attach @'s to the ends of words as needed.
5. To each word W, assign the number $f(W)$.
6. Sort the $f(W)$'s.
7. Apply f^{-1} to the sorted numbers.
8. List the resulting words (suppressing the @'s).

In view of Example A2.9, successfully implementing this algorithm as a computer program may not be straightforward. There is however a relatively

easy procedure that not so much solves as postpones the round-off error problem. *Double precision* is a phrase associated with extending the number of numerical digits carried by a computer. Using nothing more complicated than double precision arithmetic, our main algorithm returned accurate results on a desktop PC for all $M \leq 11$, enough to accomodate words as long as MISSISSIPPI. For lists containing longer words, other programming techniques are required.

EXERCISES A2

1. An algorithm is $O(1)$ if its running time is independent of the size of the input. Design an algorithm to sum the first n positive integers

(a) that is $O(n^2)$.

(b) that is $O(1)$.

2. Let a_i be a real number, $0 \leq i \leq r$. If $a_r \neq 0$, show that $f(n) = a_r n^r + a_{r-1} n^{r-1} + \cdots + a_0$ is $O(n^r)$.

3. Show that

(a) *smallest first* sorting (Algorithm A2.1) is $O(n^2)$.

(b) any $O(n)$ algorithm is $O(n^2)$.

4. Suppose $f(n)$ and $g(n)$ are $O(h(n))$. Show that

(a) $f(n) + g(n)$ is $O(h(n))$.

(b) $f(n)g(n)$ is $O(h(n)^2)$.

5. For a variety of reasons, it is not uncommon to be given the task of *merging* two (or more) sorted lists. Write an algorithm to merge the following two lists into a single list (sorted in nondecreasing order):

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

6. All three sorting algorithms in this appendix use a subroutine to generate N pseudorandom integers from the interval [0,999]. Here is a modification to generate 1000 pseudorandom integers from the interval [0,99]:

```
1. For I = 1 to 1000.
2. R(I) = ⌊100 × RND⌋.
3. Next I.
```

To the extent that RND simulates a random-number generator, each integer in [0,99] ought to occur with equal likelihood. If, e.g., the subroutine were run several times we would expect, on average, the number 99 to occur 10 times. Modify one of the sorting algorithms in the text (or write your own) so that it generates and sorts 1000 pseudorandom integers between 0 and 99 (inclusive).

(a) Run your (modified) program 10 times (using 10 different randomizing "seeds") and record the number of times 99 occurs in each run.

(b) Explain why it is helpful, in doing part (a), to sort the thousand integers before counting the occurrences of 99.

7. Write an algorithm to input N, generates N pseudorandom birthdates (month and day, but not year; exclude February 29), and output the data sorted in increasing order of dates.

8. Modify Exercise 7 so that, e.g., if "MAR 22" were to occur three times, instead of "MAR 22 MAR 22 MAR 22", the output for that date would be something like "MAR 22 (3)".

9. Another idea for sorting n numbers might be called *switch* sorting. Successively compare $R(J)$ with $R(J+1)$. If $R(J) > R(J+1)$, switch them. Otherwise leave them alone. Repeat this process as many times as necessary to sort the numbers.

(a) Write an algorithm to implement *switch* sorting.

(b) Show that *switch* sorting is (also!) $O(n^2)$.

(c) Run your program from part (a) with $n = 1000$ and compare the sorting time with *fast insertion*.

10. Restricting its domain to the set of words that can be assembled using (only) the 26 uppercase letters of the English alphabet, prove that the function defined by Equation (A15) is one-to-one.

Appendix A3

Matrix Theory

Readers of this book are presumed to have been exposed to that part of elementary linear algebra commonly found among the lower division requirement for majors in the mathematical and computer sciences. The purpose of this appendix is to provide an informal reminder of these already familiar topics, to specify certain conventions of language, and to touch on one or two nonstandard topics that may be mentioned in the text but are not essential to understanding it.

If $v = (a_1, a_2, \ldots, a_n)$, its *transpose*, v^{t}, is the $n \times 1$ column vector whose ith entry is $a_i \in K, 1 \leq i \leq n$, where K is the field of scalars. While the following discussion focuses primarily on the field $K = \mathbb{R}$, of real numbers, the techniques extend to, or have analogs for, other fields. The applications in Chapter 6, e.g., involve the scalar field $F = \{0, 1\}$, where arithmetic is *Boolean*.

The homogeneous system of linear equations

$$\begin{aligned} x_1 + 2x_2 + 3x_4 + 3x_5 &= 0 \\ x_1 + 2x_2 + x_3 + 7x_4 + 4x_5 &= 0 \\ 2x_1 + 4x_2 + 6x_4 + 5x_5 &= 0 \end{aligned} \tag{A16}$$

is equivalent to the single matrix equation $Ax = 0$, where 0 is the 3×1 zero matrix, x is the 5×1 matrix with x_i in its ith row, and the coefficient matrix is

$$A = \begin{pmatrix} 1 & 2 & 0 & 3 & 3 \\ 1 & 2 & 1 & 7 & 4 \\ 2 & 4 & 0 & 6 & 5 \end{pmatrix}. \tag{A17}$$

The Gauss–Jordan elimination method for solving such systems employs elementary row operations to transform. A to *Hermite normal form* (also called *reduced row echelon form*). For the matrix A in Equation (A17), subtracting row 1 from row 2, and twice row 1 from row 3 yields the *row equivalent* matrix

$$B = \begin{pmatrix} 1 & 2 & 0 & 3 & 3 \\ 0 & 0 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

Adding row 3 of B to row 2, three times row 3 to row 1, and then multiplying row 3 by -1, produces the Hermite normal form

$$C = \begin{pmatrix} 1 & 2 & 0 & 3 & 0 \\ 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

in which the *pivot* entries (the leading 1's in each row of C) are the only nonzero entries in their respective columns.

One virtue of elementary row operations is that they leave the solution set unchanged, i.e., $Ax = 0$, $Bx = 0$, and $Cx = 0$ all have the same solution set. In particular, x solves Equations (A16) if an only if

$$\begin{aligned} x_1 + 2x_2 + 3x_4 &= 0 \\ x_3 + 4x_4 &= 0 \\ x_5 &= 0, \end{aligned}$$

if and only if

$$\begin{aligned} x_1 &= -2x_2 - 3x_4 \\ x_3 &= -4x_4 \\ x_5 &= 0, \end{aligned} \tag{A18}$$

where the *pivot variables* are expressed as linear functions of the nonpivot variables. In other words, the *pivot columns* in the Hermite normal form correspond to dependent variables and the nonpivot columns to independent variables. In vector language, $v = (x_1, x_2, \ldots, x_5)$ solves Equations (A18) if and only if

$$\begin{aligned} (x_1, x_2, \ldots, x_5) &= (-2x_2 - 3x_4,\ x_2,\ -4x_4,\ x_4,\ 0) \\ &= x_2(-2, 1, 0, 0, 0) + x_4(-3, 0, -4, 1, 0), \end{aligned}$$

i.e., the solution set of Equations (A16) is the *vector space* $\mathscr{L}(E)$ consisting of all *linear combinations* of the *basis* $E = \{(-2, 1, 0, 0, 0), (-3, 0, -4, 1, 0)\}$. This solution set is also known as the *kernel* of A, denoted $\ker(A)$. The *nullity* of A is the *dimension* of its kernel. In this case, $\text{nullity}(A) = 2$.

Recall that $E = \{v_1, v_2, \ldots, v_n\}$ is a basis of the *vector space* V if

1. $V = \mathscr{L}(E)$
$= \{a_1v_1 + a_2v_2 + \cdots + a_nv_n : a_i \in K, 1 \le i \le n\}$ and
2. E is linearly independent,

i.e., $a_1v_1 + a_2v_2 + \cdots + a_nv_n = 0$ if and only if $a_i = 0, 1 \le i \le n$. All bases of V contain the same number of vectors, the *dimension* of V. The *rank* of A is the

dimension of its *row space*, i.e., the number of pivot entries in its Hermite normal form. For the matrix in Equation (A17), $\text{rank}(A) = 3$.

Because the rank of a fixed but arbitrary $m \times n$ matrix A is the number of pivot columns in its Hermite normal form and its nullity is the number of nonpivot columns,

$$\text{rank}(A) + \text{nullity}(A) = n. \tag{A19}$$

Returning to Equations (A16), the nonhomogeneous counterpart of $Ax = 0$ is $Ax = u^t$, where $u = (a, b, c)$, say. If x is one solution of this equation and y is another then, because matrix multiplication is distributive, $A(y - x) = 0$, i.e., $v = y - x$ is a solution of the homogeneous equation. It follows that any solution to the nonhomogeneous equation is of the form $y = x + v$, where $v \in \mathscr{L}((-2, 1, 0, 0, 0), (-3, 0, -4, 1, 0))$. Written in the form $x + \mathscr{L}((-2, 1, 0, 0, 0), (-3, 0, -4, 1, 0))$, the solution set of $Ax = u^t$ is sometimes called a *coset*. (A standard decoding array [Section 6.2] is simply a list that associates with each *syndrome u* a minimum-weight binary word from the corresponding coset.)

If $v = (a_1, a_2, \ldots, a_n)$ and $w = (b_1, b_2, \ldots, b_n)$, their *scalar* (or *dot*) *product* is

$$v \cdot w = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n. \tag{A20}$$

(In the analog for the complex field $\mathbb{C}, b_i$ would be replaced by its complex conjugate $\bar{b}_i$.) If $K = \mathbb{R}$, then

$$v \cdot w = \| v \| \| w \| \cos(\theta),$$

where $\| v \| = (v \cdot v)^{1/2}$ is the *magnitude* of v, and θ is the angle *between* v and w. In particular, $v \cdot w = 0$ if and only if $\cos(\theta) = 0$, if and only if v and w are perpendicular.

If K is the Boolean field $F = \{0, 1\}$, then $v \cdot v$ is the *parity* of v, i.e., it is 0 if an even number of coordinates of v are ones, and 1 if an odd number of components are ones. Regardless of the choice of K, v and w are said to be *orthogonal* if $v \cdot w = 0$.

If W is a subspace of V, then

$$W^{\perp} = \{v \in V : v \cdot w = 0 \text{ for all } w \in W\}.$$

If $K = \mathbb{R}$, then $W^{\perp}$ is called the *orthogonal complement* of W. If $K = F$, it is the *dual* of the linear code W. In either case, if W is the row space of an $n \times m$ matrix A, then $W^{\perp}$ is the kernel of A.

If $A = (a_{ij})$ is an $n \times n$ matrix, its *determinant* is a_{11} when $n = 1$. Otherwise, it is

$$\det(A) = \sum (-1)^{i+j} a_{ij} \det(A_{ij}), \tag{A21}$$

where A_{ij} is the $(n-1)$-square submatrix of A obtained by deleting its ith row and jth column, and the summation is over either i or j going from 1 to n. The *classical adjoint*, or *adjugate*, of A is the matrix $A^\dagger$ whose (i,j)-entry is $(-1)^{i+j}\det(A_{ji})$. It follows from Equation (A21) that

$$AA^\dagger = \det(A)I_n, \tag{A22}$$

where $I_n = (\delta_{ij})$ is the n-square *identity matrix* whose (i,j)-entry $\delta_{ij} = 1$ if $i = j$, and 0 otherwise. It follows from Equation (A22) that A is invertible if and only if $\det(A) \neq 0$, in which case $A^{-1} = [1/\det(A)]A^\dagger$.

Let A be an $n \times n$ matrix. Then a number $\lambda \in K$ is an *eigenvalue* of A if there exists a nonzero column vector v such that $Av = \lambda v$, in which case v is an *eigenvector* of A afforded by λ. Thus, $0 \neq v$ is an eigenvector of A afforded by λ if and only if $(\lambda I_n - A)v = 0$, if and only if $\lambda I_n - A$ is a singular matrix, if and only if $\det(\lambda I_n - A) = 0$.

The *characteristic polynomial* of A is

$$\begin{aligned} p(x) &= \det(xI_n - A) \\ &= x^n - c_1x^{n-1} + c_2x^{n-2} - \cdots + (-1)^n c_n. \end{aligned} \tag{A23}$$

If A is an $n \times n$ matrix over K, then λ is an eigenvalue of A if and only if $\lambda \in K$ and $p(\lambda) = 0$. The *characteristic roots* of A are the zeros of $p(x)$ (possibly over an extension field of K). If $r_1, r_2, \ldots, r_n$ are the characteristic roots of A, multiplicities included, then

$$\begin{aligned} c_n &= \prod_{i=1}^{n} r_i \\ &= \det(A), \end{aligned} \tag{A24}$$

and

$$\begin{aligned} c_1 &= \sum_{i=1}^{n} r_i \\ &= \sum_{i=1}^{n} a_{ii} \\ &= \mathrm{tr}(A), \end{aligned} \tag{A25}$$

the *trace* of A. More generally, $c_t = E_t(r_1, r_2, \ldots, r_n)$, the tth elementary symmetric function of the characteristic roots.

Of special interest is the case in which all of the characteristic roots belong to the scalar field K. (This will always be the case when $K = \mathbb{C}$.) The square matrix

$A = (a_{ij})$ is symmetric if $a_{ij} = a_{ji}$ for all i and j, i.e., if $A = A^{\mathrm{t}}$. It is shown in advanced linear algebra courses that the characteristic roots of real symmetric matrices are all real, and that any such matrix is similar (over $\mathbb{R}$) to a diagonal matrix. A real symmetric matrix all of whose characteristic roots are nonnegative is said to be *positive semidefinite*. It turns out that A is positive semidefinite symmetric if and only if $A = BB^{\mathrm{t}}$ for some real matrix B.

Suppose V and W are vector spaces (over the same scalar field K). A function $T : V \to W$ is *linear* if

$$T(au + bv) = aT(u) + bT(v)$$

for all $a, b \in K$ and all $u, v \in V$. The connection between linear transformations and matrices is via the notion of an *ordered basis*. If $E = \{v_1, v_2, \ldots, v_n\}$ and $F = \{w_1, w_2, \ldots, w_m\}$ are ordered bases of V and W, respectively, then, because $T(v_j) \in W$, there exist (unique) numbers $a_{ij} \in K, 1 \le i \le m$, such that

$$T(v_j) = \sum_{i=1}^{m} a_{ij} w_i, \qquad 1 \le j \le n. \tag{A26}$$

The *matrix representation* of T with respect to the bases E and F is $[T]_E^F = (a_{ij})$. If $u = c_1 v_1 + c_2 v_2 + \cdots + c_n v_n$, then the *coordinate representation* of u with respect to E is $[u]_E = (c_1, c_2, \ldots, c_n)^{\mathrm{t}}$, the $n \times 1$ column vector whose ith entry is c_i. Many nice things are known about such representations, e.g.,

$$[T]_E^F [u]_E = [T(u)]_F. \tag{A27}$$

We conclude this appendix with a list of useful results.

