Introduction to Combinatorics

Mark Wildon

Contents

Introduction

Combinatorial arguments may be found in all branches of mathematics. Many people become interested in mathematics through a combinatorial problem. But, strangely enough, at first many mathematicians tended to sneer at combinatorics. Thus one finds:

"Combinatorics is the slums of topology."

J. H. C. Whitehead (early 1900s, attr.)

Fortunately attitudes have changed, and the importance of combinatorial arguments is now widely recognised:

"The older I get, the more I believe that at the bottom of most deep mathematical problems there is a combinatorial problem."

I. M. Gelfand (1990)

Combinatorics is a very broad subject. This book gives a straightforward and motivated introduction to four related areas of combinatorics. Each is the subject of current research, and taken together, they give a good idea of what combinatorics is about. While one aim is to show a range of important techniques, the material is chosen primarily to maximize interest and accessibility. No attempt is made at a comprehensive treatment.

Outline

[This is not necessarily close to the final form of this section, but should give an idea of the planned content.]

[Estimated page count at most 420 pages: 200 pages for the main text, 30 pages for Appendices A, B and D, 180 pages, but probably less, for Appendix C (solutions to exercises).]

Part A: Enumeration

We begin with bijections and adding and multiplying choices: the building blocks of combinatorial enumeration.

- The derangements problem: enumerating permutations with no fixed points. This problem is solved eight times in the book, each solution illustrating a different combinatorial technique.
- Binomial coefficients, emphasising memorable bijective proofs of the key identities.
- Principle of Inclusion and Exclusion with applications to Euler's ϕ function and counting
- Rook polynomials. Applications including the *Problème des Ménages*.

Part B: Generating functions

A generating function is a power series whose coefficients record a combinatorial sequence. For example, the generating function for the Fibonacci numbers $0,1,1,2,3,5,8,13,\ldots$ is $x+x^2+2x^3+3x^4+5x^5+8x^6+13x^7+\cdots$, which has the closed form $x/(1-x-x^2)$.

- Introduction: formal and analytic interpretations of power series. First examples: enumerating compositions and tilings.
- Generating function methods for simple recurrence relations, such as the Fibonacci recurrence $a_n = a_{n-2}+a_{n-1}$ or the derangements recurrence $d_n = (n-1)(d_{n-2}+d_{n-1})$. Ansatz methods. Asymptotic results, obtained by very basic singularity analysis. Stirling numbers as example.
- Partitions, with an emphasis on bijective and involutive proofs. Asymptotic results and the abacus representation of partitions.
- Enumerating Catalan numbers and derangements, using generating functions. In each case we will see how natural 'splitting' of a combinatorial object into subobjects corresponds to a equation satisfied by a generating function. Solving these equations we obtain formulae and asymptotic results on the objects we want to count.

Part C: Ramsey Theory and probability

The slogan of Ramsey Theory is 'Complete disorder is impossible'. For example, if any two people are either friends or enemies, then in any room with six people, there must be three mutual friends or three mutual enemies.

- Ramsey's Theorem and its generalizations.
- Probability and Ramsey Theory: 'Considerable disorder is possible, if you pick at random'.
- Ramsey type results including Schur's Theorem.

- Lovasz Local Lemma and applications.
- First moment method and applications to random graphs.

Part D: Further directions

This part gives a highly selective survey of more recent results in some of the areas seen earlier in the book, bringing the reader close to the state-of-the-art. Some suggestions for further reading from advanced textbooks or the research literature are given.

Some features of this book

This book is based on a 33 lecture course lectured by the author at Royal Holloway, University of London, from 2010 to 2015. This course was attended by third year, fourth year and MSc students. With the few exceptions noted below, all the sections have been the subject of lectures, and the majority of the end of chapter exercises have been set on problem sheets. In many cases this led to significant changes in the approach.

The 'core' exercises are those set as compulsory questions. Experience suggests that most students can get somewhere with them. Students who put in this work—a large majority in most years—typically did well in the final exam and enjoyed the course. In short: this is a practical book aimed at real students.

Sections 2.4, 4.3, 6.3, 7.2, 7.3, 7.4, 7.5, 8.4, 9.1, 9.3, 9.4, 11.2, 11.3, 11.4 and 12.2 were not part of the original course. Like most of the book, their content is fairly standard, and can be found in many undergraduate textbooks. The exceptions are §7.4 on the abacus representation of partitions, §11.4 on Ramsey's Theorem for paths and Part E 'Further directions'. The four 'Interludes' are also new. These give motivated solutions, intended to shed some light on mathematical problem solving, to four easily stated and immediately appealing combinatorial problems. While techniques from the book are used, the pre-requisites are mild. You are encouraged to tackle these problems for yourself. Hints are provided to give you a head start: why not begin now with the *Egg Dropping Problem*?

Appendix A is a review of basic mathematical notation. Appendix B reviews the analysis needed in Part B and the discrete probability needed in Part D. Appendix C gives solutions to all the exercises in the main text and all the core exercises. This is intended to prevent self-learners from getting needlessly stuck. Solutions are given to many further problems, including all the problems that appeared on problem sheets for the course. The harder exercises, or parts of exercises, are marked ($\star$). Appendix D gives brief endnotes and acknowledgements of sources.

Acknowledgements

I gratefully acknowledge the significant contribution made by Eugenio Giannelli, who did much of the initial work in preparing the first two chapters of this book.

Website

Corrections or comments sent by email to `mark.wildon@rhul.ac.uk` are very welcome. Errata will be collected on the web at `www.ma.rhul.ac.uk/~uvah099/`.

PART ONE

ENUMERATION

1
The Derangements Problem

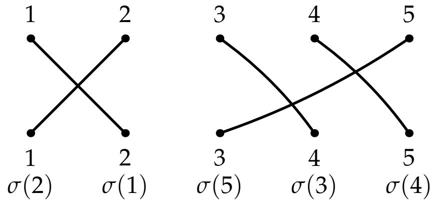
1.1 Derangements

We begin with the Derangements Problem. Later we will develop techniques that can be used to solve this problem in a routine way. Our first solution is necessarily somewhat ad-hoc. Along the way we will see three basic counting principles that are fundamental to combinatorial enumeration.

Recall that if X and Y are sets then a function $f : X \to Y$ is a *bijection* if for every $y \in Y$ there exists a unique $x \in X$ such that $f(x) = y$.

Definition 1.1.1 A *permutation* σ of a set X is a bijection $\sigma : X \to X$.

Usually we will consider permutations of $\{1,2,\ldots,n\}$ for some natural number $n \in \mathbb{N}$. It is often useful to represent permutations by diagrams. For example, the diagram below shows the permutation $\sigma : \{1,2,3,4,5\} \to \{1,2,3,4,5\}$ defined by $\sigma(1) = 2$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 5$, $\sigma(5) = 3$.



More briefly, we may write σ in *one-line form* as 21453. You might also have seen two-line form; later in §9.2 we will see the disjoint cycle decomposition of permutations.

As a starting point, consider the following questions:

(a) How many permutations are there of $\{1,2,\ldots,n\}$?

(b) How many of these permutations σ satisfy $\sigma(1) = 1$?

For (a), we construct a permutation $\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ step-by-step. Let $X = \{1,2,\ldots,n\}$. We may choose any element of X for $\sigma(1)$. For $\sigma(2)$ we may choose any element of X except $\sigma(1)$. Continuing in this way, for $\sigma(r)$ we may choose any element of X except $\sigma(1), \ldots, \sigma(r-1)$. Finally for $\sigma(n)$ we have a unique choice. Thus there are $n-(r-1)$ choices for each $\sigma(r)$. Multiplying choices, we see that there are $n(n-1)\ldots 1 = n!$ permutations of $\{1,2,\ldots,n\}$.

For (b), we have only 1 choice for $\sigma(1)$. Then as before, and for the same reasons, we have $n-1$ choices for $\sigma(2)$, $n-2$ choices for $\sigma(3)$, and so on. So there are $1(n-1)(n-2)\ldots 1 = (n-1)!$ permutations σ of $\{1,2,\ldots,n\}$ such that $\sigma(1) = 1$.

This principle of multiplying numbers of choices is very powerful.

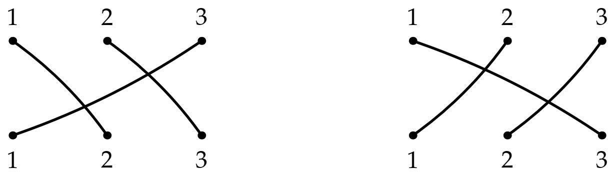
Basic Counting Principle 1 (BCP1). If an object can be specified uniquely by a sequence of k choices so that, when making the rth choice, we always have exactly c_r possibilities to choose from, then there are exactly $c_1 c_2 \ldots c_k$ objects.

Note that in (a), the choices we have for $\sigma(r)$ depend on our earlier choices of $\sigma(1)$, ..., $\sigma(r-1)$. But it was still correct to apply **BCP1** because the *number* of choices for $\sigma(r)$ is always $n-(r-1)$. In the special case where we make two choices, and one choice does not affect the next, so we first choose an element of a set A, then an element of a set B, **BCP1** simply says that $|A \times B| = |A||B|$. (See Appendix A if any of this notation is unfamiliar to you.)

Definition 1.1.2 Let σ be a permutation of a set X. A *fixed point* of σ is an element $x \in X$ such that $\sigma(x) = x$. We say that σ is a *derangement* if it has no fixed points. For $n \in \mathbb{N}_0$, let d_n be the number of derangements of $\{1,2,\ldots,n\}$.

By (b), the number of permutations of $\{1,2,\ldots,n\}$ having 1 as a fixed point is $(n-1)!$. Correspondingly, the probability a permutation fixes 1 is $(n-1)!/n! = 1/n$. This should be intuitive: if you take a fresh deck of cards, shuffle it well, and then deal, the probability that the top card is the Ace of Spades is $1/52$.

Enumerating derangements is not so easy. Clearly $d_1 = 0$, since the unique permutation of $\{1\}$ fixes 1, and $d_2 = 1$, since we have to swap 1 and 2. The diagrams below show the two derangements of $\{1,2,3\}$.



Exercise 1.1.3 Check, by listing or drawing permutations, or some cleverer method, that $d_4 = 9$. What is d_0?

The solution to this exercise given in Appendix B uses a further counting principle.

Basic Counting Principle 2 (BCP2). If a finite set of objects can be partitioned into disjoint subsets $A_1, A_2, \ldots, A_r$ then the total number of objects is $|A_1| + |A_2| + \cdots + |A_r|$.

Our final basic counting principle is arguably the most basic of all.

Basic Counting Principle 0 (BCP0). If there is a bijection between finite sets A and B then $|A| = |B|$.

Both principles should seem obvious. For instance, when $r = 2$, **BCP2** says that if X is a finite set and $X = A \cup B$ where $A \cap B = \varnothing$, then $|X| = |A| + |B|$.

Exercise 1.1.4 You are a shepherd with a flock of several hundred sheep. You are an expert on sheep, but have never learned to count above 5. How can you work out how many sheep were killed by wolves over Winter?

Exercise 1.1.5 Try to construct a derangement of $\{1,2,3,4,5\}$ such that $\sigma(1) = 2$ step-by-step. Show that there are two derangements such that $\sigma(1) = 2, \sigma(2) = 1$, and three derangements such that $\sigma(1) = 2$, $\sigma(2) = 3$. How many choices are there for $\sigma(3)$ in each case?

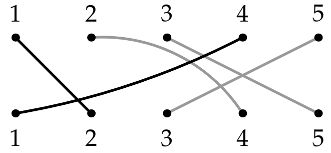
The previous exercise shows that we cannot hope to solve the derangements problem just by multiplying choices. Instead we shall find a recurrence for the numbers d_n.

Lemma 1.1.6 *If $n \geq 2$ then the number of derangements σ of $\{1,2,\ldots,n\}$ such that $\sigma(1) = 2$ is $d_{n-2} + d_{n-1}$.*

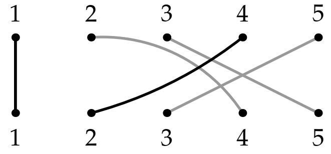
Proof A combinatorial interpretation is helpful. Imagine n parcels, sent to Persons 1, 2, …, n. By a sorting error, Parcel x is sent to Person $\sigma(x)$. Thus Parcel 1 is sent to Person 2, and no-one gets the right parcel. We consider two cases.

- *Either:* $\sigma(2) = 1$, so Parcel 2 is sent to Person 1. Then Parcels 3, …, n are sent to Persons 3, …, n. There are d_{n-2} derangements of the set $\{3,\ldots,n\}$ so there are d_{n-2} derangements in this case.
- *Or:* $\sigma(2) \neq 1$. Imagine that Persons 1 and 2 meet and swap parcels. Now Person 1 has Parcel 1, and Person 2 has the parcel sent to Person 1. Suppose

that, after the swap, Parcel x has now gone to Person $\tau(x)$. An example is shown below.



σ, before swap



τ, after swap

Since $\sigma(2) \neq 1$, Parcel 2 was not sent to Person 1. Hence, after Persons 1 and 2 swap parcels, Person 2 does not have Parcel 2. Therefore $\tau(2) \neq 2$. The swap does not affect the parcels sent to Persons 3, ..., n, so $\tau(3) \neq 3$, ..., $\tau(n) \neq n$. Clearly the swap can be undone: just repeat it! So swapping parcels defines a bijection

$$\left\{\begin{array}{c}\text{derangements } \sigma \text{ of } \{1,2,\ldots,n\} \\ \text{such that } \sigma(1)=2,\ \sigma(2)\neq 1\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{permutations } \tau \text{ of } \{1,2,\ldots,n\} \\ \text{such that } \tau(1)=1,\ \tau(2)\neq 2, \\ \tau(3)\neq 3,\ \ldots,\ \tau(n)\neq n\end{array}\right\}.$$

Since there are d_{n-1} derangements of $\{2,3,\ldots,n\}$, the set on the right-hand side has size d_{n-1}. By **BCP0** so does the set on the left-hand side.

Now add up the numbers of choices for the 'either' and 'or' cases using **BCP2**. □

Exercise 1.1.7 Let f be the 'swapping parcels' bijection defined in the proof of Lemma 1.1.6. Consider Figure 1.1 overleaf. Apply f to the permutation σ on the left, and apply $f^{-1} = f$ to the permutation τ on the right. Check in each case the image is in the expected set. Check also that $f(f(\sigma)) = \sigma$ and $f(f(\tau)) = \tau$.

It is often useful to see how proofs work by trying them out on particular examples. In the early sections of this book some exercises are included to encourage you to get into this habit.

The proof of the next theorem is modelled on the solution to Exercise 1.1.3.

Theorem 1.1.8 *If $n \geq 2$ then $d_n = (n-1)(d_{n-2} + d_{n-1})$.*

Proof Let D be the set of derangements of $\{1,2,\ldots,n\}$. For each $x \in \{1,2,\ldots,n\}$ let $D_x = \{\sigma \in D : \sigma(1) = x\}$. By Lemma 1.1.6 we have $|D_2| = d_{n-2} + d_{n-1}$. There is nothing special about 2 in this context, except that $2 \neq 1$. Hence

$$|D_2| = |D_3| = \ldots = |D_n| = d_{n-2} + d_{n-1}.$$

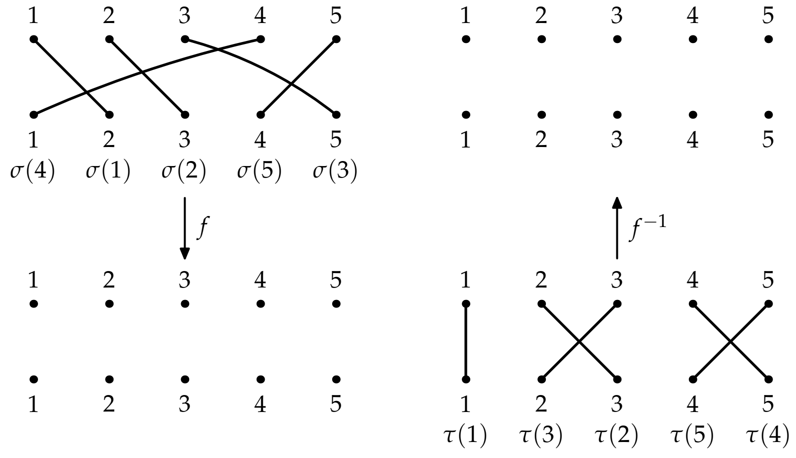


Figure 1.1 Another example of the ‘swapping parcels’ bijection f.

Since $D_1 = \varnothing$, we have, by **BCP2**,

$$|D| = |D_1| + |D_2| + |D_3| + \cdots + |D_n| = (n-1)(d_{n-2} + d_{n-1}),$$

as required. □

Using this recurrence relation it is easy to find values of d_n for much larger n. For example, you can easily compute $d_5 = (5-1)(d_3 + d_4) = 4 \times (2+9) = 44$. Compare this with the effort required to find the 44 derangements of $\{1, 2, \ldots, 5\}$ by listing all 5! permutations of $\{1, 2, \ldots, 5\}$.

Whenever one meets a new combinatorial sequence, it is a good idea to look it up in N. J. A. Sloane’s Online Encyclopedia of Integer Sequences: see `oeis.org`. You will usually find it there, along with references and often other combinatorial interpretations. The derangement numbers $d_0, d_1, d_2, \ldots$ are sequence A000166. The terms for $n \leq 10$ are

$$1, 0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961, \ldots$$

(See the answer to Exercise 1.1.3 if you are surprised that $d_0 = 1$.) We also find a formula: `a(n) = n!*Sum((-1)^k/k!, k=0..n)`. Knowing the answer, it is not hard to prove by induction that it is correct.

Corollary 1.1.9 *For all $n \in \mathbb{N}_0$,*

$$d_n = n!\big(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\big).$$

Proof When $n = 0$ both sides are 1 and when $d = 1$ both sides are 0. Let $n \geq 2$ and suppose, inductively, that the formula holds for d_{n-2} and d_{n-1}. By Theorem 1.1.8 and the inductive hypothesis we have

$$\begin{aligned}\frac{d_n}{n!} &= \frac{(n-1)(d_{n-2}+d_{n-1})}{n!}\\ &= \frac{d_{n-2}}{n(n-2)!} + \frac{n-1}{n}\frac{d_{n-1}}{(n-1)!}\\ &= \frac{1}{n}\big(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+\frac{(-1)^{n-2}}{(n-2)!}\big)\\ &\qquad + \big(1-\frac{1}{n}\big)\big(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+\frac{(-1)^{n-2}}{(n-2)!}+\frac{(-1)^{n-1}}{(n-1)!}\big).\end{aligned}$$

Each term $\frac{1}{n}\frac{(-1)^k}{k!}$ in the first summand is cancelled by a corresponding $-\frac{1}{n}\frac{(-1)^k}{k!}$ from the second summand. We are left with

$$\begin{aligned}\frac{d_n}{n!} &= \big(1-\frac{1}{1!}+\frac{1}{2!}-\cdots+\frac{(-1)^{n-2}}{(n-2)!}+\frac{(-1)^{n-1}}{(n-1)!}\big) - \frac{1}{n}\frac{(-1)^{n-1}}{(n-1)!}\\ &= 1-\frac{1}{1!}+\frac{1}{2!}-\cdots+\frac{(-1)^{n-2}}{(n-2)!}+\frac{(-1)^{n-1}}{(n-1)!}+\frac{(-1)^n}{n!}.\end{aligned}$$

Multiplying through by $n!$ gives the required formula for d_n. □

A more systematic way to derive Corollary 1.1.9 from Theorem 1.1.8 will be seen in Part 2. We will later prove Corollary 1.1.9 in many other ways, none of which require knowing the answer in advance.

The proof of Corollary 1.1.9 shows that it is helpful to consider the probability $d_n/n!$ that a permutation of $\{1,2,\ldots,n\}$ is a derangement. (This assumes that each probability is chosen *uniformly at random*, that is, with equal probability $1/n!$.) Before reading further, please take a moment to think about the next question.

Question 1.1.10 *Let n be large. Suppose that n parcels are delivered uniformly at random to n people, so that each person gets one parcel. Roughly, what is the probability that no-one gets the right parcel?*

Of course this probability is $d_n/n!$. Since all n people have to be unlucky, one reasonable guess is ‘nearly 0’. On the other hand, the chance a particular parcel (say Parcel 1) is wrongly delivered is $1-1/n$, which is very close to 1. So another reasonable guess is ‘nearly 1’. This line of thought is continued in Exercise 1.8.

In fact, by the following theorem, the probability is close to $1/\mathrm{e} = 0.36788\ldots$, and on average, exactly one person gets their own parcel.

Theorem 1.1.11 *Suppose that permutations of* $\{1,2,\dots,n\}$ *are chosen uniformly at random.*

(i) *The probability* $d_n/n!$ *that a permutation of* $\{1,2,\dots,n\}$ *is a derangement tends to* $1/\mathrm{e}$ *as* $n \to \infty$.

(ii) *The mean number of fixed points of a permutation of* $\{1,2,\dots,n\}$ *is* 1.

Proof (i) By Corollary 1.1.9,

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

Recall that the Taylor series for e^x is $1 + x + x^2/2! + \cdots + x^n/n! + \cdots$. Substituting $x = -1$ we get

$$\begin{aligned}\mathrm{e}^{-1} &= 1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!} + \cdots \\ &= \lim_{n\to\infty}\big(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\big) \\ &= \lim_{n\to\infty}\frac{d_n}{n!},\end{aligned}$$

as required.

(ii) We define a set of ordered pairs

$$P = \left\{ (\sigma, x) : \begin{array}{c} \sigma \text{ is a permutation of } \{1,2,\dots,n\}, \\ x \in \{1,2,\dots,n\},\ \sigma(x) = x \end{array} \right\}.$$

(See Appendix A if you need a reminder of the notation for ordered pairs.) Counting P by summing over all $n!$ permutations σ of $\{1,2,\dots,n\}$ we get

$$|P| = \sum_{\sigma} \big|\{x \in \{1,2,\dots,n\} : \sigma(x) = x\}\big|.$$

Hence the mean number of fixed points is $|P|/n!$. On the other hand, counting $|P|$ by summing over $x \in \{1,2,\dots,n\}$ we get

$$|P| = \sum_{x=1}^{n} \big|\{\text{permutations } \sigma \text{ of } \{1,2,\dots,n\} : \sigma(x) = x\}\big|.$$

We saw on page 8 that there are exactly $(n-1)!$ permutations of $\{1,2,\dots,n\}$ fixing 1. In this context there is nothing special about 1. Hence every summand above is $(n-1)!$. Therefore $|P| = n(n-1)! = n!$ and the mean number of fixed points is $n!/n! = 1$. □

The double-counting technique used in (ii) is often useful in combinatorial problems. A group theoretic generalization of (ii) is given in Exercise 1.11 below. It should be admitted that the proof of (ii) is far from the shortest possible: we will use probabilities and expectations to give a 'one-line proof' of a more general result in §9.2.

Exercises

Exercises 1.1 to 1.6 are core exercises intended to give you some practice in applying the Basic Counting Principles.

1.1 A menu has 3 starters, 4 main courses and 6 desserts.

(a) How many ways are there to order a three course meal, consisting of a starter, main course and dessert? [*Hint: multiply choices using* **BCP1**]

(b) How many ways are there to order a two course meal, including exactly one main course?

1.2 Let

$$\begin{aligned} T &= \{(x_1,x_2,x_3) : 1 \leq x_1,x_2,x_3 \leq 10,\, x_1,x_2,x_3 \text{ distinct}\}, \\ S &= \{X : X \subseteq \{1,\ldots,10\}, |X| = 3\}. \end{aligned}$$

Define a function $f : T \to S$ by $f\big((x_1,x_2,x_3)\big) = \{x_1,x_2,x_3\}$. For example, $(3,2,5) \in T$ and $f\big((3,2,5)\big) = \{3,2,5\} = \{2,3,5\} \in S$.

(a) Find $|T|$.

(b) Find the number of tuples $(x_1,x_2,x_3) \in T$ such that $f\big((x_1,x_2,x_3)\big) = \{2,3,5\}$.

(c) By generalizing the idea in (b), find $|S|$.
[*Hint: the point of this question is to show the ideas in one proof of the formula for binomial coefficients. So please do not assume this formula is true in* (c). *For a reminder of the difference between tuples and sets, see Appendix A.*]

1.3 Fix $n \in \mathbb{N}$. Let $X = \big\{(a,b) : 1 \leq a \leq b \leq n\big\}$. Find a simple formula for $|X|$ in terms of n.

1.4 For each $n \in \mathbb{N}$, how many subsets are there of $\{1,2,\ldots,n\}$? [*Hint: work out the answer for* $n = 1,2,3,\ldots$ *by writing down all the subsets in each case. Do not forget the empty set! Now explain the pattern using* **BCP1**.]

1.5 Let

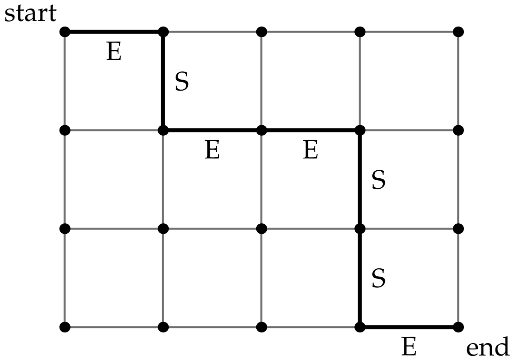
$$A = \left\{ \begin{array}{c} \text{placements of 4 indistinguishable balls into 7} \\ \text{numbered urns so that each ball is in a different urn} \end{array} \right\},$$

$$B = \left\{ \begin{array}{c} \text{ways to walk 4 blocks East and 3 blocks South} \\ \text{on a New York grid, moving only East and South} \end{array} \right\},$$

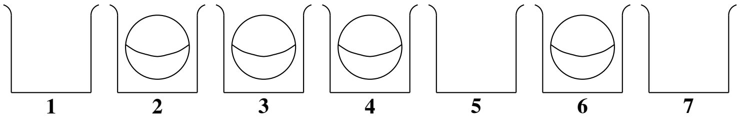
$$C = \big\{X \subseteq \{1,2,\ldots,7\} : |X| = 4\big\}.$$

(a) Define explicit bijections $f : A \to C$ and $g : B \to C$. [*Hint: it might help to first work out what you want the answers to* (b) *and* (c) *to be.*]

(b) Which element of C corresponds, by the bijection g, to the walking route ESEESSE $\in B$ shown in the diagram below?



(c) Which walking route in B corresponds to the ball-and-urn placement in A shown below?



(d) Find a binomial coefficient equal to $|A|$ and $|B|$.

1.6 A standard deck has 52 cards. There are four Aces, four Kings, four Queens and four Jacks. How many hands of five cards are there that

(a) have at least one Ace, King, Queen and Jack? [*Hint: first count hands of the form* AKQJx*, where x stands for a ten or smaller card, then hands of the form* AAKQJ*, and so on. Note that hands are unordered:* AKQJ3 *is the same hand as* KQ3JA.]

(b) have at least one Ace, King and Queen?

(In Chapter 3 we will see the Principle of Inclusion and Exclusion: it gives a simple unified way to solve both problems.)

Exercises 1.7 to 1.11 extend the results so far on permutations and derangements.

1.7 Let $p_n = d_n/n!$ be the probability that a permutation of $\{1, 2, \ldots, n\}$, chosen uniformly at random, is a derangement. Using only the recurrence in Theorem 2.4, prove by induction that $p_n - p_{n-1} = (-1)^n/n!$; hence give an alternative proof of Corollary 1.1.9.

1.8 As in Question 1.1.10, suppose that n parcels are delivered uniformly at random to n people, so that each person gets one parcel.

(a) Let $x \in \{1,\dots,n\}$. Show that the probability that Parcel x is wrongly delivered is $1-1/n$.

(b) Assuming the events that parcels are wrongly delivered are independent, show that the probability that no-one gets their own parcel is $(1-1/n)^n$.

(c) Show that $(1-1/n)^n \to 1/\mathrm{e}$ as $n \to \infty$.

(d) Show, regrettably, that the independence assumption in (b) is false whenever $n \geq 2$.

(Despite the bad news in (d), this line of reasoning can still be modified to give a rigorous proof that $d_n/n! \to 1/\mathrm{e}$ as $n \to \infty$: see Exercise 11.4.)

1.9 Use the formula for d_n in Corollary 1.1.9 to prove that if $n > 0$ then d_n is the nearest integer to $n!/\mathrm{e}$.

1.10

(a) Let $a_n(t)$ be the number of permutations of $\{1,2,\dots,n\}$ with exactly t fixed points. Note that $d_n = a_n(0)$. Prove that

$$a_n(t) = \frac{n!}{t!}\Big(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^{n-t}}{(n-t)!}\Big).$$

Hence, or otherwise, give a simple expression for $a_n(0) - a_n(1)$.

(b) Use (a) to give an alternative proof of Theorem 2.6(ii), that the mean number of fixed points of a permutation of $\{1,2,\dots,n\}$ is 1.

(c) ($\star$) Let e_n be the number of derangements of $\{1,2,\dots,n\}$ that are even permutations, and let o_n be the number that are odd permutations. By evaluating the determinant of the matrix

$$\begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & 0 \end{pmatrix}$$

in two different ways, prove that $e_n - o_n = (-1)^{n-1}(n-1)$.

1.11 This exercise needs some group theory.

(a) Let G be a subgroup of the symmetric group of all permutations of $\{1,2,\dots,n\}$. Let $P = \{(\sigma,x) : \sigma \in G, x \in \{1,2,\dots,n\}, \sigma(x) = x\}$. (Thus if G is the full symmetric group, then P is as defined in the proof of Theorem 1.1.11.) Let $\mathrm{Fix}(\sigma)$ be the set of fixed points of $\sigma \in G$. By double-counting P and using the Orbit-Stabiliser Theorem, show that

$$\frac{1}{|G|}\sum_{\sigma\in G}|\mathrm{Fix}(\sigma)|$$

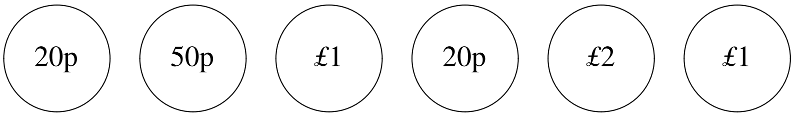
is equal to the number of orbits of G on $\{1,2,\ldots,n\}$. (This result is usually, but wrongly, attributed to Burnside.)

(b) How many ways are there to colour the faces of a tetrahedron red, blue and green? (Regard two colourings as the same if they differ by a rotation of the tetrahedron. Any combination of the three colours may be used.)

(c) How many ways are there to put 3 white balls and 2 black balls into three indistinguishable urns? (You may find Theorem 2.3.3 useful.)

Exercises 1.12 to 1.15 are more challenging. They can all be solved by elementary arguments, but you will have to think hard. Try looking at small cases to get started.

1.12 ($\star$) The hare and the tortoise—both of them capable mathematicians—play a game. The umpire places evenly many coins in a row: a possible starting position for a six coin game is shown below.



The players then alternately take coins from either end, until none are left. The winner is the player who ends up with the most money. If the players get equal amounts, the game is a draw. Tradition dictates that the tortoise starts. Show that the tortoise can guarantee never to lose. Find a reasonably general sufficient condition for the tortoise to win.

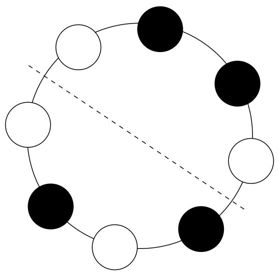
1.13 ($\star$) There are 12 numbered locked safes that can be unlocked by 12 numbered keys. Before you arrive, the keys are randomly distributed so that each safe contains one key, and the safes are shut. When you arrive, the referee unlocks the first r safes using her master key. What is the probability that you can now open all the safes? (Once you have unlocked a safe, you may take and use the key it contains.)

1.14 [American Mathematical Monthly Problem 11573] ($\star$) A square matrix of order n^2 is said to be a *Sudoku permutation matrix* if all its entries are either 0 or 1, and it has exactly one 1 in each row, each column, and each of the n^2 submatrices obtained by dividing the matrix into an $n \times n$ array of $n \times n$ submatrices. For each $n \in \mathbb{N}$, find the number of Sudoku permutation matrices of order n^2.

(See below for an example when $n = 2$. If $n = 3$ then the 1s in a completed Sudoku grid form a Sudoku permutation matrix of order 3^2.)

$$\begin{array}{cc|cc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array}$$

1.15 ($\star$) Given a necklace with 168 beads, 84 black and 84 white, can it necessarily be cut, and the new ends retied, so that two necklaces each with 42 beads of either colour are obtained? (See below for one solution with an 8 bead necklace.)