A3.1 Theorem. *If B is obtained from the $n \times n$ matrix A by*

(i) *switching two rows, then* $\det(B) = -\det(A)$;
(ii) *multiplying row s by c, then* $\det(B) = c \det(A)$;
(iii) *adding a multiple of row s to row $t \neq s$, then* $\det(B) = \det(A)$.

A3.2 Theorem. *The rank of an $m \times n$ matrix A is the size of the largest square submatrix of A whose determinant is nonzero.*

A3.3 Theorem. *If A and B are $m \times n$ and $n \times k$ matrices, respectively, then* $\operatorname{rank}(A) \ge \operatorname{rank}(AB)$. *In particular,* $\operatorname{rank}(A) \ge \operatorname{rank}(AA^{\mathrm{t}})$.

A3.4 Definition. Suppose A is an $n \times n$ matrix. If $f, g \in Q_{t,n}$, denote by $A[f|g]$ the $t \times t$ matrix whose (i,j)-entry is the $(f(i), g(j))$-entry of A.

A3.5 Theorem. *Suppose $r_1, r_2, \ldots, r_n$ are the characteristic roots of the $n \times n$ matrix A, multiplicities include. Then*

$$E_t(r_1, r_2, \ldots, r_n) = \sum_{f \in Q_{t,n}} \det(A[f|f]).$$

A3.6 (Cauchy–Binet) Theorem. *Suppose A and B are $n \times n$ matrices. Let $C = AB$. Then, for all $f, h \in Q_{t,n}$,*

$$\det(C[f|h]) = \sum_{g \in Q_{t,n}} \det(A[f|g])\ \det(B[g|h]).$$

Bibliography

GENERAL REFERENCES

V. K. Balakrishnan, *Combinatorics*, Schaum's Outlines, McGraw-Hill, New York, 1995.

K. P. Bogart, *Introductory Combinatorics*, 2nd ed., Harcourt Brace Jovanovich, San Diego, CA, 1990.

R. A. Brualdi, *Introductory Combinatorics*, 3rd ed., Prentice-Hall, Upper Saddle River, NJ, 1999.

D. I. A. Cohen, *Basic Techniques of Combinatorial Theory*, Wiley, New York, 1978.

R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, Reading, MA, 1989.

C. L. Liu, *Introduction to Combinatorial Mathematics*, McGraw-Hill, New York, 1968.

G. Pólya, R. E. Tarjan, and D. R. Woods, *Notes on Introductory Combinatorics*, Birkhäuser, Boston, MA, 1983.

SPECIAL TOPICS

E. A. Abbott, *Flatland: A Romance of Many Dimensions*, Dover, New York, 1952.

G. E. Andrews, *The Theory of Partitions*, Encyclopedia of Mathematics and Its Applications, Vol. 2, Addison-Wesley, Reading, MA, 1976.

H. Anton and R. C. Busby, *Contemporary Linear Algebra*, Wiley, New York, 2003.

N. L. Biggs, *Discrete Mathematics*, Oxford Science Publications, Clarendon Press, Oxford, 1985.

D. M. Bressoud, *Proofs and Confirmations*, Cambridge University Press, Cambridge, 1999.

W. Burnside, *Theory of Groups of Finite Order*, 2nd ed., Cambridge University Press, London, 1911; reprinted by Dover, New York, 1955.

C. J. Colbourn and J. H. Dinitz, Eds., *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, FL, 1996.

G. M. Constantine, *Combinatorial Theory and Statistical Design*, Wiley, New York, 1987.

D. Cvetković, M. Doob, I. Gutman, and A. Torĝasev, *Recent Results in the Theory of Graph Spectra*, Annals of Discrete Mathematics, Vol. 36, North-Holland, Amsterdam, 1988.

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

W. Feller, *An Introduction to Probability Theory and Its Applications*, 2nd ed., Vol. 1, Wiley, New York, 1957.

M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, Freeman, San Francisco, 1979.

R. L. Graham, B. L. Rothschild, and J. H. Spencer, *Ramsey Theory*, Wiley Interscience, New York, 1980.

M. Hall, Jr., *Combinatorial Theory*, 2nd ed., Wiley Interscience, New York, 1986.

F. Harary, *Graph Theory*, Addison-Wesley, Reading, MA, 1972.

F. Harary and E. M. Palmer, *Graphical Enumeration*, Academic Press, New York, 1973.

G. H. Hardy, *Dirichlet's Series*, Stechert-Hafner Service Agency, New York, 1964.

G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Science Publications, Clarendon Press, Oxford, 1979.

D. G. Hoffman, D. A. Leonard, C. C. Lindner, C. A. Rodger, and J. R. Wall, *Algebraic Coding Theory*, Charles Babbage Research Centre, Winnipeg, 1987.

A. Holden, *Shapes, Space, and Symmetry*, Columbia University Press, New York, 1971; reprinted by Dover, New York, 1991.

L. Lovász and M. D. Plummer, *Matching Theory,* Annals of Discrete Mathematics, Vol. 29, North-Holland, Amsterdam, 1986.

I. G. MacDonald, *Symmetric Functions and Hall Polynomials*, 2nd ed., Clarendon Press, Oxford, 1995.

P. A. MacMahon, *Combinatory Analysis*, Chelsea, New York, 1960.

F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, 1977.

A. W. Marshall and I. Olkin, *Inequalities: Theory of Majorization and Its Applications*, Academic Press, New York, 1979.

R. Merris, *Graph Theory*, Wiley, New York, 2001.

A. Nijenhuis and H. S. Wilf, *Combinatorial Algorithms*, Academic Press, New York, 1975.

D. S. Passman, *Permutation Groups*, Benjamin, New York, 1968.

G. Pólya and R. C. Read, *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*, Springer-Verlag, New York, 1987.

R. C. Read and W. T. Tutte, Chromatic Polynomials, Chapter 2 of *Selected Topics in Graph Theory,* Vol., 3 (L. W. Beineke and R. J. Wilson, Eds.), Academic Press, New York, 1988, pp. 15– 42.

J. Riordan, *An Introduction to Combinatorial Analysis*, Wiley, New York, 1958.

J. Riordan, *Combinatorial Identities*, Wiley, New York, 1968.

H. J. Ryser, *Combinatorial Mathematics*, Carus Mathematical Monograph 14, Mathematical Association of America, Washington, DC, 1963.

N. J. A. Sloane, *A Short Course on Error Correcting Codes*, Springer-Verlag, New York, 1975.

R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, Wadsworth & Brooks/Cole, Monterey, 1986.

I. Tomescu, *Problems in Combinatorics and Graph Theory*, Wiley Interscience, New York, 1985.

N. Trinajstić, *Chemical Graph Theory*, Vol. 2, CRC Press, Boca Raton, FL, 1983.

M. J. Wenninger, *Polyhedron Models*, Cambridge University Press, London, 1971.

H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

H. S. Wilf, *Generatingfunctionology*, Academic Press, New York, 1990.

Hints and Answers to Selected Odd-Numbered Exercises

People are generally better persuaded by reasons they discover for themselves than by those which have come from others.

— Blaise Pascal, *Pensées*

CHAPTER 1

1.1. The Fundamental Counting Principle

1(c) $7 \times 5 \times 7 \times 5 = 1225$. **1(d)** $12 \times 5 \times 12 \times 5 = 3600$.

3 $2^6 = 64$.

5(b) TOO, OTO, OOT.

7(a) 60. **7(d)** 120. **7(i)** 4, 989, 600.

9 Hint: $5!/(2!3!) = 10$.

11(a) 06101–9936 with a check digit of 5.

11(b) 97208–9958 with a check digit of 3.

13 Since the check digit is 2, the last six digits are $||\,|\,||$.

15(b) 121. **15(c)** 231. **15(e)** 105. **15(f)** 270.

17(a) 1296. **17(b)** 360.

19 Nearly 89 hours.

21 Hint: Some possibilities are GRITFLUBH, BLUFHGRIT, and BFGRITHLU.

23(a) $o(A) = 3^5 = 243$.

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

23(b) Hint: The answer can be expressed as a sum of six multinomial coefficients.

1.2. Pascal's Triangle

1(a) $C(7,4) = 35$. **1(b)** $C(10,5) = 252$. **1(c)** $C(12,4) = 495$.

1(e) Hint: $C(101,99) = C(101,2)$.

5(a) Hint: Pascal's relation.

7 Almost 70 billion.

9(a) Hint: Add fractions, each of which involves lots of factorials.

9(b) Hint: Consider n-letter words and break the problem into cases according to which letter comes last. (If $r_i = 1$, then $r_i - 1 = 0$ but, because $0! = 1$, no harm is done.)

11 Hint: $(2^n)^2 = 2^{2n}$.

15(e) Hint: They all have length $n = r + s$.

17 $C(n,r)C(m,s)$.

19(a) $F_7 = C(7,0) + C(6,1) + C(5,2) + C(4,3) = 1 + 6 + 10 + 4$.

19(b) Hint: Pascal's relation.

19(c) $F_7 = 13 + 8$.

21(a) 252. **21(b)** 120.

23 $C(30,2) = 435$; $C(36,2) = 630$.

25(c) The third $(n = 2)$ row is 9, 18, 36, 72, 144.

27 Hint: $63{,}000 = 2^3 3^2 5^3 7$.

1.3. Elementary Probability

1 $\frac{4}{12} = \frac{1}{3}$. **3(a)** $\frac{1}{36}$.

3(b) $\frac{25}{216}$. **3(d)** $\frac{5}{108}$.

5(a) $\frac{1}{36}$. **5(b)** $\frac{1}{24}$.

5(c) $\frac{1}{12}$. **5(d)** 0.

7 $\frac{1}{3}$.

9 $5 \times 5 \times 5 = 125$.

11 $[4 \times C(13,5)]/C(52,5)$.

13 Yes, with $p = \frac{1}{6}$ and $q = \frac{5}{6}$, the Chuck-a-Luck probabilities are given by Equation (1.5).

15 $P = 1 - (\frac{5}{6})^4 \doteq 0.518$.

17 Hint: $\log_2(100) = \ln(100)/\ln(2) > 6.6$.

19 Hint: $P(A \text{ and } B)$ is always the same as $P(B \text{ and } A)$.

21 Hint: Use Exercise 20(c). (This is a version of the so-called *birthday paradox*.)

23(a) $\frac{2}{3}$. **23(b)** $\frac{2}{3}$. **23(c)** $\frac{2}{3}$.

25 Hint: What are the chances that one or both drugs are worthless? Compute the "placebo" probabilities, (1) that 9 out of 10 snake-bite victims would survive without treatment, vs. (2) that 4 out of 4 would survive without treatment.

1.4. Error-Correcting Codes

1 $2^8 = 256$.

3(a) $(n, M, d) = (3, 4, 2)$. **3(b)** $(3, 8, 1)$. **3(d)** $(5, 10, 2)$.

5(a) The ASCII code for S is 83.

5(b) Hint: $83_{\text{ten}} = 01010011_{\text{two}}$.

5(c) 76 is the ASCII code for L.

5(d) Hint: $01010101_{\text{two}} = 85_{\text{ten}}$.

5(e) Hint: $11111011_{\text{two}} = 251_{\text{ten}}$. **5(f)** *M-A-T-H*.

7(a) Hint: $d(b, c) = 1$ if and only if c differs from b in a single bit.

7(b) $\mathscr{C} = \{11110000, 00001111\}$ is a constant weight (8,2,8) code.

7(c) Hint: Maximize $f(r) = C(8, r)$.

9(a) No, $n > 2d$. **9(b)** Yes, $2\lfloor \frac{7}{2} \rfloor = 6$.

11(a) Hint: If $i \neq j$, then $d(c_i, c_j) \geq d$.

11(b) Hint: Show that the "contribution" of the kth column of A to D is $2z_k(M - z_k)$.

11(d) Hint: Use parts (a)–(c) to show that $\frac{1}{2}nM^2 \geq M(M-1)d$.

11(f) Hint: Show that $M \leq n/(2d - n) = [2d/(2d - n)] - 1$ and observe that $\lfloor [2d/(2d - n)] - 1 \rfloor \leq 2\lfloor d/(2d - n) \rfloor$.

13 Hints: Use Exercise 12(b) to show that $M(n, 2r-1) \le M(n+1, 2r)$. To prove the reverse inequality, let $M = M(n+1, 2r)$ and suppose $\mathscr{C}$ is an $(n+1, M, 2r)$ code. Choose $b, c \in \mathscr{C}$ so that $d(b, c) = 2r$. If b and c differ in the ith bit, consider the code $\mathscr{C}'$ obtained from $\mathscr{C}$ by deleting the ith bit from every codeword.

15 $(n, M, d) = (15, 2048, 3)$.

17 Hint: Exercise 9.

19 Hint: $1024^{1/3} \times \sqrt{2} \doteq 14.25$; $6(1+\sqrt{2}) \doteq 14.49$.

21(a) Hint: The vocabulary of any (n, M, d) code can be divided into two subsets, those words that begin with 0 and those that begin with 1.

21(b) Hint: Use part (a) and the Plotkin bound from Exercise 9.

23 Hint: Why is it enough to show that $C(7,0) + C(7,1) = 2^3$?

25 Hint: Why is it enough to show that $N(23, 3) = 2^{11}$?

27(a) Hint: Consider the eight codewords of $\mathscr{H}_3$ with first bit equal to 0.

27(b) Hint: Part (a) and Exercise 12(b).

29(a) Hint: The probabilities follow a binomial distribution.

29(b) Approximately 0.000194.

1.5. Combinatorial Identities

1(a) Hint: $2 + 4 + 6 + \cdots + 2n = 2(1 + 2 + 3 + \cdots + n)$.

3(b) Hint: Gauss.

5(a) Hint: Theorem 1.5.1. **5(b)** Hint: Symmetry.

9(a) $A_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 6 & 14 & 30 \\ 0 & 0 & 6 & 36 & 150 \\ 0 & 0 & 0 & 24 & 240 \\ 0 & 0 & 0 & 0 & 120 \end{pmatrix}$.

11 Hint: The alternating-sign theorem. [See Exercise 25(h) for a generalization of this important result.]

13 Hint: Chu's theorem.

15 Hint: Imagine a bowl containing m apples and n oranges. In how many ways can r pieces of fruit be chosen from the bowl?

17(a) 3744. **17(b)** 624.

19(a) Hint: $(n+1)C(n,r-1)/r = C(n+1,r)$.

19(b) Hint: Make a change of variable in part (a).

19(c) Hint: Induction using Pascal's relation and parts (a) and (b).

19(d) Hint: Part (b).

21(b) Hint: To be consistent, the expressions must differ by n^4.

21(c) $g(5) = \frac{1}{12}(2n^6 - 6n^5 + 5n^4 - n^2)$.

23 Hint: Exercise 21.

25(b) $$C_{[2,6]} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 \\ 6 & 4 & 1 & 0 & 0 \\ 10 & 10 & 5 & 1 & 0 \\ 15 & 20 & 15 & 6 & 1 \end{pmatrix}.$$

25(f) $$C_{[2,6]}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 & 0 \\ 6 & -4 & 1 & 0 & 0 \\ -10 & 10 & -5 & 1 & 0 \\ 15 & -20 & 15 & -6 & 1 \end{pmatrix}.$$

25(h) Hint: This result generalizes Exercise 11.

27 Hint: Exercise 15.

1.6. Four Ways to Choose

1(a) $P(5,3) = 60$.

1(b) $C(5,3) = 10$.

1(d) $P(5,2) = 20$.

1(g) $7! = 5040$.

3(a) $C(4+7-1,4) = 210$.

3(b) $P(7,4) = 840$.

3(c) $C(7,4) = 35$.

3(d) $7^4 = 2401$.

5(a) 10,000.

5(b) 715.

5(c) 210.

5(d) 5040.

9(a) 2925.

9(c) 286.

9(d) 816.

11 Hint: Not all compositions of 6 have three parts.

13 Hint: Chu's theorem.

15(a) Hint: Induction on $n+k$.

15(b) Hint: Use part (a).

15(c) Hint: Use parts (a) and (b).

17 Hint: If $F_k > n > F_{k-1}$, then $0 < n - F_{k-1} < F_{k-2}$.

19 Hint: Exercise 19, Section 1.2.

21(a) $C(5,3) \times 2! = 20$. **21(b)** $5 \times C(4,2) \times 1 = 30$.

23(a) Hint: Of the 100^3 possible outcomes allowed under unlimited replacement, how many are now precluded?

23(b) 171,600. **23(c)** 99,960,300. **23(d)** 4,411,275.

27(a) 286. **27(b)** 1,048,576.

29 Hint: Induction may be easiest; a longer but perhaps more informative proof can be based on Exercise 19, Section 1.2.

1.7. The Binomial and Multinomial Theorems

1(a) $C(5,0) = 1$. **1(b)** $C(7,2) = C(7,5) = 21$.

1(d) $2^2 \times C(7,2) = 84$. **1(e)** $2^5 \times C(7,2) = 672$.

1(f) $(-1)^5 \times C(9,4) = -126$. **1(h)** $2^5 \times C(4,5) = 0$.

3(b) Hint: $M_{[5]}(1,1,1) = 3$, but $M_{[4,1]}(1,1,1) = 6$.

5(e) Hint: Set $a = b = c = d = e = 1$ in Example 1.7.8.

7(a) 3. **7(b)** $3 \times 9 = 27$.

7(c) Hint: Thirty of the 66 terms were accounted for in parts (a) and (b).

9 Hint: Consider $(w - x + y - z)^n$.

11(b) Hint: $n^p = (1 + 1 + \cdots + 1)^p$.

13(a) $M_{[6,4]}(x,y,z) = x^6y^4 + x^6z^4 + x^4y^6 + x^4z^6 + y^6z^4 + y^4z^6$.

13(b) $M_{[5,5]}(x,y,z) = x^5y^5 + x^5z^5 + y^5z^5$.

15 The $C(10+3-1,10) = 66$ monomials are grouped into 14 minimal symmetric polynomials.

19 Hint: Exercise 18.

21(a) Hint: Consider the telescoping series $\sum_{j=1}^{n-1}[(j+1)^{k+1} - j^{k+1}]$.

23(a) Hint: Exercise 22.

23(b) Hint: Section 1.2, Exercise 10(a), p. 17.

1.8. Partitions

1(a) $[6], [5,1], [4,2], [3^2], [4,1^2], [3,2,1], [2^3], [3,1^3], [2^2,1^2], [2,1^4]$, and $[1^6]$.

1(b) $[7], [6,1], [5,2], [4,3], [5,1^2], [4,2,1], [3^2,1]$, and $[3,2^2]$.

1(c) $[1^7], [2,1^5], [2^2,1^3], [2^3,1], [3,1^4], [3,2,1^2], [3,2^2]$, and $[3^2,1]$.

3 Hint: $p(15) = 176$.

5(c) $30^2/12 = 75$.

7 $[7,1^3], [6,2,1^2], [5,3,1^2], [5,2^2,1], [4^2,1^2], [4,3,2,1]$, and $[3^3,1]$.

9 Hint: Let $k = \lfloor \sqrt{n} \rfloor$. If S is a fixed but arbitrary subset of $\{1,2,\ldots,k\}$, denote the sum of its elements by $\sum(S)$. Let $\pi(S)$ be the $(o(S)+1)$-part partition of n, whose largest part is $\pi_1 = n - \sum(S) \geq k$ (when $k > 3$), and whose remaining parts (if $S \neq \varnothing$) are the elements of S. Show that $S \to \pi(S)$ is a one-to-one function.

11(a) The three odd-part partitions of 5 are $[5]$, $[3,1^2]$, and $[1^5]$; the three partitions of 5 having distinct parts are $[5]$, $[4,1]$, and $[3,2]$.

11(b) From the answer to Exercise 1(a), the four odd-part partitions of 6 are $[5,1], [3^2], [3,1^3]$, and $[1^6]$; the four partitions having distinct parts are $[6], [5,1], [4,2]$, and $[3,2,1]$.

13(a) Hint: Theorem 1.8.7.

13(b) Hint: Let $\pi \vdash n$. If $\ell(\pi) \leq m$, consider the partition of $n+m$ whose Ferrers diagram is obtained from $F(\pi)$ by adjoining a new first column containing m boxes.

15(a) Because $6+4 = 4+3+2+1$, both [6,4] and [4,3,2,1] are partitions of (the same $n =$) 10. With that (subtle!) preliminary calculation out of the way, it remains to observe that $6 \geq 4$ and $6+4 = 10 \geq 7 = 4+3$.

15(d) Hint: First show that α majorizes β if and only if $F(\beta)$ can be obtained from $F(\alpha)$ by moving boxes *down*, i.e., to higher numbered rows.

17 Hint: Let π be a self-conjugate partition of n. Suppose $F(\pi)$ has k boxes on its main diagonal. Consider the k-part partition of n whose ith part is equal to the number of boxes in row *and* column i of $F(\pi)$.

19 $p_5(10) = 7$.

21(a) $\binom{10}{8,1,1} = 90.$ **21(c)** $\binom{10}{3,3,2,2} = 25,200.$

23(a) $p(x,y,z) = 5M_{[2]}(x,y,z) - M_{[1^2]}(x,y,z)$.

23(b) $p(x,y,z) = 2M_{[1]}(x,y,z) - 3M_{[2]}(x,y,z) + 4M_{[1^3]}(x,y,z)$.

25(a) $H_2(x,y) = x^2 + y^2 + xy$.

25(b) $H_3(x, y) = x^3 + y^3 + x^2y + xy^2$.

25(c) $H_2(a, b, c) = a^2 + b^2 + c^2 + ab + ac + bc$.

25(d) $H_3(a, b, c) = a^3 + b^3 + c^3 + a^2b + a^2c + ab^2 + ac^2 + b^2c + bc^2 + abc$.

27(b) Hint: These partitions may sum to anything from $n = 1$ to $n = rs$.

1.9. Elementary Symmetric Functions

1 Hint: $(x + 1)^2$ is a factor of $f(x)$.

3(b) $E_1 = -5,\ E_2 = 6,\ E_3 = -2,$ and $E_4 = 1$.

3(c) $E_1 = -5,\ E_2 = -6,\ E_3 = -2,$ and $E_4 = -1$.

3(d) $E_1 = -5,\ E_2 = -6,\ E_3 = -2,$ and $E_4 = -1$.

3(f) $E_1 = -1,\ E_4 = -2,$ and $E_2 = E_3 = E_5 = 0$.

5(a) Hint: Row 4 of the elementary triangle.

7 Hint: For $f(x)$ to have degree n, $b_0 \neq 0$.

9(c) $M_3 = E_1^3 - 3E_1E_2 + 3E_3$.

11(a) $x^3y + xy^3 = \frac{1}{2}(M_1^2M_2 - M_2^2)$. **11(b)** $x^3y + xy^3 = E_1^2E_2 - 2E_2^2$.

13 Hint: If $p(x) = (x - a_1)(x - a_2)\cdots(x - a_n)$, then $(-1)^n p(1) = (a_1 - 1)\times (a_2 - 1)\cdots(a_n - 1)$.

15 Hint: Exercise 14.

17(a) Hint: $x^{(m)} = x(x - 1)\cdots(x - [m - 1]) = x(x - 1)\cdots(x - m + 1)$.

17(b) Hint: Induction using Pascal's relation.

19(a)

α	$[6, 1^2]$	$[5, 2, 1]$	$[4, 3, 1]$	$[4, 2^2]$	$[3^2, 2]$
$H_2(\alpha)$	51	47	45	44	43

23(a) Hint: Induction and Pascal's relation.

23(b) Hint: Newton's identities together with Equations (1.35) and (1.36).

25 Hint: If $\lambda_1, \lambda_2, \ldots, \lambda_n$ are the characteristic roots of A, then $c_t = E_t(\lambda_1, \lambda_2, \ldots, \lambda_n)$ and $\text{tr}(A^t) = M_t(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

1.10. Combinatorial Algorithms

1
```
1. For I = 1 to 100.
2. Write I.
3. Next I.
```

3 Because $r_1!/r_1!$ is not computed, the r's should be arranged so that r_1 is the largest.

5(a) Hint: Example 1.10.8.

7(a) Hint: Example 1.10.9.

11(a)
```
 1. Input x_1, x_2, ..., x_6.
 2. E_3 = 0
 3. For I = 1 to 4.
 4. For J = I + 1 to 5.
 5. For K = J + 1 to 6.
 6. E_3 = E_3 + x_I x_J x_K.
 7. Next K.
 8. Next J.
 9. Next I.
10. Return E_3.
```

13
```
 1. Input x_1, x_2, ..., x_6.
 2. P = 1 and E_5 = 0.
 3. For I = 1 to 6.
 4. P = P × x_I.
 5. Next I.
 6. For I = 1 to 6.
 7. E_5 = E_5 + P/x_I.
 8. Next I.
 9. Return E_5.
```

15(a) Hint: Count in base 2.

15(b) Hint: Consider the rearrangements of 00001111.

17(a) Interpreting "dth bit" to mean the dth bit *from the right*, the list is 0000, 0001, 0011, 0010, 0110, 0111, 0101, 0100, 1100, 1101, 1111, 1110, 1010, 1011, 1001, 1000.

17(b) Hint: The two words differ (only) in the leading bit.

17(c) Hint: Induction together with your observation in part (b).

17(e) Hint: If $X \subset \{1, 2, \ldots, n\}$, let $w(X) = x_1 x_2 \cdots x_n$ be the binary word defined by $x_i = 1$ if and only if $i \in X$.

19(a)
```
1. For I = 1 to 100.
2. X = RND.
3. If x < 1/2 then write "H";
4. If x ≥ 1/2 then write "T";
5. Next I.
```

19(b) About 50.

19(d)
```
1. H = 0 and T = 0.
2. For I = 1 to 100.
3. X = RND.
4. If X < 1/2 then write ''H'' and set H = H + 1.
5. If x ≥ 1/2 then write ''T'' and set T = T +1.
6. Write H ''heads and  '' T ''tails''.
```

19(e) Add a new line to the solution in part (d):

```
7. Write ''Empirical P(H) =''H/100.
```

21(a) Hint: $p = C(12,6)/2^{12}$.

21(b)
```
1. C = 0.
2. For I = 1 to 100.
3. H = 0 and T = 0.
4. For J = 1 to 12.
5. X = RND.
6. If X < 1/2 then H = H +1.
7. If X ≥1/2 then T = T +1.
8. Next J.
9. If H = T then C = C + 1.
10. Next I.
11. Write ''Empirical P(6&6) = ''C/100.
```

23
```
1. For I = 1 to 100.
2. Write 1 +⌊6 × RND⌋.
3. Next I.
```

25 Hint: Begin by changing 6 to 12 in the previous solution.

CHAPTER 2

2.1. Stirling Numbers of the Second Kind

1(a) $f(3) = 5$; $f^{-1}(4) = \{1\}$.

1(b) $f(3) = 5$; $f^{-1}(4) = \{2,4\}$.

1(e) $f(3)$ doesn't exist; $f^{-1}(4) = \varnothing$.

1(f) $f(3) = 4$; $f^{-1}(4) = \{1,2,3,4,5\}$.

3(a) (1,2), (2,1), (1,3), (3,1), (2,3), (3,2).

3(b) Hint: There are six of them. **3(c)** There are none.

3(d) Every function in $Q_{m,n}$ is one-to-one.

5

n	1	2	3	4	5	6	7	8	9
$S(8,n)$	1	127	966	1701	1050	266	28	1	
$S(9,n)$	1	255	3025	7770	6951	2646	462	36	1

7 Hint: Because n is "square free", d and q cannot be equal. Mimic Example 2.1.21, but compare with Exercise 28, Section 1.2.

9(a) $G_{2,3} = \{(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}$.

9(b) $G_{3,3} = \{(1,1,1),(1,1,2),(1,1,3),(1,2,2),(1,2,3),(1,3,3),(2,2,2),(2,2,3),(2,3,3),(3,3,3)\}$.

11(a) Hint: Generalize your solution to Exercise 10(d).

11(c) Hint: Part (b).

11(d) Hint: Part (c) and Exercise 10(a).

13 Hint: In any $(n+1)$-part partition of $\{1,2,\ldots,m,m+1\}$, the number $m+1$ will belong to a block of size $t+1$, were $0 \le t \le m-n$. There are $C(m,t)$ ways to choose the companions of $m+1$ and $S(m-t,n)$ ways to partition the remaining $m-t$ numbers among the remaining n blocks.

15 $(2,0,2),(2,0,5),(2,1,2),(2,1,3),(4,0,5),(4,1,5),(7,0,7),(8,0,5),(8,1,8)$.

17 Hint: The sum of your answers to parts (a) and (b) should be $S(5,1)+\cdots+S(5,5)$, the (total) number of partitions of 5.