2
Binomial coefficients

2.1 Binomial coefficients and bijective proofs

The following notation is standard and often useful.

Notation 2.1.1 If X is a set of size $k \in \mathbb{N}_0$ then we say that X is a *k-set*. To emphasise that X is a subset of a set Y, we say that X is a *k-subset of Y*.

We define binomial coefficients combinatorially.

Definition 2.1.2 Let n, $k \in \mathbb{N}_0$. The *binomial coefficient* $\binom{n}{k}$ is the number of k-subsets of $\{1,2,\ldots,n\}$.

For example $\binom{4}{2} = 6$: the six 2-subsets of $\{1,2,3,4\}$ are $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$. Note that, by definition, if $k > n$ then $\binom{n}{k} = 0$. We could replace $\{1,2,\ldots,n\}$ with any other set of size n and still define the same numbers $\binom{n}{k}$.

Exercise 2.1.3

(a) Show that $\binom{n}{0} = \binom{n}{n} = 1$ for all $n \in \mathbb{N}_0$.

(b) Show that $\binom{n}{1} = n$ for all $n \in \mathbb{N}_0$.

In each case, does your argument work when $n = 0$?

We now check that the expected formula holds for binomial coefficients. Note this is a non-trivial result: it is not true by definition! The proof uses the same idea as Exercise 1.2.

Lemma 2.1.4 *If n, $k \in \mathbb{N}_0$ and $k \leq n$ then*

$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}.$$

Proof Let

$$T = \big\{(x_1,\ldots,x_k) : x_1,\ldots,x_k \in \{1,2,\ldots,n\}, x_1, \ldots, x_k \text{ distinct}\big\}.$$

Constructing an element of T step-by-step, we have n choices for x_1, $n-1$ choices for x_2, $\dots$, $n-(r-1)$ choices for x_r, $\dots$, $n-(k-1)$ choices for x_k. Therefore $|T| = n(n-1)\dots(n-k+1)$ by **BCP1**. Let

$$S = \big\{X : X \subseteq \{1,2,\dots,n\}, |X| = k\big\}.$$

By Definition 2.1.2, $|S| = \binom{n}{k}$. Consider the function $f : T \to S$ defined by

$$f\big((x_1,\dots,x_k)\big) = \{x_1,\dots,x_k\}.$$

Let $X \in S$. There are $k!$ tuples $(x_1,\dots,x_k) \in T$ such that $f\big((x_1,\dots,x_k)\big) = X$, one for each of the $k!$ permutations of X. Hence

$$\binom{n}{k} = |S| = \frac{|T|}{k!} = \frac{n(n-1)\dots(n-k+1)}{k!}.$$

The second equality then follows from $n(n-1)\dots(n-k+1) = n!/(n-k)!$. □

Many of the basic properties of binomial coefficients have combinatorial proofs using explicit bijections and the three basic counting principles. We say that such proofs are *bijective*. They are not always shorter than algebraic proofs, but they are often more illuminating.

Lemma 2.1.5 *If n, $k \in \mathbb{N}_0$ and $n \geq k$ then*

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

Proof By definition, there are $\binom{n}{k}$ subsets of $\{1,2,\dots,n\}$ of size k and $\binom{n}{n-k}$ subsets of $\{1,2,\dots,n\}$ of size $n-k$. Taking complements in $\{1,2,\dots,n\}$ defines a bijection between the two collections of subsets. By **BCP0**, they have the same size. □

As ever, looking at a particular example may clarify the proof.

Exercise 2.1.6 Take $n = 4$ and $k = 1$. What explicitly is the bijection

$$\big\{\{1\},\{2\},\{3\},\{4\}\big\} \to \big\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\big\}$$

proving that $\binom{4}{1} = \binom{4}{3}$ in the previous proof? What is its inverse?

Lemma 2.1.5 has a one-line algebraic proof. The next result also has a short algebraic proof, although some care is needed to deal with the case $k = n$. The bijective proof works in a uniform way, and really explains *why* the result is true.

Lemma 2.1.7 (Fundamental Recurrence) *If n, $k \in \mathbb{N}$ then*

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

Proof Let X be a k-subset of $\{1,2,\ldots,n\}$. We consider two cases.

- *Either $n \in X$*. Removing n from X gives a $(k-1)$-subset of $\{1,2,\ldots,n-1\}$. Conversely, given such a set, inserting n gives a k-subset of $\{1,2,\ldots,n\}$ containing n. Hence the k-subsets containing n are in bijection with the $(k-1)$-subsets of $\{1,2,\ldots,n-1\}$, and so there are $\binom{n-1}{k-1}$ such subsets.
- *Or $n \notin X$*. Then X is a k-subset of $\{1,2,\ldots,n-1\}$. By definition there are $\binom{n-1}{k}$ such subsets.

There are $\binom{n}{k}$ k-subsets of $\{1,2,\ldots,n\}$ and each k-subset is counted in a unique case. By **BCP1** we have $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, as required. □

Our next result is the Binomial Theorem. Probably you have already seen this proved by induction. The bijective proof may require more thought from you, but once mastered, is far shorter.

Theorem 2.1.8 (Binomial Theorem) *Let z, $w \in \mathbb{C}$. If $m \in \mathbb{N}_0$ then*

$$(z+w)^m = \sum_{k=0}^{m} \binom{m}{k} z^k w^{m-k}.$$

Proof When we multiply out

$$(z+w)^m = \underbrace{(z+w)(z+w)\cdots(z+w)}_{m}$$

we must choose either z or w from each bracket $(z+w)$. If we choose z from k brackets and w from the other $m-k$ brackets, then we get a contribution of 1 to the coefficient of $z^k w^{m-k}$. Since there are $\binom{m}{k}$ ways to choose k of the n brackets, this coefficient is $\binom{m}{k}$. □

Here is an example of a deliberately informal bijective proof that is nonetheless entirely rigorous.

Claim 2.1.9 *Let n, $k \in \mathbb{N}_0$. If $k \le n$ then $(n-k)\binom{n}{k} = (k+1)\binom{n}{k+1}$.*

Proof Take n people. To form a team consisting of $k+1$ people, one of whom is the leader, we can choose k people in $\binom{n}{k}$ ways, and then choose one of the remaining $n-k$ people to be the leader. Hence, by **BCP1**, there are $\binom{n}{k}(n-k)$ teams-with-leaders. Or, more democratically, we could choose $k+1$ people in $\binom{n}{k+1}$ ways, and then let them elect a leader, in $k+1$ ways. Hence, by **BCP1**, there are $\binom{n}{k+1}(k+1)$ teams-with-leaders. These numbers must be equal. □

See Exercise 2.1 for a similar identity proved bijectively. If you doubt the rigour of the previous proof, then you might be happier with the formalized version, giving in the exercise below. Or you might feel, perhaps correctly, that in this case the bijective proof is too much work, and the algebraic proof

$$(n-k)\binom{n}{k} = (n-k)\frac{n!}{k!(n-k)!} = \frac{n!}{k!(n-k-1)!}$$
$$= (k+1)\frac{n!}{(k+1)!(n-(k+1))!} = (k+1)\binom{n}{k+1}$$

is preferable. (Note however that the second equality is only valid when $k < n$, so the case $k = n$ has to be treated separately.)

Exercise 2.1.10 Formalize the proof of Claim 2.1.9 by defining a bijection

$$f : \left\{(X,y) : \begin{matrix} X \subseteq \{1,2,\ldots,n\},\ |X| = k, \\ y \in \{1,2,\ldots,n\},\ y \notin X \end{matrix}\right\} \to \left\{(Z,y) : \begin{matrix} Z \subseteq \{1,2,\ldots,n\}, \\ |Z| = k+1,\ y \in Z \end{matrix}\right\}.$$

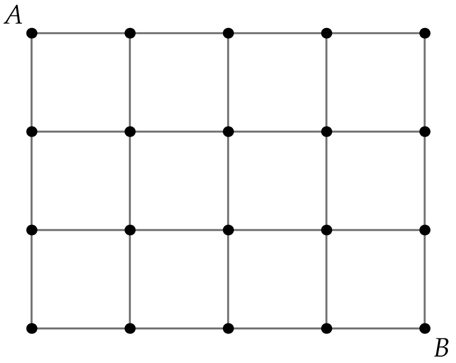
Give a formula for $f^{-1}\big((Z,y)\big)$ where (Z,y) is in the right-hand set above.

2.2 Basic binomial identities

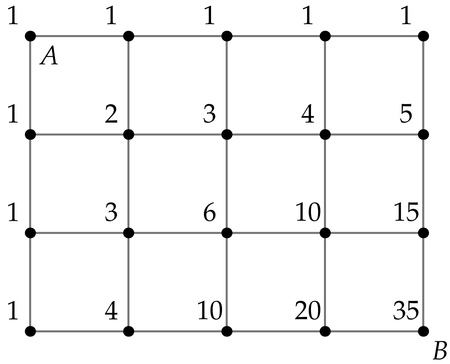
Sums involving binomial coefficients often appear in mathematical problems. In this section we see some of the basic identities that are most useful for simplifying such sums.

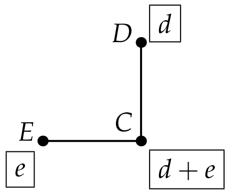
Identities from Pascal's Triangle

We introduce Pascal's Triangle by solving part of Exercise 1.5: how many ways are there to walk 4 blocks East and 3 blocks South on a New York grid, starting at A and ending at B as shown below, and moving only East and South?



The answer is $\binom{7}{4}$: each walking route has 7 steps, of which we must choose exactly 4 to be East. Alternatively, we can compute iteratively. Let C be a street junction. If C is due East or due South of A then there is a unique walking route from A to C. Otherwise, suppose that there are d ways to go to D (immediately to the North of C), and e ways to go to E (immediately to the West of C). Then there are $d+e$ ways to go from A to C, since we must reach C either from D or from E. Applying these two rules we count the walking routes as shown below.

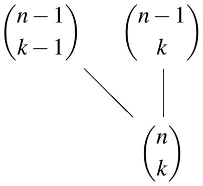




The numbers form a tilted version of Pascal's Triangle: the number of routes going to a junction k steps East and $n-k$ steps South of A is, as expected, $\binom{n}{k}$.

Exercise 2.2.1 Computing iteratively, we obtain 35 as the sum $35 = 20 + 15$. Correspondingly, $\binom{7}{4} = \binom{6}{3} + \binom{6}{4}$. Explain the connection with the proof of the Fundamental Recurrence $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

In practice it is more convenient to draw Pascal's Triangle as below; the entry in row n and column k is $\binom{n}{k}$. The Fundamental Recurrence is shown graphically to the left.



$n\backslash k$	0	1	2	3	4	5	6	7	8	9	10
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			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

We now prove some identities that come from summing adjacent entries in Pascal's Triangle. Consider row 8. Taking the alternating sum of the entries, we get $1-8=-7=-\binom{7}{1}$, $1-8+28=21=\binom{7}{2}$, $1-8+28-56=-35=-\binom{7}{3}$, and so on. This suggests the following result.

Lemma 2.2.2 (Alternating row sums) *If $n \in \mathbb{N}$, $m \in \mathbb{N}_0$ and $m \le n$ then*

$$\sum_{k=0}^{m} (-1)^k \binom{n}{k} = (-1)^m \binom{n-1}{m}.$$

Proof We work by induction on m. If $m=0$ then the left-hand side is $(-1)^0\binom{n}{0} = 1$ and the right-hand side is $(-1)^0\binom{n-1}{0} = 1$. By induction we may assume that $\sum_{k=0}^{m-1}(-1)^k\binom{n}{k} = (-1)^{m-1}\binom{n-1}{m-1}$. Now

$$\begin{aligned}\sum_{k=0}^{m}(-1)^k\binom{n}{k} &= \sum_{k=0}^{m-1}(-1)^k\binom{n}{k} + (-1)^m\binom{n}{m}\\ &= (-1)^{m-1}\binom{n-1}{m-1} + (-1)^m\binom{n}{m}\\ &= (-1)^m\left(\binom{n}{m} - \binom{n-1}{m-1}\right)\\ &= (-1)^m\binom{n-1}{m}\end{aligned}$$

where the final step uses the Fundamental Recurrence. □

Perhaps surprisingly, there is no simple formula for the unsigned row sums $\sum_{k=0}^{m}\binom{n}{k}$. But there *are* simple formulae for many, apparently more complicated, sums along the rows. See for example Exercises 2.2 and 2.8.

Now consider the diagonals. Suppose we start at $\binom{4}{0} = 1$ and step right and down. The sums are $1+5=6=\binom{6}{1}$, $1+5+15=21=\binom{7}{2}$, $1+5+15+35=56=\binom{8}{3}$, and so on. To see the reason for this pattern, think of the initial 1 not as $\binom{4}{0}$, but as $\binom{5}{0}$, one position below. Then the sum $\binom{5}{0}+\binom{5}{1}+\binom{6}{2}+\binom{7}{3}$ simplifies, by three applications of the Fundamental Recurrence, to $\binom{6}{1}+\binom{6}{2}+\binom{7}{3} = \binom{7}{2}+\binom{7}{3} = \binom{8}{4}$. This is a special case of the following result.

Lemma 2.2.3 (Diagonal sums) *If n, $m \in \mathbb{N}_0$ then*

$$\sum_{k=0}^{m}\binom{n+k}{k} = \binom{n+m+1}{m}.$$

Proof Again we work by induction on m. If $m=0$ then both sides are 1. For the inductive step we have

$$\sum_{k=0}^{m}\binom{n+k}{k}=\sum_{k=0}^{m-1}\binom{n+k}{k}+\binom{n+m}{m}=\binom{n+m}{m-1}+\binom{n+m}{m}=\binom{n+m+1}{m}$$

where, as expected, the final equality uses the Fundamental Recurrence. □

For the column sums on Pascal's Triangle see Exercise 2.3. For the other diagonal sum, see Exercise 2.6. For a bijective proof of Lemma 2.2.3, see Exercise 2.13(e).

Incidentally, while it is common to credit Pascal with the triangle of binomial coefficients, the Fundamental Recurrence and the Binomial Theorem were already known around 1000 CE by the Iranian mathematician al-Karaji.

Arguments with subsets

The two identities below are among the most useful in practice. Both have memorable and illuminating bijective proofs.

Lemma 2.2.4 (Subset of a subset) *If k, r, $n \in \mathbb{N}_0$ and $k \le r \le n$ then*

$$\binom{n}{r}\binom{r}{k}=\binom{n}{k}\binom{n-k}{r-k}.$$

Proof Let

$$P=\big\{(X,Y): X\subseteq Y\subseteq\{1,2,\ldots,n\}, |X|=k, |Y|=r\big\}.$$

We can first choose Y in $\binom{n}{r}$ ways, then choose $X\subseteq Y$ in $\binom{r}{k}$ ways. So $|P|=\binom{n}{r}\binom{r}{k}$. Or, we can first choose X in $\binom{n}{k}$ ways, and then choose $Z\subseteq\{1,2,\ldots,n\}\backslash X$ such that $|Z|=r-k$ in $\binom{n-k}{r-k}$ ways, and then take $Y=X\cup Z$. Hence $|P|=\binom{n}{k}\binom{n-k}{r-k}$. □

Exercise 2.2.5 'Deformalize' the previous proof using the setting of Claim 2.1.9. So you might start 'Take n people and form a (generalized) football team of r of them in $\binom{n}{r}$ ways. Then choose k of these r people to be defenders in $\binom{r}{k}$ ways. Hence there are $\binom{n}{r}\binom{r}{k}$ teams-with-defenders. Alternatively ...'

Lemma 2.2.6 (Vandermonde's convolution) *If a, $b \in \mathbb{N}_0$ and $m \in \mathbb{N}_0$ then*

$$\sum_{k=0}^{m}\binom{a}{k}\binom{b}{m-k}=\binom{a+b}{m}.$$

Proof The pet-shop has a alsatians and b budgies for sale. Each animal has its own distinctive personality and coat/plumage. Suppose I want to buy m pets. Here are two ways to do this.

(i) I go into the petshop, announce to the surprised owner that I want m pets, of any species. There are $a+b$ pets on sale, so there are $\binom{a+b}{m}$ possible purchases.

(ii) Alternatively, I first buy k alsatians for some $k \in \{0,1,\ldots,m\}$, in $\binom{a}{k}$ ways, and then buy $m-k$ budgies, in $\binom{b}{m-k}$ ways. Multiplying choices, by **BCP1**, there are $\binom{a}{k}\binom{b}{m-k}$ ways to do this. Summing over k, using **BCP2**, we count all $\sum_{k=0}^{m}\binom{a}{k}\binom{b}{m-k}$ possible purchases.

Comparing (i) and (ii) we get $\sum_{k=0}^{m}\binom{a}{k}\binom{b}{m-k} = \binom{a+b}{m}$. □

Note that there is no restriction on a, b and m, except that they are all in $\mathbb{N}_0$. For instance, if $a < m$ then the summands in Vandermonde's convolution for $k > a$ are all zero, because $\binom{a}{k} = 0$; correspondingly, there is no way to buy $k > a$ alsatians.

Exercise 2.2.7 Let $A = \{x_1,\ldots,x_a\}$ and $B = \{y_1,\ldots,y_b\}$ be disjoint sets of sizes a and b respectively. Formalize the previous proof by counting the number of m-subsets of $A \cup B$ in two different ways.

Corollaries of the Binomial Theorem

The Binomial Theorem (Theorem 2.1.8) states that if $m \in \mathbb{N}_0$ and z, $w \in \mathbb{C}$ then $\sum_{k=0}^{m}\binom{m}{k}z^k w^{m-k} = (z+w)^m$. The following results can be obtained by making a strategic choice of z and w. Ask yourself: *How can I make* $\binom{m}{k}z^k w^{m-k}$ *look like* $\binom{m}{k}$ *and* $(-1)^k\binom{m}{k}$*?*

Corollary 2.2.8

(i) *If* $m \in \mathbb{N}_0$ *then* $\displaystyle\sum_{k=0}^{m}\binom{m}{k} = 2^m.$

(ii) *If* $m \in \mathbb{N}$ *then* $\displaystyle\sum_{k=0}^{m}(-1)^k\binom{m}{k} = 0.$

Proof For (i) take $z = 1$ and $w = 1$ to get $\sum_{k=0}^{m}\binom{m}{k}1^k 1^{m-k} = (1+1)^n = 2^n$. For (ii), take $z = -1$ and $w = 1$ to get $\sum_{k=0}^{m}\binom{m}{k}(-1)^k 1^{n-k} = (-1+1)^m$. Since $m \geq 1$ the right-hand side is 0. □

An alternative proof of (i) was given in Exercise 1.4; (ii) is also a special case of Lemma 2.2.2.

Corollary 2.2.9 *For all $m \in \mathbb{N}$ there are equally many subsets of* $\{1,2,\ldots,m\}$ *of even size as there are of odd size.*

Proof Written out without the summation notation, Corollary 2.2.8(ii) states that

$\binom{m}{0} - \binom{m}{1} + \binom{m}{2} - \binom{m}{3} + \cdots = 0$. Add $\binom{m}{1} + \binom{m}{3} + \cdots$ to both sides. This cancels the negative terms on the left-hand side, giving

$$\binom{m}{0} + \binom{m}{2} + \binom{m}{4} + \cdots = \binom{m}{1} + \binom{m}{3} + \binom{m}{5} + \cdots .$$

The left-hand side is the number of subsets of $\{1,2,\ldots,m\}$ of even size, and the right-hand side is the number of subsets of $\{1,2,\ldots,m\}$ of odd size. □

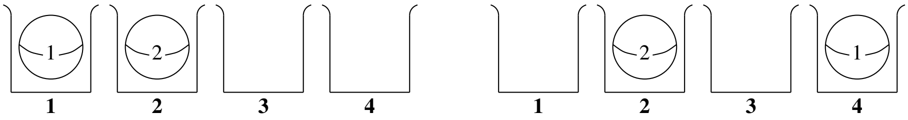
Exercise 2.2.10 Find a bijective proof of Corollary 2.2.9 when m is odd. You may find your bijection also works when m is even. If not, find a bijective proof that also works in this case.

Exercise 2.15 gives some further identities involving alternating sums of binomial coefficients that have bijective proofs.

2.3 Balls and urns

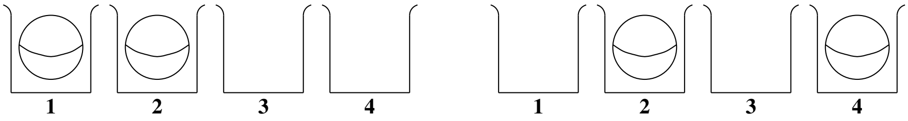
Using binomial coefficients and the basic counting principles we can answer a fundamental combinatorial question: *How many ways are there to put k balls into n numbered urns?* We consider both balls that are numbered from 1 to k, and indistinguishable balls. The answer also depends on the capacity of the urns: we consider *small urns*, that can contain only one ball, and *large urns*, that have unlimited capacity. Some urns may be empty.

For example, two of the twelve placements of 2 numbered balls into 4 small urns are shown below.



Exercise 2.3.1 Using **BCP1** find the number of ways to put k numbered balls into n numbered urns that are (i) small, (ii) large.

A placement of k indistinguishable balls into n small urns is completely determined by the set $\{r \in \{1,\ldots,n\} : \text{urn } r \text{ has a ball}\}$. For example, the placements when $n = 4$ and $k = 2$ corresponding to the subsets $\{1,2\}$ and $\{2,3\}$ of $\{1,2,3,4\}$ are shown below.



This gives a bijection between the placements of k indistinguishable balls into n small urns and the k-subsets of $\{1,2,\dots,n\}$. By definition, there are $\binom{n}{k}$ such subsets.

We now have the three entries shown in the table below.

	Numbered balls	Indistinguishable balls
small urns	$n(n-1)\dots(n-k+1)$	$\binom{n}{k}$
large urns	n^k	

Exercise 2.3.2 Explain why there are number of placements of k numbered balls into small urns is $k!$ times the number of placements of k indistinguishable balls. [*Hint: compare the diagrams on the previous page. How many ways are there to add labels to the indistinguishable balls?*] Will the same result hold for large urns?

The final entry is revealed below. If you compute a few small cases by hand, and compare the answers with Pascal's Triangle (see page 23) you will discover it for yourself.

Theorem 2.3.3 *Let $n \in \mathbb{N}$ and let $k \in \mathbb{N}_0$. The number of ways to place k indistinguishable balls into n numbered urns of unlimited capacity is $\binom{n+k-1}{k}$.*

We give two proofs, one inductive, using the same idea as the proof of the Fundamental Recurrence (Lemma 2.1.7), and one bijective.

Inductive proof Let $f(n,k)$ be the number of ways to place k indistinguishable balls into n large urns. We consider two cases.

- *Either urn n has a ball.* Removing this ball gives a placement of $k-1$ balls into n urns, and putting the ball back restores the original placement. Hence there are $f(n,k-1)$ such placements.
- *Or urn n is empty.* Then all the balls are in urns 1 up to $n-1$, and so there are $f(n-1,k)$ such placements.

By **BCP2**, we have

$$f(n,k) = f(n,k-1) + f(n-1,k) \quad \text{provided } n \geq 2 \text{ and } k \geq 1. \qquad (\star)$$

The restriction in ($\star$) is necessary for $f(n,k-1)$ and $f(n-1,k)$ to both be defined.

We want to assume that the claimed formula holds for $f(n,k-1)$ and $f(n-1,k)$. But there is a problem: we cannot do induction on n, because we need to know $f(n,k-1)$. And we cannot do induction on k, because we need to know $f(n-1,k)$.

So how can we capture the sense that finding $f(n,k-1)$ and $f(n-1,k)$ are ‘smaller’ problems than finding $f(n,k)$?

The solution is to do induction $n+k$, the sum of the number of balls and urns. The base cases come from the restriction in ($\star$). When $n=1$ we have $f(1,k)=1$ for all k (we have to put all k balls in urn 1). This agrees with $\binom{1+k-1}{k}=\binom{k}{k}=1$. When $k=0$ we have $f(n,0)=1$ for all n (the unique placement has no balls in any urn). This agrees with $\binom{n+0-1}{0}=\binom{n-1}{0}=1$. For the inductive step we use ($\star$) to get

$$f(n,k)=f(n,k-1)+f(n-1,k)=\binom{n+k-2}{k-1}+\binom{n+k-2}{k}=\binom{n+k-1}{k}$$

where the final equality uses the Fundamental Recurrence. □

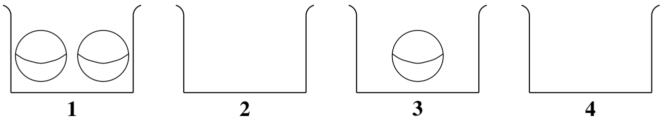
Bijective proof Given a placement of k indistinguishable balls into n numbered urns, perform the following procedure:

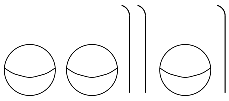
(1) Draw the balls and urns from left to right, starting with urn 1.

(2) Erase the left wall of urn 1 and all right urn walls, urn floors, urn numbers.

(3) Replace each ball with 0 and each remaining left urn wall with 1.

For example, when $n=4$ and $k=3$ we have



$\longmapsto$  $\longmapsto$ 001101.

This procedure defines a bijection between the placements of k indistinguishable balls into n urns and strings of length $n+k-1$ with k 0s and $n-1$ 1s. There are $\binom{n+k-1}{k}$ such strings, since we can choose any k positions of the $n+k-1$ positions to have 0s. (For example, 001101 corresponds to the 3-subset $\{1,2,5\}$ of $\{1,2,3,4,5,6\}$.) Hence, by **BCP0**, the number of ball-and-urn placements is $\binom{n+k-1}{k}$. □

Exercise 2.3.4 By reversing steps (1), (2) and (3) find the ball-and-urn placements corresponding to the strings 100110, 000111 and 111000.

The following reinterpretation of Theorem 2.3.3 is often useful.

Corollary 2.3.5 *Let $n\in\mathbb{N}$ and let $k\in\mathbb{N}_0$. The number of n-tuples $(t_1,t_2,\ldots,t_n)$ such that $t_1,t_2,\ldots,t_n\in\mathbb{N}_0$ and $t_1+t_2+\cdots+t_n=k$ is $\binom{n+k-1}{k}$.*

Proof Let T be the set of n-tuples $(t_1,t_2,\ldots,t_n)$ such that $t_1,t_2,\ldots,t_n\in\mathbb{N}_0$ and

$t_1 + t_2 + \cdots + t_n = k$. Given $(t_1, t_2, \ldots, t_n) \in T$, we define a corresponding placement of k indistinguishable balls into n large urns by putting t_r balls into urn r for each $r \in \{1, 2, \ldots, n\}$. Conversely, a ball-and-urn placement with t_r balls in urn r corresponds to the tuple $(t_1, t_2, \ldots, t_n) \in T$. By Theorem 2.3.3 and **BCP0**, we get $|T| = \binom{n+k-1}{k}$, as required. □

2.4 Binomial coefficients as polynomials

We may extend the definition of binomial coefficients to define $\binom{z}{k}$ for $z \in \mathbb{C}$ by

$$\binom{z}{k} = \frac{z(z-1)\ldots\big(z-(k-1)\big)}{k!}.$$

By Lemma 2.1.4 this agrees with the combinatorial definition (Definition 2.1.2) when $z \in \mathbb{N}_0$.

For example, $\binom{-1}{k} = (-1)^k$ and $\binom{-2}{k} = (-1)^k(k+1)$ for all $k \in \mathbb{N}_0$. More generally there is the following lemma, which is often useful for simplifying sums in which binomial coefficients appear with alternating signs.

Lemma 2.4.1 *Let $z \in \mathbb{C}$ and let $k \in \mathbb{N}_0$. Then*

$$\binom{z}{k} = (-1)^k \binom{k-z-1}{k}.$$

Proof This is a straightforward check. □

In particular, $\binom{n+k-1}{k} = (-1)^k \binom{-n}{k}$. Thus $\binom{n}{k}$ is the number of placements of k balls into n small urns, and, up to a sign, $\binom{-n}{k}$ is the number of placements of k balls into n large urns. A reason for this remarkable connection will be seen in §5.1.

Many of the identities proved so far hold for these generalized binomial coefficients. To show this we must think of $\binom{z}{k}$ as a polynomial of degree k in z. For example, $\binom{z}{3} = \frac{1}{6}z(z-1)(z-2) = \frac{1}{6}z^3 - \frac{1}{2}z^2 + \frac{1}{3}z$. We then use a key principle, proved in Exercise 2.16: *if two polynomials of degree k agree at $k+1$ distinct points then they are equal.*

As an example we prove the generalization of Lemma 2.2.2.

Lemma 2.4.2 *If $z \in \mathbb{C}$ and $m \in \mathbb{N}_0$ then*

$$\sum_{k=0}^{m} (-1)^k \binom{z}{k} = (-1)^m \binom{z-1}{m}.$$

Proof The left-hand side is a polynomial of degree at most m in z. The degree of the right-hand side is m. By Lemma 2.2.2, the two sides agree for all $z \in \mathbb{N}$. Hence, by the key principle, they are equal as polynomials in z. □

Similarly, the Fundamental Recurrence (Lemma 2.1.7), Claim 2.1.9, Lemma 2.2.3 and Lemma 2.2.4 all hold with n replaced with a general $z \in \mathbb{C}$. Vandermonde's Convolution (Lemma 2.2.6) holds with a and b replaced with general z, $w \in \mathbb{C}$. However Lemma 2.1.5, that $\binom{n}{k} = \binom{n}{n-k}$, does not generalize, because $\binom{n}{n-k} = n(n-1)\dots(k+1)/(n-k)!$ is not a polynomial in n.

Exercise 2.4.3 Using Lemma 2.4.1, deduce the general form of Lemma 2.2.3, namely $\sum_{k=0}^{m} \binom{z+k}{k} = \binom{z+m+1}{m}$, from Lemma 2.4.2.

As another application of Lemma 2.4.1 we prove a variant of Vandermonde's Convolution in which the sum of the upper parts of the binomial coefficients is constant.

Claim 2.4.4 *If c, $d \in \mathbb{N}_0$ and $m \in \mathbb{N}_0$ then*

$$\sum_{k=0}^{m} \binom{c+k}{c}\binom{d+m-k}{d} = \binom{m+c+d+1}{c+d+1}.$$

Proof By Lemma 2.1.5 and Lemma 2.4.1, $\binom{c+k}{c} = \binom{c+k}{k} = (-1)^k \binom{-c-1}{k}$ and similarly $\binom{d+m-k}{d} = \binom{d+m-k}{m-k} = (-1)^{m-k}\binom{-d-1}{m-k}$. Hence the left-hand side is

$$(-1)^m \sum_{k=0}^{m} \binom{-c-1}{k}\binom{-d-1}{m-k}.$$

By the general version of Vandermonde's Convolution, taking $a = -c-1$ and $b = -d-1$, this is $(-1)^m\binom{-c-d-2}{m}$. The claim now follows by another application of the two lemmas used at the start of the proof. □

Exercise 2.14 asks for a bijective proof of this identity. To finish we prove a tougher binomial identity.

Claim 2.4.5 *If n, $\ell \in \mathbb{N}_0$ and $n \geq \ell$ then*

$$\sum_{k=\ell}^{n} \frac{(-1)^{n-k}}{k+1}\binom{n}{k}\binom{\ell+k}{k}\binom{k+1}{\ell+1} = \frac{1}{\ell+1}\binom{2\ell}{\ell}\binom{\ell}{n-\ell}.$$

Proof Our aim in each step is to reduce the number of appearances of the summation variable k. The $1/(k+1)$ looks particularly troublesome, but it can easily be removed using the identity $\frac{1}{k+1}\binom{k+1}{\ell+1} = \frac{1}{\ell+1}\binom{k}{\ell}$. (See Exercise 2.1 at the end of this chapter for the combinatorial proof.) Hence the left-hand side is

$$\frac{1}{\ell+1}\sum_{k=\ell}^{n}(-1)^{n-k}\binom{n}{k}\binom{\ell+k}{k}\binom{k}{\ell}.$$

Now use Lemma 2.2.4 to rewrite $\binom{n}{k}\binom{k}{\ell}$ as $\binom{n}{\ell}\binom{n-\ell}{k-\ell}$ to get

$$\frac{1}{\ell+1}\binom{n}{\ell}\sum_{k=\ell}^{n}(-1)^{n-k}\binom{n-\ell}{k-\ell}\binom{\ell+k}{k}.$$

The sum is now somewhat similar to Vandermonde's convolution, suggesting that the technique used to prove Claim 2.4.4 may be effective. Indeed, negating the binomial coefficient $\binom{\ell+k}{k}$ and applying Lemma 2.1.5 to $\binom{n-\ell}{k-\ell}$ gives

$$\frac{(-1)^n}{\ell+1}\binom{n}{\ell}\sum_{k=\ell}^{n}\binom{n-\ell}{n-k}\binom{-\ell-1}{k}$$

which simplifies, by the general version of Vandermonde's Convolution with $a = n-\ell$ and $b = \ell-1$ to $\frac{(-1)^n}{\ell+1}\binom{n}{\ell}\binom{n-2\ell-1}{n}$. Another negation gives $\frac{1}{\ell+1}\binom{n}{\ell}\binom{2\ell}{n}$ and the required form then follows from another application of Lemma 2.2.4. □

It should be admitted this identity was strategically chosen to show the methods of this chapter in a good light. Further techniques for proving binomial coefficient identities are given in the exercises below and Chapter 5, and in §8.3 and §14.2.