19 Hint: Exercise 18(d).

21 $n[C(n-1,0)+C(n-1,1)+\cdots+C(n-1,m-2)]$.

25

```
1.  For M = 1 to 12.
2.  S (M, 1) = 1.
3.  S(M,M) = 1.
4.  Next M.
5.  For M = 3 to 12.
6.  For N = 2 to M − 1.
7.  S(M, N) = S(M -1, N-1) + N × S(M-1, N).
8.  Next N.
9.  Next M.
```

2.2. Bells, Balls, and Urns

1(a) Hint:

$$\begin{aligned} x^{(5)} &= x(x-1)(x-2)(x-3)(x-4) \\ &= x(x^2-3x+2)(x^2-7x+12) \\ &= x(x^4-[7+3]x^3+[12+3\times 7+2]x^2-[3\times 12+2\times 7]x+24). \end{aligned}$$

1(b) Hint:

$$\sum_{r=1}^{5} S(5,r)x^{(r)} = x^{(5)} + 10x^{(4)} + 25x^{(3)} + 15x^{(2)} + x$$
$$= [x^5 - 10x^4 + 35x^3 - 50x^2 + 24x] + \cdots + x.$$

1(c) When $m = 5$ and $r = 3$, $3!S(5,3) = 6 \times 25 = 150 = 3 - 96 + 243 = C(3,1) \times 1^5 - C(3,2) \times 2^5 + C(3,3) \times 3^5$.

1(d) When $m = 5$ and $n = 3$, $3!S(5,3) = 3 \times 20 + 3 \times 30 = 3\binom{5}{3,1,1} + 3\binom{5}{2,2,1}$.

3(a)

r	1	2	3	4	5
$r!S(5,r)$	1	30	150	240	120

7 Hint: $B_7 = 877$.

11(a) $2!S(6,2) = 2 \times 31 = 62 = 12 + 30 + 20 = 2\binom{6}{5,1} + 2\binom{6}{4,2} + \binom{6}{3,3}$.

13 Hint: because the falcons are identical, all that matters is the number of falcons that each brother receives.

15 Hint: Explain the connection with n-part compositions of m.

17 $p_3(5) = 2$.

21(a) 10. **21(b)** $S(6,4) = 65$.

21(c) $4!S(6,4) = 1560$. **21(d)** $p_4(6) = 2$.

23 $p_4(10) = 9$.

25(a) $S(9,1) + S(9,2) + \cdots + S(9,5) = 1 + 255 + \cdots + 6951 = 18,002$.

25(b) $p_1(9) + p_2(9) + \cdots + p_5(9) = 1 + 4 + \cdots + 5 = 23$.

25(c) $C(5 + 9 - 1, 9) = 715$. **25(d)** $5^9 = 1,953,125$.

27(c) Hint: Parts (a) and (b).

29 Multinomial coefficient $\binom{m}{r_1, r_2, \ldots, r_n}$.

31 Hint: In Exercise 30(b), $203 = B_6$.

33 Hint: Set $r = m$ and $t = n$ in Stirling's identity to obtain

$$m! = \sum_{n=1}^{m} (-1)^{m+n} C(m,n) n^m.$$

If p is an odd prime, replace m with (the even integer) $p - 1$ and use $n^{p-1} \equiv 1 (\text{mod } p)$.

35(a) Hint: The students are labeled.

35(b) $C(10,4) \times C(6,3) = \binom{10}{4,3,3} = 4200$.

2.3. The Principle of Inclusion and Exclusion

1 The nine derangements are (2,1,4,3), (2,3,4,1), (2,4,1,3), (3,1,4,2), (3,4,1,2), (3,4,2,1), (4,1,2,3), (4,3,1,2), and (4,3,2,1).

3(a) $C(6,2)D(4) = 135$. **3(b)** 40.

3(d) No permutation in S_n has exactly $n-1$ fixed points.

5 Hint: Find a derangement that is its own inverse.

7 $C(15,5)D(10) = 4,008,887,883$; $15!/(5!e) \doteq 4,008,887,640$.

9 A total of 31 students have taken trigonometry.

11 Hint: If $A_k = \{p \in S_8 \ : \ p(2k) = 2k\}$, $1 \leq k \leq 4$, then $g \in S_8$ deranges the even integers if and only if $g \notin A_1 \cup A_2 \cup A_3 \cup A_4$. Use the principle of inclusion and exclusion.

13(a) Hint: If $p \in S_n$ is a derangement, then $p(n) = k \neq n$. Consider the two cases $p(k) = n$ and $p(k) \neq n$.

13(b) Hint: Use part (a) together with an induction hypothesis of the form $(n-1)D(n-2) = D(n-1) + (-1)^n$.

13(c) Hint: part (b).

15(a) Hint: Choose 30 times from $\{A, B, C, D\}$, with replacement, where order doesn't matter.

15(b) Hint: Example 1.6.14. **15(c)** 1540.

15(d) Hint: Let A_1 be the set of nonnegative integer solutions to $a+b+c+d = 30$ in which $a \geq 11$, A_2 be those solutions in which $b \geq 11$, and so on. Use PIE.

17(a) There are three rearrangements of the partition $[5^2, 2]$, six of $[5,4,3]$, and only one of $[4^3]$.

19 Hint: Mimic the approach of Exercise 18.

21(d) Hint: First compute $\varphi(p^k)$, where p is a prime and k is a positive integer. Then consider the case in which $m = p^k$, where p is a prime that is not a factor of n.

25(b) Consider $p = (i_1, i_2, \ldots, i_{n+1}) \in S_{n+1}$, where $p(t) = i_t = n+1$. If p has k inversions, how many inversions does

$$g = (p(1), \ldots, p(t-1), p(t+1), \ldots, p(n+1)) \in S_n$$

have?

27(a) Hint: Why is this the same as asking for the probability that a permutation, randomly chosen from S_{15}, is a derangement?

29 Hint: How is this different from listing the $m!$ different "words" that can be produced by rearranging the "letters" of $12 \ldots m$?

2.4. Disjoint Cycles

1(a) (126) (345) (7). **1(b)** (17) (26) (35) (4).

1(c) (17) (26) (345). **1(f)** (13579) (24) (68).

3(a) (2,3,1,5,4,7,6). **3(b)** (3,4,5,6,1,2).

3(c) (3,4,1,6,5,2). **3(d)** (2,1,3,4,5).

5 Hint: $p(g(x)) = x$ if and only if x follows y in $C_p(x)$ whenever y follows x in $C_g(x)$.

7 $S_4 = \{(1)(2)(3)(4), (12)(3)(4), (13)(2)(4), (14)(2)(3), (1)(23)(4), (1)(24)(3), (1)(2)(34), (12)(34), (13)(24), (14)(23), (1)(234), (1)(243), (134)(2), (143)(2), (124)(3), (142)(3), (123)(4), (132)(4), (1234), (1243), (1324), (1342), (1423), (1432)\}$.

9

Type	$[5]$	$[4,1]$	$[3,2]$	$[3,1^2]$	$[2^2,1]$	$[2,1^3]$	$[1^5]$
Number	24	30	20	20	15	10	1

11(a) Hint: $[P(12,3)/3][P(9,3)/3][P(6,3)/3][P(3,3)/3]/4! = 12!/[3^4 4!]$.

11(b) Hint: $[P(12,4)/4][P(8,4)/4][P(4,4)/4]/3! = 12!/[4^3 3!]$.

13 A total of $C(m,2)$ transpositions belong to S_m.

15 $s(7,2) = 1764$.

17 Hint: Interchange m and n in the proof of Theorem 1.8.7 on p. 78.

19(a) Hint: If the cycle type of p is $[m^{k_m}, \ldots, 3^{k_3}, 2^{k_2}, 1^{k_1}]$, then $c_t(p) = k_t, 1 \leq t \leq m$.

19(b) Hint: See the hints to Exercises 11(a)–(b).

2.5. Stirling Numbers of the First Kind

1 (12)(34), (13)(24), (14)(23), (1)(234), (1)(243), (134)(2), (143)(2), (124)(3), (142)(3), (123)(4), and (132)(4).

5 Partial answer:

$n =$	2	3	4	5	6	...
$m = 8$	13,068	13,132	6,769	1,960	322	...
$m = 9$	109,584	118,124	67,284	22,449	4,536	...

7 Hint: If $p \in S_m$ has $m - 1$ cycles in its disjoint cycle factorization, how many fixed points does p have?

9(a) Hint: Example 1.9.5.

11(b) Hint: Set $x = m = n$ in Equations (2.33)–(2.34).

15 Hint: $x^{(m+1)} = x \cdot (x-1)^{(m)}$.

17 Hint: Compare with Exercise 11, Section 1.5.

19 Hint: Bell numbers are sums of Stirling numbers of the second kind.

21(b) Hint: The first odd composite integer is 9.

27
```
1. s(1,1) = 1, s(2,1) = 1, and s(2,2) = 1.
2. For m = 3 to 10.
3. s(m, 1) = (m −1) × s(m −1, 1) and s(m, m) = 1.
4. For n = 2 to m − 1.
5. s (m,n) = s(m − 1, n − 1) + (m − 1) × s(m − 1, n).
6. Next n.
7. Next m.
```

29(a) Hint: Exercise 15.

29(b)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 2 & 3 & 1 & 0 & 0 \\ 6 & 11 & 6 & 1 & 0 \\ 24 & 50 & 35 & 10 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 3 & 1 & 0 \\ 0 & 6 & 11 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix}$$

31(a) Hint: Exercise 13, Section 2.1.

31(b)

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 1 & 7 & 6 & 1 & 0 \\ 1 & 15 & 25 & 10 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 \\ 0 & 1 & 7 & 6 & 1 \end{pmatrix}$$

CHAPTER 3

3.1. Function Composition

1(a) $f \circ g = (3, 1, 5, 2, 2)$.

1(b) $g \circ f = (4, 1, 4, 5, 2)$.

1(c) $f \circ h = (1, 1, 1, 1, 1)$.

1(d) $h \circ f = (1, 3, 1, 1, 3)$.

1(e) $g \circ h = (4, 5, 4, 5, 5)$.

1(g) $f \circ g \circ h = (3, 5, 3, 5, 5)$.

1(m) $f \circ f = (1, 2, 1, 1, 5)$

1(n) $g \circ g = (2, 4, 2, 1, 1)$.

3(a) $fg = (12345)$.

3(b) $gf = (13542)$.

3(e) $gh = (12)(34)(5)$.

3(m) $ff = (1)(235)(4)$.

3(n) $fff = e_5$.

3(q) $f^{-1} = (1)(235)(4)$.

3(r) $g^{-1} = (15243)$.

3(t) $f^{-1}gf = (15432)$.

5(a) $f(x) = \frac{1}{2}(3x^2 - 13x + 16)$.

5(b) $f = (3, 1, 2)$.

5(c) $f = (132)$.

7 Hint: Let $f = p$ and $g = p$. Then $fg \in \{p\}$ if and only if $pp = p$.

9 Hint: To prove the "curious fact" for row f, suppose $fg = fh$ and use the fact that $f^{-1} \in S_m$.

11(a)

	e_4	$(12)(3)(4)$	$(1)(2)(34)$	$(12)(34)$
e_4	e_4	$(12)(3)(4)$	$(1)(2)(34)$	$(12)(34)$
$(12)(3)(4)$	$(12)(3)(4)$	e_4	$(12)(34)$	$(1)(2)(34)$
$(1)(2)(34)$	$(1)(2)(34)$	$(12)(34)$	e_4	$(12)(3)(4)$
$(12)(34)$	$(12)(34)$	$(1)(2)(34)$	$(12)(3)(4)$	e_4

13(a) Because $[(12)(3)] \circ [(13)(2)] = (132) \notin G$, G is not closed.

13(b) Hint: Construct a Cayley table.

13(c) Because $(12345)(13245) = (14)(25)(3) \notin S$, S is not a subgroup.

15 Note: If k is the smallest positive integer such that $p^{k+1} \in \{p, p^2, \ldots, p^k\}$, then $p^k = e_m$.

17 Hint: This is a big job, in part because the Cayley table for A_4 is *not* symmetric. Work carefully. *Save* your work for future reference.

19 Hint: Using associativity, compute gfh in two different ways.

3.2. Permutation Groups

1(a) $o(p) = 12$.

1(b) $o(p) = 15$.

1(c) $o(p) = 2$. **1(d)** $o(p) = 3$.

3(a) (1234), (13) (24), (1432), e_m, (1234), (13) (24), (1432), e_m, (1234), (13) (24).

3(b) (12345), (13524), (14253), (15432), e_m, (12345), (13524), (14253), (15432), e_m.

3(d) (12345678), (1357) (2468), (14725836), (15) (26) (37) (48), (16385274), (1753) (2864), (18765432), e_m, (12345678), (1357) (2468).

5 Hint: G is cyclic if and only if G has a generator, i.e., a permutation $p \in G$ such that $o(p) = o(G)$.

7(a) The generators of G are (1234) and (1432).

7(b) The generators of G are (12345), (13524), (14253), and (15432).

7(c) The generators of G are p^r, $1 \leq r \leq 4$. (Is this G the same as the group in part (b)?)

7(d) The generators of G are p and $p^{-1} = p^5$.

7(f) Hint: G has four generators.

9(a)

	e_4	(1234)	(1432)	(13)	(24)	(12)(34)	(13)(24)	(14)(23)
e_4	e_4	(1234)	(1432)	(13)	(24)	(12)(34)	(13)(24)	(14)(23)
(1234)	(1234)	(13)(24)	e_4	(14)(23)	(12)(34)	(13)	(1432)	(24)
(1432)	(1432)	e_4	(13)(24)	(12)(34)	(14)(23)	(24)	(1234)	(13)
(13)	(13)	(12)(34)	(14)(23)	e_4	(13)(24)	(1234)	(24)	(1432)
(24)	(24)	(14)(23)	(12)(34)	(13)(24)	e_4	(1432)	(13)	(1234)
(12)(34)	(12)(34)	(24)	(13)	(1432)	(1234)	e_4	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(1432)	(1234)	(24)	(13)	(14)(23)	e_4	(12)(34)
(14)(23)	(14)(23)	(13)	(24)	(1234)	(1432)	(13)(24)	(12)(34)	e_4

9(b) $G_3 = \{e_4, (24)\}$. **9(c)** $G_4 = \{e_4, (13)\}$.

9(d) (1432) and (14) (23).

9(f) G has seven different cyclic subgroups.

11 Hint: $(p^n)^{-1}$ is the unique permutation f such that $fp^n = e_m = p^n f$. Show that $f = (p^{-1})^n$ solves these equations. Use associativity.

13 Hint: Exercise 11.

15 It is false. One counterexample is $p = (1234)$.

17 $(12345) = (15)(14)(13)(12) = (12)(23)(34)(45)$.

19 Hint: Sets A and B are equal if and only if $A \subset B$ and $B \subset A$.

21 The only idempotent permutation in S_m is e_m; the cycle type of e_m is $[1^m]$.

23(a) Hint: even + even = even.

23(b) Hint: $e_m = (12)(12)$. **23(d)** Hint: Part (c).

25 Hint: $\langle p \rangle$ is one of the subgroups of S_m that contains p.

3.3. Burnside's Lemma

1(a) $O_1 = \{1, 4\}$. **1(b)** $O_2 = \{2, 3\}$.

3(a) If $f = (12)(34)$, $g = (13)(24)$, and $h = (14)(23)$, then

$$\begin{array}{llll} e_4(1) = 1, & f(1) = 2, & g(1) = 3, & h(1) = 4; \\ f(2) = 1, & e_4(2) = 2, & h(2) = 3, & g(2) = 4; \\ g(3) = 1, & h(3) = 2, & e_4(3) = 3, & f(3) = 4; \\ h(4) = 1, & g(4) = 2, & f(4) = 3, & e_4(4) = 4. \end{array}$$

3(b) $\frac{1}{8}[4 + 0 + 0 + 2 + 2 + 0 + 0 + 0] = 1$.

3(c) G is not doubly transitive, e.g., no $p \in G$ maps 1 to 2 *and* 2 to 4. Alternatively, $\frac{1}{8}[16 + 0 + 0 + 4 + 4 + 0 + 0 + 0] = 3 > 2$.

5(a) $\frac{1}{6}[5 + 0 + 2 + 3 + 2 + 0] = 2$.

5(b) $\frac{1}{6}[6 + 1 + 3 + 4 + 3 + 1] = 3$.

5(c) $\frac{1}{4}[4 + 0 + 0 + 0] = 1$.

5(d) $\frac{1}{4}[8 + 4 + 4 + 4] = 5$.

7(b) $\frac{1}{12}[16 + 8 \times 1 + 3 \times 0] = 2$.

7(c) Hint: $\frac{1}{12}[64 + 8 \times 1 + 3 \times 0] = 6$.

9(a) Hint: Show that $o(O_x) = o(O_y)$.

9(b) Hint: If $p(1) = x$ and $q(1) = y$, then $qp^{-1}(x) = y$.

11(a) Hint: Example 3.3.17.

11(b) Hint: Exercise 9, Section 2.4.

13 It's off by about 0.03.

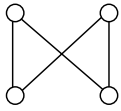
15 Hint: Mimic the proof of Theorem 3.3.18.

17 Hint: $F(e_m) = m > 1$.

19 Hint: Exercise 16.

3.4. Symmetry Groups

1



3(b) The plane symmetries are e_3, (123), and (132).

5(a) $\langle(12345)\rangle = \{e_5, (12345), (13524), (14253), (15432)\}$.

5(b) $\langle(12345)\rangle \cup \{(12)(35), (13)(45), (14)(23), (15)(24), (25)(34)\}$.

7 Hint: As in Example 3.4.6. show that half the symmetries are rotations and half are reflections.

9(b) It is the group A_4 from Exercise 7, Section 3.3.

11

q	$\tilde{q}$	q	$\tilde{q}$
(16) (25) (34)	**(18) (27) (36) (45)**	(16) (2453)	**(1647) (2835)**
(25)	**(13) (24) (57) (68)**	(15) (26)	**(17) (28)**
(34)	**(12) (34) (56) (78)**	(14) (36)	**(16) (38)**
		(16) (2354)	**(1746) (2538)**
(145632)	**(124875) (36)**	(12) (56)	**(35) (46)**
(124653)	**(126873) (45)**	(13) (46)	**(25) (47)**
(153624)	**(18) (243756)**		
(132645)	**(156843) (27)**	(24) (35)	**(14) (58)**
(154623)	**(134865) (27)**	(1265) (34)	**(1674) (2583)**
(142635)	**(18) (265734)**	(1364) (25)	**(1764) (2358)**
(135642)	**(137862) (45)**	(23) (45)	**(23) (67)**
(123654)	**(157842) (36)**	(1562)(34)	**(1476) (2385)**
(16)	**(15) (26) (37) (48)**	(1463) (25)	**(1467) (2853)**

13 Hint: It shouldn't be necessary to start over from scratch.

17(a) Hint: Each face is incident with five vertices, but 12×5 is not the number of vertices; it is too large by a factor of 3. (Why?)

19 Hint: What angle do two adjacent sides of the hexagon make?

21(a) $6 + 8 = 12 + 2$. **21(b)** $4 + 4 = 6 + 2$.

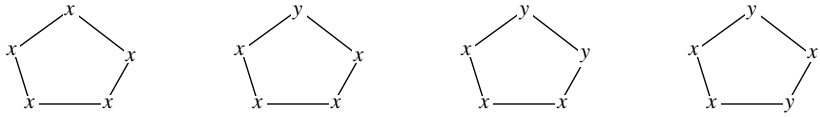
3.5. Color Patterns

1(a) $g = (y, b, w, r)$. **1(b)** $g = (b, r, y, w)$.

1(c) $P = \{(r, r, w, b), (w, r, b, r), (b, w, r, r), (r, b, r, w)\}$.

1(d) Hint: $o(P) = 8$. **1(e)** 70.

1(f) 55. (Don't forget the 1-cycles.)

3(b) 

and the four colorings obtained by interchanging the x's and y's.

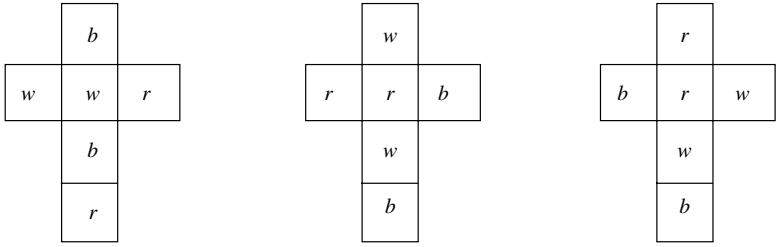
3(d) 208.

3(e) Hint: The number of patterns is an integer.

3(f) Hint: Part (e).

3(g) Hint: If $q \in S_m$ is a p-cycle, then q^i is a p-cycle, $1 \leq i < p$.

5 Hint: Exercise 5(b), Section 3.4.

7(a) 

9(a) Hint: Exercise 10, Section 3.4.

9(b) $C(4+3-1,4) = 15$.

11 Hint: Exercise 10.

13(a) Hint: Figure 3.4.7. Answer: 23.

13(b) 333. **13(c)** 4,173,775.

15 $\frac{1}{8}(n^8 + n^4 + 2n^2 + 4n)$.

17 4,783,131.

21 Hint: $\hat{p} = \hat{q}$ if and only if $f = f(q^{-1}p)$, for all $f \in C_{m,n}$, and $p = q$, if and only if $q^{-1}p = e_m$.

3.6. Pólya's Theorem

1(a) Hint: Eliminate all colorings with a white vertex from Fig. 3.6.2.

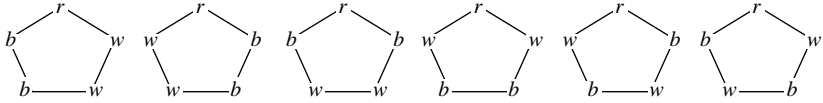
1(b) $W_G(r,b) = \frac{1}{4}[M_1^4 + M_2^2 + 2M_4]$.

3(b) Hint: Using part (a), show that $W_G(r,w,b) = (r^3 + w^3 + b^3) + (r^2w + r^2b + rw^2 + rb^2 + w^2b + wb^2) + 2rwb$.

3(c) Hint: Recall that a system of distinct representatives consists of one coloring from each of the 11 color patterns. In particular, more than one correct answer is possible.

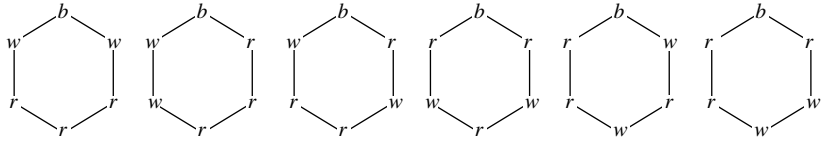
5(b) Hint: Compare with Exercise 3(c), Section 3.5.

5(e)



7(a) $W_G(r,w,b) = M_{[6]} + M_{[5,1]} + 3M_{[4,2]} + 3M_{[3^2]} + 3M_{[4,1^2]} + 6M_{[3,2,1]} + 11M_{[2^3]}$.

7(b)



9 $W_G(r,w,b) = M_{[8]} + M_{[7,1]} + 3M_{[6,2]} + 3M_{[5,3]} + 7M_{[4^2]} + 3M_{[6,1^2]} + 7M_{[5,2,1]} + 13M_{[4,3,1]} + 22M_{[4,2^2]} + 24M_{[3^2,2]}$.

11 There are five patterns of weight $r^2w^2b^2$.

13 $W_G(r,w,b,y) = M_{[4]} + M_{[3,1]} + M_{[2^2]} + M_{[2,1^2]} + 2M_{[1^4]}$.

15(a) 1. **15(b)** 1. **15(c)** 2.

17 $\frac{1}{3}\binom{15}{5,5,5} = 252,252$.

19(a) 3. **19(b)** 2. **19(c)** Hexagon.

19(d) No, it is much easier simply to exhibit all possible inequivalent "color" patterns.

3.7. The Cycle Index Polynomial

1 $Z_3 = \frac{1}{6}(s_1^3 + 3s_1s_2 + 2s_3)$.

3 $\frac{1}{6}(n^3 + 3n^2 + 2n) = (n+2)(n+1)n/6 = C(3+n-1,3)$.

5(a) Hint: Figure 3.4.5. **5(b)** Hint: Figure 3.4.7.

11 Hint: Exercise 8.

13 Hint: Use "0" to represent "10" in the disjoint cycle factorization of $\tilde{p} \in S_5^{(2)} \subset S_{10}$. Use Exercise 8 and mimic Example 3.7.15.

19 Hint: Exercise 18 in this section and Exercise 17(b) in Section 2.5. (Compare with Equation (2.6) in Section 2.2.)

23(b) Hint: For matrix L_3, the diagonal product $\prod_p$ corresponding to permutation $p \in S_3$ is given in the following table. Show that $\text{per}(L_3) = \sum \prod_p = 6Z_3(M_1, M_2, M_3)$. Use Theorem 3.7.8(a).

p	e_3	(12)	(13)	(23)	(123)	(132)
$\prod_p$	M_1^3	M_1M_2	0	$2M_1M_2$	$2M_3$	0

25(b) $H_{5-3}(x,y,z) = H_2(x,y,z) = M_{[2]}(x,y,z) + M_{[1^2]}(x,y,z)$, so $H_{5-3}(1,2,3) = [1^2 + 2^2 + 3^2] + [1 \times 2 + 1 \times 3 + 2 \times 3] = 14 + 11 = 25 = S(5,3)$.

CHAPTER 4

4.1. Difference Sequences

1(a) $a_{497} = 1492$. **1(b)** $a_{497} = 1066$. **1(c)** $a_{497} = 2004$.

3(c)
$$\begin{array}{cccccccccc} 3 & 4 & 9 & 18 & 31 & 48 & 69 & 94 & 123 & \cdots \\ 1 & 5 & 9 & 13 & 17 & 21 & 25 & 29 & \cdots & \\ 4 & 4 & 4 & 4 & 4 & 4 & 4 & \cdots & & \\ & & & & \cdots & & & & & \end{array}$$

3(d) Hint: Equation (4.10).

3(e) $b_n = \frac{1}{6}(4n^3 - 9n^2 + 23n + 6)$.

5(a)
$$\begin{array}{cccccccc} 1 & 2 & 4 & 8 & 16 & 32 & \cdots \\ 1 & 2 & 4 & 8 & 16 & 32 & \cdots \\ 1 & 2 & 4 & 8 & 16 & 32 & \cdots \\ & & & \cdots & & & & \end{array}$$

7 Hint: Mimic Gauss's approach to summing the first n positive integers.

9 Hint: Chu's theorem.

11(c) Hint: Exercise 3(a).

11(d) $C(9,1) \times 3 + C(9,2) \times 1 + C(9,3) \times 4 = 399$.

11(e) HInt: Given that $1131 = 2n^2 - n + 3$, what is n?

11(f) The sum is 652,050.

13(a) $C(k+1,1) \times 0 + C(k+1,2) \times 1 + C(k+1,3) \times 2 = k(k+1)(2k+1)/6$.

17 Hint: By induction, it suffices to show that x^m is a linear combination of $x^{(r)}/r!$, $0 \le r \le m$.

19(c) Hint: $p_m(n) - p_{m-1}(n-1) = p_m(n-m)$, $1 < m < n$.

21(c) $f(x) = \frac{1}{6}[x^3 + 6x^2 + 5x + 6]$.

21(d) $f(x) = \frac{1}{6}[x^3 + 6x^2 + 5x + 6]$.

23(a) Hint: One possibility is induction on n; another involves proving that $\Delta^4 S(n+2, n) = 3$, $n \geq 0$; a third approach counts the partitions of $\{1, 2, \ldots, n+2\}$ into n subsets.

23(b) Hint: One approach is to use induction on n; another uses part (a).

25 $f(n) = C(n, 0) + 5C(n, 1) + 6C(n, 2)$.

27(a) $S(n+1, n) = 0 \times C(n, 0) + 1 \times C(n, 1) + 1 \times C(n, 2) = C(n+1, 2)$.

27(b) Hint: Recall that $S(n+1, n)$ is the number of ways to partition an $(n+1)$-element set into the disjoint union of n nonempty subsets.

29(a) Hint: Exercise 7.

29(b) Hint: Show that $n = (r - s)(r + s)$.

31 Hint: Exercise 29(a).

33 Hint: Show that any such n is a difference of squares; use Exercise 32.

4.2. Ordinary Generating Functions

1 Hint: $C(m, n) = 0$, $n > m$. (A closed formula for $g(x) = \sum_{n \geq 0} C(n, r)x^n$, where r is a fixed but arbitrary nonnegative integer, can be found in Theorem 4.2.11.)

3(a) $g(x) = (1 - x)/(1 - 3x - 2x^2)$.

3(b) $(2 - 3x)/(1 - 2x + 3x^2)$.