Exercises

The core exercises are 2.1 to 2.4. Exercises 2.1 to 2.7 were used on the problem sheet for this part of the course.

2.1 Prove that

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

for n, $k \in \mathbb{N}$ in two ways:

(a) using the formula for a binomial coefficient;

(b) bijectively.

2.2 Prove that if m, $n \in \mathbb{N}_0$ then

$$\sum_{r=0}^{n} r\binom{m}{r}\binom{n}{r} = n\binom{m+n-1}{n}.$$

[*Hint: use Exercise 2.1 and then aim to apply Vandermonde's convolution.*]

2.3 Let n, $k \in \mathbb{N}_0$. Prove if $n \geq k$ then

$$\binom{k}{k}+\binom{k+1}{k}+\binom{k+2}{k}+\cdots+\binom{n}{k} = \binom{n+1}{k+1}$$

in two ways:

(a) by induction on n (where k is fixed in the inductive argument);

(b) bijectively, by reasoning with subsets of $\{1,2,\ldots,n+1\}$. [*Hint: interpret the summand* $\binom{r}{k}$ *as counting the* $(k+1)$*-subsets of* $\{1,2,\ldots,n+1\}$ *with a specific maximum element.*]

2.4 A lion tamer has $n \in \mathbb{N}_0$ cages in a row. For $k \in \{0,1,\ldots,n\}$, let $g(n,k)$ be the number of ways in which she may accommodate k indistinguishable lions so that no cage contains more than one lion, and no two lions are housed in adjacent cages.

(a) Show that $g(n,k) = g(n-2,k-1) + g(n-1,k)$ if $n \geq 2$ and $k \geq 1$.

(b) Prove by induction that $g(n,k) = \binom{n-k+1}{k}$ for all $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$ such that $k \leq n$. [*Hint: the base cases are determined by the conditions* $n \geq 2$ *and* $k \geq 1$ *in* (a).]

(c) ($\star$) Find a bijective proof of the formula for $g(n,k)$.

2.5 Let $n, k \in \mathbb{N}$. How many solutions are there to the equation $u_1 + u_2 + \cdots + u_n = k$ if the u_r are *strictly* positive integers, that is $u_r \in \mathbb{N}$ for each r?

2.6 Define

$$b_n = \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots$$

for $n \in \mathbb{N}_0$.

(a) Find the first few terms of the sequence $b_0, b_1, b_2, b_3, \ldots$.

(b) State and prove a recurrence relating b_{n+2} to b_{n+1} and b_n. Hence identify the numbers b_n.

2.7

(a) What is 11^4? Explain the connection to binomial coefficients.

(b) Let $m \in \mathbb{N}$. Prove that

$$\binom{2m}{0} < \ldots < \binom{2m}{m-1} < \binom{2m}{m} > \binom{2m}{m+1} > \ldots > \binom{2m}{2m}$$

and that

$$\binom{2m+1}{0} < \ldots < \binom{2m+1}{m} = \binom{2m+1}{m+1} > \ldots > \binom{2m+1}{2m+1}.$$

(c) By considering a suitable binomial expansion prove that

$$\frac{4^m}{2m+1} \leq \binom{2m}{m} \leq 4^m.$$

In some of the further exercises below we use the convention that if no bounds are given on a sum then it is over all elements of $\mathbb{N}_0$. *For example, by Corollary 2.2.8*(i) *we have* $\sum_k \binom{m}{k} = 2^m$, *since* $\binom{m}{k} = 0$ *for* $k > n$.

2.8 Prove that if $m \in \mathbb{N}_0$ then

$$\sum_k \binom{m}{k}^2 = \binom{2m}{m}.$$

(The sum is defined using the convention just described.)

2.9 Show that if $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$ then

$$\sum_r \binom{n}{r}\binom{r}{k} x^r = \binom{n}{k} x^k (1+x)^{n-k}.$$

Deduce that $\displaystyle\sum_r \binom{n}{r}\binom{r}{k} = \binom{n}{k} 2^{n-k}$. Show also that $\displaystyle\sum_r (-1)^r \binom{n}{r}\binom{r}{k} = 0$, provided $n > k$.

2.10 Prove that if $m, n, k \in \mathbb{N}_0$ then

$$\sum_r \binom{r}{k}\binom{m}{r}\binom{n}{r} = \binom{n}{k}\binom{m+n-k}{n}$$

generalizing Exercise 2.2.

2.11 Let $n, m \in \mathbb{N}_0$.

(a) Prove that

$$\sum_{k=0}^{m} \left(\frac{n}{2} - k\right)\binom{n}{k} = \frac{m+1}{2}\binom{n}{m+1}.$$

(b) Deduce that $\sum_{k=0}^{m} (n-2k)\binom{n}{k} = (n-m)\binom{n}{m}$.

(c) ($\star$) Find a bijective proof of the identity in (b).

(This exercise is a generalization of Problem A4 in the 1974 Putnam Mathematical Competition, a mathematics olympiad for students at USA universities. For a probabilistic interpretation and a suggestion for further reading, see Exercise B.1.)

2.12 Given sets X and Y define their *symmetric difference* by

$$X \triangle Y = (X \cup Y) \backslash (X \cap Y).$$

Thus $X \triangle Y$ consists of the elements lying in exactly one of X and Y.

(a) Let S be the set of all subsets of a set Ω. Show that S is a commutative ring with addition defined by $X + Y = X \triangle Y$ and multiplication by $XY = X \cap Y$. (Identify the zero and one elements explicitly.)

(b) Show that $X \triangle X = \varnothing$ for all $X \in S$. Thus every element of S is its own additive inverse.

(c) Let X, Y, $Z \in S$. Show that

$$X \triangle Y = Z \iff Y \triangle Z = X \iff Z \triangle X = Y.$$

[*Hint: imagine X, Y and Z are numbers. How would you solve the equation $X + Y = Z$ for X?*]

(d) Let X, Y, Z, $W \in S$. Show that

$$X \triangle Y = Z \triangle W \iff X \triangle Z = Y \triangle W$$

and $(X \triangle Y) \cap (Z \triangle W) = (X \cap Z) \triangle (Y \cap Z)$ if and only if $X \cap Z = Y \cap W$.

2.13 Fix $k \in \mathbb{N}$. Given distinct k-subsets X and Y of $\mathbb{N}$, say that X is smaller than Y, and write $X < Y$ if the largest element of $X \cup Y$ not contained in $X \cap Y$ is in Y. This defines the *colexicographic order* on k-subsets of $\mathbb{N}$.

(a) The first six sets in the colexicographic order on 3-subsets of $\mathbb{N}$ are

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

Find the next six sets.

(b) Let $r \in \mathbb{N}$. What is the $\binom{r}{k}$th set in the colexicographic order on k-subsets of $\mathbb{N}$?

(c) Find the 2016th set in the colexicographic order on 5-subsets of $\mathbb{N}$.

(d) What is the ten millionth set in the colexicographic order on 10-subsets of $\mathbb{N}$?

(e) Give a bijective proof that if r, $m \in \mathbb{N}_0$ and $r \geq m$ then $\binom{r-m}{0} + \binom{r-m}{1} + \cdots + \binom{r}{m} = \binom{r+1}{m}$. (This is equivalent to Lemma 2.2.3.)

2.14 Give a bijective proof of Claim 2.4.4.

2.15 Some binomial identities have elegant proofs using self-inverse bijections. Such functions are known as *involutions*. The solution to Exercise 2.2.10 gives a more basic example of this method.

(a) Let $n \in \mathbb{N}$. Let

$$P = \{(X,Y) : X, Y \subseteq \{1,2,\ldots,n\}, |X| + |Y| = n\}.$$

Define $\operatorname{sgn}(X,Y) = (-1)^{|X|}$. Define $f : P \to P$ by

$$f\big((X,Y)\big) = \begin{cases} (X,Y) & \text{if } X = Y \\ \big(X \backslash \{z\}, Y \cup \{z\}\big) & \text{if } z \in X \\ \big(X \cup \{z\}, Y \backslash \{z\}\big) & \text{if } z \in Y \end{cases}$$

where z is the maximum element of $X \triangle Y$. (For the definition of $\triangle$ see Exercise 2.12. Note that $X \triangle Y$ is non-empty, and so has a maximum, whenever this definition uses z.) Show that f is an involution on P and that if $f\big((X,Y)\big) \neq (X,Y)$ then $\operatorname{sgn} f(X,Y) = -\operatorname{sgn}(X,Y)$. Deduce that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^2 = \begin{cases} (-1)^{n/2}\binom{n}{n/2} & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ odd.} \end{cases}$$

(For a simpler proof see Exercise 5.2.)

(b) Let $n \in \mathbb{N}_0$. Adapt the involution in (a) to prove that

$$\sum_{k=1}^{n} (-1)^k \binom{n}{k}\binom{n}{k-1} = \begin{cases} 0 & \text{if } n \text{ is even} \\ (-1)^{(n+1)/2}\binom{n}{(n+1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

The following exercises use the generalized definition of binomial coefficients introduced in §2.4

2.16

(a) Let $h(z) = a_0 + a_1 z + \cdots + a_d z^d$ be a polynomial in $\mathbb{C}[z]$. Show that if there exist distinct complex numbers $c_1, c_2, \ldots, c_{d+1} \in \mathbb{C}$ such that $h(c_i) = 0$ for all $i \in \{1, 2, \ldots, d+1\}$ then $h = 0$.

(b) Hence show that if f and g are polynomials of degree at most d that agree at $d+1$ distinct elements of $\mathbb{C}$ then $f = g$.

2.17 Let $b \in \mathbb{N}$ and let $n \in \mathbb{N}_0$. Give a bijective proof that $(b+1)^n = \sum_k \binom{n}{k} b^k$. Deduce the Binomial Theorem using the previous exercise.

2.18 Show that if $z \in \mathbb{C}$ and $n \in \mathbb{N}_0$ then

$$\sum_{r=0}^{m} (-1)^r \binom{z+1}{r} r = (-1)^m \binom{z-1}{m-1}(z+1).$$

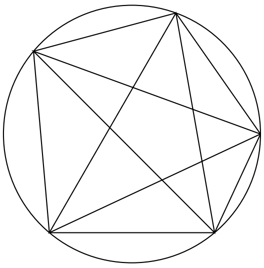
2.19 Let $f(z) = z^3 - 3z^2 + 1$. The table below has $f(0), f(1), \ldots, f(6)$ in its first row. Each entry in each subsequent row is computed by taking the difference between the two entries in the row above.

$$\begin{array}{ccccccccccccc}
1 & & -1 & & -3 & & 1 & & 17 & & 51 & & 109 \\
 & -2 & & -2 & & 4 & & 16 & & 34 & & 58 & \\
 & & 0 & & 6 & & 12 & & 18 & & 24 & & \\
 & & & 6 & & 6 & & 6 & & 6 & & & \\
 & & & & 0 & & 0 & & 0 & & & &
\end{array}$$

(a) Show that $f(z) = 6\binom{z}{3} + 0\binom{z}{2} - 2\binom{z}{1} + \binom{z}{0}$. What is the connection with the table? (The connection is proved in Exercise 2.21.)

(b) Find a polynomial $g(z)$ of small degree such that $g(0), g(1), g(2), g(3), g(4)$ equal $0, 1, 0, -1, 0$, respectively.

2.20 Let a_n be the maximum number of regions inside a circle that can be formed by taking n points on its circumference and joining every two distinct points by a line. For example, counting regions in the diagram below shows that $a_5 = 16$.



(a) Find a_1, a_2, a_3, a_4.

(b) Conjecture (if you feel brave) a formula for a_n.

(c) Find a_0 and a_6.

(d) Using the table method in Exercise 2.19 conjecture a formula for a_n.

(The formula given by (d) is in fact correct: this is proved in Exercise 6.1 using generating functions.)

2.21 Given a function $f : \mathbb{C} \to \mathbb{C}$, define $\Delta f : \mathbb{C} \to \mathbb{C}$ by $(\Delta f)(z) = f(z+1) - f(z)$. Set $\Delta^0 f = f$ and define $\Delta^k f = \Delta(\Delta^{k-1} f)$ inductively for $k \in \mathbb{N}$. For example, if $f(z) = z^2$ then $(\Delta f)(z) = (z+1)^2 - z^2 = 2z + 1$ and hence $(\Delta^2 f)(z) = (2(z+1)+1) - (2z+1) = 2$.

(a) Prove by induction on n that

$$\Delta^n \binom{z}{r} = \begin{cases} \dbinom{z}{r-n} & \text{if } 0 \leq n \leq r \\ 0 & \text{otherwise.} \end{cases}$$

(b) Let $b(z) = \binom{z}{r}$. Let $k \in \mathbb{N}_0$. Show that $(\Delta^n b)(0) = 1$ if $k = n$ and $(\Delta^n b)(0) = 0$ if $k \neq r$.

(c) Show that the binomial coefficients $\binom{z}{r}$ for $r \in \mathbb{N}_0$ are a basis for $\mathbb{C}[z]$. (Equivalently, for each polynomial $f(z) \in \mathbb{C}[z]$ of degree d, there exist unique coefficients $c_0, c_1, \ldots, c_d \in \mathbb{C}$ such that $f(z) = \sum_{r=0}^{d} c_r \binom{z}{r}$.)

(d) Using (b) and (c) show that if $f(z)$ is a polynomial of degree at most d then $f(z) = \sum_{r=0}^{d} c_r \binom{z}{r}$ where $c_r = (\Delta^r f)(0)$ and that the coefficients $c_0, c_1, \ldots, c_d$ are the entries on the diagonal of a table constructed as in Exercise 2.19.

(e) Show that $(\Delta^n f)(z) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} f(z+n-k)$.

2.22 Let $z \in \mathbb{C}$ and let $m \in \mathbb{N}_0$. Prove that

$$\sum_{k=0}^{2m} (-1)^k \binom{2m}{k} \binom{z}{k} \binom{z}{2m-k} = (-1)^m \binom{2m}{m} \binom{z+m}{2m}.$$

by showing that the two sides are equal for $z \in \{-m, \ldots, -1, 0, 1, \ldots, m\}$. Deduce Dixon's Identity,

$$\sum_{k=0}^{2m} (-1)^k \binom{2m}{k}^3 = (-1)^m \frac{(2m)!}{m!^3}.$$

Interlude I: The Egg Dropping Problem

Problem *You are given three Fabergé eggs by the owner of a building with* 100 *floors. The owner wants to know the highest floor from which an egg will survive being dropped. What is the smallest number of drops that guarantees to give the correct answer?*

(The eggs are identical in every respect. If an egg smashes it is gone for ever, if it survives the fall then it is as good as new. It is possible that the eggs can survive the drop from floor 100.)

Hints

Try simplifying the problem: take two eggs and a building with 10 floors.

- How many drops might be needed if the first egg is dropped from floor 5?
- How many drops might be needed if the first egg is dropped from floor 3?
- How is the optimal floor for the first drop related to the total number of drops, in the worst case for your strategy?

Now solve the problem for some other small buildings and look for a pattern.

Solution

Following the hints, we start by looking at the smaller two egg problem. You should have found that if there are 10 floors and the first egg is dropped from floor 4 then 4 drops always suffice:

- if the first drop smashes an egg then we drop the remaining egg from floor 1, then floor 2 (if it survives), then floor 3 (if it survives again);
- if the egg survives the first drop then, after making the next drop from floor 7, two more drops suffice.

Exercise Check the second claim above, and show, if you have not already done so, that if the first drop is made from floor 5 or floor 3 then four more drops (making five in total) may be necessary.

The analysis so far shows two key ideas:

(A) If we are down to one egg, because the other egg smashed when dropped from floor r, and we have not made any drops from floors below r, then there is nothing better than to make up to $r-1$ further drops working from floor 1 upwards.

(B) If an egg survives a drop from floor r then we can ignore floors 1 up to r, and think of the building as having $n-r$ floors.

Let $f(n)$ be the number of drops needed, in the worst case, to find the highest egg-safe floor in a building of n floors. Suppose we make the first drop from floor r. If this smashes an egg then, by (A), we need at most $r-1$ further drops. If it survives then, by (B), we need at most $f(n-r)$ further drops. (This is correct even when $r=n$, provided we set $f(0)=0$.) Hence

$$f(n) \le 1+\max\bigl(r-1,\, f(n-r)\bigr) = \max\bigl(r,\, 1+f(n-r)\bigr) \qquad (\star)$$

for each $r \in \mathbb{N}$ with $r \le n$. Moreover, the true value of $f(n)$ is given by choosing r to minimize the right-hand side of $(\star)$. Using $(\star)$ and computing iteratively, starting with $f(1)=1$, we get the table shown below.

n	0	1	2	3	4	5	6	7	8	9	10	11
$f(n)$	0	1	2	2	3	3	3	4	4	4	4	5

For example, if $n=5$ we have $f(5) \le \max(1, f(4)+1) = 4$, $f(5) \le \max(2, f(3)+1) = 3$, $f(5) \le \max(3, f(2)+1) = 3$, $f(5) \le \max(4, f(1)+1) = 4$ and $f(5) \le \max(5, f(0)+1) = 5$. So $f(5)=3$ and we can drop the first egg from either floor 2 or floor 3.

Exercise Check some more entries from the table. In each case, show that an optimal strategy drops the first egg from floor $f(n)$.

The jumps in $f(n)$ occur immediately after the triangle numbers 1, 3, 6, 10, ... This motivates the following conjecture.

Conjecture *For all $n \in \mathbb{N}$, $f(n)$ is the minimum d such that $\binom{d+1}{2} \ge n$. Moreover, an optimal strategy drops the first egg from floor d.*

Proof We work by induction on n. If $n=1$ then after dropping an egg from floor 1 we know the highest egg-safe floor. Hence $f(1)=1$, and correspondingly, the minimal d such that $\binom{d+1}{2} \ge 1$ is 1. Now let $n \in \mathbb{N}$ and let d be minimal such that

$\binom{d+1}{2} \geq n$. If the first drop is from floor d then $(\star)$ gives

$$f(n) \leq \max(d,\, 1 + f(n-d)). \qquad (\dagger)$$

Since $\binom{d+1}{2} - d = \binom{d+1}{2} - \binom{d}{1} = \binom{d}{2}$, we have $\binom{d}{2} \geq n - d$. Hence $f(n-d)$, being the minimal e such that $\binom{e+1}{2} \geq n - d$, satisfies $f(n-d) \leq d - 1$. Suppose $f(n-d) \leq d-2$. Then $\binom{d-1}{2} \geq n - d$, and repeating the previous argument in reverse, we get $\binom{d}{2} \geq n$, contradicting the minimality of d. Therefore $f(n-d) = d-1$ and $(\dagger)$ implies that $f(n) \leq \max(d,d) = d$.

Now suppose that there is an optimal strategy in which the first drop is from floor r. By (A) we have $r \leq d$. If the egg survives then, by (B), and we may need $f(n-r)$ more drops. Since $n - r \geq n - d$, we have $f(n-r) \geq f(n-d) = d-1$. Therefore $\max\bigl(r,\, 1 + f(n-r)\bigr) \geq 1 + f(n-r) \geq 1 + (d-1) = d$. Hence dropping from floor d is optimal and $f(n) = d$. □

It is possible to solve the 3 egg problem by generalizing this argument. But the analysis so far motivates a much more elegant approach. For brevity, let us say that $f(n)$ drops *solve* a building with n floors. Note that $\binom{\sqrt{2n}}{2} = \sqrt{2n}(\sqrt{2n}+1)/2 = n + \sqrt{n/2} \geq n$, so we have $f(n) \leq \sqrt{2n}$. (This uses the generalized definition of binomial coefficients introduced in §2.4.) The square-root function is not so easy to work with, and is responsible for the slow, but jumpy, growth of $f(n)$. Maybe it would be more convenient to work with something like an inverse function ....

Let $g(d)$ be the number of floors in the tallest building that can be solved using at most d drops of two eggs. We know that a building of height $\binom{d+1}{2}$ can be solved with d drops, so $g(d) \geq \binom{d+1}{2}$.

Conjecture *If $d \in \mathbb{N}$ then $g(d) = \binom{d+1}{2}$.*

Proof Let $n = \binom{d+1}{2}$. By the conjecture before this, d drops suffice to solve a building of height n, and d drops do not suffice to solve a building of height $n+1$, since $\binom{d+1}{2} < n+1$. □

Generalizing the definition of g, let $g_e(d)$ be the number of floors in the tallest building that can be solved using at most d drops of e eggs. Clearly $g_e(1) = 1$ for all $e \in \mathbb{N}$ and, by (A), $g_1(d) = d$ for all $d \in \mathbb{N}$. We now run the argument proving the first conjecture, thinking about g_e. An instructive exercise is to prove the following claim in the special case $e = 2$.

Claim *For any d, $e \in \mathbb{N}$ we have $g_e(d) = g_{e-1}(d-1) + g_e(d-1) + 1$.*

Proof Let $n = g_e(d)$. Suppose an optimal strategy drops the first egg from floor r. If it smashes, we are left with $e-1$ eggs and $d-1$ drops to deal with a building of effective height $r-1$. Hence $r - 1 \leq g_{e-1}(d-1)$. If the first egg survives, we have e eggs and $d-1$ drops to deal with a building of effective height $n-r$. Hence $n-r \le g_e(d-1)$. Adding these two inequalities implies that

$$g_e(d) \le g_{e-1}(d-1) + g_e(d-1) + 1. \qquad (\star\star)$$

Moreover, taking $r = g_{e-1}(d-1)+1$ we see that a building with $g_{e-1}(d-1) + g_e(d-1)+1$ floors can be solved using d drops. Hence equality holds. □

Using the recurrence ($\star\star$) and the boundary conditions $g_e(1) = 1$ and $g_1(d) = d$, it is easy to calculate the following table of values for small d and e.

$d\backslash e$	1	2	3	4	5	6
1	1	1	1	1	1	1
2	2	3	3	3	3	3
3	3	6	7	7	7	7
4	4	10	14	15	15	15
5	5	15	25	30	31	31
6	6	21	41	56	62	63
7	7	28	63	98	119	126
8	8	36	92	162	218	246
9	9	45	129	255	381	465
10	10	55	175	385	637	847

From the table we see that with 3 eggs, 8 drops do not suffice to solve a building with 100 floors, but 9 drops are sufficient. (In fact 9 drops can solve a building with 129 floors.) This answers the original problem.

The values of $g_1(d)$ and $g_2(d)$ appearing in the first and second column and the almost powers of 2 along the diagonal now suggest a final conjecture.

Conjecture *For all d, $e \in \mathbb{N}$ we have*

$$g_e(d) = \binom{d}{1} + \binom{d}{2} + \cdots + \binom{d}{e}.$$

Proof We work by induction on d. If $d = 1$ then we have $g_e(1) = 1$, which agrees with $\binom{1}{1} + \binom{1}{2} + \cdots + \binom{1}{e} = 1$. Suppose inductively that the conjecture holds for $d-1$. Then, by ($\star\star$) and the Fundamental Recurrence (Lemma 2.1.7) we get

$$\begin{aligned} g_e(d) = g_{e-1}(d-1) + g_e(d-1) + 1 &= \sum_{k=1}^{e-1}\binom{d-1}{k} + \sum_{k=1}^{e}\binom{d-1}{k} + 1 \\ &= \sum_{k=1}^{e-1}\left(\binom{d-1}{k} + \binom{d-1}{k+1}\right) + \binom{d-1}{1} + 1 = \sum_{k=1}^{e-1}\binom{d}{k+1} + d = \sum_{k=1}^{e}\binom{d}{k} \end{aligned}$$

as required. □

Going back to the inverse function, we see that the minimum number of drops of e eggs needed, in the worst case, to find the highest egg-safe floor in a building with n floors is the minimum d such that $\binom{d}{1} + \binom{d}{2} + \cdots + \binom{d}{e} \geq n$.

Final discussion

After solving a problem, it is very tempting to (metaphorically) throw a quick party with oneself as the guest of honour, and then forget all about it. But often the greatest insights come from asking oneself further questions: "Is there an easier solution?", "Is the answer intuitive?", "What techniques did I use that might be applicable elsewhere?", "Are there appealing generalizations or connections with other areas of mathematics?" Here are some thoughts suggested by these questions.

- To get started we generalized the problem, by allowing buildings of arbitrary height and any number of eggs, before simplifying it, by considering just two eggs and small buildings. It is often useful, but humbling, to ask "What is the simplest related problem that I still can't solve?"
- One key idea was to switch from minimizing the number of drops, for a fixed building height, to maximizing the building height, for a fixed number of drops. This kind of 'inversion' is a common theme in mathematics. Jacobi, who made important contributions to the theory of elliptic functions using inversion, famously said "man muss immer umkehren" (one must always invert).
- The proof of the recurrence $g_e(d) = g_{e-1}(d-1) + g_e(d-1) + 1$ shows that when we drop the first egg from floor $g_{e-1}(d-1)+1$ in a building with $g_e(d)$ floors, we are indifferent to the outcome. If the egg smashes, we are left with a building of effective height $g_{e-1}(d-1)$, solvable in $d-1$ drops with the remaining $e-1$ eggs; if it survives we are left with a building of effective height $g_e(d) - (g_{e-1}(d-1)+1) = g_e(d-1)$, solvable in $d-1$ drops of the e eggs. This feature, that with optimal play we are indifferent to our adversary's response, often appears in the analysis of games.
- When we started, computing even the two-egg number $f(10)$ was a non-trivial problem. At the end, the explicit formula for $g_e(d)$ gives a fast algorithm for finding the number of drops needed to solve any building, with any number of eggs. As seen earlier for the derangement numbers, better understanding leads to faster computation.
- Next we ask "Is the answer intuitive?" Suppose we make d drops. Interpreting $\binom{d}{s}$ as the number of ways to choose s of these drops to smash an egg, we see that the number of different outcomes of a sequence of d drops is $\binom{d}{1} + \binom{d}{2} +$

$\cdots + \binom{d}{e}$. Hence, using d drops, we can distinguish at most $\binom{d}{1} + \binom{d}{2} + \cdots + \binom{d}{e}$ outcomes, and so $g_e(d) \leq \binom{d}{1} + \binom{d}{2} + \cdots + \binom{d}{e}$. Given this, it is a reasonable guess that equality is attained, and one can jump immediately to the recurrence $(\star\star)$ to prove this.

- Finally, if you have done some coding theory, you might remember the definition of the *Hamming ball of radius r* about a vector $w \in \mathbb{F}_2^n$ as the set of all $v \in \mathbb{F}_2^n$ such that v differs from w in at most r positions. For example, the Hamming ball of radius 2 about $(1,1,1) \in \mathbb{F}_2^3$ is $\mathbb{F}_2^3 \backslash \{(0,0,0)\}$. By the final conjecture, $g_e(d)+1$ is the size of a Hamming ball of radius e in $\mathbb{F}_2^d$. The previous remark goes some way to explaining this surprising connection.

Exercise Investigate the asymptotics of $g_e(d)$. [*Hint: Shannon's entropy function is relevant.*]

3

Principle of Inclusion and Exclusion

3.1 Introduction to the Principle of Inclusion and Exclusion

The Principle of Inclusion and Exclusion is a way to find the size of the union of a finite collection of subsets of a finite *universe set*, Ω. Typically we really want the complement of the union. We start with the two smallest non-trivial examples.

If X is a subset of Ω, its *complement* in Ω is

$$\overline{X} = \{x \in \Omega : x \notin X\}.$$

Clearly $|\overline{X}| = |\Omega| - |X|$.

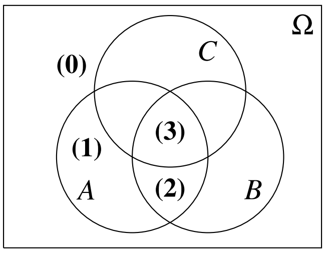
Example 3.1.1 Let A and B be subsets of the finite universe set Ω. In $|A| + |B|$, each member of $A \cap B$ is counted twice. To count $|A \cup B|$ we must therefore subtract $|A \cap B|$, giving $|A \cup B| = |A| + |B| - |A \cap B|$. Taking the complement we get

$$|\overline{A \cup B}| = |\Omega| - |A| - |B| + |A \cap B|.$$

Now let C be a further subset of Ω. We claim that

$$|\overline{A \cup B \cup C}| = |\Omega| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|.$$

The Venn diagram and table below show the non-zero contributions from the members of each region to the right-hand side. Up to symmetry, there are four cases. For example, in case **(2)**, $x \in A \cap B \cap \overline{C}$ is counted in the summands $|\Omega|$, $-|A|$, $-|B|$ and $|A \cap B|$, for an overall contribution of $1 - 1 - 1 + 1 = 0$.

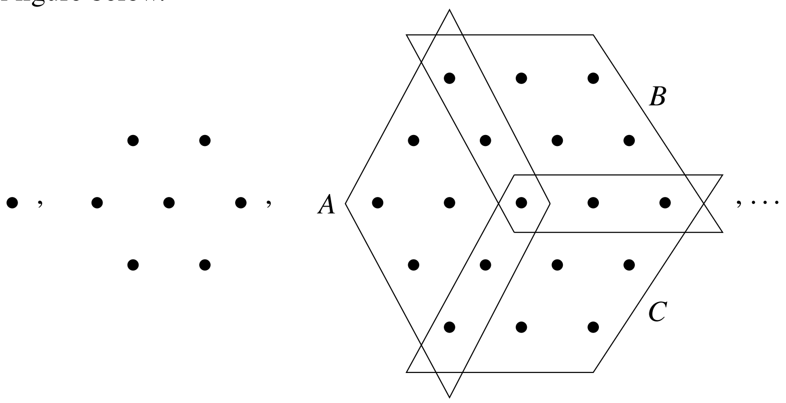


(0)	$\overline{A} \cap \overline{B} \cap \overline{C}$	1
(1)	$A \cap \overline{B} \cap \overline{C}$	$1 - 1$
(2)	$A \cap B \cap \overline{C}$	$1 - 1 - 1 + 1$
(3)	$A \cap B \cap C$	$1 - 1 - 1 - 1 + 1 + 1 + 1 - 1$

Thus elements of $\overline{A}\cap\overline{B}\cap\overline{C}=\overline{A\cup B\cup C}$ each contribute 1, and all other elements of Ω contribute 0, as required. Taking the complement we get

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

Example 3.1.2 The m-th (centred) hexagonal number h_m is the number of dots in the m-th figure below.



Let A, B, C be the three rhombic subsets of the m-th diagram, as indicated above for h_3. By counting dots we see that $|A| = m^2$, $|A\cap B| = m$ and $|A\cap B\cap C| = 1$. Hence, by symmetry and the final formula in Example 3.1.1,

$$h_m = m^2+m^2+m^2-m-m-m+1 = 3m(m-1)+1.$$

Observe that it was easier to find the sizes of the intersections of the three rhombi than it was to find the size of their unions. Whenever intersections are easier to think about than unions, the Principle of Inclusion and Exclusion may be helpful.

In the general result, we have subsets $A_1, A_2, \dots, A_n \subseteq \Omega$. For each non-empty subset $I \subseteq \{1,2,\dots,n\}$ we define

$$A_I = \bigcap_{i\in I} A_i.$$

Thus A_I is the set of elements which belong to each set A_i for $i\in I$. (We deliberately do not specify which other sets, if any, these elements lie in.) For example $x\in A_{\{1,3\}}$ if and only if $x\in A_1$ and $x\in A_3$. More generally, if $i,j\in\{1,2,\dots,n\}$ then $A_{\{i\}} = A_i$ and $A_{\{i,j\}} = A_i\cap A_j$. By convention the empty intersection is the universe set Ω. Thus

$$A_\emptyset = \Omega.$$

Theorem 3.1.3 (Principle of Inclusion and Exclusion) *If $A_1, A_2, \dots, A_n$ are subsets of a finite universe set Ω then*

$$|\overline{A_1\cup A_2\cup\cdots\cup A_n}| = \sum_{I\subseteq\{1,2,\dots,n\}} (-1)^{|I|}|A_I|.$$

Exercise 3.1.4 Check that you understand the A_I notation by writing out the Principle of Inclusion and Exclusion when $n = 3$ as a sum with eight summands and comparing with Example 3.1.1.

We prove the Principle of Inclusion and Exclusion by generalizing the argument in Example 3.1.1. We need the identity $\sum_{k=0}^{m}(-1)^k\binom{m}{k} = 0$ for $m \in \mathbb{N}$, proved in Corollary 2.2.8(ii) by expanding $(-1+1)^m$ using the Binomial Theorem. The special case $\binom{3}{0} - \binom{3}{1} + \binom{3}{2} - \binom{3}{3} = 0$ may be seen in case **(3)** of this example.

Proof of Theorem 3.1.3 Let $x \in \Omega$. Suppose that x is not a member of any of the sets $A_1, A_2, \ldots, A_n$. Then x is counted once on the left-hand side. Since $A_\emptyset = \Omega$, on the right-hand side x contributes 1 to $|A_\emptyset|$ and 0 to every other summand, giving an overall contribution of 1, as required.

Now suppose that $x \in A_j$ if and only if $j \in J$, where J is a non-empty subset of $\{1,2,\ldots,n\}$. On the right-hand side, x contributes to $|A_I|$ if and only if x lies in A_i for every $i \in I$, so if and only if $I \subseteq J$. Hence the contribution from x to the right-hand side is $\sum_{I\subseteq J}(-1)^I$. Since there are $\binom{|J|}{k}$ subsets of J of size k, this sum is

$$\sum_{k=0}^{|J|}(-1)^k\binom{|J|}{k} = 0$$

where the final equality is the case $|J| = m$ of the identity just mentioned. Hence the contribution of x to the right-hand side is 0, again as required. □

Exercise 3.1.5 Deduce from Theorem 3.1.3 that

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ I\neq\emptyset}} (-1)^{|I|-1}|A_I|.$$

Exercises 3.14 and 3.15 strengthen the Principle of Inclusion and Exclusion, using a more formal argument in which a function from Ω to $\mathbb{Z}$ records the contributions from each $x \in \Omega$ to its right-hand side.

3.2 Counting derangements

The Principle of Inclusion and Exclusion gives a particularly elegant proof of the formula for the derangement numbers d_n first proved in Corollary 1.1.9:

$$d_n = n!\big(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\big).$$

Recall from Definition 1.1.2 that a permutation $\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ is a derangement if and only if it has no fixed points. Let Ω be the set of all permutations of $\{1,2,\ldots,n\}$. Let A_i be the set of permutations we *do not want to count*, because they fix i. (The permutation in A_i might have other fixed points too, but in the spirit of the Principle of Inclusion and Exclusion, we use just one property to define A_i.) Thus

$$A_i = \{\sigma \in \Omega : \sigma(i) = i\}$$

and $\overline{A_1 \cup A_2 \cup \ldots \cup A_n}$ is the set of derangements. To apply the Principle of Inclusion and Exclusion we need to know the sizes $|A_I|$ on its right-hand side.

Lemma 3.2.1 *Let $\sigma \in \Omega$ and let $I \subseteq \{1,2,\ldots,n\}$. Then $\sigma \in A_I$ if and only if $\sigma(i) = i$ for all $i \in I$. Moreover $|A_I| = (n-|I|)!$.*

Proof Let σ be a permutation of $\{1,\ldots,n\}$. Then $\sigma \in A_I$ if and only if $\sigma \in A_i$ for each $i \in I$, so if and only if σ fixes every element of I. The remaining elements in $\{1,\ldots,n\}\backslash I$ can be permuted in any way. (For instance, some might be fixed.) Since there are $(n-|I|)!$ permutations of $\{1,\ldots,n\}\backslash I$, we have $|A_I| = (n-|I|)!$. □

We are now ready to apply the Principle of Inclusion and Exclusion to the right-hand side in $d_n = |\overline{A_1 \cup \ldots \cup A_n}|$. It gives

$$d_n = \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{|I|}|A_I| = \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{|I|}(n-|I|)! = \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)!.$$

The final equality holds because there are $\binom{n}{k}$ subsets of $\{1,\ldots,n\}$ of size k, and for each such subset I, we have $(-1)^{|I|}(n-|I|)! = (-1)^k(n-k)!$. Since $\binom{n}{k}(n-k)! = n!/k!$ by Lemma 2.1.4, it follows that

$$d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

as expected.

3.3 Counting five card hands

We apply the Principle of Inclusion and Exclusion to solve Exercise 1.6 on counting hands of five cards from a standard deck. The universe set Ω is all $\binom{52}{5}$ hands of five cards. Let H be those hands with at least one Ace, King and Queen. We have three relevant types of card, so we aim to express H as $\overline{C_{\mathrm{A}} \cup C_{\mathrm{K}} \cup C_{\mathrm{Q}}}$ for three well-chosen subsets of Ω.

Exercise 3.3.1 Think of C_{K} as those hands we *do not want to count*, because of a reason to do with the King. What property defines C_{K}?

The answer is that C_{K} is the set of hands with no King. (Again the hands in C_{K} might also be unwanted because they lack other cards.) The notation C_{K} is chosen to suggest 'King complement'. Similarly, C_{A} is the set of hands with no Ace, and C_{Q} is the set of hands with no Queen. A hand is in H if and only if it is in none of C_{A}, C_{K} and C_{Q}, hence $H = \overline{C_{\mathrm{A}} \cup C_{\mathrm{K}} \cup C_{\mathrm{Q}}}$. Of the 52 cards in the pack, 48 are not aces, so $|C_{\mathrm{A}}| = \binom{48}{5}$. Similarly $|C_{\mathrm{K}}| = |C_{\mathrm{Q}}| = \binom{48}{5}$. There are 44 cards that are not Aces or Kings, so $|C_{\mathrm{A}} \cap C_{\mathrm{K}}| = \binom{44}{5}$, and similarly $|C_{\mathrm{A}} \cap C_{\mathrm{Q}}| = |C_{\mathrm{K}} \cap C_{\mathrm{Q}}| = \binom{44}{5}$. Finally $|C_{\mathrm{A}} \cap C_{\mathrm{K}} \cap C_{\mathrm{Q}}| = \binom{40}{5}$. By the Principle of Inclusion and Exclusion, in the three subset case from Example 3.1.1, we get

$$\begin{aligned}|\overline{C_{\mathrm{A}} \cup C_{\mathrm{K}} \cup C_{\mathrm{Q}}}| &= |\Omega| - |C_{\mathrm{A}}| - |C_{\mathrm{K}}| - |C_{\mathrm{Q}}| \\ &\qquad + |C_{\mathrm{A}} \cap C_{\mathrm{K}}| + |C_{\mathrm{A}} \cap C_{\mathrm{Q}}| + |C_{\mathrm{K}} \cap C_{\mathrm{Q}}| - |C_{\mathrm{A}} \cap C_{\mathrm{K}} \cap C_{\mathrm{Q}}| \\ &= \binom{52}{5} - 3\binom{48}{5} + 3\binom{44}{5} - \binom{40}{5} \\ &= 62064.\end{aligned}$$

You should now have no difficulty in counting the five card hands in Exercise 1.6(a) with at least one Ace, King, Queen and Jack. The answer, from the Principle of Inclusion and Exclusion applied with four sets, is $\binom{52}{5} - 4\binom{48}{5} + 6\binom{44}{5} - 4\binom{40}{5} + \binom{36}{5} = 10752$.

Part of the strength of the Principle of Inclusion and Exclusion is that, once one has grasped one application, it can often be adapted to solve similar problems. As an example (see also Exercise 3.4), we count hands with at least one Ace, King and Queen, and at least one of the two red Jacks. We redefine C_{J} to be those hands we *do not want to count*, because they are missing both red Jacks. Thus $|C_{\mathrm{J}}| = \binom{50}{5}$, and, for instance, $|C_{\mathrm{A}} \cap C_{\mathrm{J}}| = \binom{46}{5}$, and $|C_{\mathrm{A}} \cap C_{\mathrm{K}} \cap C_{\mathrm{J}}| = \binom{42}{5}$. The number of hands is

$$\binom{52}{5} - 3\binom{48}{5} - \binom{50}{5} + 3\binom{44}{5} + 3\binom{46}{5} - \binom{40}{5} - 3\binom{42}{5} + \binom{38}{5} = 5504.$$

3.4 Prime numbers and Euler's ϕ function

The Sieve of Eratosthenes

Start by writing out the numbers $1, 2, 3, \ldots, M$ for an M of your choice. Immediately cross out 1. On each subsequent step, circle the smallest unmarked number, and then cross out all its proper multiples. (After the first step, some of these multiples may already have been crossed out.) Stop when no number is unmarked. Since a number gets circled if and only if it is not 1 and not divisible by any smaller number, the circled numbers are precisely the primes. For example, the diagram overleaf shows the sieve on $\{1, 2, 3, \ldots, 48\}$ after crossing out the multiples of 2, 3 and 5. Any composite number in $\{1, 2, \ldots, 48\}$ is divisible by one of the primes 2, 3 or 5, so the uncrossed numbers are precisely the primes between 2 and 48. In each subsequent step, a prime is circled, and there are no new crossings-out.

$\xcancel{1}$	$\textcircled{2}$	$\textcircled{3}$	$\xcancel{4}$	$\textcircled{5}$	$\xcancel{6}$	7	$\xcancel{8}$	$\xcancel{9}$	$\xcancel{10}$
11	$\xcancel{12}$	13	$\xcancel{14}$	$\xcancel{15}$	$\xcancel{16}$	17	$\xcancel{18}$	19	$\xcancel{20}$
$\xcancel{21}$	$\xcancel{22}$	23	$\xcancel{24}$	$\xcancel{25}$	$\xcancel{26}$	$\xcancel{27}$	$\xcancel{28}$	29	$\xcancel{30}$
31	$\xcancel{32}$	$\xcancel{33}$	$\xcancel{34}$	$\xcancel{35}$	$\xcancel{36}$	37	$\xcancel{38}$	$\xcancel{39}$	$\xcancel{40}$
41	$\xcancel{42}$	43	$\xcancel{44}$	$\xcancel{45}$	$\xcancel{46}$	47	$\xcancel{48}$		

We now interpret the diagram using the Principle of Inclusion and Exclusion. Generally let $\Omega = \{1, 2, \ldots, M\}$ and for $m \in \mathbb{N}$ let

$$D(m) = \{x \in \Omega : x \text{ is divisible by } m\}.$$

Example 3.4.1 Take $\Omega = \{1, 2, \ldots, 48\}$. We have seen that any composite number in Ω is in the set $D(2) \cup D(3) \cup D(5)$. Also this set contains 2, 3 and 5. The complement of $D(2) \cup D(3) \cup D(5)$ is therefore all the primes $p \in \Omega$ such that $p \geq 7$, *together with* 1. (This appearance of 1 is annoying, but inevitable, since 1 is clearly not in $D(2) \cup D(3) \cup D(5)$.) In symbols,

$$\{1\} \cup \{p \in \Omega : p \geq 7 \text{ and } p \text{ is prime}\} = \overline{D(2) \cup D(3) \cup D(5)}.$$

Let Q be the size of either side. By the Principle of Inclusion and Exclusion,

$$\begin{aligned} Q = |\Omega| - |D(2)| - |D(3)| - |D(5)| + |D(2) \cap D(3)| \\ + |D(2) \cap D(5)| + |D(3) \cap D(5)| - |D(2) \cap D(3) \cap D(5)|. \end{aligned}$$

Either using Lemma 3.4.2 below, or by direct enumeration, one finds that $Q = 48 - 24 - 16 - 9 + 8 + 4 + 3 - 1 = 13$. For example, since a number is divisible by 3 and 5 if and only if it is divisible by 15, $D(3) \cap D(5) = D(15) = \{15, 30, 45\}$. Reintroducing the primes 2, 3, and 5, and remembering to remove the non-prime 1, we have shown that there are $13 + 3 - 1 = 15$ primes in $\{1, 2, \ldots, 48\}$. Observe that we did this using only properties of 2, 3 and 5.

Sieves and the ϕ function

We start by finding the sizes of the sets $D(d)$. Recall that if $y \in \mathbb{R}$ then $\lfloor y \rfloor$ is the greatest natural number s such that $s \leq y$. For instance $\lfloor 2 \rfloor = \lfloor \frac{5}{2} \rfloor = \lfloor \mathrm{e} \rfloor = 2$. It is often useful that if $c \in \mathbb{Z}$ then $c \leq y$ if and only if $c \leq \lfloor y \rfloor$.

Lemma 3.4.2 *Let $M \in \mathbb{N}$. There are exactly $\lfloor M/d \rfloor$ numbers in $\{1,2,\ldots,M\}$ that are divisible by d.*

Proof For $x \in \mathbb{N}$ we have $xd \leq M$ if and only if $x \leq M/d$. By the useful property of the floor function, this holds if and only if $x \leq \lfloor M/d \rfloor$. □

We can now generalize Example 3.4.1 to a sieve over an arbitrary set of primes.

Proposition 3.4.3 *Let p_1, p_2, $\ldots$, p_n be distinct prime numbers and let $M \in \mathbb{N}$. Let S be the set of numbers in $\{1,2,\ldots,M\}$ that are not divisible by any of primes p_1, p_2, $\ldots$, p_n. Then*

$$|S| = \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \left\lfloor \frac{M}{\prod_{i \in I} p_i} \right\rfloor .$$

Proof Let $\Omega = \{1,2,\ldots,M\}$. The numbers in $D(p_i)$ are those we *do not want to count*, because they are divisible by p_i. (Again, they might also be unwanted because they are divisible by other primes, but we define $D(p_i)$ using p_i only.) Therefore $S = \overline{D(p_1) \cup \ldots \cup D(p_n)}$. Let $I \subseteq \{1,\ldots,n\}$. Since the p_i are distinct primes, a number is divisible by p_i for all $i \in I$ if and only if it is divisible by $\prod_{i \in I} p_i$. Thus $\bigcap_{i \in I} D(p_i) = D\bigl(\prod_{i \in I} p_i\bigr)$. (When $I = \varnothing$ this holds by our convention that the empty intersection is the universe Ω; by a standard convention, the empty product is 1.) By Lemma 3.4.2 and the Principle of Inclusion and Exclusion, we get

$$|S| = \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \Bigl| \bigcap_{i \in I} D(p_i) \Bigr| = \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \left\lfloor \frac{M}{\prod_{i \in I} p_i} \right\rfloor$$

as required. □

We say that natural numbers are *coprime* if they share no prime factors. Let $\phi(M)$ be the number of natural numbers in $\{1,2,\ldots,M\}$ that are coprime to M. For example, $\phi(15) = 8$ counts 1, 2, 4, 7, 8, 11, 13, 14.

Observe that if M has distinct prime factors $p_1, p_2, \ldots, p_n$ then $x \in \{1,2,\ldots,M\}$ is coprime to M if and only if x is not divisible by any of p_1, p_2, $\ldots$, p_n. Hence $\phi(M) = |S|$ where S is the set in Proposition 3.4.3. Since each product $\prod_{i \in I} p_i$ divides M exactly, we have

$$\phi(M) = M \sum_{I \subseteq \{1,2,\ldots,n\}} \frac{(-1)^{|I|}}{\prod_{i \in I} p_i} .$$

For example, if $M = 15$ then $p_1 = 3$ and $p_2 = 5$ and

$$\phi(15) = 15\Bigl(1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{15}\Bigr) = 15\Bigl(1 - \frac{1}{3}\Bigr)\Bigl(1 - \frac{1}{5}\Bigr).$$

More generally,

$$\phi(M) = M \sum_{I \subseteq \{1,2,\ldots,n\}} \frac{(-1)^{|I|}}{\prod_{i \in I} p_i} = M \prod_{i=1}^{n} \Big(1 - \frac{1}{p_i}\Big)$$

since the summand $(-1)^{|I|}/\prod_{i \in I} p_i$ in the middle is obtained by multiplying out the product taking $-p_i$ from $1 - \frac{1}{p_i}$ if $i \in I$ and taking 1 if $i \notin I$.

Proposition 3.4.4 *Let $M \in \mathbb{N}$ have prime factorization $p_1^{e_1} p_2^{e_2} \ldots p_n^{e_n}$ where $e_i \in \mathbb{N}$ for each i. Then*

$$\phi(p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}) = \prod_{i=1}^{n} p_i^{e_i} \Big(1 - \frac{1}{p_i}\Big).$$

Proof This is a restatement of the formula for $\phi(M)$ just proved. □

Euler's ϕ function is important in number theory and has applications in public key cryptography: see Exercises 3.6 and 3.7.

Sieving to count primes

Let $\pi(M)$ be the number of primes in $\{1,2,\ldots,M\}$. We use Proposition 3.4.3 and the ideas in Example 3.4.1 to estimate $\pi(M)$. Rather than pull the correct sieving parameters out of a hat, we prove a more general result and then specialize it.

Theorem 3.4.5 *Let $p_1, p_2, \ldots, p_n$ be the first n prime numbers and let $M \geq p_n$. Then*

$$\pi(M) \leq n + \frac{M}{\log p_n} + 2^n.$$

Proof Let S be the numbers in $\{1,2,\ldots,M\}$ not divisible by any of $p_1, \ldots, p_n$. By Proposition 3.4.3 we know $|S|$ exactly. But the floor functions make it hard to use the right-hand side. Motivated by the formula for $\phi(M)$, we approximate the summand $(-1)^{|I|}\lfloor M/\prod_{i \in I} p_i \rfloor$ by $(-1)^{|I|} M/\prod_{i \in I} p_i$. Since $\prod_{i \in I} p_i$ might not divide M, this introduces an error $\varepsilon \in \mathbb{R}$ such that $-1 < \varepsilon < 1$. Since there are 2^n summands, one for each subset of $\{1,2,\ldots,n\}$, the overall error is between -2^n and 2^n. Hence

$$|S| \leq \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \frac{M}{\prod_{i \in I} p_i} + 2^n.$$

By Proposition 3.4.4, we get $|S| \leq M \prod_{i=1}^{n} \big(1 - \frac{1}{p_i}\big) + 2^n$. Since S contains all the primes in $\{1,2,\ldots,M\}$ other than $p_1, p_2, \ldots, p_n$, we have $\pi(M) \leq |S| + n$. Therefore

$$\pi(M) \leq n + M \prod_{i=1}^{n} \Big(1 - \frac{1}{p_i}\Big) + 2^n.$$

To get an upper bound on $\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)$ we estimate its reciprocal, as follows:

$$\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)^{-1}=\prod_{i=1}^{n}\left(1+\frac{1}{p_i}+\frac{1}{p_i^2}+\cdots\right)\geq\sum_{x=1}^{p_n}\frac{1}{x}\geq\log p_n.$$

(For details of the two inequalities above see Exercise 3.11.) We conclude that $\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)\leq 1/\log p_n$ and so $\pi(M)\leq n+M/\log p_n+2^n$. □

Restated, this theorem says that if we choose a number in $\{1,2,\ldots,M\}$ uniformly at random, the probability that it is prime is at most $n/M+1/\log p_n+2^n/M$. To get a non-trivial bound, we need 2^n to be smaller than M. More precisely, since $2^n/M=\mathrm{e}^{n\log 2-\log M}$, we need $n\leq\log M/\log 2$.

Corollary 3.4.6 *We have* $\lim_{M\to\infty}\pi(M)/M=0$.

Proof Take $n=\lfloor\log M\rfloor$ in Theorem 3.4.5. Since $p_n\geq n+1\geq\log M$, we have $\log p_n\geq\log\log M$. Using $2^{\lfloor\log M\rfloor}\leq 2^{\log M}=M^{\log 2}$ to bound the third summand, we get

$$\frac{\pi(M)}{M}\leq\frac{\log M}{M}+\frac{1}{\log\log M}+\frac{M^{\log 2}}{M}.$$

Now observe that each summand tends to 0 as M tends to infinity. □

This makes precise the intuitive idea that as numbers get larger, they become increasingly unlikely to be prime. In Exercise 3.10 you are asked to refine the previous proof to show that $\pi(M)/M\leq 2/\log\log M$ for all M sufficiently large. Regrettably, this is still significantly weaker than the asymptotically correct result. Known as the Prime Number Theorem, it states that

$$\lim_{M\to\infty}\frac{\pi(M)}{M/\log M}=1.$$

While it seems that sieve methods cannot prove the Prime Number Theorem, they are still very important in number theory. A sieve was used in Zhang's breakthrough proof in 2013 that there are infinitely many prime numbers p and q such that $q>p$ and $q-p\leq 70\times 10^6$. Before Zhang's theorem, no constant upper bound was known. Thanks to the work of Maynard, Tao and the Polymath project (an ad-hoc collaborative network of mathematicians) we now know that there are infinitely many pairs of primes differing by at most 246. It is conjectured, but as yet unproved, that there are infinitely many primes p such that $p+2$ is also prime.

Exercises

The core exercises are 3.1 to 3.4.

3.1 Let $\Omega = \{1,\ldots,2019\}$. Let $A = \{x \in \Omega : x \text{ is even}\}$ and let $B = \{x \in \Omega : x \text{ is divisible by } 5\}$. What numbers are in $\overline{A \cup B}$? Find $|A|$, $|B|$, $|A \cap B|$ and $|\overline{A \cup B}|$. Illustrate your answer with a Venn diagram.

3.2 How many numbers in $\{1,2,\ldots,100\}$ are not divisible by any of 2, 3, 5 or 7? Use the Principle of Inclusion and Exclusion, making it clear which sets you apply it to. Hence find the number of primes in $\{1,2,\ldots,100\}$.

3.3 Let p, q and r be distinct primes. Find (a) $\phi(pq)$, (b) $\phi(p^2q)$ and (c) $\phi(pqr)$ using the Principle of Inclusion and Exclusion. Define the sets you use precisely. (Do not apply Proposition 3.4.4: instead you should adapt the argument.)

3.4 Recall that a deck of cards has four suits each of 13 cards: spades ♠, hearts ♡, diamonds ♢ and clubs ♣.

(a) How many five card hands are there with at least one card of each suit?

(b) How many five card hands are there with at least one card of each suit and at least one Ace, King, Queen and Jack? You may give your answer as a sum but try to simplify it as much as possible.

3.5 Let Ω be the set of all functions $f : \{1,2,\ldots,m\} \to \{1,2,\ldots,n\}$. For each $i \in \{1,2,\ldots,n\}$ define

$$A_i = \big\{ f \in \Omega : f(t) \neq i \text{ for any } t \in \{1,2,\ldots,m\} \big\}.$$

(a) What is $|\Omega|$? What is $|A_i|$?

(b) Let $I \subseteq \{1,2,\ldots,n\}$ be a non-empty subset and let $A_I = \bigcap_{i \in I} A_i$. What condition must a function $f \in \Omega$ satisfy to lie in A_I? Hence find $|A_I|$.

(c) Use the Principle of Inclusion and Exclusion to show that the number of surjective functions from $\{1,2,\ldots,m\}$ to $\{1,2,\ldots,n\}$ is

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.$$

(d) Show that the above expression is the number of ways to put m numbered balls into n numbered urns, so that each urn contains *at least* one ball.

(For the connection with Stirling Numbers of the Second Kind, see §**??** and Exercise 6.3.)

3.6 Recall that M and N are coprime if they share no common prime factor. Using Proposition 3.4.4, prove that if M and N are coprime then $\phi(MN) = \phi(M)\phi(N)$. Does this result hold for general M and N?

3.7 In the RSA cryptosystem, Alice chooses two distinct primes p and q and calculates $M = pq$. She chooses an encryption exponent $a \in \mathbb{N}$ coprime to $\phi(M)$, and calculates a decryption exponent d such that $ad \equiv 1 \bmod \phi(M)$. She publishes (M,a) as her *public key* and keeps p, q and d private. When Bob sends a message to Alice, he looks up her public key (M,a), and encrypts his message $x \in \{0,1,\ldots,M-1\}$ as $x^a \bmod M$. When Alice receives an encrypted message y, she decrypts by calculating $y^d \bmod M$.

(Why this works to find x, and why, when p and q are large, it is believed that an attacker cannot easily compute d, is explained in Exercise 3.9 below.)

In this toy example, we suppose that Alice takes $p = 11$ and $q = 17$ and $a = 9$. She publishes $(187,9)$ as her public key.

(a) Encrypt the message 7 using Alice's public key.

(b) Using Euclid's Algorithm find $d \in \mathbb{N}$ such that $ad \equiv 1 \bmod \phi(M)$.

(c) Alice has agreed with Bob that he will encrypt her exam mark using her public key. She receives 51 from Bob. What is her exam mark?

(d) What are some problems with the scheme as described? [*Hint: even if p and q were far larger, there is a simple way for an attacker who observes Bob's encrypted message to deduce Alice's exam mark.*]

3.8 Suppose that M is the product of two distinct primes p and q. Show how to find p and q given M and $\phi(M)$.

3.9 (This exercise needs some basic group theory.) Let $M = pq$ where p and q are distinct primes. Let $U = \big\{x \in \{0,1,\ldots,M-1\} : x \text{ is coprime to } p \text{ and } q\big\}$.

(a) Show that if x, $y \in U$ then $xy \bmod M$ is also in U.

(b) Let $x \in U$. Define $f_x : \{0,1,\ldots,M-1\} \to \{0,1,\ldots,M-1\}$ by $f_x(y) = xy \bmod M$. Show that f_x is injective.

(c) Deduce from (b) that if $x \in U$ then there exists a unique $x' \in U$ such that $xx' \equiv 1 \bmod M$.

(d) Hence show that U is a group under multiplication modulo M. What is the order of U?

(e) Show that if a is coprime to $\phi(M)$ then the function $x \mapsto x^a$ from U to itself is invertible and find the inverse function. Can you compute the inverse function knowing only a and M, but not $\phi(M)$ or p or q?

3.10 The displayed equation in the proof of Corollary 3.4.6 implies that

$$\frac{\pi(M)\log\log M}{M} \leq \frac{\log M}{M}\log\log M + 1 + \frac{M^{\log 2}}{M}\log\log M.$$

(a) Prove that if $c \in \mathbb{R}$ and $c > 0$ then $y\mathrm{e}^{-cy} \to 0$ as $y \to \infty$.

(b) Using (a) and the crude inequality $\log\log M \leq \log M$, or otherwise, show that $\pi(M)/M \leq 2/\log\log M$ for all sufficiently large M.

3.11 As in the proof of Theorem 3.4.5, let $p_1, p_2, \ldots, p_n$ be the first n prime numbers.

(a) By the formula for the sum of a geometric progression,

$$\left(1 - \frac{1}{p_i}\right)^{-1} = 1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots.$$

Using that each natural number has a unique prime factorization, deduce that

$$\prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right)^{-1} \geq \sum_{x=1}^{p_n} \frac{1}{x}.$$

(b) Show that $\sum_{x=1}^{S} \frac{1}{x} \geq \int_1^S \frac{\mathrm{d}t}{t} = \log S$ for any $S \in \mathbb{N}$.

(c) Deduce from (a) and (b) that there are infinitely many primes.

3.12 The Riemann ζ function is defined for $z \in \mathbb{C}$ such that $\operatorname{Re} z > 1$ by $\zeta(z) = \sum_{m=1}^{\infty} 1/m^z$.

(a) Use $|m^z| = m^{\operatorname{Re} z}$ to show that the series converges absolutely when $\operatorname{Re} z > 1$. What happens when $z = 1$?

(b) By adapting the argument in Exercise 3.11(a), show that

$$\zeta(z) = \prod_{n=1}^{\infty} \left(1 - \frac{1}{p_i^z}\right)^{-1}$$

for $z \in \mathbb{C}$ such that $\operatorname{Re} z > 1$.

(c) For $z \in \mathbb{C}$ such that $\operatorname{Re} z > 0$, let $\eta(z) = \sum_{m=1}^{\infty} (-1)^{m-1}/m^z$. Show that if $\operatorname{Re} z > 1$ then

$$\zeta(z) = \frac{\eta(z)}{1 - 2^{-(z-1)}}.$$

(d) Prove that $\eta(z)$ converges if $z \in \mathbb{R}$ and $z > 0$. ($\star$) Prove that $\eta(z)$ converges whenever $\operatorname{Re} z > 0$.

(The Prime Number Theorem was first proved in 1896, independently by Hadamard and de la Vallée Poussin. Both proofs used complex analysis and the Riemann ζ function extended, as the stronger result in (d) shows is possible, to the domain $\{z : \operatorname{Re} z > 0, z \neq 1\}$. The Riemann Hypothesis, one of the Clay Mathematics Institute's million dollar open problems in mathematics, states that if $\zeta(z) = 0$ and $\operatorname{Re} z > 0$ then $z = \frac{1}{2} + it$ for some $t \in \mathbb{R}$.)

3.13 Given $M \in \mathbb{N}$, let $\pi_2(M)$ be the number of numbers in $\{1, 2, \ldots, M\}$ that are *square-free*; that is, they are not divisible by the square of any prime.

(a) Let $p_1, p_2, \ldots, p_n$ be the primes less than or equal to $\sqrt{M}$. By adapting the argument used to estimate $\pi(M)$, show that

$$\Big|\frac{\pi_2(M)}{M} - \prod_{i=1}^{n}{}^{\star}\big(1-\frac{1}{p_i^2}\big)\Big| \leq \frac{1}{\sqrt{M}}.$$

where $\star$ denotes that all terms $\pm 1/d^2$ with $d > M$ that arise when expanding the product are to be ignored. (This technicality is necessary to get the good error bound $1/\sqrt{M}$.)

(b) Deduce from (a) and Exercise 3.12(a) that

$$\lim_{M\to\infty} \frac{\pi_2(M)}{M} = \zeta(2).$$

(c) Why does this sieve give a more precise result than the sieve used in Theorem 3.4.5 to estimate $\pi(M)$?

(It is known that $\zeta(2) = \frac{\pi^2}{6}$: you will easily find proofs using techniques including real variable integration, contour integration, and Fourier series if you search on the web.)

3.14 This question builds on the proof of the Principle of Inclusion and Exclusion (Theorem 3.1.3). For $r \in \{0,1,\ldots,n\}$, define $g_r : \Omega \to \mathbb{Z}$ by

$$g_r(x) = \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ |I|\leq r}} \begin{cases} (-1)^{|I|} & \text{if } x \in A_I \\ 0 & \text{otherwise.}\end{cases}$$

(a) Let $c_r = \sum_{x\in\Omega} g_r(x)$. Show that

$$c_r = \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ |I|\leq r}} (-1)^{|I|}|A_I|$$

is the sum in Principle of Inclusion and Exclusion, restricted to those indexing sets of size at most r.

(b) Let $x \in \Omega$. Suppose that $x \in A_j$ if and only if $j \in J$ where $J \subseteq \{1,2,\ldots,n\}$. Show that $g_r(x) = \sum_{k=0}^{r}(-1)^k\binom{|J|}{k}$ and hence that $g_r(x) = (-1)^r\binom{|J|-1}{r}$. Deduce that

$$c_r = \sum_{x\in\Omega}(-1)^r\binom{m_x-1}{r}$$

where $m_x = \big|\{j \in \{1,2,\ldots,n\} : x \in A_j\}\big|$.

(c) By taking $r = n$ in (b) deduce Theorem 3.1.3.

(d) Prove that if r is even then $|\overline{A_1 \cup A_2 \cup \ldots \cup A_n}| \leq c_r$.

(e) Prove that if r is odd then $c_r \leq |\overline{A_1 \cup A_2 \cup \ldots \cup A_n}|$.

(f) Prove that if $r \geq (n-1)/2$ then $c_r \leq c_{r+2}$ if r is odd and $c_{r+2} \leq c_r$ if r is even.

(g) ($\star$) In fact the bound on r in (f) can be slightly improved. Find the strongest possible improvement.

(Thus the c_r alternately under- and over-estimate the size of $|\overline{A_1 \cup A_2 \cup \ldots \cup A_n}|$, and the approximations get strictly better once $r \geq (n-1)/2$.)

3.15 Again this question can be answered by adapting the proof of the Principle of Inclusion and Exclusion in Theorem 3.1.3.