5 Hint: Factor $1 - 3x - 10x^2 + 24x^3$.

7 Hint: This is the Maclaurin series expansion from calculus.

11(a) $g(x) = x^4 + 4x^5 + 10x^6 + 16x^7 + 19x^8 + 16x^9 + 10x^{10} + 4x^{11} + x^{12}$.

11(b) Hint: From part (a), the coefficient of x^7 in $g(x)$ is $a_7 = 16$. Show that 12 compositions of 7 having 4 parts, none of which is larger than 3, can be obtained by rearranging the parts of the partition $[3, 2, 1^2]$, and that the remaining 4 come from rearranging the parts of $[2^3, 1]$.

11(d) Using your answer to part (a), show that $a_7 = 16 = a_9$.

13 Hint: This gives an independent proof that Example 4.2.10 ends with a correct solution.

15 $b_0 = a_0$ and $b_{n+1} = \Delta a_n$, $n \geq 0$.

19(a) Hint: Corollary 2.2.3.

19(d) Hint: Section 1.5, Exercise 11.

25(a) $g(x) = 1/(1-3x)$.

25(b) Hint: $n^3 = C(n,1) + 6C(n,2) + 6C(n,3)$.

27(a) $a_n = n - 1 + 1/(n+1) = n^2/(n+1)$.

27(b) Hint: $D_x(xf(x)) = \sum_{n\geq 0} n^2 x^n$.

4.3. Applications of Generating Functions

1(a) $C(-3,4) = 15$. **1(b)** $C(-4,3) = -20$.

1(c) $C\left(\frac{2}{3},2\right) = -\frac{1}{9}$. **1(d)** $C\left(-\frac{2}{3},2\right) = \frac{5}{9}$.

3 Hint: Example 4.3.2.

5 Hint: If all else fails, try induction.

9 Hint: Exercise 6, Section 4.2, and the ratio test.

13 Hint: Exercise 10.

15 Hint: Exercises 13–14.

17(a) $g(x) = (1+x+x^2)(1+x^2+x^4)(1+x^3+x^6)\cdots(1+x^r+x^{2r})\cdots$

19(c) Suppose π is a distinct m-part partition of n. What's left when the first column is removed from its Ferrers diagram $F(\pi)$?

19(e) Hint: Suppose $\pi = [\pi_1, \pi_2, \ldots, \pi_m] \vdash n$ satisfies $\pi_1 > \pi_2 > \cdots > \pi_m > 0$. Define $\varphi(\pi) = [\mu_1, \mu_2, \ldots, \mu_m]$ by $\mu_i = \pi_i - (m-i)$, $1 \leq i \leq m$. Show that φ is a one-to-one function from the partitions of n having distinct parts and length m, onto the m-part partitions of $n - C(m,2)$.

21 Hint: $x^m = \sum_{r\geq 1} S(m,r)x^{(r)}$.

23 Hint: In Theorem 4.3.5, $f_r(x) = xf_{r-1}(x)/(1-rx)$.

27(a) $(1+x+x^2+\cdots+x^{10})^4 = [(1-x^{11})/(1-x)]^4$.

27(b) $(x+x^3+x^5+\cdots)^4 = [x/(1-x^2)]^4$.

27(c) $(x^2+x^3+x^4+x^5)(x^7+x^8+x^9)(x^4+x^5+x^6+\cdots)(1+x+x^2+\cdots+x^6) = x^{13}(1-x^4)(1-x^3)(1-x^7)/(1-x)^4$.

27(d) $1/(1-x)^4$. (See Equation (4.29).)

29(a) $[x/(1-x)]^8$. **29(b)** $[x^3/(1-x)]^8$.

31(a) $g_k(x) = [x+x^2+\cdots+x^6]^k = [(x-x^7)/(1-x)]^k$.

31(d) $a_4(20) = 35$.

35(a) Hint: Show that the coefficient of x^n in the product

$$(1 + a_1x + a_1^2x^2 + \cdots)(1 + a_2x + a_2^2x^2 + \cdots)\cdots(1 + a_mx + a_m^2x^2 + \cdots)$$

is a sum of terms $a_1^{n_1}a_2^{n_2}\cdots a_m^{n_m}$, one for each of the $C(n + m - 1, n)$ nonnegative integer solutions to $n_1 + n_2 + \cdots + n_m = n$.

35(e) Hint: $H_3(a, b, c) = [(a^3 + b^3 + c^3) + (a^2b + a^2c + ab^2 + ac^2 + b^2c + bc^2) + abc], H_2(a, b, c) = [(a^2 + b^2 + c^2) + (ab + ac + bc)], H_1(a, b, c) = E_1(a, b, c) = (a + b + c), E_2(a, b, c) = (ab + ac + bc)$, and $E_3(a, b, c) = abc$.

35(f) Hint: Part (d).

37 Hint: Make appropriate choices for $a_1, a_2, \ldots, a_m$ in Exercise 35(d).

39(f) Hint: Show that the right-hand side obeys the same boundary conditions and recursion as the left-hand side, i.e., confirm the analogs of parts (c) and (e) for the right-hand side.

4.4. Exponential Generating Functions

1(a) $a_n = n2^{n-1}$, $n \geq 0$. **1(b)** $a_n = 1 + 3^n$, $n \geq 0$.

1(c) Hint: Equation (4.52).

3(f) Hint: It is a consequence of the mean value theorem that if $f'(x) = g'(x)$ for all x in some open interval I, then there exists a constant C such that $g(x) = f(x) + C$, $x \in I$.

3(g) Hint: Part (f).

5(e) Hint: $S(n + 1, r) = S(n, r - 1) + rS(n, r)$.

5(g) Hint: $B_0 = 1 = \exp(0)$.

7 Hint: Equation (4.59).

9(a) Hint: Apply the fundamental theorem of calculus to the $k = 2$ case of Equation (4.58).

11(a) Hint: Equation (4.30a).

11(c) Hint: Theorem 4.4.5 and Exercise 15, Section 4.2.

13 Hint: Use Exercise 12, Section 2.3, and obtain a new proof of Theorem 4.4.5.

17 $f(x, y) = 1/(1 - x - xy)$

19

n	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
$\mu(n)$	-1	1	1	0	-1	0	-1	0	1	1	-1	0	0	1	0

21(a) Hint: One approach is this: Let $S = \{1, 2, \ldots, n\}$. Suppose $1 = d_1 < d_2 < \cdots < d_r = n$ are the distinct positive divisors of n. Let $S_i = \{k \in S : \text{GCD}(k, n) = d_i\}$, $1 \leq i \leq r$. Show that $o(S_i) = \varphi(n/d_i)$.

21(b) $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2$.

21(d) Hint: Part (a) and Corollary 4.4.19.

21(e) $6\mu(1) + 3\mu(2) + 2\mu(3) + \mu(6) = 2$.

23 Hint: Equations (4.62) and (4.66).

25 Hint: Corollary 4.4.19.

27(a) Hint: Section 4.3, Exercises 33 and 34.

27(b) Hint: Section 4.3, Exercises 34 and 35.

29 Hint: Show that $g(x)(e^x - 1) = x$.

31(b) Hint: Exercise 13, Section 2.1, and $S(n+1, r+1) - S(n, r) = (r+1)S(n, r+1)$.

31(c) Hint: From part (b), $2s_n = s_n + \sum_{r \geq 1} C(n, r)s_{n-r} = \sum_{r \geq 0} C(n, r)s_{n-r}$, $n \geq 1$, so $2g(x) = 1 + e^x g(x)$.

31(e) Hint: $1 = \sum_{k \geq 1} 1/2^k$.

33 Hint: Exercise 32.

4.5. Recursive Techniques

1(b) $|L_n^2 - L_{n-1}L_{n+1}| = 5$, $n \geq 1$.

1(c) Hint: Exercise 16(b), Section 1.6.

1(e) $\lim L_{n+1}/L_n = \varphi$.

3(a) $a_n = 3^n - 2^n$, $n \geq 0$. **3(b)** $a_n = 3^n + 2^n$, $n \geq 0$.

3(c) $a_n = 5(3^n) - 3(2^n)$, $n \geq 0$.

5(a) $a_n = 5n + 2 + 2^n$, $n \geq 0$.

5(b) $a_n = (n^2 + n + 1)2^n$, $n \geq 0$.

5(c) $a_n = (n^2 + 2n + 1)2^n$, $n \geq 0$.

7(a) $a_n = \frac{1}{2}(3n^2 - n + 6)$, $n \geq 0$. **7(b)** $a_n = (n-1)^2$, $n \geq 0$.

7(c) $a_n = \frac{1}{6}(2n^3 + 3n^2 + 7n + 12)$, $n \geq 0$.

9(a) $a_n = (n+2)3^n$, $n \geq 0$. **9(b)** $a_n = (n+2)3^n$, $n \geq 0$.

11(a) $a_n = 4(3^n) + 3(-2)^n - 2^n$, $n \geq 0$.

11(b) $a_n = (-3)^n + (2n+3)2^n$, $n \geq 0$.

11(c) $a_n = (-3)^n + (2n+3)2^n$, $n \geq 0$.

13 $L_n = \varphi^{n+1} + (-1/\varphi)^{n+1}$, $n \geq 0$, where $\varphi = (1 + \sqrt{5})/2$. (Now can you prove your conjecture in Exercise 1(b)?)

15 Hint: Suppose $a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_ka_{n-k} + w(n)$, $n \geq k$, and $b_n = c_1b_{n-1} + c_2b_{n-2} + \cdots + c_kb_{n-k} + w(n)$, $n \geq k$. Define $\{d_n\}$ (not to be confused with a difference sequence) by $d_n = b_n - a_n$. Show that $\{d_n\}$ satisfies the homogeneous recurrence $d_n = c_1d_{n-1} + c_2d_{n-2} + \cdots + c_kd_{n-k}$, $n \geq k$.

17(c) $r_n = \frac{1}{2}(n^2 + n + 2)$.

CHAPTER 5

5.1. The Pigeonhole Principle

1 Hint: Let $S = \{s_1, s_2, \ldots, s_n\}$. Consider the remainders left when $s_1 + s_2 + \cdots + s_t$ is divided by n, $1 \leq t \leq n$.

3 Hint: the midpoint of the segment joining $P_i = (x_i, y_i)$ and $P_j = (x_j, y_j)$ is $M = (\frac{1}{2}[x_i + x_j], \frac{1}{2}[y_i + y_j])$.

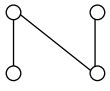
5 Hint: Consider the average weight of the n objects.

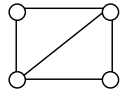
7 Hint: Factor each element of S as the product of a power of 2 and an odd integer.

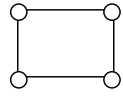
9(b) The other three isomorphisms are (c, b, a, d), (b, c, d, a), and (c, b, d, a).

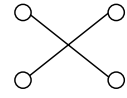
11 Hint: List the four nonisomorphic graphs on three vertices.

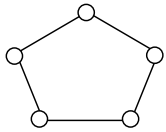
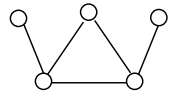
13 Hint: The first theorem of graph theory.

15(a) 

15(b) 

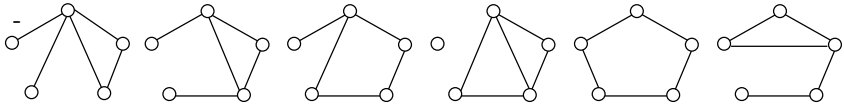
15(c) 

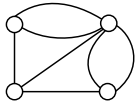
15(d) 

17(a)  or 

23(a) 5×3 is odd.

23(b) The largest vertex degree cannot be as large as the number of vertices of positive degree.

25 - 

27(a) 

29(a) Hint: "A picture is worth a thousand words."

5.2. Edge Colorings and Ramsey Theory

3(a) Hint: Using $N(2,4) = 4$ and $N(3,3) = 6$, mimic the proof that $N(3,3) \leq 6$.

3(b) Hint: Show directly, without using Theorem 5.2.3, that $N(4,4) \leq N(3,4) + N(4,3)$.

5 Hint: Corollary 5.2.10 or Fig. 5.2.6.

9(b) $f_3(x) = \frac{1}{6}[(1+x)^3 + 3(1+x)(1+x^2) + 2(1+x^3)] = 1 + x + x^2 + x^3$.

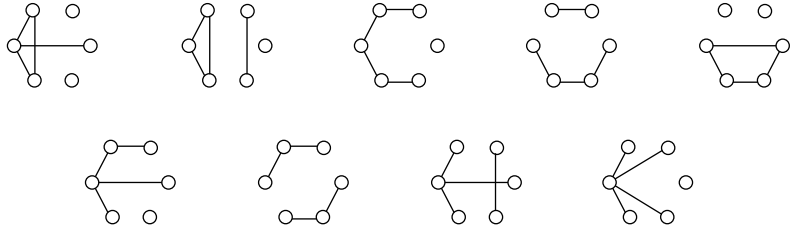
11 Either the edges are adjacent or they are not.

13(a) Hint: Draw some pictures.

13(b) In view of Example 3.7.17, the coefficient of x^3 in $f_6(x)$ is $\frac{1}{720}[455 + 15(35+28) + 40(1+4) + 60(1+18) + 180(1) + 144(0) + 120(1+2) + 40(5) + 120(1)] = 5$.

15 Hint: Examples 3.7.17 and 5.2.9.

17(a)



17(b) The complements of the graphs in part (a).

19 Hint: Consider their complements.

21(a) Hint: Six colorful pictures should suffice.

21(c) Hint: Figure 5.2.2.

5.3. Chromatic Polynomials

1(a) $p(G,x) = x(x-1)(x-2)(x^2-3x+3)$.

1(b) Hint: Show that this graph is isomorphic to the graph in part (a).

1(c) Hint: Theorem 5.3.11. **1(d)** Hint: Equation (5.13).

1(e) $p(G,x) = x(x-1)(x-2)^3$.

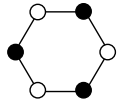
3(b) $p(G,x) = x(x-1)(x-2)(x-3)(x^2-4x+5)$.

5(a) Hint: This is a statement about binomial coefficients.

5(b) Hint: This is a statement about Stirling numbers of the first kind.

7(a) $p(G,x) = x^{(5)} + x^{(4)} = x(x-1)(x-2)(x-3)^2$.

7(b) $p(G,x) = x^{(6)} + 3x^{(5)} + 3x^{(4)} + x^{(3)} = x(x-1)(x-2)(x^3 - 9x^2 + 29x - 32)$.

9(a)  ;  .

9(b) $p(C_4, x) = x(x-1)(x^2 - 3x + 3)$; $p(C_6, x) = x(x-1)(x^4 - 5x^3 + 10x^2 - 10x + 5)$.

11(b) Hint: Compute $f(1)$.