(a) Show there exist coefficients e_1, e_2, ..., $e_n \in \mathbb{N}$ such that the number of elements of Ω in *exactly* one of the sets $A_1, A_2, \ldots, A_n$ is

$$\sum_{k=1}^{n} (-1)^{k-1} e_k \sum_{\substack{I \subseteq \{1,2,\ldots,n\} \\ |I|=k}} |A_I|.$$

[*Hint: suppose, as in (a) in the previous exercise, that the sum is truncated to the terms for $k = 1, \ldots, r$. By analogy with (b) in the previous exercise, the formula should then be correct for elements lying in at most r of the sets A_1, A_2, ..., A_n.*]

(b) Prove a generalization of the Principle of Inclusion and Exclusion counting the number of elements of Ω that lie in *exactly t* of the sets A_1, A_2, ..., A_n, for each $t \in \mathbb{N}_0$.

(c) Fix $t \in \{0, 1, \ldots, n\}$. Check your result in (b) by counting the number of permutations of $\{1, 2, \ldots, n\}$ that have *exactly t* fixed points. (See Exercise 1.10 for the answer.)

3.16 ($\star$) Exercises 3.14 and 3.15 strengthen the Principle of Inclusion and Exclusion in two different ways. Prove a still stronger version that implies both.

3.17 This question gives an alternative proof of the Principle of Inclusion and Exclusion (Theorem 3.1.3). Fix a universe set Ω. For each $X \subseteq \Omega$, define a function $1_X : \Omega \to \{0, 1\}$ by

$$1_X(x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{if } x \notin X. \end{cases}$$

We say that 1_X is the *indicator function* of X.

(a) Let $X \subseteq \Omega$. What is $\sum_{x \in \Omega} 1_X(x)$?

(b) Show that if $B, C \subseteq \Omega$ then $1_{B \cap C}(x) = 1_B(x) 1_C(x)$ for all $x \in \Omega$ and so $1_{B \cap C} = 1_B 1_C$.

(c) Let $A_1, A_2, \ldots, A_n$ be subsets of Ω. Show that

$$1_{\overline{A_1 \cup A_2 \cup \cdots \cup A_n}} = (1_\Omega - 1_{A_1})(1_\Omega - 1_{A_2}) \ldots (1_\Omega - 1_{A_n}).$$

(d) By multiplying out the right-hand side in (c) and using (b), show that

$$1_{\overline{A_1 \cup A_2 \cup \cdots \cup A_n}} = \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} 1_{A_I}$$

where A_I has its usual definition.

(e) Prove Theorem 3.1.3 by summing the previous equation over all $x \in \Omega$.

3.18 There are many binomial coefficient identities that can be proved by a well-chosen application of the Principle of Inclusion and Exclusion.

(a) Prove that if $m, n \in \mathbb{N}_0$ then

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{m+n-k}{r} = \binom{m}{r-n}.$$

[*Hint: count the r-subsets of* $\{1,\ldots,m+n\}$ *not meeting* $\{m+1,\ldots,m+n\}$. *An alternative proof uses Exercise 2.21(a) and (e).*]

(b) Prove that if $n, s \in \mathbb{N}_0$ then

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{2n-2k}{n-s-2k} = 2^{n-s} \binom{n}{s}$$

and hence find $\sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{2k}{n+s}$.

(c) (American Mathematical Monthly Problem 11862). Prove that if $m, n \in \mathbb{N}_0$ then

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{(n-k)m}{n+1} = \frac{n}{2}(m^{n+1} - m^n).$$

3.19 By applying the Principle of Inclusion and Exclusion to the set of functions $f : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ such that f has no fixed points, prove Ryser's formula for the number of derangements of $\{1,2,\ldots,n\}$:

$$d_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k-1)^k (n-k)^{n-k}.$$

[*Hint: Exercise 3.5 is related.*] How does this use of the Principle of Inclusion and Exclusion compare with its use in §3.2?

4

Rook Polynomials

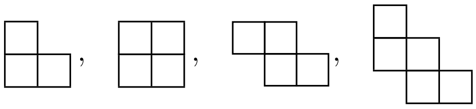
4.1 Introduction to rook polynomials

The derangements problem asks us to count permutations with no fixed points. Many other combinatorial problems can be interpreted as counting permutations of a special type. In this chapter we shall see a unified way to solve these problems.

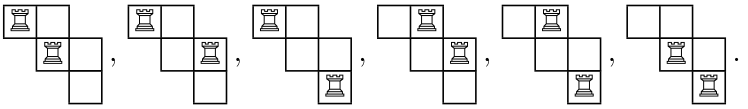
Definition 4.1.1 A *board* is a subset of the squares of an $n \times n$ grid. Given a board B, let $r_k(B)$ be the number of ways to place k rooks on B, so that no two rooks are in the same row or column. Such placements are said to be *non-attacking*. The *rook polynomial* of B is defined to be

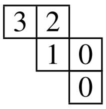
$$f_B(z) = r_0(B) + r_1(B)z + r_2(B)z^2 + \cdots + r_n(B)z^n.$$

For example, the rook polynomials of the four boards shown below



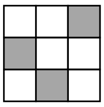
are $1+3z+z^2$, $1+4z+2z^2$, $1+4z+3z^2$ and $1+5z+6z^2+z^3$. Writing B for the final board, the six rook placements counted by $r_B(2)$ are



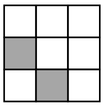


The diagram in the margin summarizes the enumeration above by counting numbers of placements according to the position of the top-left rook.

Exercise 4.1.2 Let B be a board. Show that $r_1(B)$ is the number of squares in B. What is $r_0(B)$?

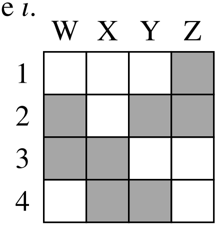


Exercise 4.1.3 Show that the rook polynomial of the six-square board in the margin is $1+6z+9z^2+2z^3$.



Exercise 4.1.4 Find the rook polynomial of the seven-square board in the margin. [*Hint: the non-attacking rook placements not having a rook in the top right are counted by the previous exercise.*]

Example 4.1.5 After the recent cutbacks, only four professor remain at the University of Erewhon. The basic course 1 can be lectured by Prof. W, Prof. X, or Prof. Z, the trickier course 2 only by Prof. X, course 3 by Prof. Y or Prof. Z and course 4 by Prof. W or Prof. Z. We model this timetabling problem using the board B shown below, in which there is a square in row i and column P if and only if Prof. P can lecture course i.

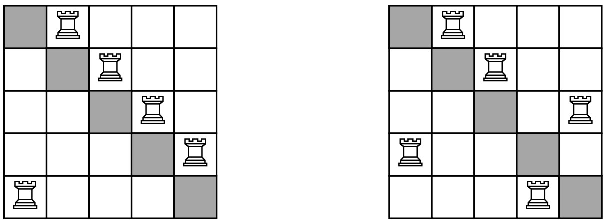


Assignments of professors to courses, so that each professor lectures at most one course and no course is lectured twice, are in bijection with non-attacking rook placements on B. Thus $r_B(k)$ is the number of ways in which exactly k courses can be lectured. For instance $r_B(4) = 2$: putting four rooks down the diagonal defines one of the two possible assignments. We find the rook polynomial $f_B(z)$ and hence $r_B(2)$ and $r_B(3)$ using a general method in Example 4.2.3.

Example 4.1.6 Let $n \in \mathbb{N}$. Given a permutation $\sigma : \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ we may define a non-attacking placement of n rooks on the $n \times n$ grid by putting a rook on the square (i, j) in row i and column j if and only if $\sigma(i) = j$. Clearly each row has one rook. Since

- σ is injective, no two rooks lie in the same column;
- σ is surjective, each column has a rook.

Conversely, any non-attacking placement of n rooks corresponds to a permutation. Taking $n = 5$, it follows that derangements of $\{1,2,3,4,5\}$ are in bijection with non-attacking placements of 5 rooks on the board below; the left rook placement corresponds to the derangement σ such that $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$, $\sigma(4) = 5$ and $\sigma(5) = 1$.



Going back, the right rook placement corresponds to the derangement τ such that $\tau(1) = 2$, $\tau(2) = 3$, $\tau(3) = 5$, $\tau(4) = 1$ and $\tau(5) = 4$. We use rook polynomials to calculate derangement numbers in §4.3 below.

4.2 Splitting boards

A special case of the next lemma was indicated by the hint to Exercise 4.1.4.

Lemma 4.2.1 *Let B be a board contained in the $n \times n$ grid and let s be a square in B. Let D be the board obtained from B by deleting s and let E be the board obtained from B by deleting the entire row and column containing s. Then*

$$f_B(z) = f_D(z) + z f_E(z).$$

Proof For each $k \in \mathbb{N}_0$ there is an obvious bijection

$$\left\{\begin{array}{c}\text{non-attacking placements of } k\\ \text{rooks on } B \text{ with no rook on } s\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{non-attacking placements}\\ \text{of } k \text{ rooks on } D\end{array}\right\}.$$

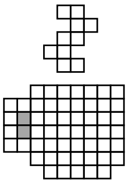
Suppose there are k rooks on B including a rook on s. No other rook lies in the row and column containing s. Deleting the row and column containing s therefore defines a bijection

$$\left\{\begin{array}{c}\text{non-attacking placements of } k\\ \text{rooks on } B \text{ with a rook on } s\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\text{non-attacking placements}\\ \text{of } k-1 \text{ rooks on } E\end{array}\right\}.$$

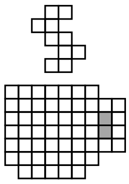
Combining these bijections shows that $r_k(B) = r_k(D) + r_{k-1}(E)$ for $k \in \mathbb{N}$. By Exercise 4.1.2, $r_0(B) = r_0(D) = 1$. Since at most n non-attacking rooks can be placed on B, and at most $n-1$ on E, we have

$$\begin{aligned} f_B(z) &= r_0(B) + \sum_{k=1}^{n} \bigl(r_k(D) + r_{k-1}(E)\bigr) z^k \\ &= r_0(D) + \sum_{k=1}^{n} r_k(D) z^k + \sum_{\ell=0}^{n-1} r_\ell(E) z^{\ell+1} \\ &= f_D(z) + z f_E(z) \end{aligned}$$

as required. □



To illustrate another very helpful result, consider the single large board split between the left and right margin of this page. A rook in the left subboard can never attack attack a rook in the right subboard. Therefore we may treat these two subboards independently. The next lemma makes this precise. In the proof, we take one final chance to emphasise the use of the basic counting principles from Chapter 1.



Lemma 4.2.2 *Let B be a board. Suppose that B can be partitioned into subboards C and C' so that no square in C lies in the same row or column as a square of C'. Then $r_k(B) = \sum_{\ell=0}^{k} r_\ell(C) r_{k-\ell}(C')$ for each $k \in \mathbb{N}$ and*

$$f_B(z) = f_C(z) f_{C'}(z).$$

Proof Let $k \in \mathbb{N}_0$. Given $\ell \in \{0, 1, \ldots, k\}$ we may place k rooks on B by putting ℓ non-attacking rooks on C and $k - \ell$ non-attacking rooks on C'. Since rooks on C never attack rooks on C', any such placement is non-attacking, and every non-attacking placement of k rooks on B is obtained in this way.

By **BCP0**, that sets in bijection have the same size, and **BCP1**, the basic counting principle on multiplying choices, there are exactly $r_k(C) r_{k-\ell}(C')$ non-attacking placements with ℓ rooks on C. Hence, by **BCP2**, the basic counting principle on adding choices,

$$r_k(B) = \sum_{\ell=0}^{k} r_\ell(C) r_{k-\ell}(C'),$$

as required. The right-hand side is the coefficient of z^k when we multiply $f_C(z) = \sum_{\ell=0}^{n} r_\ell(C) z^\ell$ and $f_{C'}(z) = \sum_{m=0}^{n} r_m(C') z^m$ by adding $r_\ell(C) z^\ell r_m(C') z^m$ for all ℓ and m. (The relevant products for the coefficient of z^k are those with $\ell + m = k$.) This holds for each $k \in \mathbb{N}_0$, hence $f_B(z) = f_C(z) f_{C'}(z)$. □

We will see later that Lemma 4.2.2 is a special case of Theorem 8.0.1 on products of generating functions.

We now show how the two previous lemmas are used in practice.

Example 4.2.3 Let B be the board in Example 4.1.5. Figure 4.2 overleaf shows the four boards DD, DE, ED and EE given by applying Lemma 4.2.1 first to the square s, then to the square u. By this lemma,

$$f_B(z) = f_D(z) + z f_E(z) = \big(f_{DD}(z) + z f_{DE}(z)\big) + z\big(f_{ED}(z) + z f_{EE}(z)\big).$$

To calculate the rook polynomials on the right-hand side, we use Lemma 4.2.2:

$$\begin{aligned}
f_{DD}(z) &= f_{\begin{smallmatrix}\square&\square&\square\\ &\square& \end{smallmatrix}}(z) f_{\begin{smallmatrix}\square\\ \square\end{smallmatrix}}(z) = (1 + 4z + 2z^2)(1 + 2z) = 1 + 6z + 10z^2 + 4z^3\\
f_{DE}(z) &= f_{\begin{smallmatrix}\square&\square\\ \square& \end{smallmatrix}}(z) f_{\square}(z) = (1 + 3z + z^2)(1 + z) = 1 + 4z + 4z^2 + z^3\\
f_{ED}(z) &= f_{\begin{smallmatrix}\square&\square\\ &\square \end{smallmatrix}}(z) f_{\square}(z) = (1 + 3z + z^2)(1 + z) = 1 + 4z + 4z^2 + z^3
\end{aligned}$$

Clearly $f_{EE}(z) = 1 + 2z$. Remembering to include the powers of z, we get

$$\begin{aligned}
f_B(z) = (1 &+ 6z + 10z^2 + 4z^3) + z(1 + 4z + 4z^2 + z^3)\\
&+ z(1 + 4z + 4z^2 + z^3) + z^2(1 + 2z) = 1 + 8z + 19z^2 + 14z^3 + 2z^4.
\end{aligned}$$

In particular, $r_B(2) = 19$ and $r_B(3) = 14$. The squares s and u were chosen so that Lemma 4.2.2 could be applied after two steps. Other choices are also sensible, and are, of course, permitted.

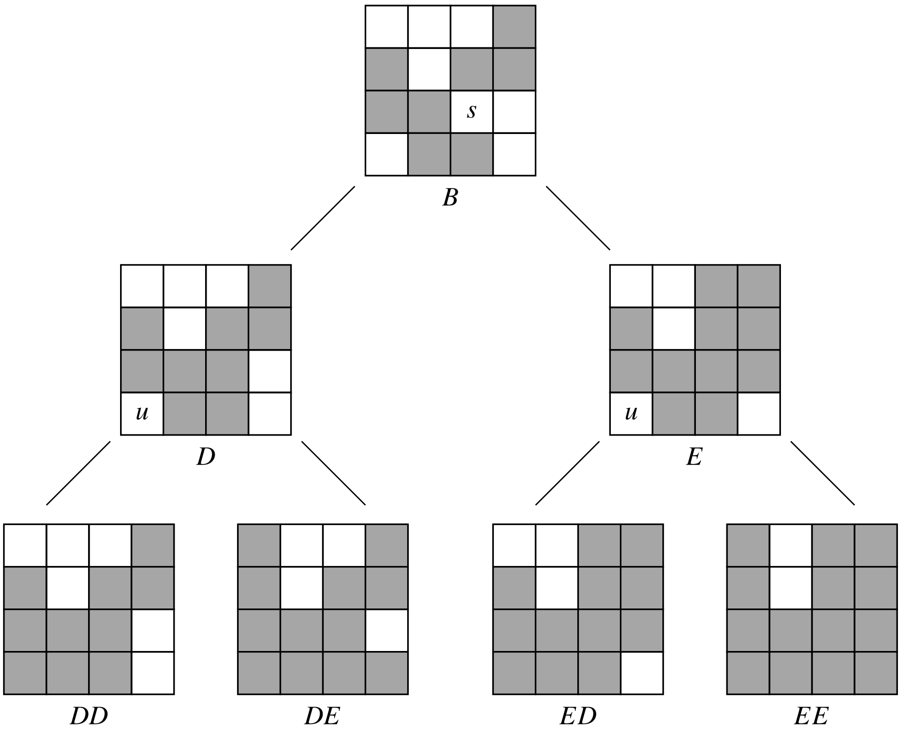


Figure 4.1 Lemma 4.2.1 applied to the board B in Examples 4.1.5 and 4.2.3, first to the square s in position $(3,3)$, then the square u in position $(4,1)$.

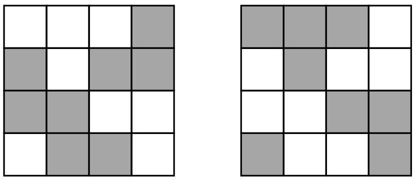
To give another example, if B is the board split across the previous page and C and C' are the left and right subboards then, by symmetry, $f_C(z) = f_{C'}(z)$. Hence, by Lemma 4.2.2, $f_B(z) = f_C(z)^2$. The simple algorithm based on Lemma 4.2.1 suggested in Exercise 4.9 takes about a minute to compute $f_C(z)$, and reveals that

$$f_B(z) = (1 + 63z + 1544z^2 + 18984z^3 + \cdots + 270000z^8 + 23760z^9)^2.$$

By contrast, computing $f_B(z)$ directly by this algorithm, even on a supercomputer, would not finish within the lifetime of our universe.

4.3 Complementary boards and the *Problème des Ménages*

Given a board B contained in the $n \times n$ grid, let $\overline{B}$ denote the *complementary* board consisting of all the squares in the grid not in B. For instance the board B in Example 4.1.4 and its complement $\overline{B}$ in the 4×4 grid are below.



In this section we explore the surprisingly close connection between the non-attacking rook placements on B and $\overline{B}$.

Placements on the complement

Let Ω be the set of all $n!$ non-attacking placements of n rooks on the $n \times n$ grid. Let B be a board contained in Ω. We shall use the Principle of Inclusion and Exclusion to express $r_n(\overline{B})$ in terms of $r_0(B), r_1(B), \ldots, r_n(B)$.

Exercise 4.3.1 For each $i \in \{1,2,\ldots,n\}$, let A_i be those placements in Ω *we do not want to count* because of a reason to do with row i (and only row i). How should A_i be defined?

The answer is that A_i is the placements in which the rook on row i is on B. More generally, if $I \subseteq \{1,2,\ldots,n\}$, then A_I is those placements in which the rooks on the rows in I are in B. We use the following lemma to find the sum over the sizes $|A_I|$ in the right-hand side of the Principle of Inclusion and Exclusion.

Lemma 4.3.2 *Let* $k \in \{0,1,\ldots,n\}$. *Then*

$$\sum_{\substack{I \subseteq \{1,2,\ldots,n\} \\ |I|=k}} |A_I| = r_k(B)(n-k)!.$$

Proof Given a rook placement in A_I, colouring the rooks in the rows in I red gives a rook placement with k black rooks on B and $n-k$ white rooks on either B or $\overline{B}$, such that all n rooks are non-attacking. Let $\mathscr{C}_k$ be the set of such coloured rook placements. Going back, given a placement in $\mathscr{C}$, the k black rooks identify an indexing set I. Hence the left-hand side is $|\mathscr{C}_k|$.

We may construct a rook-placement in $\mathscr{C}_k$ by putting k non-attacking black rooks on B, in $r_k(B)$ ways, and a further $n-k$ non-attacking white rooks on the $n-k$ rows and columns not yet used, in $(n-k)!$ ways. Hence $|\mathscr{C}_k|$ is the right-hand side. □

This proof is more subtle than it might seem. For instance, except when $k=0$, the set $\mathscr{C}_k$ (which consists of coloured placements) is not $\bigcup_{I \subseteq \{1,2,\ldots,n\}, |I|=k} A_I$. As ever, seeing how the proof works by trying it out on a particular example is helpful: one relevant to derangements is suggested in Exercise 4.6 below. See Exercise 4.12 for another application of the colouring idea.

Corollary 4.3.3 *Let B be a board contained in an $n \times n$ grid. Then*

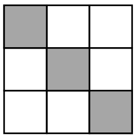
$$r_n(\overline{B}) = \sum_{k=0}^{n} (-1)^k r_k(B)(n-k)!.$$

Proof By the Principle of Inclusion and Exclusion,

$$r_n(\overline{B}) = \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|}|A_I| = \sum_{k=0}^{n} (-1)^k \sum_{\substack{I \subseteq \{1,2,\ldots,n\} \\ |I|=k}} |A_I| = \sum_{k=0}^{n} (-1)^k r_k(B)(n-k)!$$

where the final equality uses Lemma 4.3.2. □

Derangements



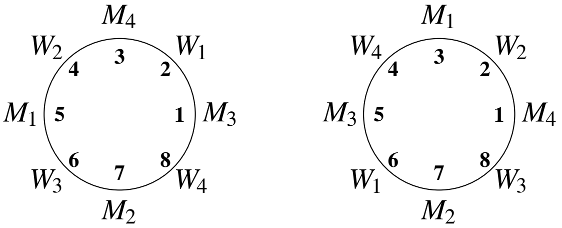
Fix $n \in \mathbb{N}$ with $n \geq 2$ and let B be the board of all diagonal squares in the $n \times n$ grid, as shown by the *shaded* squares in the margin when $n = 3$. As seen in Example 4.1.6, derangements of $\{1,2,\ldots,n\}$ are in bijection with non-attacking placements of n rooks on $\overline{B}$. To apply Corollary 4.3.3 we need $r_0(B), r_1(B), \ldots, r_n(B)$. Note that any placement on B is non-attacking. Since there are $\binom{n}{k}$ to choose k rows of B on which to put rooks, we have $r_k(B) = \binom{n}{k}$ for each k. Hence, by Corollary 4.3.3,

$$r_n(\overline{B}) = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}$$

where the final equality uses Lemma 2.1.4. This is our usual formula for d_n.

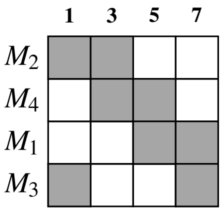
Problème des Ménages

Let $n \in \mathbb{N}$ with $n \geq 2$. How many ways can n heterosexual couples be seated around a circular table with $2n$ numbered seats so that men and women alternate, and no-one sits next to his or her partner? For example if $n = 4$ then labelling the people $W_1, M_1, W_2, M_2, W_3, M_3, W_4, M_4$, two possible seating placements are shown below.

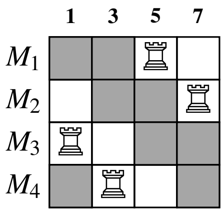


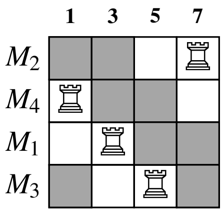
Observe that the women are either all sat in odd-numbered seats or all sat in even-numbered seats. Suppose, as in the both examples above, the women are in even seats. Define a permutation $\sigma : \{1,\dots,n\} \to \{1,\dots,n\}$ so that woman $W_{\sigma(i)}$ sits in seat $2i$. The men can now choose their seats in any way such that $M_{\sigma(i)}$ is not in seat $2i-1$ or seat $2i+1$. (When $i=n$, regard seat $2n+1$ as seat 1.) This puts the problem in the same setting as Examples 4.1.5 and 4.1.6.

For instance, if women sit as in the second example above, then the permutation is $\sigma(1)=2$, $\sigma(2)=4$, $\sigma(3)=1$, $\sigma(4)=3$ and ways to seat the men correspond to placements of 4 non-attacking rooks on the board below.

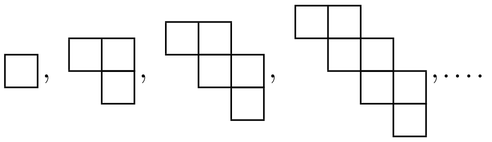


In the first example, the board is the same, but since the permutation σ is now $\sigma(1)=1$, $\sigma(2)=2$, $\sigma(3)=3$, $\sigma(4)=4$, the row labels change to M_1, M_2, M_3, M_4. The rook placements for the two examples above are shown below.





In general we label row i of the $n \times n$ grid by man $M_{\sigma(i)}$. Then ways to seat the n men correspond to placements of n non-attacking rooks on the complement of the board B_n obtained by taking the *staircase board* S_{2n-1} with $2n-1$ squares in the sequence below and extending it by a square in the bottom-left corner.



For example, B_4 is the board of *shaded* squares seen three times above. It follows from Lemma 4.2.1, taking the distinguished square to be one in the top-right corner, that the rook polynomial of B_n is $f_{S_{2n-1}}(z) + x f_{S_{2(n-1)-1}}(z)$.

Exercise 4.3.4 Using the formula $f_{S_m}(z) = \sum_{k=0}^{n} \binom{m-k+1}{k}$, which you are asked to discover in Exercise 4.5, prove that

$$f_{B_n}(z) = \sum_{k=0}^{n} \binom{2n-k}{k} \frac{2n}{2n-k}.$$

Therefore, by Corollary 4.3.3, the number of ways to place the men is the *ménage* number u_n defined by

$$u_n = \sum_{k=0}^{n} (-1)^k \binom{2n-k}{k} \frac{2n}{2n-k}(n-k)!.$$

For example $f_{B_4}(z) = 1+8z+20z^2+16z^3+2z^4$ and so $u_4 = 4! - 8\times 3! + 20 \times 2! - 16\times 1! + 2\times 0! = 2$, as can easily be seen directly. The table below shows the small values of u_n; the reason for defining $u_0 = 2$ and $u_1 = -1$ is seen after Proposition 4.3.6 below.

n	0	1	2	3	4	5	6	7	8
u_n	2	-1	0	1	2	13	80	579	4738

To count all the seating arrangements we multiply u_n by $n!$ counting the $n!$ permutations σ and by 2, since women might also have sat in the even-numbered seats, getting $2n!u_n$.

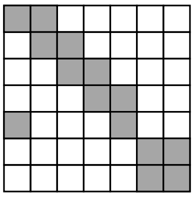
Discordant permutations and les ménages aux tables multiples

We end with a generalization of the Probème des Ménages. Given permutation σ, $\tau : \{1,2,\dots,n\} \to \{1,2,\dots,n\}$, we say that σ and τ are *discordant* if $\sigma(i) \neq \tau(i)$ for each $i \in \{1,2,\dots,n\}$. For example, τ is discordant with the identity permutation if and only if τ is a derangement. For $n \geq 2$, permutations discordant with both the identity permutation, and the permutation σ defined by

$$\sigma(1) = 2, \sigma(2) = 3, \dots, \sigma(n) = 1,$$

correspond to placements of n rooks on the complement of the board B_n. Therefore the number of such permutations is the ménage number u_n tabulated above.

For $n \in \mathbb{N}$ with $n \geq 2$ let $g_n(z) = f_{B_n}(z)$.



Example 4.3.5 Let $\sigma : \{1,2,3,4,5,6,7\} \to \{1,2,3,4,5,6,7\}$ be the permutation defined by $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4$, $\sigma(4) = 5, \sigma(5) = 1, \sigma(6) = 7, \sigma(7) = 6$. Let B be the board of *shaded* squares shown in the margin, defined so that permutations τ discordant with both the identity permutation and σ are counted by $r_7(\overline{B})$. By Exercise 4.3.4, $g_5(z) = 1+10z+35z^2+50z^3+25z^4+2z^5$. By splitting up the shaded squares using Lemma 4.2.1 we get

$$\begin{aligned} f_B(z) = g_5(z)g_2(z) &= (1+10z+35z^2+50z^3+25z^4+2z^5)(1+4z+2z^2) \\ &= 1+14z+77z^2+210z^3+295z^4+202z^5+58z^6+4z^7. \end{aligned}$$

We could now apply Corollary 4.3.3 to find $r_7(\overline{B})$. Instead, we motivate a more general result by observing that $g_7(z) = 1+14z+77z^2+210z^3+294z^4+196z^5+49z^6+2z^7$. Since $g_3(z) = 1+6z+9z^2+2z^3$, it follows that

$$g_5(z)g_2(z) = g_7(z)+z^4 g_3(z).$$

Hence $r_k(B) = r_k(B_7)+r_{k-4}(B_3)$. Now using Corollary 4.3.3, we get

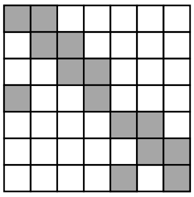
$$\begin{aligned} r_7(\overline{B}) = \sum_{k=0}^{7} \big(r_k(B_7)+r_{k-4}(B_3)\big)(-1)^k(7-k)! \\ = \sum_{k=0}^{7} r_k(B_7)(-1)^k(7-k)! + \sum_{\ell=0}^{3} r_\ell(B_3)(-1)^\ell(3-\ell)!. \end{aligned}$$

(In the second summand, we replaced $k-4$ with ℓ.) By two more applications of Corollary 4.3.3, this is u_7+u_3, or $579+1=580$.

The decomposition $g_5(z)g_2(z) = g_7(z)+z^4g_3(z)$ is a special case of a remarkable general rule. If you would like to discover it for yourself, calculate $g_r(z)g_s(z) - g_{r+s}(z)$ for other small r and s. The results motivate defining $g_0(z) = 2$ and $g_1(z) = 1+2z$.

Proposition 4.3.6 *Let ℓ, $m \in \mathbb{N}_0$ with $\ell \geq m$. Then $g_\ell(z)g_m(z) = g_{\ell+m}(z)+z^{2m}g_{\ell-m}(z)$.*

Proposition 4.3.6 is proved in Exercise 4.14. Using the proposition one can generalize Example 4.3.5 to arbitrary permutations σ: see Exercise 4.16.



For example, to show why we defined $u_1 = -1$, suppose that σ has cycles of lengths $m+1$ and m. (Cycles are formally defined in §9.2: the permutation σ in Example 4.3.5 has cycles of lengths 5 and 2.) Defining B by analogy with Example 4.3.5, so if $m=3$ then B is as shown in the margin, Proposition 4.3.6 implies that

$$f_B(z) = g_{m+1}(z)g_m(z) = g_{2m+1}(x)+z^{2m}g_1(x) = g_{2m+1}(z)+z^{2m}(1+2z).$$

By Corollary 4.3.3, the number of permutations discordant with both the identity permutation and σ is

$$\begin{aligned} \sum_{k=0}^{2m-1} r_k(B_{2m+1})(-1)^k(2m+1-k)! + \big(r_{2m}(B_{2m+1})+1\big)1! - \big(r_{2m+1}(B_{2m+1})+2\big)0! \\ = \sum_{k=0}^{2m+1} r_k(B)(-1)^k(2m+1-k)! + 1 - 2 = u_{2m+1} - 1 = u_{2m+1} + u_1. \end{aligned}$$

The useful linearity property in Corollary 4.3.3 seen in this calculation generalizes as follows. In practice the signs are often always $+1$: see Exercise 4.15(d).

Exercise 4.3.7 Suppose that B is a board in the $n \times n$ grid such that $f_B(z) = \sum_{\ell=0}^{n} a_\ell z^{n-\ell} g_\ell$. Show that $r_n(\overline{B}) = \sum_{\ell=0}^{n} (-1)^{n-\ell} a_\ell u_\ell$.

As motivation for our final result, fix $m \in \mathbb{N}$ and observe that by repeatedly multiplying by g_m using Proposition 4.3.6, we have $g_m^2 = g_{2m} + 2z^{2m}$, $g_m^3 = g_{3m} + 3z^{2m} g_m$, $g_m^4 = g_{4m} + 4z^{2m} g_{2m} + 6z^{4m}$ and $g_m^5 = g_{5m} + 5z^{3m} g_{3m} + 10z^{4m} g_m$. The coefficients should seem familiar.