13 Hint: Chromatic reduction.

15 Hint: Theorem 5.3.23.

17(a) Hints: $K_{s,t} = K_s^c \vee K_t^c$ and $x^m = \sum_{r=1}^{m} S(m,r)x^{(r)}$.

17(b) $p(K_{2,3}, x) = (x^{(1)} + x^{(2)}) \vee (x^{(1)} + 3x^{(2)} + x^{(3)}) = x^{(2)} + 4x^{(3)} + 4x^{(4)} + x^{(5)}$.

17(c) $p(K_{3,3}, x) = x^{(6)} + 6x^{(5)} + 11x^{(4)} + 6x^{(3)} + x^{(2)}$.

19(a) Hint: From the answer to Exercise 9(b), $p(C_4, x) = x(x-1) \times (x^2 - 3x + 3)$.

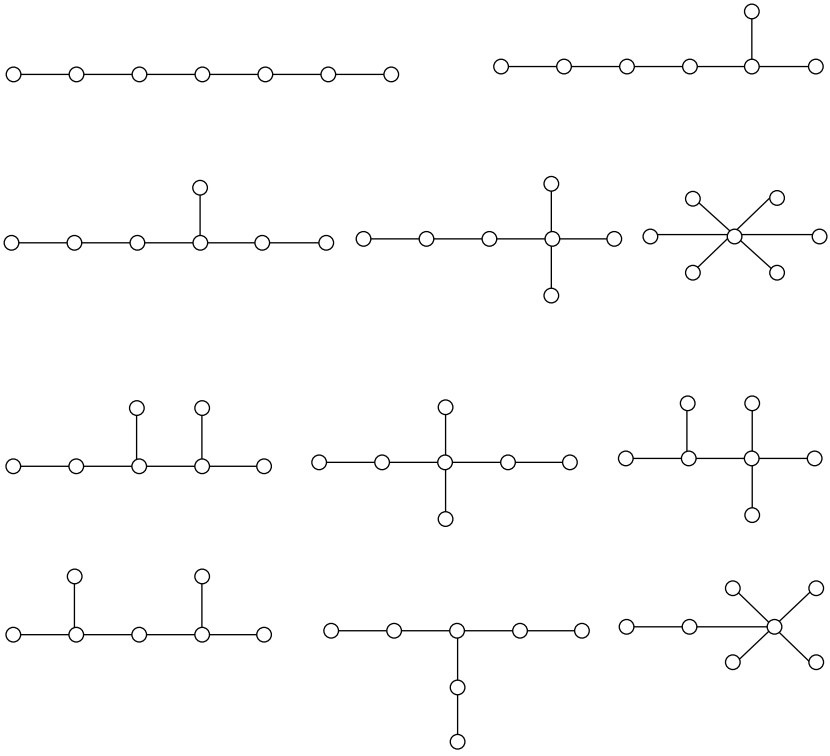
19(b) Hint: Let $f(x) = p(K_{4,3}, x) = x(x-1)(x^5 - 11x^4 + 55x^3 - 147x^2 + 204x - 115)$. Show that $f(1.7) \doteq -0.58$ and $f(1.8) \doteq +0.15$.

19(c) Hint: Use the fact that the coefficients of $p(G, x)$ alternate in sign.

21 Hint: Factor $f(x)$.

23(a) Hint: How many of the 11 nonisomorphic graphs on 4 vertices are trees?

23(c)



25 Hint: Explain why this is a restatement of Exercise 7(b).

27(a) Hint: One of them can be found in Exercise 1.

29 Hint: Show by induction on the number of edges that $p(G,t)$ is nonzero with sign $(-1)^{n-c}$, $t \in (0,1)$, where c is the number of components.

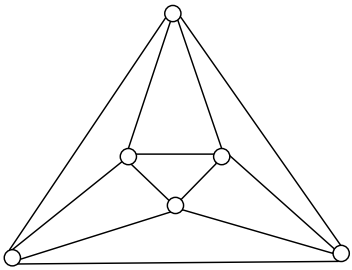
31(a) Hint: Revisit the proof of Theorem 5.2.5.

31(b) Hint: Induction on $s+t$.

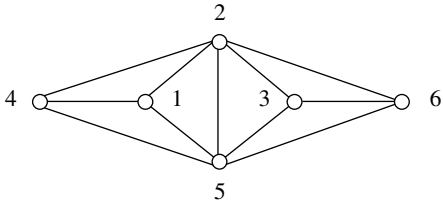
5.4. Planar Graphs

1 Hint: Lemma 5.3.17.

3(c)



5(a)

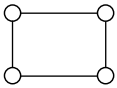


7 Hint: $K_{3,3}$ is bipartite.

9 Hint: Show that G has a nonplanar subgraph.

13(b) The dual of a cube is a regular octahedron.

17



19 Hint: If H^{d} is a graph, then $G = H^{\mathrm{d}}$. Otherwise, let G be a graph obtained from H^{d} by subdividing some of its edges. Explain why $G_{\mathrm{d}} = H$.

5.5. Matching Polynomials

3(a) $M(K_6,x) = x^6 - 15x^4 + 45x^2 - 15$.

3(c) $M(P_7,x) = x^7 - 6x^5 + 10x^3 - 4x$.

3(e) $M(C_7, x) = x^7 - 7x^5 + 14x^3 - 7x$.

5 Hint: If G_1 and G_2 are isomorphic graphs, prove that there is a one-to-one correspondence between the r-matchings of G_1 and the r-matchings of G_2.

7(b) If e is the "middle" edge of P_4, then the 1-matching $M = \{e\}$ is a maximal matching but not a maximum matching.

9(a) K_3. **9(b)** $K_{1,2}$.

9(e) Hint: The clique number, $\omega(G) = \alpha(G^c)$.

9(g) $K_4 - e$.

13(a) Both have degree sequence $(4, 3^2, 2^4, 1^2)$.

13(b) Both have chromatic polynomial $x(x-1)^6(x-2)^2$.

13(c) Both have matching polynomial $x^9 - 10x^7 + 29x^5 - 25x^3 + 5x$.

15 Hint: The sum of the characteristic roots of the $n \times n$ matrix $A = (A_{ij})$ is the *trace* of A, defined by $\text{tr}(A) = \sum a_{ii}$.

17 Hint: Use the quadratic formula to find squares of roots. Then use a calculator. Two-decimal-place accuracy should suffice.

19(c) Hint: Exercise 14, Section 5.3.

23 Hint: Like the determinant, the permanent can be expanded by rows or columns. For example, if A_{ij} is the matrix obtained from A by deleting row i and column j, then

$$\text{per}(A) = \sum_{j=1}^{n} a_{ij}\,\text{per}(A_{ij}), \qquad 1 \le i \le n.$$

27 Let $G_1 = (V, E)$ and $G_2 = (V, F)$, where $V = \{1, 2, \ldots, n\}$. Suppose $f \in S_n$ is fixed but arbitrary. Let $A(G_1) = (a_{ij})$, $A(G_2) = (b_{ij})$, and $P = P(f) = (\delta_{if(j)})$. We will prove the equivalent formulation that f is an isomorphism from G_1 onto G_2 if and only if $P^{-1}A(G_2)P = A(G_1)$. Because the (i,j)-entry of P^{-1} is the (j,i)-entry of P, the (i,j)-entry of $P^{-1}A(G_2)P$ is

$$\sum_{s,t=1}^{n} \delta_{sf(i)} b_{st} \delta_{tf(j)} = b_{f(i)f(j)}.$$

Now, $b_{f(i)f(j)} = a_{ij}$, $1 \le i, j \le n$, if and only if $F = \{\{f(i), f(j)\} : \{i,j\} \in E\}$, if and only if $f : V \to V$ is an isomorphism from G_1 onto G_2.

5.6. Oriented Graphs

1(a) All $2^3 = 8$ orientations of the tree $K_{1,3}$ are acyclic.

1(c) Hint: Evaluate $(-1)^4 x(x-1)(x-2)^2$ at $x = -1$.

3(a) $Q = \begin{pmatrix} -1 & 0 & 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \end{pmatrix}$.

5(a) $L(G) = \begin{pmatrix} 3 & -1 & -1 & 0 & -1 \\ -1 & 2 & -1 & 0 & 0 \\ -1 & -1 & 3 & -1 & 0 \\ 0 & 0 & -1 & 2 & -1 \\ -1 & 0 & 0 & -1 & 2 \end{pmatrix}$.

5(b) Hint: $t(G) = 11$.

7(a) $s(K_{1,3}) = (4, 1, 1, 0)$. **7(b)** $s(K_4 - e) = (4, 4, 2, 0)$.

9 Hint: Exercise 8.

11(a) $s(C_6) = (4, 3, 3, 1, 1, 0)$ majorizes $d(C_6) = (2, 2, 2, 2, 2, 2)$ because $4 \geq 2$; $4 + 3 \geq 2 + 2$; $4 + 3 + 3 \geq 2 + 2 + 2$; ... ; and $4 + 3 + 3 + 1 + 1 + 0 = 2 + 2 + 2 + 2 + 2 + 2$.

11(b) Hint: $s(G) = (5, 3, 3, 2, 1, 0)$.

11(c) Hint: $s(G) = (5, 5, 3, 3, 2, 0)$.

13 Hint: Show that $L(G) + L(G^c) = nI_n - J_n$, where J_n is the $n \times n$ matrix each of whose entries is 1; use the fact from linear algebra that commuting symmetric matrices are simultaneously diagonalizable.

15 Hint: Exercise 13.

17 Hint $G_1 \vee G_2 = (G_1^c + G_2^c)^c$. Use Exercise 13.

19(a) Hint: Because $s(K_{2,2}) = (4, 2, 2, 0)$, it suffices to show (independently) that $t(K_{2,2}) = [4 \times 2 \times 2]/4 = 4$.

19(b) Hint: $s(K_{2,3}) = (5, 3, 2, 2, 0)$.

19(c) Hint: $s(K_{1,4}) = (5, 1, 1, 1, 0)$.

21(a) $s(P_4) = (2 + \sqrt{2},\ 2,\ 2 - \sqrt{2},\ 0)$.

23(a) $s(G) = (4, 3, 3, 1, 1, 0)$. **23(b)** $s(G^c) = (5, 5, 3, 3, 2, 0)$.

23(c) $s(H) = (5, 3, 3, 2, 1, 0)$. **23(d)** $s(H^c) = (5, 4, 3, 3, 1, 0)$.

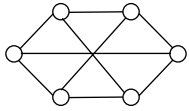
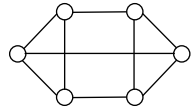
23(g) $s(G + G^c) = (5, 5, 4, 3, 3, 3, 3, 2, 1, 1, 0, 0)$.

5.7. Graphic Partitions

1 Only (3,1) fails to weakly majorize (2.5,1.5,1).

3(a) The partitions $[6^2, 2^2]$, $[5^4]$, $[3, 2^2, 1^2]$, and $[2, 1^5]$ are not graphic.

5(a) C_6 and the union, $C_3 + C_3$.

5(b)  and 

7 Hint: Each graph will have three edges, but the numbers of vertices may differ.

9 Hint: Mimic the argument that led to Inequalities (5.40).

11 *Threshold Algorithm.* Suppose $\tau = [\tau_1, \tau_2, \ldots, \tau_n] \vdash 2m$ is a threshold partition.

```
1. Let V = {1,2,..., n} and E = ∅.
2. For i = 1 to f (τ).
3. For j = i to τ_i.
4. E = E ∪ {{i,j + 1}}.
5. Next j.
6. Next i.
7. Return G = (V, E).
```

13(a) Hint: One alternative is to show that $\det(xI_4 - L(G)) = x(x-1)(x-3)\times(x-4)$. Another is to find eigenvectors for $L(G)$ corresponding to eigenvalues $\lambda = 1$, 3, and 4.

15(a) The combination $f(v) = d_G(v)$, $v \in V(G)$, and $t = 3$ will work.

17(a) Hint: If $f(v) = d_G(v)$, $v \in V(G)$, is a threshold labeling, then $4 > t \geq 5$. (Why?)

19 Hint: The easiest solution uses the characterization of threshold graphs from Exercise 18. Can you find a more revealing solution?

21 Hint: If you have access to appropriate computer software, work out the Laplacian eigenvalues of the Petersen graph from Example 5.1.7. Otherwise, look for examples that have $n \leq 6$ vertices.

23 Hint: To show that a graph is split, it suffices to exhibit an appropriate partitioning of its vertices. One way to do that is to *color* the vertices of the clique one color and the vertices of the independent set a different color, e.g., dark and light.

25 Hint: The degree sequence of a connected graph on five vertices is a partition with five parts, the largest of which is at most 4.

CHAPTER 6

6.1. Linear Codes

1(a) $\text{wt}(110100010) = 4$. **1(b)** $\text{wt}(001011101) = 5$.

3(a) S, itself, is a basis. **3(c)** Hint: $\dim(\mathscr{L}(S)) = 3$.

5 Hint: $\mathscr{L}(S)$ is a $(4, 2^3, 2)$ code.

7 Hint: Consider $S = \{1100, 0011, 1111\}$.

9 Hint: $\{u \in F^n \ : \ \text{wt}(u) = 1\} \subset S$.

11 Hint: If $w = x_1x_2x_3x_4$ then $w \cdot 1100 = 0$, if and only if $x_1 + x_2 = 0$, if and only if $x_1 = x_2$.

13(a) Hint: Lemma 6.1.18.

15(b) One solution is $\{110000, 101010, 100001\}$. (Your solution should consist of three vectors that span the same space.)

17(b) Hint: Show that $C_2(n,k) = C_2(n-1,k-1) + 2^k C_2(n-1,k)$ by distinguishing two cases according to whether the (k,n)-entry is a pivot entry.

19 Hint: If $u \cdot w = 0$ and $v \cdot w = 0$, then $(au + bv) \cdot w = a(u \cdot w) + b(v \cdot w) = 0$ for all $a, b \in F$. Conversely, if $(au + bv) \cdot w = 0$ for all $a, b \in F$, then $(au + bv) \cdot w = 0$ when $a = 1$ and $b = 0$.

6.2. Decoding Algorithms

3(a) $\mathscr{H}_2$ is a $(3, 2, 3)$ code. **3(b)** $\mathscr{H}_2 = \{000, 111\}$.

3(c) $G = (1 \quad 1 \quad 1)$.

5(a) Hint: Suppose $1 \le k \le m$. Let S be the set of integers j, between 1 and $2^m - 1$ inclusive, such that the kth digit in the binary expansion of j is 1. Use the fundamental counting principle to show that $o(S) = 2^{m-1}$.