Proposition 4.3.8 *Fix $m \in \mathbb{N}$ and $c \in \mathbb{N}_0$. Suppose that there are c circular tables, each seating $2m$ diners, and that there are mc couples who must be seated obeying the restrictions of the Problème des Ménages. The number of seating arrangements is*

$$2^c (mc)!\Big(\sum_{0 \le k < c/2} \binom{c}{k} u_{m(c-2k)} + \binom{c}{c/2} \Big)$$

where the final summand is regarded as 0 *if c is odd.*

Proof As before, we begin by letting the women choose their seats. Seating arrangements for the men are then in bijection with placements of mc rooks on the board B formed from c diagonal copies of the board B_m. By Lemma 4.2.1, $f_B(z) = g_m(z)^c$. Suppose inductively, as suggested by the calculations above, that

$$g_m(z)^c = \sum_{0 \le k < c/2} \binom{c}{k} z^{2mk} g_{m(c-2k)}(z) + \binom{c}{c/2} z^{mc}$$

where again the final summand is regarded as 0 if c is odd. If c is even, with say $c = 2s$, then multiplying the equation above by g_m using Proposition 4.3.6, we get

$$\begin{aligned} g_m(z)^{2s+1} &= \sum_{k=0}^{s-1} \binom{2s}{k} z^{2mk} \big(g_{m(2s-2k+1)}(z) + z^{2m} g_{m(2s-2k-1)}(z) \big) + \binom{2s}{s} g_m z^{2ms} \\ &= \sum_{k=0}^{s-1} \Big(\binom{2s}{k} + \binom{2s}{k-1} \Big) z^{2mk} g_{m(2s+1-2k)}(z) + \Big(\binom{2s}{s-1} + \binom{2s}{s} \Big) g_m(z) z^{2ms} \\ &= \sum_{k=0}^{s} \binom{2s+1}{k} z^{2mk} g_{m(2s+1-2k)}(z) \end{aligned}$$

where the final step uses the Fundamental Recurrence (Lemma 2.1.7). The inductive step is similar if c is odd. Hence, by Exercise 4.3.7, the number of ways to seat the men is

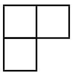
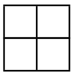
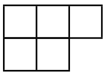
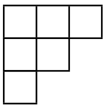
$$\sum_{0 \le k < c/2} \binom{c}{k} u_{m(c-2k)} + \binom{c}{c/2}.$$

To count all seating arrangements we must multiply this by 2^c, counting the choices of whether women are in even or odd seats at each table, and then by $(mc)!$, counting the ways the women may choose seats of the chosen parity at each table. □

An alternative proof of the formula for g_m^c direct from the Binomial Theorem is given in Exercise 4.15(e). We apply the results in this section to find the number of permutations discordant with *any* two given permutations, and hence to count $3 \times n$ Latin rectangles, in §9.4.

Exercises

The core exercises are 4.1 to 4.7.

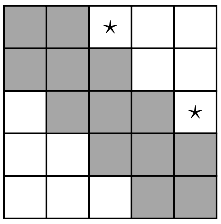
4.1 Find the rook polynomials of the boards , , , .

4.2 Show that the rook polynomial of the $m \times n$ grid is $\sum_{k=0}^{n} k! \binom{m}{k} \binom{n}{k} z^k$.

4.3 Let T be the set of all derangements σ of $\{1,2,3,4,5\}$ such that

- $\sigma(i) \neq i+1$ if $1 \leq i \leq 4$,
- $\sigma(i) \neq i-1$ if $2 \leq i \leq 5$.

(a) Explain why $|T|$ is the number of ways to place 5 non-attacking rooks on the board B formed by the unshaded squares below. (Include in your answer an explicit example of how a permutation corresponds to a rook placement.)



(b) Find the rook polynomial of B, and hence find $|T|$. [*Hint: consider the four possibilities for the starred squares. For example, if both are occupied, the contribution to the rook polynomial is $z^2 f_1(z) f_2(z)$ where $f_n(z)$ is the rook polynomial of the $n \times n$ square board. You could also use Lemma 4.2.1.*]

(c) Use Corollary 4.3.3 to find the number of ways to place 5 non-attacking rooks on the shaded squares.

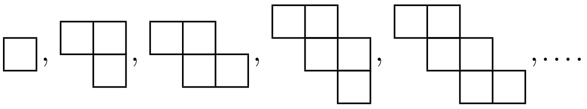
(d) ($\star$) By adapting the argument used to prove Corollary 4.3.3, find the number of ways to place 4 non-attacking rooks on the shaded squares. (See Exercise 4.13 for a generalization.)

4.4

(a) Show that permuting the rows or columns of a board does not change its rook polynomial.

(b) Let B be the board in Example 4.1.5. Show that B and its complement $\overline{B}$ in the 4×4 grid have the same rook polynomial.

4.5 Let S_m denote the *staircase board* with exactly m squares in the sequence shown below.



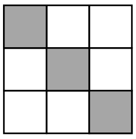
(a) Calculate the rook polynomials of S_m for $m \in \{1,2,3,4,5\}$.

(b) Find $f_{S_6}(z)$ using Lemma 4.2.1.

(c) Conjecture a formula for f_{S_m}. [*Hint: look at the southwest to northeast diagonals on the Pascal's Triangle on page 23. The answer is revealed in* §*4.3.*]

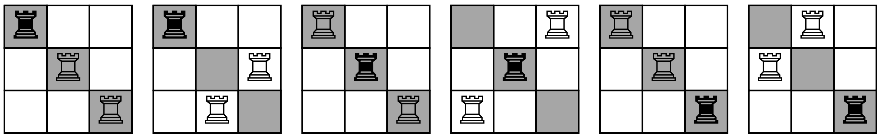
(d) Prove your conjecture. [*Hint: while you could generalize (b), there is also a very short proof using Exercise 2.4.*]

4.6 Let $n = 3$ and let B be the board formed by the *shaded* squares below.



Draw the rook placements lying in each of the sets $A_{\varnothing}$, $A_{\{1\}}$, $A_{\{2\}}$, $A_{\{3\}}$, $A_{\{1,2\}}$, $A_{\{1,3\}}$, $A_{\{2,3\}}$, $A_{\{1,2,3\}}$ in the proof of Lemma 4.3.2 and hence find the set $\mathscr{C}_k$ of coloured rook placements for each $k \in \{0,1,2,3\}$. Check that it has the expected size.

For instance you should find that $\mathscr{C}_1$ has the six coloured placements



and correspondingly $|\mathscr{C}_1| = 6$ agreeing with $|A_{\{1\}}| + |A_{\{2\}}| + |A_{\{3\}}| = 2+2+2 = 6$ and $r_1(\overline{B})(3-1)! = 3 \times 2! = 6$.

4.7 A *Latin rectangle* of order n is a rectangle in which every row contains each of the numbers 1, 2, …, n exactly once and the entries in each column are distinct. Let L be the Latin rectangle shown below

1	2	3	4	5
2	3	1	5	4

.

Let B be the board contained in the 5×5 grid with a square in position (i, j) if and only if the number i can be put in row 3 and column j of L.

(a) Find the rook polynomial of B and hence find $r_5(\overline{B})$.

(b) Explain why $r_5(\overline{B})$ is the number of ways to extend L to a $3 \times n$ Latin rectangle.

(c) Use Proposition 4.3.6 and Exercise 4.3.7 to express $r_5(\overline{B})$ as a sum of the ménage numbers u_n.

4.8 Find the number of permutations σ of $\{1,2,3,4,5,6\}$ such that $\sigma(m) \neq m$ for any even number m.

4.9 Rook polynomials can be computed recursively by repeated applications of Lemma 4.2.1.

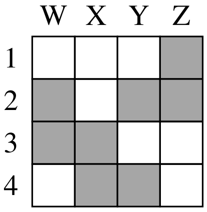
(a) Representing boards as list of squares, implement this algorithm in the programming language of your choice, choosing as the square s the first square in the list. (One possibility is MATHEMATICA: it has polynomial addition and multiplication built-in and good support for lists and recursion.)

(b) Refine the algorithm by instead choosing the square on which a rook attacks the maximum number of other squares.

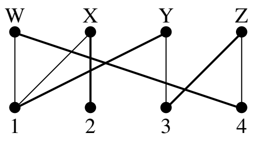
(c) Refine the algorithm further by splitting boards using Lemma 4.2.2.

(d) Which, if any, of the algorithms in (a), (b), (c) can compute the rook polynomial of the 'coffee' board on page 62 in a short time? (A MATHEMATICA notebook including the squares in this board may be downloaded from the author's website, see page 4.)

4.10 Given a board B contained in the $n \times n$ grid. Let $M(B)$ be the matrix with a 1 in each position where B has a square, and 0 in all other positions. Let $H(B)$ be the bipartite graph with adjacency matrix $M(B)$. For example, if B is the board in Example 4.1.5 with rows labelled by courses and columns by professors, then B, $M(B)$ and $H(B)$ are as shown below.



$$\longleftrightarrow \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix} \longleftrightarrow$$



(The thick edges in $H(B)$ are used in (b) below.)

(a) The *permanent* of a matrix is defined like the determinant, but omitting the signs. Thus if M is an $n \times n$ matrix then per $M = \sum_\sigma \prod_{i=1}^n M_{i\sigma(i)}$ where the sum is over all permutations of $\{1, \ldots, n\}$. Show that per $M(B)$ is the coefficient of z^n in the rook polynomial $f_B(z)$.

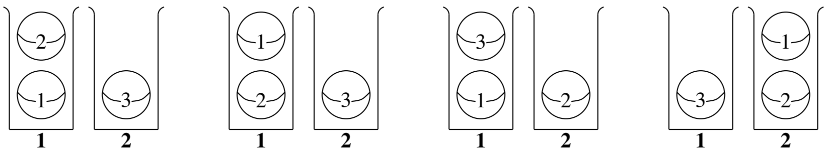
(b) A *matching* in a bipartite graph is a set of edges such that every vertex is in exactly one edge; one of the two matchings in the graph $H(B)$ above is shown by thick edges above. Show that per $M(B)$ is the number of matchings in $H(B)$.

(c) (For those who know a little about computational complexity.) Show that computing the coefficient of z^n in the rook polynomial of a board contained in the $n \times n$ grid is in the complexity class #P. [*Hint: an important early result of Valiant is that computing the permanent of a matrix with* 0, 1 *entries is in this class.*] How does this compare with the difficulty of deciding if the coefficient is non-zero?

4.11 The Lah Number $\rceil{n \atop k}\lceil$ may be defined as the number of ways to put $n-k$ non-attacking rooks on the $(n-1) \times n$ grid.

(a) Show that $\rceil{n \atop k}\lceil = \frac{n!}{k!}\binom{n-1}{k-1}$.

(b) Show that $k!\rceil{n \atop k}\lceil$ is the number of ways to put n labelled balls into k labelled tubes so that each tube is non-empty. For example, $1!\rceil{n \atop 1}\lceil = n!$ for all n and 4 of the 12 placements counted by $2!\rceil{3 \atop 2}\lceil$ are shown below.

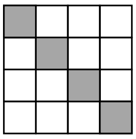


[*Hint: Exercise 2.5 is relevant; you will need to swap the roles of n and k.*]

(c) Deduce that $\rceil{n \atop k}\lceil$ is the number of ways to put n labelled balls into k unlabelled tubes so that each tube is non-empty. (This is the usual definition of the Lah Numbers.)

(d) ($\star$) Give a bijective proof of (c).

4.12 Fix $n \in \mathbb{N}$ and let B be a board contained in the $n \times n$ grid. The *hit number* $h_t(B)$ is the number of ways to put n non-attacking rooks on the $n \times n$ grid so that *exactly* t rooks are on B. For example, if $n = 4$ and B is the board of *shaded* squares in the margin then $h_0(B)$ counts the 9 derangements and $h_1(B) = 8$, $h_2(B) = 6$, $h_3(B) = 0$ and $h_4(B) = 1$.



(a) Show that

$$\sum_{t=k}^{n} h_t(B) \binom{t}{k} = r_k(B)(n-k)!.$$

[*Hint: interpret each side as the number of ways to put k black rooks on B and n − k white rooks anywhere on the grid, so that all n rooks are non-attacking.*]

(b) Deduce that $\sum_{t=0}^{n} h_t(B)(1+z)^t = \sum_{k=0}^{n} r_k(B)(n-k)!z^k$ and hence that

$$\sum_{t=0}^{n} h_t(B) w^t = \sum_{k=0}^{n} r_k(B)(n-k)!(w-1)^k.$$

(c) By substituting $w = 0$ give a new proof of Corollary 4.3.3.

(d) Let $a_n(t)$ be the number of permutations of $\{1, 2, \ldots, n\}$ with precisely t fixed points. Use the previous question with the board in §4.3 to prove that

$$a_n(t) = \frac{n!}{t!}\Big(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^{n-t}}{(n-t)!}\Big)$$

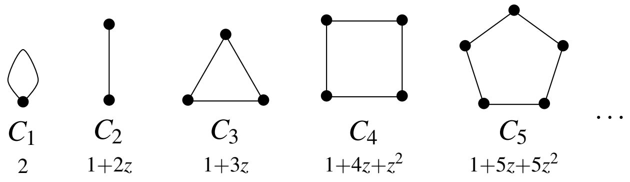
as seen in Exercise 1.10.

(e) Find a formula for the number of seating arrangements in the Problème des Ménages if exactly t couples sit in adjacent seats. (As before, women and men must sit in alternating positions.)

4.13 Generalize Corollary 4.3.3 and Exercise 4.3(d) by proving that if B is a board contained in the $n \times n$ grid then

$$r_m(\overline{B}) = \sum_{k=0}^{m} (-1)^k r_k(B) \binom{n-k}{m-k}^2 (m-k)!.$$

4.14 For $m \in \mathbb{N}$, let C_m be the m-vertex cycle, as shown below.



Let $r_k(C_m)$ be the number of ways to put k rooks on the vertices of C_m so that no two rooks are on adjacent vertices. Let $p_m(z) = \sum_{k=0}^{m} r_k(C_m) z^k$. Let

$p_0 = 2$ and note that, because of the self-loop on its unique vertex, $p_1(z) = 1$, as shown above.

(a) Show that if $n \geq 2$ then $p_{2n}(z)$ is the rook polynomial $g_n(z)$ of the board B_n with $2n$ squares used in the *Problème des Ménages.*

(b) Show that $r_k(C_m) = r_k(S_{m-1}) + r_{k-1}(S_{m-3})$ and hence $p_m(z) = \sum_{k=0}^{m/2} \binom{m-k}{k} \frac{m}{m-k} z^k$ for $m \in \mathbb{N}$, generalizing Exercise 4.3.4.

(c) Show that if $m \geq 2$ then $p_m(z) = p_{m-1}(z) + zp_{m-2}(z)$. [*Hint: the direct proof from (b) is not hard. There is also a more enlightening bijective proof using Exercise 4.18(e) below.*]

(d) Show by induction on m that $p_m(z)p_2(z) = p_{m+2}(z) + z^2 p_{m-2}(z)$ for $m \geq 2$.

(e) For $n \in \mathbb{N}$ let $\widetilde{g}_n(w) = w^n g_n(-w^{-1})$. Thus $\widetilde{g}_n(w) = \sum_{k=0}^{n} r_{B_n}(n-k)(-1)^{n-k} w^k$ for $n \geq 2$ and, because of our earlier definitions, $\widetilde{g}_0(w) = 2$, $\widetilde{g}_1(w) = w - 2$. Show that for all $n \in \mathbb{N}$,

$$\widetilde{g}_n(w)\widetilde{g}_1(w) = \widetilde{g}_{n+1}(w) + \widetilde{g}_{n-1}(w).$$

(f) Deduce that there is an injective ring homomorphism $\theta : \mathbb{C}[w] \to \mathbb{C}[t^{-1}, t]$ such that $\theta\big(\widetilde{g}_n(w)\big) = t^{-n} + t^n$ for all $n \in \mathbb{N}_0$. [*Hint: do not be scared by the ring theory. Since $\widetilde{g}_1(w) = w - 2$ generates $\mathbb{C}[w]$, it suffices to prove that θ respects multiplication by $\widetilde{g}_1(w)$; that is,*

$$\theta\big(\widetilde{g}_n(w)\widetilde{g}_1(w)\big) = \theta\big(\widetilde{g}_n(w)\big)\theta\big(\widetilde{g}_1(w)\big)$$

for all $n \in \mathbb{N}$. The details of this reduction are given in the answer.]

(g) Using (f) and the identity $(t^{-n} + t^n)^2 = t^{-2n} + 2 + t^{2n}$ prove that $g_n(z)^2 = g_{2n}(z) + 2z^{2n}$ for all $n \in \mathbb{N}_0$.

(h) Show more generally that $g_\ell(z)g_m(z) = g_{\ell+m}(z) + z^{2m} g_{\ell-m}(z)$ for all $\ell, m \in \mathbb{N}_0$ with $\ell \geq m$, as claimed in Proposition 4.3.6.

(i) ($\star$) Is there a bijective proof of (g)?

4.15 Suppose that B is a board in the $n \times n$ grid such that $f_B(z) = g_2(z)^{c_2} \ldots g_n(z)^{c_n}$. See Proposition 4.3.8 and the two following exerciss for cases where this arises.

(a) Show that $w^n f_B(-w^{-1}) = \widetilde{g}_2(w)^{c_2} \ldots \widetilde{g}_n(w)^{c_n}$, where $\widetilde{g}_n(w)$ is as defined in Exercise 4.14(e).

(b) Show that there are constants $b_\ell \in \mathbb{N}_0$ such that

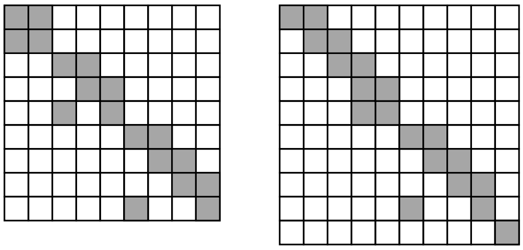
$$(t^{-2} + t^2)^{c_2} \ldots (t^{-n} + t^n)^{c_n} = \sum_{0 \leq \ell \leq n/2} b_\ell (t^{-(n-2\ell)} + t^{n-2\ell}).$$

(c) Deduce from Exercise 4.14(f) that $f_B(z) = \sum_{0 \leq \ell \leq n/2} b_\ell z^{2\ell} g_{n-2\ell}(z)$.

(d) Deduce from Exercise 4.3.7 that $r_{\overline{B}}(n) = \sum_{0 \leq \ell \leq n/2} b_\ell u_{n-2\ell}$.

(e) Use the Binomial Theorem applied to $(t^{-m}+t^{m})^{c}$ and (d) to give an alternative proof of Proposition 4.3.8.

4.16 Let B and C be the boards of shaded squares shown below.



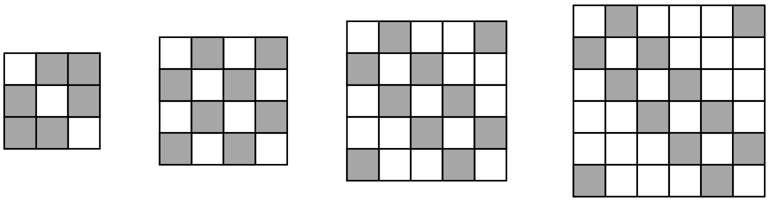
(a) Express $r_{\overline{B}}(9)$ as a sum of the ménage numbers u_n. [*Hint: a very quick method uses the machine developed in Exercise 4.15.*]

(b) Express $r_{\overline{C}}(10)$ as a sum of the ménage numbers u_n. [*Hint: Exercise 4.15 generalizes to products with $g_1(z)$; note that $f_{\square}(z) = 1+z = (1+2z)-z = g_1(z)-z$.*]

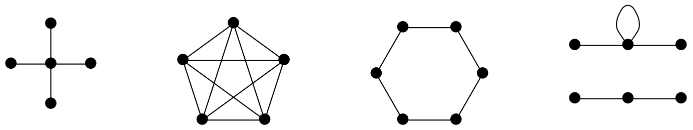
4.17

(a) Let σ, $\tau : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ be permutations. Give a bijection between permutations discordant with both σ and τ and permutations discordant with both the identity permutation and $\sigma^{-1}\tau$.

(b) For $n \geq 3$ let D_n be the board of unshaded squares contained in the $n \times n$ grid, shown below for D_3, D_4, D_5, D_6. Find the number of ways to put n non-attacking rooks on D_n in terms of the ménage numbers u_n. (See Lemma 9.4.1 for the general result behind this.)

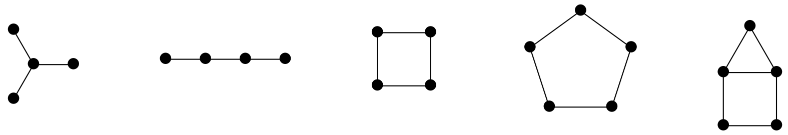


4.18 Let G be a graph (possibly with self-loops) with m vertices. For $k \in \mathbb{N}_0$, we say that a placement of k rooks on the vertices of G is *non-attacking* if no two rooks are on vertices connected by an edge. Let $r_k(G)$ be the number of such placements. Generalizing Exercise 4.14, we define the *independence polynomial* G to be the polynomial $f_G(z) = \sum_{k=0}^{m} r_k(G)z^k$. For example, the independence polynomials of the graphs



are $1+5z+6z^2+4z^3$, $1+5z$, $1+6z+9z^2+2z^3$ and $(1+z)^2(1+3z+z^2)$. The name comes from graph theory: a subset of the vertices of G is *independent* if it contains no two adjacent vertices.

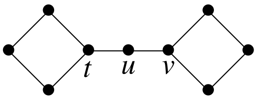
(a) Find the independence polynomials of the graphs below.



(b) State a generalization of Lemma 4.2.1 to independence polynomials. Does the proof of this lemma also generalize?

(c) State a generalization of Lemma 4.2.2 to independence polynomials. Does the proof of this lemma also generalize?

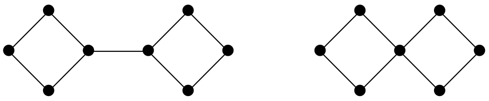
(d) Find the independence polynomial of the graph below by applying (b) and then (c).



(e) Let G be a graph having vertices $\{t,u,v\}$ such that the only edges involving u are $\{t,u\}$ and $\{u,v\}$. Let

- G/u be G with vertex u and its incident edges deleted and (unless it is already an edge), a new edge $\{t,v\}$ inserted;
- $G//u$ be G with vertex v deleted and vertices u and w identified.

(If $\{t,v\}$ is an edge of G then $G//u$ has a self-loop on the vertex replacing t and v.) For example, if G is the graph in (d) with t, u, v as marked, then G/u and $G//u$ are as shown below.



Show that $f_G(z) = f_{G/v}(z) + zf_{G//v}(z)$.

(f) Show that given a board B with m boxes there is a graph $G(B)$ with m vertices such that $f_B(z) = f_{G(B)}(z)$.

(g) Which of the graphs in (a) are graphs of boards?

(h) ($\star$) Give a necessary and sufficient condition for a graph to be the graph of a board.

4.19 [This 'exercise' and the answer in Appendix C are included for more expert readers as in indication of how the machinery of Lemma 4.15 leads to a quick proof of Riordan's formula for the number of $3 \times n$ Latin rectangles. It will be part of the text in §9.4.]

Notation. For $n \in \mathbb{N}$ let u_n be the ménage number defined in §4.3; this could also have been defined as the number of permutations of $\{1,2,\ldots,n\}$ discordant with both the identity and an n-cycle. By definition, $u_0 = 2$. (Alas, here $u_0 = 1$ would be the better choice.) Let $F(z) = \sum_{n=0}^{\infty} d_n \frac{z^n}{n!}$ be the exponential generating function of the derangement numbers d_n.

(a) Show that if σ is a permutation of $\{1,2,\ldots,n\}$ with cycle type $(2^{c_2},\ldots,n^{c_n})$ then the number of permutations discordant with both the identity and σ is $\sum_{0\le\ell\le n/2} b_\ell(\sigma)u_{n-2\ell}$ where the coefficients $b_\ell(\sigma)$ are defined by

$$(t^{-2}+t^2)^{c_2}\ldots(t^{-n}+t^n)^{c_n} = \sum_{0\le\ell\le n/2} b_\ell(\sigma)(t^{-(n-2\ell)}+t^{n-2\ell}).$$

(b) Let $\mathscr{D}_n$ be the set of derangements of $\{1,2,\ldots,n\}$. By specializing Polya's Cycle Index Formula appropriately show that

$$F(z/t)F(zt) = \sum_{n=0}^{\infty}\frac{z^n}{n!}\sum_{\sigma\in\mathscr{D}_n}\sum_{0\le\ell\le n} b_\ell(\sigma)(t^{-(n-2\ell)}+t^{n-2\ell}).$$

(c) Show that formally specializing the right-hand side in (b) by replacing $t^{-k}+t^k$ with u_k for each $k \in \mathbb{N}$ gives the exponential generating function for $3 \times n$ Latin rectangles.

(d) Show that if $0 \le \ell \le n/2$ then the coefficient of $z^n t^{n-2\ell}/n!$ on the right-hand side in (b) is $\binom{n}{\ell}d_\ell d_{n-\ell}$ and hence that the number of $3 \times n$ Latin rectangles with first row 1, 2, ..., n is

$$\sum_{\ell}\binom{n}{\ell}d_\ell d_{n-\ell}v_{n-2\ell}$$

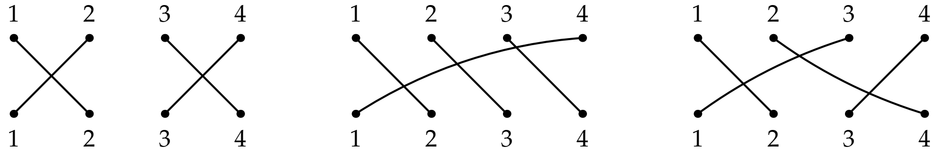
where $v_k = u_k$ for $k \in \mathbb{N}$ and $v_0 = 1$.

Appendix C

Solutions to exercises

1. The Derangements Problem

Exercise 1.1.3 We first count the derangements σ of $\{1,2,3,4\}$ such that $\sigma(1) = 2$. Clearly $\sigma(2) \in \{1,3,4\}$. If $\sigma(2) = 1$ then, to avoid fixing 3, we must have $\sigma(3) = 4$ and $\sigma(4) = 3$. Hence $\sigma = 2143$ in one-line form. Similarly if $\sigma(2) = 3$ then $\sigma = 1342$ and if $\sigma(2) = 4$ then $\sigma = 1432$. The diagrams are shown below.



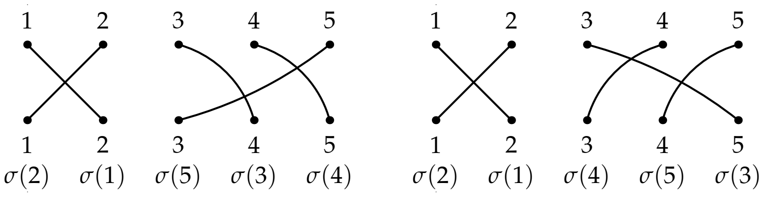
Similarly, or by symmetry if you prefer, there are three derangements such that $\sigma(1) = 3$, and three derangements such that $\sigma(1) = 4$. Hence $d_4 = 3 \times 3 = 9$.

Exercise 1.1.4 Before Winter sets in, walk around your land. For each sheep you see, put a stone in your pocket. Keep the stones safe until Spring. At Spring, take the stones and again walk around your land. For each sheep you see, throw away a stone. The number of remaining stones is the number of lost sheep. If this number is less than 10, you can count it. Otherwise, make another bijection between the remaining stones and a subset of the remaining sheep to visualize how many sheep were eaten by wolves. (This only fails if more than half the sheep were lost.)

Remark: Tally marks have been found carved on bones dating back to 30000BC and clay tokens, such as the ones in Figure A.1 overleaf, were used to represent sheep in neolithic times. More sophisticated recording devices, known as *quipu*, using knots on cords, were made by the Incans.

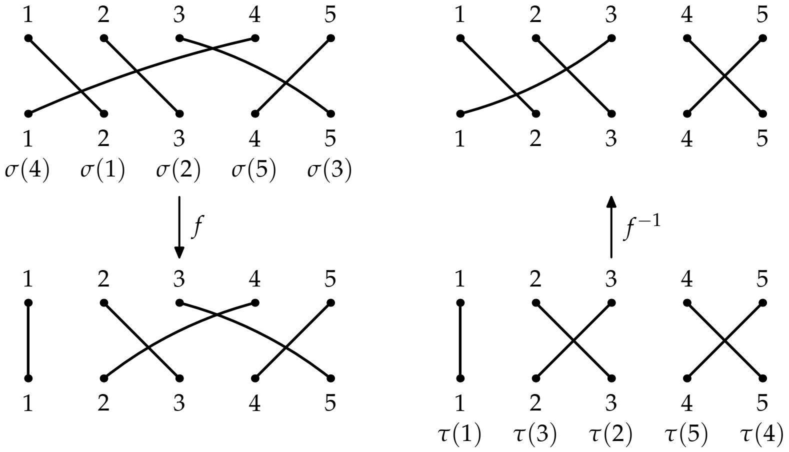
Exercise 1.1.5 The two derangements σ of $\{1,2,3,4,5\}$ such that $\sigma(1) = 2$ and $\sigma(2) = 1$ are shown overleaf.

Figure A.1 Clay accounting tokens, Susa, Uruk period. Louvre Museum.



We have $\sigma(3) \in \{4,5\}$ so there are two choices for $\sigma(3)$. On the other hand, the three derangements of $\{1,2,3,4,5\}$ such that $\sigma(1) = 2$ and $\sigma(2) = 3$ are 23154, 23451 and 23514 in one-line form, so now there are 3 choices for $\sigma(3)$.

Exercise 1.1.7 The missing diagrams in Figure 1.1.7 are shown below.



End of chapter exercises

1.1 (a) Multiplying choices we get $3 \times 4 \times 6 = 72$ meals.

(b) By **BCP1** there are $3 \times 4 = 12$ two course meals with a starter and main course and $4 \times 6 = 24$ two course meals with a main course and dessert. Adding up, using **BCP2**, we count $12 + 24 = 36$ two course meals with exactly one main course.

1.2 (a) Constructing (x_1, x_2, x_3) step-by-step we have 10 choices for x_1 (any number in $\{1, 2, \ldots, 10\}$, then 9 choices for x_2 (since x_1 may not be chosen), then 8 choices for x_3 (since x_1 and x_2 may not be chosen). Hence $|X| = 10 \times 9 \times 8 = 720$ by **BCP1**.

(b) $f\big((x_1, x_2, x_3)\big) = \{2, 3, 5\} \iff \{x_1, x_2, x_3\} = \{2, 3, 5\}$. We have 3 choices for x_1, then 2 choices for x_2, then 1 choice for x_3, giving $3 \times 2 \times 1 = 3!$ tuples.

(c) By the general version of part (b), for each $X \in S$, there are exactly 3! tuples $(x_1, x_2, x_3) \in T$ such that $f\big((x_1, x_2, x_3)\big) = X$. Hence

$$|S| = \frac{|T|}{3!} = \frac{720}{3!} = 120.$$

Note that $|S| = \binom{10}{3}$, as you probably expected.

1.3 We partition X as follows:

$$X = \big\{(a, a) : 1 \leq a \leq n\big\} \cup \big\{(a, b) : 1 \leq a < b \leq n\big\}.$$

There are n pairs in the first set. Pairs in the second set are in bijection with subsets of $\{1, 2, \ldots, n\}$ of size 2, by the map $(a, b) \mapsto \{a, b\}$. So there are $\binom{n}{2} = n(n-1)/2$ pairs in the second set. Hence

$$|X| = n + \frac{n(n-1)}{2} = \frac{n(n+1)}{2}.$$

1.4 There are 2 subsets of $\{1\}$, namely $\varnothing$ and $\{1\}$, and 4 subsets of $\{1, 2\}$, namely $\varnothing, \{1\}, \{2\}, \{1, 2\}$. You should find there are 8 subsets of $\{1, 2, 3\}$. So it looks like the number of subsets of $\{1, 2, \ldots, n\}$ is 2^n. We can construct a subset X of $\{1, 2, \ldots, n\}$ step-by-step: for each $x \in \{1, 2, \ldots, n\}$ make a yes/no choice of whether to put it into X. We have 2 choices for each x, and n choices to make, so by **BCP1**, there are $2 \times 2 \times \cdots \times 2 = 2^n$ subsets.

When $n = 0$ this formula says, correctly, that the empty set $\varnothing$ has a unique subset, namely itself.

1.5 (a) Send a placement with balls in urns a_1, a_2, a_3, a_4 to $\{a_1, a_2, a_3, a_4\}$. This defines a bijection $f : A \to C$. A walking route in B consists of seven steps, of which exactly four are East. If the steps numbered a_1, a_2, a_3, a_4 are East, then send the route to $\{a_1, a_2, a_3, a_4\}$. This defines a bijection $g : B \to C$.

(b) The steps East are steps number 1, 3, 4, 7 so the element of C corresponding to this walk is $\{1,3,4,7\}$.

(c) Urns 2, 3, 4 and 6 have balls, so the corresponding element of C is $\{2,3,4,6\}$, and the corresponding walking route is SEEESES.

(d) By definition $|C| = \binom{7}{4}$. The sets A and B are in bijection with C, so by **BCP0** we have

$$|A| = |B| = |C| = \binom{7}{4}.$$

1.6 (a) See the table below. The 'x-card' in AKQJx stands for any ten or lower. There are $52-16=36$ such cards, and 4 of each royal card, so the number of AKQJx hands is $4\times4\times4\times4\times36=9216$.

Hand type	Number
AKQJx	$4\times4\times4\times4\times36=9216$
AAKQJ	$6\times4\times4\times4=384$
AKKQJ	$4\times6\times4\times4=384$
AKQQJ	$4\times4\times6\times4=384$
AKQJJ	$4\times4\times4\times6=384$

For instance, the number of AAKQJ hands is $\binom{4}{2}\times4\times4\times4$, since we can choose two aces in $\binom{4}{2}=6$ ways, and then we have 4 choices for the King, Queen and Jack. The other rows of the table below are found similarly. Adding up, we count $9216+4\times384=10752$ hands.

(b) Now an x-card is any Jack or lower: there are 40 such cards.

Hand type	Number
AKQxx	$4\times4\times4\times\binom{40}{2}=49920$
AAKQx, AKKQx, AKQQx	each $\binom{4}{2}\times4\times4\times40=3840$
AAKKQ, AAKQQ, AKKQQ	each $\binom{4}{2}\times\binom{4}{2}\times4=144$
AAAKQ, AKKKQ, AKQQQ	each $\binom{4}{3}\times4\times4=64$

Adding up, we count $49920+3\times3840+3\times144+3\times64=62064$ hands.

1.7 We have $d_0=1$, $d_1=0$ and so $p_0=1$, $p_1=0$. Hence $p_1-p_0=-1=(-1)^1/1!$, as required. For the inductive step, suppose that $p_n-p_{n-1}=(-1)^n/n!$.

Using the recurrence in Theorem 2.4 to rewrite d_{n+1} as $n(d_n + d_{n-1})$ we get

$$\begin{aligned} p_{n+1} - p_n &= \frac{d_{n+1}}{(n+1)!} - \frac{d_n}{n!} = \frac{n(d_n + d_{n-1})}{(n+1)!} - \frac{d_n}{n!} \\ &= \Big(\frac{n}{n+1} - 1\Big)\frac{d_n}{n!} + \frac{d_{n-1}}{(n+1)(n-1)!} = \frac{-1}{n+1}(p_n - p_{n-1}). \end{aligned}$$

Hence, by induction, we have

$$p_{n+1} - p_n = \frac{-1}{n+1}\frac{(-1)^n}{n!} = \frac{(-1)^{n+1}}{(n+1)!}$$

as required.

It now follows by an easier induction on $n \in \mathbb{N}_0$ that $d_n = n!p_n$ is as claimed in Corollary 1.1.9.

1.8 (a) Let $x \in \{1,2,\dots,n\}$. There are $(n-1)!$ permutations σ of $\{1,2,\dots,n\}$ that fix x. (See page 8 for the case $x = 1$; we argued in the proof of Theorem 1.1.11(ii) that there was nothing special about 1 in this context.) Since each permutation is chosen with equal probability $1/n!$, the probability that x is fixed is $(n-1)!/n! = 1/n$. Hence the probability that Parcel x is wrongly delivered is $1 - 1/n$.

(b) Let W_x be the event that Parcel x is wrongly delivered. The event that all parcels are wrongly delivered is $\bigcap_{x=1}^n W_x$. Assuming independence, we have

$$\mathbf{P}\Big[\bigcap_{x=1}^n W_x\Big] = \prod_{x=1}^n \mathbf{P}[W_x] = \prod_{x=1}^n \big(1 - \frac{1}{n}\big) = \big(1 - \frac{1}{n}\big)^n.$$

(c) Fix $\alpha > 0$. A sketch graph shows that $\mathrm{e}^{-y} \geq 1 - y$ for all $y \geq 0$, and $1 - y \geq \mathrm{e}^{-(1+\alpha)y}$ for all sufficiently small y. (These inequalities are surprisingly useful.) Putting $y = 1/n$ and taking nth powers we get

$$\mathrm{e}^{-1} = \big(\mathrm{e}^{-1/n}\big)^n \geq \big(1 - \frac{1}{n}\big)^n \geq \big(\mathrm{e}^{-(1+\alpha)/n}\big)^n = \mathrm{e}^{-(1+\alpha)}$$

for all sufficiently large n. Since α was arbitrary, it follows that $\lim_{n\to\infty}(1 - 1/n)^n = 1/\mathrm{e}$, as required.

(d) Suppose Parcel 1 is correctly delivered. Then the probability that Parcel 2 is correctly delivered is $1/(n-1)$, which is more than the usual $1/n$ chance. (In particular, if $n = 2$, then once Parcel 1 is correctly delivered, it is certain that Parcel 2 is correctly delivered.) The events that the parcels are correctly delivered are therefore not independent.

1.9 Corollary 1.1.9 states that

$$d_n = n!\Big(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^n}{n!}\Big).$$

Evaluating the Taylor series for e^x at $x = -1$, as in the proof of Theorem 1.1.11(a), we get

$$\mathrm{e}^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^n}{n!} + \frac{(-1)^{n+1}}{n+1} + \cdots .$$

Hence

$$\Big|d_n - \frac{n!}{\mathrm{e}}\Big| = n!\Big|\frac{d_n}{n!} - \frac{1}{\mathrm{e}}\Big| = n!\Big|\sum_{m=n+1}^{\infty} \frac{(-1)^m}{m!}\Big|.$$

If $a_1, a_2, \ldots$ is a decreasing sequence of positive real numbers then $a_1 - a_2 + a_3 - \cdots < a_1$. Applying this with $a_i = 1/(n+i)!$ we get

$$\Big|d_n - \frac{n!}{\mathrm{e}}\Big| < \frac{n!}{(n+1)!} = \frac{1}{n+1}.$$

If $n \geq 2$ then $1/(n+1) \leq 1/3 < 1/2$. So provided $n \geq 2$, the nearest integer to $\frac{n!}{\mathrm{e}}$ is d_n. This result also holds if $n = 1$ since $d_1 = 0$ and $1/\mathrm{e} < 1/2$.

1.10 (a) Observe that if σ is a permutation of $\{1,2,\ldots,n\}$ fixing exactly the elements of $Y \subseteq \{1,2,\ldots,n\}$ then σ permutes $\{1,2,\ldots,n\}\backslash Y$ as a derangement. If $|Y| = k$ then we have $\binom{n}{k}$ choices for Y and d_{n-k} choices for the derangement on $\{1,2,\ldots,n\}\backslash Y$. By the formula for d_{n-k}, the number of permutations with exactly k fixed points is

$$a_n(k) = \binom{n}{k}(n-k)!\Big(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^{n-k}}{(n-k)!}\Big).$$

Since $\binom{n}{k}(n-k)! = n!/k!$, this agrees with the claimed formula for $a_n(k)$.

Hence

$$\begin{aligned} a_n(0) - a_n(1) = n!\Big(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^n}{n!}\Big) \\ - n!\Big(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^{n-1}}{(n-1)!}\Big) = n!\frac{(-1)^n}{n!} = (-1)^n. \end{aligned}$$

(For a bijective proof of this identity see Herbert S. Wilf, *A bijection in the theory of derangements*, Mathematics Magazine **57** (1984) 37–40.)

(b) The mean number of fixed points is

$$\frac{1}{n!}\sum_{k=1}^{n} k a_n(k) = \sum_{k=1}^{n} \frac{1}{(k-1)!}\Big(1 - \frac{1}{1!} + \frac{1}{2!} - \cdots + \frac{(-1)^{n-k}}{(n-k)!}\Big).$$

We get a summand $(-1)^\ell/j!\ell!$ for every j, $\ell \in \mathbb{N}_0$ such that $j + \ell \leq n-1$. The contribution from those summands for which $j+\ell=m$ is

$$\sum_{\ell=0}^{m}\frac{(-1)^\ell}{(m-\ell)!\ell!}=\sum_{\ell=0}^{m}(-1)^k\frac{1}{m!}\binom{m}{\ell}=\frac{1}{m!}\sum_{\ell=0}^{m}(-1)^\ell\binom{m}{\ell}.$$

By Corollary 2.2.8(ii) the right-hand side is 0 unless $m=0$, in which case it is 1. Hence the mean number of fixed points is 1.

(c) $(\star)$ Let A be the matrix in the question. By one definition of the determinant,

$$\det A=\sum_{\sigma}\operatorname{sgn}(\sigma)\prod_{i=1}^{n}A_{i\sigma(i)}$$

where σ varies over all permutations of $\{1,2,\dots,n\}$. Since $A_{i\sigma(i)}=1$ if $\sigma(i)\neq i$ and $A_{i\sigma(i)}=0$ if $\sigma(i)=i$, we have

$$\prod_{i=1}^{n}A_{i\sigma(i)}=\begin{cases}1 & \text{if } \sigma \text{ is a derangement}\\ 0 & \text{otherwise.}\end{cases}$$

Hence $\det A=e_n-o_n$.

Another way to find the determinant uses that $\det A$ is the product of the eigenvalues of A. Since $A+I$ is the all-ones matrix, of rank 1, it has $n-1$ linearly independent vectors in its kernel. Hence -1 is an eigenvalue of A with multiplicity $n-1$. Another eigenvalue of A is $n-1$, since every column of A has sum $n-1$ and so $(1,\dots,1)A=(n-1,\dots,n-1)$. Hence $\det A=(-1)^n(n-1)$. Comparing we get $e_n-o_n=(-1)^n(n-1)$.

1.11 (a) We have defined $P=\{(\sigma,x):\sigma\in G, x\in\{1,2,\dots,n\},\sigma(x)=x\}$. Let $\operatorname{Fix}\sigma$ be the set of fixed points of $\sigma\in G$ and let $\operatorname{Stab}x=\{\sigma\in G:\sigma(x)=x\}$. Counting $|P|$ by summing over $\sigma\in G$ we get

$$|P|=\sum_{\sigma\in G}|\operatorname{Fix}\sigma|.$$

Recall that, by the orbit stabiliser theorem, if $\operatorname{Orb}x$ is the orbit of x under G then $|\operatorname{Orb}x|=|G|/|\operatorname{Stab}x|$. Hence, counting $|P|$ by summing over $x\in\{1,2,\dots,n\}$, we get

$$|P|=\sum_{x=1}^{n}|\operatorname{Stab}x|=\sum_{x=1}^{n}\frac{|G|}{|\operatorname{Orb}x|}.$$

Thus each x in an orbit of size r contributes $|G|/r$ to the sum. Hence each orbit contributes $|G|$ to the sum, and $|P|/|G|$ is the number of orbits of G on $\{1,2,\dots,n\}$.

(b) Take a tetrahedron with faces labelled 1, 2, 3, 4. Any permutation of the faces can be realised by a rotation that leaves the tetrahedron occupying the same position in space. Conversely, any rotation is clearly determined by what it does to the faces. Thus the symmetry group of the tetrahedron is $\mathrm{Sym}(\{1,2,3,4\})$.

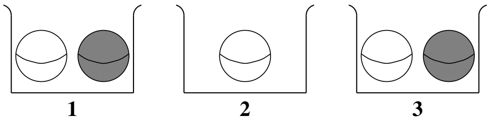
The table below shows the number C_σ of red-blue-green colourings fixed by an element σ of each cycle type. (See §9.2 for disjoint cycle notation.) For example, the double-transposition $\sigma = (1,2)(3,4)$ fixes a colouring if and only if faces 1 and 2 have the same colour, and faces 3 and 4 have the same colour. So there are $C_{(1,2)(3,4)} = 3^2 = 9$ such colourings.

σ	id	$(1,2)$	$(1,2,3)$	$(1,2)(3,4)$	$(1,2,3,4)$
C_σ	3^4	3^3	3^2	3^2	3
N_σ	1	6	8	3	6

The bottom row shows the number of elements N_σ with each cycle type. The number of coloured tetrahedra up to rotation is the number of orbits of $\mathrm{Sym}(\{1,2,3,4\})$ on the set of all 3^4 coloured tetrahedra. By (a), it is

$$\frac{1}{4!}\sum_\sigma C_\sigma = \frac{3^4+3^3\times 6+3^2\times 8+3^2\times 3+3\times 6}{4!} = 15.$$

(c) Attach labels 1, 2 to 3 to the three urns. We will ‘undo’ this labelling by counting ball-urn placements up to the action of the symmetric group $\mathrm{Sym}(\{1,2,3\})$ on the labels. For example, the ball and urn placement drawn below



is sent by the 3-cycle $(1,2,3)$ to the placement with the same diagram, but with the urns instead labelled $2,3,1$ from left to right.

The total number of placements (into labelled urns) is $\binom{3+3-1}{3}\binom{3+2-1}{2} = \binom{5}{3}\binom{4}{2} = 60$, by **BCP1** and Theorem 2.3.3.

A ball and urn placement is fixed by the transposition $(1,2)$ if and only if urns 1 and 2 have the same number of balls of each colour. Writing (w,b) for w white balls and b black balls, the contents could be $(0,0)$, $(1,0)$, $(0,1)$ or $(1,1)$. Therefore there are 4 placements fixed by each of the transpositions $(1,2)$, $(1,3)$ and $(2,3)$. Since there are exactly 2 black balls, no placement is fixed by a three cycle. By (a), the number of placements into indistinguishable urns is $(60+3\times 4)/3! = 12$.

1.12 Number the coins $1, 2, \ldots, 2m$ from left to right. The tortoise can guarantee to take all the odd coins (just do it!). Similarly the tortoise can guarantee to take all the even coins. So unless the value of the odd coins equals the value of the even coins, the tortoise has a winning strategy.

Suppose that the even coins and the odd coins both have total value V. Let c_i be the value of coin i. Suppose that $c_1 > c_2$ and $c_1 > c_{2m}$. Let $W = \min(V - c_2, V - c_{2m})$. Since $V - c_1 < V - c_2$ and $V - c_1 < V - c_{2m}$ we have $V - c_1 < W$. Since $V - c_2 = c_4 + \cdots + c_{2m}$ and $V - c_{2m} = c_2 + \cdots + c_{2(m-1)}$, it follows that if the tortoise starts by taking coin 1, and then switches to the even coins, he takes at least $W + c_1 > V$. By symmetry we see that the tortoise wins in the tied case whenever the coins at each end are not equally valuable, and the more valuable one is worth more than its neighbour.

1.13 The problem is no harder generalized to n safes. The keys can be distribution uniformly at random as follows: start by putting key i in safe i, for each $i \in \{1, \ldots, n\}$. Then for each k working from 1 up to n, choose a number j between 1 and k uniformly at random, and swap the keys in safes j and k. (If $j = k$ then leave the key in safe k where it is.) The first r swaps are irrelevant to the probability that all safes can be opened. Then for each $k > r$, the key k in safe k must be moved into an earlier openable safe. The probability this happens in every case is

$$\frac{k}{k+1}\frac{k+1}{k+2}\cdots\frac{n-1}{n} = \frac{k}{n}.$$

This solution is due to Igors Stepanovs.

1.14 We build up a Sudoku permutation matrix one column at a time, starting with column 1 and ending with column n^2. Let $i, j \in \{0, 1, \ldots, n-1\}$. When we choose the row to contain the unique 1 in column $ni + j + 1$, there are j blocks, each of n rows, that are barred because of the 1s in columns $ni + 1, \ldots, ni + j$. Let B be the nj-set of such rows. There are also ni rows that are barred because of 1s in columns 1, 2, ..., ni. However, this double-counts any row containing a 1 in columns 1, 2, ..., ni whose number lies in B. In each block of columns $nk + 1, \ldots$, $nk + n$ for $0 \le k < i$ there are exactly j such rows. Hence there are

$$n^2 - nj - ni + ij$$

possible positions for the 1 in column $ni + j + 1$. The total number of Sudoku permutation matrices is therefore

$$\prod_{i=0}^{n-1}\prod_{j=0}^{n-1}(n-i)(n-j) = \prod_{j=0}^{n-1} n!(n-j)^n = n!^n n!^n = n!^{2n}.$$

1.15 We give the start of one possible solution and invite the reader to complete it.

Working with a $4n$-bead necklace, with $2n$ black beads and $2n$ white beads, number the positions by integers, so $m, m+4n, m+8n, \ldots$ all label the same position. For each $m \in \{1, \ldots, 4n\}$, let b_m be the difference between the number of black beads in positions $\{m, m+1, \ldots, m+2n-1\}$ and the number of black beads in positions $\{m+2n, \ldots, m+4n-1\}$. If $b_m = 0$ then we may cut in position m to get two necklaces, each with n black and white beads. Now consider how b_m may vary for m between 0 and $4m-1$.

2. Binomial coefficients

Exercise 2.1.3 (a) The empty set $\varnothing$ is the unique subset of $\{1,2,\ldots,n\}$ of size 0, and $\{1,2,\ldots,n\}$ is the unique subset of $\{1,2,\ldots,n\}$ of size n. Hence $\binom{n}{0} = \binom{n}{n} = 1$. (If $n = 0$ then $\{1,2,\ldots,n\} = \varnothing$; since $\varnothing \subseteq \varnothing$, the empty set is the unique subset in both cases.)

(b) Let $n \in \mathbb{N}$. The subsets of $\{1,2,\ldots,n\}$ of size 1 are $\{1\}, \{2\}, \ldots, \{n\}$. Clearly the empty set $\varnothing$ has no subsets of size 1, so $\binom{0}{1} = 0$. Hence $\binom{n}{1} = n$ for all $n \in \mathbb{N}_0$.

Exercise 2.1.6 The bijection

$$f : \big\{\{1\},\{2\},\{3\},\{4\}\big\} \rightarrow \big\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\big\}$$

is defined by $f(X) = \{1,2,3,4\}\backslash X$. Thus $f(\{1\}) = \{2,3,4\}$, $f(\{2\}) = \{1,3,4\}$, and so on. The inverse of f is

$$g : \big\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\}\big\} \rightarrow \big\{\{1\},\{2\},\{3\},\{4\}\big\}$$

defined by $g(Y) = \{1,2,3,4\}\backslash Y$.

Remark: It would not be accurate to say that f and g are the same function, because they have different domains. However, if we let P be the set of all subsets of $\{1,2,3,4\}$ then we can define a function $h : P \rightarrow P$ by $h(X) = \{1,2,3,4\}\backslash X$; then (i) h is a self-inverse bijection; (ii) f is the restriction of h to the 1-subsets in P, and (iii) g is the restriction of h to the 3-subsets in P.

Exercise 2.1.10 The bijection

$$f : \left\{(X,y) : \begin{array}{c} X \subseteq \{1,2,\ldots,n\},\ |X| = k, \\ y \in \{1,2,\ldots,n\},\ y \not\in X \end{array}\right\} \rightarrow \left\{(Z,y) : \begin{array}{c} Z \subseteq \{1,2,\ldots,n\}, \\ |Z| = k+1,\ y \in Z \end{array}\right\}$$

defined in the informal proof is

$$f\big((X,y)\big) = (X \cup \{y\}, y).$$

The inverse of f is defined by $f^{-1}\big((Z,y)\big) = (Z\backslash\{y\}, y)$.

Exercise 2.2.1 Following the bijective proof of the Fundamental Recurrence we see that $\binom{6}{3}$ counts the 4-subsets of $\{1,2,\ldots,7\}$ containing 7, and $\binom{6}{4}$ counts the 4-subsets of $\{1,2,\ldots,7\}$ not containing 7. The former subsets are in bijection with the walking routes A to B where step 7 (the final step) is East, and the latter are in bijection with the walking routes A to B where step 7 is South. (In either case we put a number in the subset if it corresponds to a step East, as in the solution to Exercise 1.5.)

Exercise 2.2.5 Take n people and form a (generalized) football team of r of them in $\binom{n}{r}$ ways. Then choose k of these r people to be defenders in $\binom{r}{k}$ ways. Hence there are $\binom{n}{r}\binom{r}{k}$ teams-with-defenders. Alternatively, we first choose k of the n people to be defenders in $\binom{n}{k}$ ways, and then complete the team by choosing $r-k$ attackers from the remaining $n-k$ people in $\binom{n-k}{r-k}$ ways. So the number of teams-with-defenders is also $\binom{n}{k}\binom{n-k}{r-k}$.

Exercise 2.2.7 Let $P = \{Z : Z \subseteq A \cup B, |Z| = m\}$. Since $A \cup B$ has size $a+b$,we have $|P| = \binom{a+b}{a}$. Observe that if $Z \in P$ then $|Z \cap A| \in \{0,1,\ldots,m\}$. For each $k \in \{0,1,\ldots,m\}$, let

$$P_k = \{Z \in P : |Z \cap A| = k\}.$$

The size of P_k is $\binom{a}{k}\binom{b}{m-k}$ since we must choose exactly k elements of A for $Z \cap A$ and then exactly $m-k$ elements of B for $Z \cap B$. Hence

$$\binom{a+b}{m} = |P| = \sum_{k=0}^{m} |P_k| = \sum_{k=0}^{m} \binom{a}{k}\binom{b}{m-k},$$

as required.

Exercise 2.2.10 When n is odd there is a bijection

$$f : \big\{X : X \subseteq \{1,2,\ldots,n\}, |X| \text{ is even}\big\} \to \big\{X : X \subseteq \{1,2,\ldots,n\}, |X| \text{ is odd}\big\}$$

defined by $f(X) = \{1,2,\ldots,n\}\backslash X$.

This fails when n is even, because then $|X|$ and $|\{1,2,\ldots,n\}\backslash X|$ always have the same size. Instead, let P be the set of all subsets of $\{1,2,\ldots,n\}$ and define $g : P \to P$ by

$$g(X) = \begin{cases} X \cup \{1\} & \text{if } 1 \notin X \\ X\backslash\{1\} & \text{if } 1 \in X. \end{cases}$$

Observe that $|g(X)| = |X| \pm 1$ for all $X \in P$, so $|g(X)|$ and $|X|$ have different parities. Moreover, $g(g(X)) = X$ for all $X \in P$, so g is its own inverse. Hence the restriction of g to even sized sets is a bijection

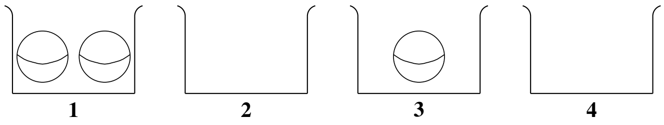
$$\big\{X : X \subseteq \{1,2,\ldots,n\}, |X| \text{ is even}\big\} \to \big\{X : X \subseteq \{1,2,\ldots,n\}, |X| \text{ is odd}\big\}.$$

The choice of 1 in the definition of g is arbitrary; some such choice is unavoidable when n is even.

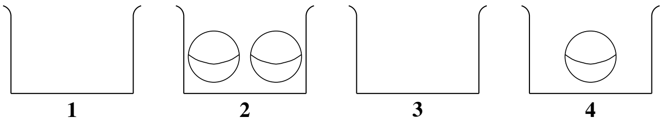
Exercise 2.3.1 (i) We have k numbered balls and n numbered small urns. For ball 1 we have n choices for its urn; for ball 2 we have $n-1$ choices, and so on, until ball k when we have $n-(k-1)$ choices. Hence, by **BCP1**, the number of placements is $n(n-1)\dots(n-k+1)$.
(ii) If the urns are large then an urn can be reused. Hence the number of choices is n every time and the number of placements is n^k.

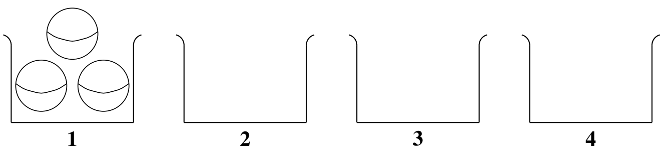
Exercise 2.3.2 We have k indistinguishable balls, each in a unique small urn. There are $k!$ ways we can add numbers to these balls, one for each permutation of $\{1,2,\dots,k\}$, each giving a different placement of numbered balls. So the number of placements of k numbered balls is $k!$ times the number of placements of k indistinguishable balls.

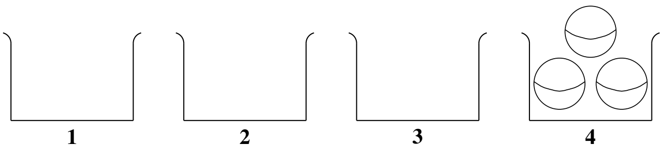
The number of placements of k numbered balls into n large urns is n^k. This number is not divisible by $k!$ in general. To see why the rule breaks down, imagine 2 balls in a single urn. When we add labels 1 and 2, we get labelled balls 1 and 2, still in a single urn. So there is one way to do this, not two. For a bigger example, take $n=4$ and $k=3$, and check that there are 3, not $3!=6$ ways to add numbers to the 3 indistinguishable balls below.



Exercise 2.3.4 The ball-and-urn placements corresponding to the strings 100110, 000111 and 111000 are shown below.







Exercise 2.4.3 We have

$$\sum_{k=0}^{m}\binom{z+k}{k}=\sum_{k=0}^{m}(-1)^k\binom{-z-1}{k}=(-1)^m\binom{-z-2}{m}=\binom{m+z+1}{m}$$

where the first and last equalities follow from Lemma 2.4.1 and the middle from Lemma 2.4.2.

End of chapter exercises

2.1 (a) By Lemma 2.1.4 we have

$$k\binom{n}{k}=k\frac{n!}{k(k-1)!(n-k)!}=\frac{n!}{(k-1)!(n-k)!}=\frac{n(n-1)!}{(k-1)!(n-k)!}=n\binom{n-1}{k-1}.$$

(b) We count pairs (y,X) where X is an k-subset of $\{1,2,\ldots,n\}$ and $y\in X$. On the one hand, there are $\binom{n}{k}$ ways to choose X; then we can choose any of the k elements of X to be y. Hence the number of pairs is $k\binom{n}{k}$. On the other hand, we can choose any $y\in\{1,2,\ldots,n\}$ in n ways; then we can choose any $k-1$ elements of $\{1,2,\ldots,n\}\backslash\{y\}$ to form $X\backslash\{y\}$. So the number of pairs is also $n\binom{n-1}{k-1}$.

Remark: This exercise is the special case $k=1$ of Lemma 2.2.4. For a ‘deformalized’ proof just put $k=1$ in the answer to Exercise 2.2.5 above.

2.2 By Exercise 2.1 and Lemma 2.1.5 we have $r\binom{n}{r}=n\binom{n-1}{r-1}$. Hence

$$\sum_{r=0}^{n}r\binom{m}{r}\binom{n}{k}=n\sum_{r=0}^{n}\binom{m}{r}\binom{n-1}{r-1}.$$

To apply Vandermonde’s Convolution (Lemma 2.2.6) we need the bottom parts of the binomial coefficients to have constant sum, so we use Lemma 2.1.5 to rewrite $\binom{n-1}{r-1}$ as $\binom{n-1}{n-r}$. (This trick is often useful.) Therefore

$$\sum_{r=0}^{n}r\binom{m}{r}\binom{n}{k}=n\sum_{r=0}^{n}\binom{m}{r}\binom{n-1}{n-r}=n\binom{m+n-1}{n},$$

where the final equality uses Vandermonde’s Convolution.

2.3 (a) Fix $k\in\mathbb{N}_0$. When $n=k$ the left-hand side is $\binom{k}{k}=1$ and the right-hand side is $\binom{k+1}{k+1}=1$. Suppose inductively, that the formula holds for $n-1\in\mathbb{N}_0$, where $n-1\geq k$. Then

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

which is $\binom{n+1}{k+1}$ by the Fundamental Recurrence (Lemma 2.1.7).

(b) The maximum element of an $(k+1)$-subset of $\{1,2,\ldots,n\}$ is at least $k+1$ and at most n. Hence,

$$\begin{aligned}&\big\{(k+1)\text{-subsets of }\{1,2,\ldots,n+1\}\big\}\\ &\qquad = \bigcup_{m=k+1}^{n}\left\{\begin{matrix}(k+1)\text{-subsets of }\{1,2,\ldots,n+1\}\\ \text{with maximum element } m\end{matrix}\right\}\end{aligned} \qquad (\star)$$

where the union is disjoint. Let X be a $(k+1)$-subset of $\{1,2,\ldots,n\}$ with maximum element m. Removing m from X gives a k-subset of $\{1,2,\ldots,m-1\}$. Conversely, given an k-subset of $\{1,2,\ldots,m-1\}$, we can insert m into it, and get a subset of size $k+1$ with m as its maximum element. Hence there is a bijection

$$\left\{\begin{matrix}(k+1)\text{-subsets of }\{1,2,\ldots,n+1\}\\ \text{with maximum element } m\end{matrix}\right\} \longleftrightarrow \Big\{k\text{-subsets of }\{1,2,\ldots,m-1\}\Big\}.$$

The right-hand set has size $\binom{m-1}{k}$. By **BCP0**, the mth set in the union in the right-hand side of $(\star)$ also has size $\binom{m-1}{k}$. Since the left-hand side of $(\star)$ has size $\binom{n+1}{k+1}$, we get

$$\binom{n+1}{k+1} = \sum_{m=k+1}^{n+1}\binom{m-1}{k} = \binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{n}{k}$$

as required.

2.4 (a) Number the cages from 1 up to n. If cage n has a lion then cage $n-1$ is empty, so there are $k-1$ lions in cages 1 up to $n-2$; by definition, there are $g(n-2,k-1)$ ways to place these $k-1$ lions. If cage n is empty then there are $k-1$ lions in cages 1 up to $n-1$; by definition there are $g(n-1,k)$ such placements. This counts each lion placement exactly once, so $g(n,k) = g(n-2,k-1) + g(n-1,k)$.

(b) We work by induction on n, dealing with all $k \in \mathbb{N}_0$ at once. Since the recurrence for g in (a) assumes that $n \geq 2$ we need two base cases. When $n = 0$ we have $g(0,0) = 1$ which agrees with $\binom{1}{0}$. When $n = 1$ we have $g(1,0) = g(1,1) = 1$ which agrees with $\binom{1-k+1}{k}$ for each k, since $\binom{2}{0} = \binom{1}{1} = 1$.

We also need to check the formula holds when $k = 0$, since $k \geq 1$ is assumed in (a). Clearly $g(n,0) = 1$ for all $n \in \mathbb{N}$, and this agrees with $\binom{n-0+1}{0} = 1$.

For the inductive step, suppose that $n \geq 2$ and $k \geq 1$. By induction, we may assume that

$$\begin{aligned} g(n-1,k) &= \binom{(n-1)-k+1}{k} = \binom{n-k}{k} \\ g(n-2,k-1) &= \binom{(n-2)-(k-1)+1}{k} = \binom{n-k}{k-1}. \end{aligned}$$

Using these and (a) we get

$$g(n,k) = g(n-2,k-1) + g(n-1,k) = \binom{n-k}{k-1} + \binom{n-k}{k} = \binom{n-k+1}{k}$$

where the final equality follows from the Fundamental Recurrence (Lemma 2.1.7). Hence $g(n,k) = \binom{n-k+1}{k}$ for all $k \in \mathbb{N}_0$.

Bijective proof of (a) Assume that $k \in \mathbb{N}$. Take $n-k+1$ cages in a row and choose k to have lions in $\binom{n-k+1}{k}$ ways. For each cage containing a lion, except the left-most, put a new cage to its left. This gives a bijection between lion placements counted by $g(n,k)$ and the k-subsets of $\{1,\dots,n-k+1\}$. □

2.5 If $u_r \in \mathbb{N}$ for each r and

$$u_1 + u_2 + \cdots + u_n = k$$

then $u_r - 1 \in \mathbb{N}_0$ for each r and

$$(u_1 - 1) + (u_2 - 1) + \cdots + (u_n - 1) = k - n.$$

This gives a bijection between solutions to the equation $u_1 + u_2 + \cdots + u_n = k$ with $u_r \in \mathbb{N}$ for each r and solutions to the equation $t_1 + t_2 + \cdots + t_n = k - n$ with $t_r \in \mathbb{N}_0$ for each r. By Corollary 2.3.5 there are exactly $\binom{k-n+n-1}{k-n}$ solutions to the latter equation. Hence there are

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

solutions to the original equation.

2.6 (a) The first few terms are $b_0 = 1$, $b_1 = 1$, $b_2 = 2$, $b_3 = 3$, $b_4 = 5, \dots$.

(b) The numbers in (a) are all Fibonacci numbers. We conjecture that $b_{n+2} = b_{n+1} + b_n$ for all $n \in \mathbb{N}_0$. This follows easily from the Fundamental Recurrence:

$$\begin{aligned} b_{n+1} + b_n &= \binom{n+1}{0} + \left(\binom{n}{1} + \binom{n}{0}\right) + \left(\binom{n-1}{2} + \binom{n-1}{1}\right) + \cdots \\ &= 1 + \binom{n+1}{1} + \binom{n}{2} + \cdots \\ &= b_{n+2}. \end{aligned}$$

Hence the b_n are the Fibonacci numbers, defined starting at 1.