7(a) $\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$. **7(b)** $\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$.

9(a) $\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$. **9(b)** $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$.

11(a) Hint: $s = 00$. **11(b)** $c = 01011$. **11(c)** $c = 01110$.

13(a) $c = 0001111$. **13(b)** $c = 0001111$.

13(c) $c = 0111100$.

15(b) Hint: $X^{\mathrm{t}} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$.

17(a) $c = 1011010$. **17(b)** $c = 0010110$.

17(c) $c = 0010110$. **17(d)** v is a codeword.

19 Hint: Exhibit an invertible linear transformation from $\mathscr{H}_3$ onto F^4.

21(a) $d = 2$.

21(b) Hint: There are eight such words.

23 Hint: Suppose s_1 and s_2 are two syndromes. Let $X_i = \{v \in F^n : s_i \text{ is the syndrome of } v\}$, $i = 1, 2$. Show that $o(X_1) = o(X_2)$.

25(c) Hint: If all else fails, try induction.

27 $\mathscr{C}$ is an (8, 16, 4) code.

29(b) Hint: Why is it enough to show that $C(23, 0) + C(23, 1) + C(23, 2) + C(23, 3) = 2^{11}$?

6.3. Latin Squares

1 Hint: Explain why $1 + 2 + \cdots + n^2 = nm$.

3 Hint: Begin by setting $x = 0$, $y = 1$, and $z = 2$.

5 Use A and B from Fig. 6.3.6 together with

$$C = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix}.$$

7 Hint: Suppose $p, g, h \in G$ satisfy $pg = ph$.

9 Hint: Theorem 6.3.6 and Exercise 8.

11 Hint: If A, P, and Q are $n \times n$ matrices, then $\det(PAQ) = \det(P) \times \det(A) \det(Q)$.

13 Because $n = 6 = 4(1) + 2$ and $3 = 4(0) + 3$ is a prime factor of the square-free part of 6, it follows from the Bruck–Ryser theorem (and Theorem 6.3.16) that there does not exist a family of *five* pairwise orthogonal Latin squares of order 6.

15 Hint: A recipe can be found in the proof of Theorem 6.3.8.

17(a) $A \otimes B = \begin{pmatrix} 1 & 0 & 2 & 2 & 0 & 4 \\ 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 2 & 1 & 0 & 4 & 2 \\ 3 & 0 & 6 & 4 & 0 & 8 \\ 3 & 3 & 3 & 4 & 4 & 4 \\ 0 & 6 & 3 & 0 & 8 & 4 \end{pmatrix}$.

17(b) $A \otimes B = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$.

19 Hint: Exercise 18 and Theorem 6.3.9.

21(a) Hint: Exercise 6.

21(c) $A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix}$.

6.4. Balanced Incomplete Block Designs

1 The die model comes close to being a BIBD. However, with respect to the standard numbering of dice, face 1 and j share two vertices, $2 \leq j \leq 5$, but faces 1 and 6 share none.

3(a) Hint: The dependent parameter, q, is an integer.

3(b) Hint: The dependent parameter, b, is an integer.

5(b) The triple of parameters for $\mathscr{D}^c$ is $(v, v-k, b+\lambda-2q)$.

5(d) The complement of the design afforded by the finite projective plane of order 2 is a (7,4,2)-design.

5(e) Hint: Figure 6.4.2.

7(b) Hint: Mimic the proof of Theorem 6.4.12 using part (a).

7(c) Hint: Part (b) and the assumption that $v > k$.

7(d) Hint: Part (c).

7(e) Hint: Part (d).

9(a) Hint: Example 6.4.8.

11(a) Show that $AA^t = 3I_{11} + 3J_{11}$.

11(b) Hint: Theorem 6.4.19.

15 Hint: Show that $\det(HH^{\mathrm{t}}) = n^n$.

17 Hint: Theorem 6.4.19.

19(a) Hint: Exercise 18.

19(c) Hint: Exercise 5.

21(b) Hint: Exercise 18.

21(c) Hint: Of the n^2 entries in a Hadamard matrix of order n, how many are equal to 0?

23 Hint: Corollary 6.4.7 and Theorem 6.4.19.

27 Hint: $A = \frac{1}{2}(K + J_{n-1})$.

Appendix A2 Sorting Algorithms

1(a)
```
1. Input N and set S = 0.
2. For I = 1 to N.
3. S = S + I.
4. Next I.
5. Write S.
```

1(b)
```
1. Input N.
2. Write N × (N − 1)/2.
```

3(a) Hint: Since "Big Oh" involves an upper bound, it suffices to consider a "worst-case" scenario.

5
```
 1. L = M = 10.
 2. For I = 1 to M.
 3. "Read" (from data steps) X(I).
 4. Next I.
 5. For I = 1 to L.
 6. Read Y(I).
 7. Next I.
 8. J = K = T = 1.
 9. If X(J) > Y(K) then go to step 13.
10. A(T) = X(J).
11. J = J + 1 and T = T + 1.
12. Go to step 15.
13. A(T) = Y(K).
14. K = K + 1 and T = T + 1.
15. If J > M then go to step 18.
16. If K > L then go to step 22.
```

```
17. Go to step 9.
18. For I = K to L.
19. A (M + I) = Y(I).
20. Next I.
21. Go to step 25.
22. For I = J to M.
23. A(L + I) = X(I).
24. Next I.
25. For I = 1 to M + L.
26. Write A(I).
27. Next I.
28. DATA 1,2,3,4,4,4,5,5,5,7
29. DATA 2,3,3,4,5,5,6,6,8,9
```

9(a)

```
 1. Input N.
 2. For I = 1 to N.
 3. R (I) = ⌊ 1000 × RND⌋.
3.1. Write R(I).
 4. Next I.
4.1. Start = Time.
 5. T = 0.
 6. For J = 1 to N − 1.
 7. If R (J) ≤ R(J + 1) then go to step 12.
 8. T = 1.
 9. X = R(J).
10. R(J) = R(J + 1).
11. R(J + 1) = X.
12. Next J.
13. If T = 1 then go to step 5.
14. For I = 1 to N.
15. Write R(I).
16. Next I.
17. Write Time − Start.
```

Index of Notation

Combinatorics, Second Edition, by Russell Merris.
ISBN 0-471-26296-X

$\Delta^{k+1}a_n$	$\Delta^k a_{n+1} - \Delta^k a_n$	256
$\Delta f(n)$	$f(n+1) - f(n)$	255
$\mathscr{D}$	BIBD	463
$\det(A)$	determinant of matrix A	227, 497
$d(G)$	degree sequence	341
$D(G)$	diagonal matrix of vertex degrees	398
$d(n)$	no. divisors of n	312
$D(n)$	derangement number	141
D_n	dihedral group	207
$d(b,w)$	distance from b to w	34
$d(u,w)$	distance from u to w	364
$d(v) = d_G(v)$	degree of vertex v in G	341
$E(G)$	edge set of graph G	338
$E_r(x_1, x_2, \ldots, x_n)$	elementary symmetric function	88
e_m	identity of S_m	178
$e(n,t)$	$E_t(1,2,\ldots,n)$	90
F	$\{0,1\}$	34
F^n	set of binary words of length n	34
$F(\pi)$	Ferrers diagram of partition π	79
$f(\pi)$	trace of partition π	409
$f(D)$	image$(f) = \{f(x) : x \in D\}$	175
$F(p)$	number of fixed points of p	197
fH	$\{fh : h \in H\}$	190
$F_{m,n}$	set of all functions from $\{1,2,\ldots,m\}$ to $\{1,2,\ldots,n\}$	118
$f^{-1}(y)$	$\{x : f(x) = y\}$	120
f^{-1}		177
$\gamma_i(G)$	adjacency (graph) eigenvalue	392
$G = (V,E)$	Graph G	338
G^{c}	complement of graph G	343
G^{d}	dual pseudograph	378
G_{d}	graph obtained from G^{d}	379
G_x	$\{p \in G : p(x) = x\}$	189
$G_1 + G_2$	graph union	360
$G_1 \vee G_2$	graph join	361
$G - e$	edge deleted subgraph	357
G/e	graph obtained from $G - e$	358
$g \circ f = gf$	composition of g and f	176
$G_{m,n}$	nondecreasing functions in $F_{m,n}$	125, 245
$g(n,m)$	number of graphs	351
$G - u$	vertex deleted subgraph	385
$G[W]$	subgraph induced on W	348
$x \equiv y (\mathrm{mod}\ G)$	equivalence modulo G	195

$\mathscr{H}_m$	Hamming code	433
H_m	parity check matrix for $\mathscr{H}_m$	432
$H_n(x_1, x_2, \ldots, x_k)$	Homogeneous symmetric function	245
fH	$\{fh : h \in H\}$	190
image(f)	$f(D)$ where $D = \text{domain}(f)$	175
I_n	identity matrix	498
J_v	$v \times v$ matrix of 1's	466
K_n	complete graph	343
$K_{s,t}$	complete bipartite graph	361
$\ker(A)$	kernel of matrix A	496
$\lambda_i(G)$	Laplacian (graph) eigenvalue	401
$\ell(\pi)$	length of partition π	77
$L(G)$	Laplacian matrix	398
$\mathscr{L}(S)$	linear span of set S	424, 496
$\mu(G)$	matching number	383
$\mu(n)$	Möbius function	313
$M(G, x)$	matching polynomial	384
$d \mid n$	d divides n	312
$M_r(x_1, x_2, \ldots, x_n)$	rth power sum	95
(n, M, d)	binary code parameters	35
$N(n, r)$	$C(n, 0) + C(n, 1) + \cdots + C(n, r)$	36
$N(s, t)$	Ramsey number	349
$\binom{n}{r_1, r_2, \ldots, r_k}$	multinomial coefficient	5
$\binom{n}{r}$	binomial coefficient $C(n, r)$	14
$\omega(G)$	clique number	367
$o(E)$	cardinality of set E	24
$o(p)$	order of permutation p	186
O_x	$\{p(x) : x \in G\}$	195
$O(g(n))$	Big Oh	489
φ	golden ratio	282
$\varphi(n)$	Euler totient function	147
$\pi \vdash n$	π is a partition of n	77
π^*	partition conjugate to π	79
$\tilde{p}$	induced action p	212
$\hat{p}$	induced action p	219

Index

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

WILEY-INTERSCIENCE
SERIES IN DISCRETE MATHEMATICS AND OPTIMIZATION

AARTS AND KORST • Simulated Annealing and Boltzmann Machines: A Stochastic Approach to Combinatorial Optimization and Neural Computing
AARTS AND LENSTRA • Local Search in Combinatorial Optimization
ALON, SPENCER, AND ERDŐS • The Probabilistic Method, Second Edition
ANDERSON AND NASH • Linear Programming in Infinite-Dimensional Spaces: Theory and Application
ARLINGHAUS, ARLINGHAUS, AND HARARY • Graph Theory and Geography: An Interactive View E-Book
AZENCOTT • Simulated Annealing: Parallelization Techniques
BARTHÉLEMY AND GUÉNOCHE • Trees and Proximity Representations
BAZARRA, JARVIS, AND SHERALI • Linear Programming and Network Flows
CHANDRU AND HOOKER • Optimization Methods for Logical Inference
CHONG AND ŻAK • An Introduction to Optimization, Second Edition
COFFMAN AND LUEKER • Probabilistic Analysis of Packing and Partitioning Algorithms
COOK, CUNNINGHAM, PULLEYBLANK, AND SCHRIJVER • Combinatorial Optimization
DASKIN • Network and Discrete Location: Modes, Algorithms and Applications
DINITZ AND STINSON • Contemporary Design Theory: A Collection of Surveys
DU AND KO • Theory of Computational Complexity
ERICKSON • Introduction to Combinatorics
GLOVER, KLINGHAM, AND PHILLIPS • Network Models in Optimization and Their Practical Problems
GOLSHTEIN AND TRETYAKOV • Modified Lagrangians and Monotone Maps in Optimization
GONDRAN AND MINOUX • Graphs and Algorithms (*Translated by S. Vajdā*)
GRAHAM, ROTHSCHILD, AND SPENCER • Ramsey Theory, Second Edition
GROSS AND TUCKER • Topological Graph Theory
HALL • Combinatorial Theory, Second Edition
HOOKER • Logic-Based Methods for Optimization: Combining Optimization and Constraint Satisfaction
IMRICH AND KLAVŽAR • Product Graphs: Structure and Recognition
JANSON, LUCZAK, AND RUCINSKI • Random Graphs
JENSEN AND TOFT • Graph Coloring Problems
KAPLAN • Maxima and Minima with Applications: Practical Optimization and Duality
LAWLER, LENSTRA, RINNOOY KAN, AND SHMOYS, Editors • The Traveling Salesman Problem: A Guided Tour of Combinatorial Optimization
LAYWINE AND MULLEN • Discrete Mathematics Using Latin Squares
LEVITIN • Perturbation Theory in Mathematical Programming Applications
MAHMOUD • Evolution of Random Search Trees
MAHMOUD • Sorting: A Distribution Theory

Combinatorics, *Second Edition*, by Russell Merris.
ISBN 0-471-26296-X

MARTELLI • Introduction to Discrete Dynamical Systems and Chaos
MARTELLO AND TOTH • Knapsack Problems: Algorithms and Computer Implementations
McALOON AND TRETKOFF • Optimization and Computational Logic
MERRIS • Combinatorics, Second Edition
MERRIS • Graph Theory
MINC • Nonnegative Matrices
MINOUX • Mathematical Programming: Theory and Algorithms (*Translated by S. Vajdā*)
MIRCHANDANI AND FRANCIS, Editors • Discrete Location Theory
NEMHAUSER AND WOLSEY • Integer and Combinatorial Optimization
NEMIROVSKY AND YUDIN • Problem Complexity and Method Efficiency in Optimization (*Translated bv E. R. Dawson*)
PACH AND AGARWAL • Combinatorial Geometry
PLESS • Introduction to the Theory of Error-Correcting Codes, Third Edition
ROOS AND VIAL • Ph. Theory and Algorithms for Linear Optimization: An Interior Point Approach
SCHEINERMAN AND ULLMAN • Fractional Graph Theory: A Rational Approach to the Theory of Graphs
SCHRIJVER • Theory of Linear and Integer Programming
SPALL • Introduction to Stochastic Search and Optimization: Estimation, Simulation, and Control
SZPANKOWSKI • Average Case Analysis of Algorithms on Sequences
TOMESCU • Problems in Combinatorics and Graph Theory (*Translated by R. A. Melter*)
TUCKER • Applied Combinatorics, Second Edition
WOLSEY • Integer Programming
YE • Interior Point Algorithms: Theory and Analysis