2.7 (a) By the Binomial Theorem $(10+1)^4 = 10^4 + \binom{4}{1}10^3 + \binom{4}{2}10^2 + \binom{4}{3}10 + \binom{4}{4} = 10000 + 4000 + 600 + 40 + 1 = 14641$. The digits $\binom{4}{0}, \binom{4}{1}, \dots, \binom{4}{4}$ are the entries in row 4 of Pascal's Triangle. (The pattern breaks down for $(10+1)^5$ because $\binom{5}{2} = \binom{5}{3} = 10$ creates a carry when we add in base 10.)

(b) Putting $n = 2m$ in Claim 2.1.9 gives $(2m-k)\binom{2m}{k} = (k+1)\binom{2m}{k+1}$. Hence $\binom{2m}{k} < \binom{2m}{k+1}$ if and only if $2m-k > k+1$, which holds if and only if $k < m$. Therefore

$$\binom{2m}{0} < \ldots < \binom{2m}{m-1} < \binom{2m}{m}.$$

The remaining inequalities $\binom{2m}{m} > \binom{2m}{m+1} > \ldots > \binom{2m}{2m}$ follow from $\binom{2m}{k} = \binom{2m}{2m-k}$. The proof for $2m+1$ is similar.

(c) Consider

$$2^{2m} = (1+1)^{2m} = \sum_{k=0}^{2m} \binom{2m}{k}.$$

There are $2m+1$ summands, of which the largest is $\binom{2m}{m}$ by (b). Hence $2^{2m} \geq \binom{2m}{m}$ and, since the largest summand is at least the mean summand,

$$\frac{2^{2m}}{2m+1} \leq \binom{2m}{m}.$$

2.8 By Lemma 2.1.5 we have $\binom{m}{k} = \binom{m}{m-k}$ for $k \in \{0,1,\ldots,m\}$. Hence

$$\sum_k \binom{m}{k}^2 = \sum_{k=0}^{m} \binom{m}{k}\binom{m}{k} = \sum_{k=0}^{n} \binom{m}{k}\binom{m}{n-k} = \binom{2m}{m}$$

where the final equality uses Vandermonde's Convolution (Lemma 2.2.6).

2.9 Since $\binom{n}{r}\binom{r}{k} = 0$ if $r < k$ or $r > n$, we have $\sum_r \binom{n}{r}\binom{r}{k}x^r = \sum_{r=k}^n \binom{n}{r}\binom{r}{k}x^r$. Now use Lemma 2.2.4, that $\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$ whenever $k \leq r \leq n$, to get

$$\begin{aligned}\sum_r \binom{n}{r}\binom{r}{k}x^r &= \sum_{r=k}^{n} \binom{n}{k}\binom{n-k}{r-k}x^r = \binom{n}{k}\sum_{r=k}^{n}\binom{n-k}{r-k}x^r \\ &= \binom{n}{k}x^k\sum_{r=k}^{n}\binom{n-k}{r-k}x^{r-k} = \binom{n}{k}x^k\sum_{m=0}^{n-k}\binom{n-k}{m}x^m = \binom{n}{k}x^k(1+x)^{n-k}\end{aligned}$$

where the final step uses the Binomial Theorem. Substituting $x = 1$ we get $\sum_r \binom{n}{r}\binom{r}{k} = \binom{n}{k}2^{n-k}$ and substituting $x = -1$ we get $\sum_r (-1)^r\binom{n}{r}\binom{r}{k} = 0$, provided $n > k$.

2.10 Again we use Lemma 2.2.4 to replace $\binom{n}{r}\binom{r}{k}$ with $\binom{n}{k}\binom{n-k}{r-k}$. This gives

$$\begin{aligned}\sum_r \binom{r}{k}\binom{m}{r}\binom{n}{r} &= \sum_{r=k}^{n}\binom{m}{r}\binom{n}{k}\binom{n-k}{r-k} = \binom{n}{k}\sum_{r=k}^{n}\binom{m}{r}\binom{n-k}{r-k} \\ &= \binom{n}{k}\sum_{r=k}^{n}\binom{m}{r}\binom{n-k}{n-r} = \binom{n}{k}\binom{m+n-k}{n}\end{aligned}$$

where the final step uses Vandermonde's convolution (Lemma 2.2.6).

2.11 (a) We work by induction on m. If $m = 0$ then the left-hand side is $\frac{n}{2}\binom{n}{0} = \frac{n}{2}$ and the right-hand side is $\frac{1}{2}\binom{n}{1}$, so they agree. We now suppose, by induction, that $\sum_{k=0}^{m-1}\left(\frac{n}{2}-k\right)\binom{n}{k} = \frac{m}{2}\binom{n}{m}$. Hence

$$\sum_{k=0}^{m}\left(\frac{n}{2}-k\right)\binom{n}{k} = \frac{m}{2}\binom{n}{m} + \left(\frac{n}{2}-m\right)\binom{n}{m} = \frac{n-m}{2}\binom{n}{m} = \frac{m+1}{2}\binom{n}{m+1}$$

where the final step uses Claim 2.1.9.

(b) Stop at the penultimate equality above and double each side.

(c) ($\star$) Observe that the summands for k and $n-k$ in (b) are equal in magnitude but have opposite signs. So it is sufficient to prove that

$$\sum_{k=0}^{m}(n-2k)\binom{n}{k} = (n-m)\binom{n}{m} \qquad (\dagger)$$

when $m < n/2$. For this we use the team-and-leader combinatorial interpretation. Take n people, all of different ages. Given a team X of $r \leq n/2$ of these people, say that Person x is *paired* with Person $x^\star$ if Person x is the jth youngest person in the team and Person $x^\star$ is the jth youngest person not in the team. Say Person y is a *suitable leader* for X if she is not in the team and is not paired with any team member. The left-hand side of (†) counts the number of teams-and-suitable-leaders where the team has size at most m.

The right-hand side of (†) counts the number of teams-and-leaders where the team has size m. (The leader is not in the team, but need not be suitable.) Given such a team X and a leader, either the leader is suitable, and we stop, or the leader is paired with a unique team-member, say Person x. Sack the leader, and promote Person x. If Person x is a suitable leader for the new team of size $m-1$, then stop. Otherwise repeat this process. Since any leader is suitable for the empty team, the process eventually stops with a team and suitable leader.

We illustrate the inverse by example. Take $n = 6$ and $m = 3$ and number the people 1, 2, 3, 4, 5, 6 in increasing seniority. Then Person 4 is a suitable leader for the team with members Persons 1 and 5. This team must have been obtained by sacking an unsuitable leader of a team with Persons 1, 4 and 5 and promoting Person 4. This unsuitable leader was paired with Person 4. Since 4 is in the middle of $\{1,4,5\}$ and 3 is in the middle of $\{2,3,6\}$, this leader was Person 3.

2.12 (a) Since $X \triangle Y = Y \triangle X$ and $X \cap Y = Y \cap X$ for all subsets X and Y, addition and multiplication are commutative. The zero element is $\varnothing$, since $\varnothing \triangle X = X$ for all subsets X and the one element is Ω since $\Omega \cap X = X$ for all subsets X. Since $(X \triangle Y) \triangle Z$ and $X \triangle (Y \triangle Z)$ are both equal to

$$\{w \in \Omega : w \text{ is in exactly one or exactly three of } X, Y, Z,\}$$

the addition is associative. Clearly the multiplication is associative. The distributivity law holds because

$$\begin{aligned}(X \triangle Y) \cap Z &= \big((X \cup Y)\backslash(X \cap Y)\big) \cap Z\\ &= \big((X \cup Y) \cap Z\big)\backslash\big(X \cap Y \cap Z\big)\\ &= \big((X \cap Z) \cup (Y \cap Z)\big)\backslash\big((X \cap Z) \cap (Y \cap Z)\big)\\ &= (X \cap Z) \triangle (Y \cap Z).\end{aligned}$$

(b) We have $X \triangle X = X\backslash X = \varnothing$ for all $X \in S$.

(c) Take the symmetric difference of both sides of $X \triangle Y = Z$ with Z. This gives $X \triangle Y \triangle Z = Z \triangle Z = \varnothing$. (One can think of this as adding Z to both sides.) By symmetry we have

$$X \triangle Y = Z \iff Y \triangle Z = X \iff Z \triangle X = Y \iff X \triangle Y \triangle Z = \varnothing.$$

(d) Similarly, by adding $Y \triangle Z$ to both sides, we get

$$X \triangle Y = Z \triangle W \iff X \triangle Y \triangle Y \triangle Z = Z \triangle W \triangle Y \triangle Z \iff X \triangle Z = W \triangle Y.$$

Since $(X \triangle Y) \cap (Z \triangle W) = (X \cap Z) \triangle (Y \cap W) \triangle (X \cap W) \triangle (Y \cap Z)$ by the distributivity of multiplication over addition, the left-hand side equals $(X \cap Z) \triangle (Y \cap W)$ if and only if $(X \cap W) \triangle (Y \cap Z) = \varnothing$. This is the case if and only if $X \cap W = Y \cap Z$.

2.13 (a) The next six sets in the colexicographic order on 3-subsets of $\mathbb{N}$ are $\{2,3,5\}, \{1,4,5\}, \{2,4,5\}, \{3,4,5\}, \{1,2,6\}$, $\{1,3,6\}$.

(b) There are $\binom{r}{k}$ subsets of $\{1,2,\ldots,r\}$; of these $\{r-k+1,\ldots,n\}$ is the greatest under the colexicographic order. Any k-subset of $\mathbb{N}$ containing an element strictly greater than r is bigger than $\{r-k+1,\ldots,r\}$ in the colexicographic order. Hence $\{r-k+1,\ldots,r\}$ is the $\binom{r}{k}$th element of the colexicographic order on k-subsets of $\mathbb{N}$.

(c) Since $\binom{14}{5} = 2002$, the 2002nd element of the colexicographic order on 5-subsets of $\mathbb{N}$ is $\{10,11,12,13,14\}$. The 2003rd element is $\{1,2,3,4,15\}$, and it is now routine to step forward to get the element in position 2016. Or, to indicate a more general approach, we argue that the 2016th set is $\{x_1,x_2,x_3,x_4,15\}$ where $\{x_1,x_2,x_3,x_4\}$ lies in position $2016-2002 = 14$ of the colexicographic order on 4-subsets of $\mathbb{N}$. Since $\binom{5}{4} = 5$, whereas $\binom{6}{4} = 15$, we take the set immediately before $\{3,4,5,6,15\}$, namely $\{2,4,5,6,15\}$.

(d) Using the method from (c) we note that $\binom{28}{10} \geq 10^7$ whereas $\binom{27}{10} < 10^7$, so the maximum element in the required 10-subset is 28. We then need the set in position $10^7 - \binom{27}{10} = 1563715$ of the colexicographic order on 9-subsets; since $\binom{25}{9} \geq$

1563715 whereas $\binom{24}{9} < 1563715$, this set has maximum element 25, and we now need the set in position $10^7 - \binom{27}{10} - \binom{24}{9} = 256211$ of the colexicographic order on 8-subsets. Continuing in this way we arrive at $\{?,5,7,10,12,14,20,22,25,28\}$, corresponding to

$$10^7 = \binom{27}{10} + \binom{24}{9} + \binom{21}{8} + \binom{19}{7} + \binom{13}{6} + \binom{11}{5} + \binom{9}{4} + \binom{6}{3} + \binom{4}{2} + 3.$$

The least entry, marked ? above, is therefore $3 = \binom{3}{1}$.

(e) By (b), the set in position $\binom{r}{m}$ in the colexicographic order on m-subsets of $\{1,2,\ldots,r\}$ is $\{r-m+1,\ldots,r\}$. Specifying this set by the 'coding' in (d), we get

$$\binom{r-1}{m} + \cdots + \binom{r-m+1}{2} + \binom{r-m+1}{1} = \binom{r}{m}.$$

(The argument, as in (d), starts 'since $\binom{r-1}{m} < \binom{r}{m}$ whereas $\binom{r}{m} \geq \binom{r}{m}$, the maximum element is r, ...'.) Now rewrite $\binom{r-m+1}{1} = \binom{r-m}{1} + \binom{r-m}{0}$.

2.14 Let $S(r,k)$ be the set of strings of 0s and 1s with exactly r 1s and k 0s. There are $\binom{r+k}{k}$ ways to choose k positions in a string of length $r+k$ to be zero, so $|S(r,k)| = \binom{r+k}{k}$. The left-hand side of Claim 2.4.4 therefore counts the number of pairs (s,t) where $s \in S(c,k)$ and $t \in S(d,m-k)$, for some $k \in \{0,1,\ldots,m\}$. Given such a pair, we can form a new string $s1t \in S(c+d+1,m)$ by inserting 1 between s and t. Conversely, given a string in $S(c+d+1,m)$, split it at the $(c+1)$th 1, and discard this 1. This gives a left string in $S(c,k)$ and a right string in $S(d,m-k)$, where k is the number of 0s in the left string. Hence,

$$\sum_{k=0}^{m} |S(c,k)||S(d,m-k)| = |S(c+d+1,m)|.$$

Claim 2.4.4 is an immediately corollary.

Remark: another bijective proof, related to the one given here by the bijective proof of Theorem 2.3.3, interprets $\binom{c+k}{k}$ as the number of ways to place k indistinguishable balls in $c+1$ numbered urns. and $\binom{d+m-k}{m-k}$ as the number of ways to place $m-k$ indistinguishable balls in a further $d+1$ numbered urns.

2.15 (a) Let $(X,Y) \in P$. If $X = Y$ then, by definition, $f(X,Y) = (X,Y)$. Otherwise, let $z = \max(X \triangle Y)$ and let $f(X,Y) = (X',Y')$. If $z \in X$ then the sets X', Y' are defined by moving z from X to Y, so $z = \max(X' \triangle Y')$, $z \in Y'$ and $f(X',Y')$ is defined by moving z from Y' to X'. Therefore $f(X',Y') = (X,Y)$. The proof is similar if $z \in Y$. Hence f is an involution. Since $|X'| = |X| \pm 1$, we have $\operatorname{sgn}(X',Y') = (-1)^{|X'|} = -(-1)^{|X|} = -\operatorname{sgn}(X,Y)$.

Rewriting $\binom{n}{k}^2$ as $\binom{n}{k}\binom{n}{n-k}$, we see that

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}^2 = \sum_{(X,Y)\in P}\operatorname{sgn}(X,Y).$$

Split up the right-hand side as

$$\sum_{\substack{(X,Y)\in P\\ f((X,Y))=(X,Y)}}\operatorname{sgn}(X,Y)+\sum_{\substack{(X,Y)\in P\\ f((X,Y))\neq(X,Y)}}\operatorname{sgn}(X,Y).$$

Let $Q=\{(X,Y): f\big((X,Y)\big)=(X,Y)\}$ be the set of summands in the first sum. Note that f restricts to the identity map on Q and to a sign-reversing involution on $P\backslash Q$. Evaluating the second sum by applying f we get

$$\sum_{(X,Y)\in P\backslash Q}\operatorname{sgn}(X,Y)=\sum_{f(X,Y)\in P\backslash Q}\operatorname{sgn}(X,Y)=\sum_{(X,Y)\in P\backslash Q}\operatorname{sgn} f(X,Y)=\sum_{(X,Y)\in P\backslash Q}-\operatorname{sgn}(X,Y).$$

Hence the second sum is zero and

$$\sum_{(X,Y)\in P}\operatorname{sgn}(X,Y)=\sum_{(X,Y)\in Q}\operatorname{sgn}(X,Y). \qquad (\star\star)$$

(This is the key identity for the involutive method.)

We have $f(X,Y)=(X,Y)$ if and only if $X=Y$. In particular, this implies that $|X|=|Y|=n/2$. Hence if n is odd then $Q=\varnothing$ and the right-hand side of $(\star\star)$ is zero. If n is even then $Q=\{(Z,Z)\in P:|Z|=n/2\}$ and the right-hand side of $(\star\star)$ is $(-1)^{n/2}\binom{n}{n/2}$, as required.

(b) *Hint: interpret* $\binom{n}{k-1}$ *as* $\binom{n}{n-(k-1)}$ *and define an involution on the pairs* (X,Y) *of subsets of* $\{1,2,\ldots,n\}$ *such that* $|X|+|Y|=n+1$.

2.16 (a) We work by induction on d. If $d=0$ then $h(x)=a_0$ and, by hypothesis, $h(c_1)=0$. Hence $a_0=0$ and $h=0$. Let $d\in\mathbb{N}$. By the Factor Theorem, there is a polynomial $k(z)=b_0+b_1z+\cdots+b_{d-1}z^{d-1}$ such that

$$h(z)=(z-c_{d+1})k(z).$$

Note that $0=h(c_i)=(c_i-c_{d+1})k(c_i)$ for each $i\in\{1,\ldots,d\}$. Since $c_1,\ldots,c_d,c_{d+1}$ are distinct, it follows that $k(c_i)=0$ for each $i\in\{1,\ldots,d\}$. By induction $k=0$ and hence $h=0$.

(b) Apply (a) to $f-g$.

2.17 Let P be the set of functions $f:\{1,2,\ldots,n\}\to\{1,2,\ldots,b+1\}$. For each $x\in\{1,2,\ldots,n\}$ we have $b+1$ choices for $f(x)$, so $|P|=(b+1)^n$. Let P_k be the subset of P containing those functions f such that

$$\big|\{x\in\{1,2,\ldots,n\}: f(x)\in\{1,2,\ldots,b\}\}\big|=k.$$

To specify $f \in P_k$ we can choose k elements $x \in \{1,2,\ldots,n\}$ such that $f(x) \neq b+1$ in $\binom{n}{k}$ ways; then for each such x, we have b choices for $f(x)$. Multiplying choices we get $|P_k| = \binom{n}{k}b^k$. Summing over k we get $(b+1)^n = \sum_k \binom{n}{k}b^k$, as required.

Let $f(z) = (z+1)^n$ and let $g(z) = \sum_k \binom{n}{k}z^k$. We have shown that $f(b) = g(b)$ for all $b \in \mathbb{N}_0$. By Exercise 2.16, we have $f = g$. Hence

$$(z+1)^n = \sum_k \binom{n}{k} z^k$$

for all $z \in \mathbb{C}$. To get the form in Theorem 2.1.8, replace z with z/w and multiply through by w^n. (A separate argument is required if $w = 0$.)

2.18 Let $n \in \mathbb{N}_0$. By Exercise 2.1 we have $r\binom{n+1}{r} = (n+1)\binom{n}{r-1}$ for each $r \in \mathbb{N}$. Hence

$$\sum_{r=1}^{m}(-1)^r\binom{n+1}{r}r = (n+1)\sum_{r=1}^{m}(-1)^r\binom{n}{r-1} = (-1)^m(n+1)\binom{n-1}{m-1}$$

where the final equality uses Lemma 2.2.2. The required identity therefore holds for all $z \in \mathbb{N}_0$. Since each side is a polynomial in z, it holds for all $z \in \mathbb{C}$.

2.19 (a) Starting with the right-hand side we have $6\binom{x}{3} - 2\binom{x}{1} + \binom{x}{0} = \frac{6x(x-1)(x-2)}{6} - 2x+1 = x(x-1)(x-2) - 2x + 1 = x^3 - 3x^2 + 1$. The coefficients of $\binom{x}{d}$ for $0 \leq d \leq 3$ are $1, -2, 0, 6$; these are the numbers appearing on the diagonal of the table.

(b) Using 0, 1, 0, -1, 0 as the top row of a table gives

$$\begin{array}{ccccccccc}
0 & & 1 & & 0 & & -1 & & 0 \\
 & 1 & & -1 & & -1 & & 1 & \\
 & & -2 & & 0 & & 2 & & \\
 & & & 2 & & 2 & & & \\
 & & & & 0 & & & &
\end{array}$$

Motivated by (a), we take

$$g(x) = 2\binom{x}{3} - 2\binom{x}{2} + \binom{x}{1} = \frac{x^3}{3} - 2x^2 + \frac{8x}{3} = \frac{1}{3}x(x-2)(x-4).$$

Clearly g has roots at 0, 2 and 4 and $g(1) = 1$, $g(3) = -1$, as required.

2.20 (a) You should find $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $a_4 = 8$.

(b) Since $a_5 = 16$, just looking at the values computed so far, it is very tempting to conjecture that $a_n = 2^{n-1}$.

(c) Clearly $a_0 = 1$; this is not consistent with the conjecture in (b). It is surprisingly rare in combinatorial problems for the 'empty' case to be truly exceptional, so already this casts doubt on the conjecture. If you draw a sufficiently generic diagram for $n = 6$ and carefully count the regions you should find that $a_6 = 31$.

(d) The table below is constructed as in Exercise 2.19:

$$\begin{array}{ccccccccccccc}
1 & & 1 & & 2 & & 4 & & 8 & & 16 & & 31 \\
 & 0 & & 1 & & 2 & & 4 & & 8 & & 15 & \\
 & & 1 & & 1 & & 2 & & 4 & & 7 & & \\
 & & & 0 & & 1 & & 2 & & 3 & & & \\
 & & & & 1 & & 1 & & 1 & & & & \\
 & & & & & 0 & & 0 & & & & &
\end{array}$$

We therefore conjecture (surely no more rashly than before) that $a_n = \binom{n}{4} + \binom{n}{2} + 1$ for all $n \in \mathbb{N}_0$.

2.21 (a) If $n = 0$ then $\Delta^n \binom{z}{r} = \binom{z}{r}$. Suppose inductively that $\Delta^{n-1}\binom{z}{r} = \binom{z}{r-(n-1)}$. Then

$$\Delta^n \binom{z}{r} = \Delta\bigl(\Delta^{n-1}\binom{z}{r}\bigr) = \Delta\binom{z}{r-n+1} = \binom{z+1}{r-n+1} - \binom{z}{r-n+1} = \binom{z}{r-n}$$

where the final equality follows from the general form of the Fundamental Recurrence (Lemma 2.1.7).

(b) We have $b(z) = \binom{z}{r}$. By (a), if $n < r$ then $(\Delta^n b)(0) = \binom{0}{r-n} = 0$. When $n = r$ we have $(\Delta^n b)(z) = \binom{z}{0} = 1$. So $(\Delta^n b)(0) = 1$, and since $\Delta^r b$ is a constant polynomial $\Delta^n b = 0$ for all $n > r$.

(c) Suppose that $\sum_{r=0}^{d} c_r \binom{z}{r} = 0$ where $c_r \in \mathbb{C}$ for each r, and $c_d \neq 0$. Since $\binom{z}{r}$ has degree r, the left-hand side has degree d, a contradiction. Therefore Therefore the binomial coefficients $\binom{z}{r}$ for $r \in \mathbb{N}_0$ are linearly independent and the subspace of $\mathbb{C}[z]$ spanned by $\binom{z}{0}, \ldots, \binom{z}{d}$ has dimension $d+1$. It is contained in the $(d+1)$-dimensional subspace of polynomials of degree at most d. Hence these subspaces are equal, and so the binomial coefficients $\binom{z}{r}$ for $r \in \mathbb{N}_0$ span $\mathbb{C}[z]$.

(d) By (c), there exist unique coefficients $c_r \in \mathbb{C}$ such that $f(z) = \sum_{r=0}^{d} c_r \binom{z}{r}$. Let $n \in \mathbb{N}_0$. By (b), $(\Delta^n f)(0) = \sum_{r=0}^{d} c_r (\Delta^n \binom{z}{r})(0) = c_n$. Hence $f(z) = \sum_{r=0}^{d} (\Delta^r f)(0)\binom{z}{r}$, as claimed. A table of differences, as in Exercise 2.19, has $f(0)$, $f(1)$, $\ldots$ in its first row, and $(\Delta f)(0) = f(1) - f(0)$, $(\Delta f)(1) = f(2) - f(1)$, $\ldots$ in its second row. A routine induction shows that, more generally, the entries in row n are $(\Delta^n f)(0)$, $(\Delta^n f)(1)$, $\ldots$. In particular, the nth entry on the diagonal is $(\Delta^n f)(0) = c_n$, as required.

(e) When $n = 0$ we have $(\Delta^0 f)(z) = f(z)$, which agrees with the right-hand side.

Suppose inductively that $(\Delta^n f)(z) = \sum_{k=0}^{n}(-1)^k\binom{n}{k}f(z+n-k)$. Then

$$\begin{aligned}
&(\Delta^{n+1}f)(z)\\
&\quad = \Delta\big(\Delta^n f\big)(z)\\
&\quad = \sum_{k=0}^{n}(-1)^k\binom{n}{k}f(z+1+n-k) - \sum_{k=0}^{n}(-1)^k\binom{n}{k}f(z+n-k)\\
&\quad = \sum_{k=0}^{n}(-1)^k\binom{n}{k}f(z+n+1-k) - \sum_{j=1}^{n+1}(-1)^{j-1}\binom{n}{j-1}f(z+n-(j-1))\\
&\quad = \sum_{k=0}^{n+1}(-1)^k\left(\binom{n}{k}+\binom{n}{k-1}\right)f(z+n+1-k)\\
&\quad = \sum_{k=0}^{n+1}(-1)^k\binom{n+1}{k}f(z+n+1+k)
\end{aligned}$$

where again the final step uses the Fundamental Recurrence. This gives the inductive step.

2.22 Considered as polynomials in z, both sides have degree $2m$. If $z=m$ then $\binom{z}{k}\binom{z}{2m-k}$ is non-zero only when $k=m$, and so both sides equal $(-1)^m\binom{2m}{m}$. If $z\in\{0,1,\dots,m-1\}$ then both sides are zero. If $z=-r$ where $r\in\{1,\dots,m\}$ then, using Lemma 2.4.1 and Lemma 2.1.5, the left-hand side is

$$\sum_{k=0}^{2m}(-1)^k\binom{2m}{k}g(k)$$

where $g(y)=\binom{r+y-1}{r-1}\binom{r+2m-y-1}{r-1}$. Since g is a polynomial of degree $2(r-1)<2m$ in y, we have $\Delta^{2m}g=0$ by Exercise 2.21. So both sides are again zero. This shows that the two sides agree at $2m+1$ values of z, and so, by the key principle, they are equal as polynomials in z.

3. Principle of Inclusion and Exclusion

Exercise 3.1.4 Taking $n=3$ in the Principle of Inclusion and Exclusion (Theorem 3.1.3) we get $|\overline{A_1\cup A_2\cup A_3}| = \sum_{I\subseteq\{1,2,3\}}(-1)^{|I|}|A_I|$. The eight summands, indexed by the subsets of $\{1,2,3\}$, are the sizes of the sets $A_\varnothing=\Omega$, $A_{\{1\}}=A_1$, $A_{\{2\}}=A_2$, $A_{\{3\}}=A_3$, $A_{\{1,2\}}=A_1\cap A_2$, $A_{\{1,3\}}=A_1\cap A_3$, $A_{\{2,3\}}=A_2\cap A_3$ and $A_{\{1,2,3\}}=A_1\cap A_2\cap A_3$. Thus written out, the formula is

$$\begin{aligned}
|\overline{A_1\cup A_2\cup A_3}| = |\Omega| - |A_1| - |A_2| - |A_3| + |A_1\cap A_2|&\\
+ |A_1\cap A_3| + |A_2\cap A_3| - |A_1\cap A_2\cap A_3|&.
\end{aligned}$$

This agrees with Example 3.1.1 if we change the labels of the sets from A_1, A_2, A_3 to A, B, C.

Exercise 3.1.5 Since $|\overline{X}| = |\Omega| - |X|$ for any subset X of Ω, we have $|A_1 \cup A_2 \cup \ldots \cup A_n| = |\Omega| - |\overline{A_1 \cup A_2 \cup \ldots \cup A_n}|$. Using the Principle of Inclusion and Exclusion we get

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |\Omega| - \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} |A_I|.$$

By the convention that $A_\varnothing = \Omega$, the summand for $I = \varnothing$ is $|\Omega|$; this cancels with the first term. We are left with

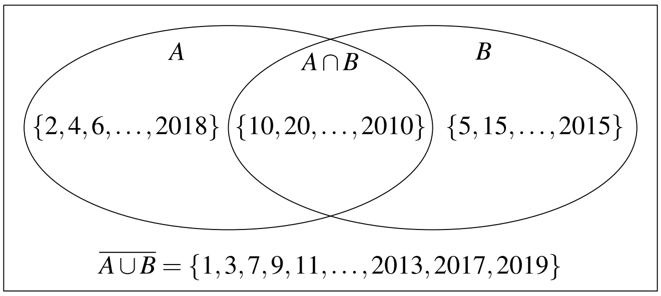
$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{\substack{I \subseteq \{1,2,\ldots,n\} \\ I \neq \varnothing}} (-1)^{|A_I|-1} |A_I|.$$

End of chapter exercises

3.1 We have $A = \{2,4,6,\ldots,2018\}$ and $B = \{5,10,15,\ldots,2015\}$. Hence $|A| = 2018/2 = 1009$ and $|B| = 2015/5 = 403$. Clearly $x \in A \cap B$ if and only if $x \in \Omega$ and x is divisible by 10. Hence $A \cap B = \{10,20,\ldots,2010\}$ and $|A \cap B| = 201$. It follows from Example 3.1.1 that

$$|\overline{A \cup B}| = |\Omega| - |A| - |B| + |A \cap B| = 2019 - 1014 - 403 + 201 = 808.$$

The elements of $\overline{A \cup B}$ are precisely those $x \in \mathbb{N}$ such that $x \leq 2019$ and x is an odd number not divisible by 5, as shown in the Venn diagram below.



3.2 Let $\Omega = \{1,2,\ldots,100\}$ and let $D(m) = \{x \in \{1,\ldots,100\} : x \text{ is divisible by } m\}$ as in §3.4. By adapting Example 3.4.1, we find $|\overline{D(2) \cup D(3) \cup D(5) \cup D(7)}|$. By the

Principle of Inclusion and Exclusion and Lemma 3.4.2, we have

$$\begin{aligned}|\overline{D(2)\cup D(3)\cup D(5)\cup D(7)}| &= \sum_{P\subseteq\{2,3,5,7\}} (-1)^{|P|}\Big|\bigcap_{p\in P} D(p)\Big| \\ &= \sum_{P\subseteq\{2,3,5,7\}} (-1)^{|P|}\Big|D(\prod_{p\in P} p)\Big| \\ &= \sum_{P\subseteq\{2,3,5,7\}} (-1)^{|P|}\left\lfloor \frac{100}{\prod_{p\in P} p}\right\rfloor .\end{aligned}$$

Calculating the 16 summands we get $|\overline{D(2)\cup D(3)\cup D(5)\cup D(7)}| = 100-50-33-20-14+16+10+7+6+4+2-3-2-1-0+0 = 22$. The two zero summands come from $D(3\times 5\times 7) = D(105) = \varnothing$ and $D(2\times 3\times 5\times 7) = D(210) = \varnothing$.

If $x\in\Omega$ and x is composite then x is divisible by either 2, 3, 5 or 7. (If not the smallest prime dividing x is 11, and since x is composite, $x \geq 11^2 > 100$, a contradiction.) Hence $x\in D(2)\cup D(3)\cup D(5)\cup D(7)$. Remembering that 1 is not composite, we get

$$\overline{D(2)\cup D(3)\cup D(5)\cup D(7)} = \{1\}\cup\{p\in\Omega : p\geq 11 \text{ and } p \text{ is prime}\}$$

and so the number of primes in $\{1,2,\dots,100\}$ is $22-1+4=25$.

3.3 As usual, for $\Omega\subseteq\mathbb{N}$, let $D(m) = \{x\in\Omega : x \text{ is divisible by } m\}$. For (a) we take $\Omega = \{1,2,\dots,pq\}$. If $x\in\Omega$ then

$$\begin{aligned} x \text{ is coprime to } pq &\iff x \text{ is not divisible by } p \text{ and } x \text{ is not divisible by } q \\ &\iff x\in\overline{D(p)\cup D(q)}.\end{aligned}$$

Hence $\phi(pq) = \overline{D(p)\cup D(q)}$ and so using the Principle of Inclusion and Exclusion we get

$$\begin{aligned}\phi(pq) &= |\Omega| - |D(p)| - |D(q)| + |D(p)\cap D(q)| \\ &= |\Omega| - |D(p)| - |D(q)| + |D(pq)| \\ &= pq - \frac{pq}{p} - \frac{pq}{q} + \frac{pq}{pq} \\ &= pq\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{q}\Big).\end{aligned}$$

In (b) we take $\Omega = \{1,2,\dots,p^2q\}$ and argue similarly that

$$\begin{aligned} x \text{ is coprime to } p^2q &\iff x \text{ is not divisible by } p \text{ and } x \text{ is not divisible by } q \\ &\iff x\in\overline{D(p)\cup D(q)}.\end{aligned}$$

The conclusion is the same as (a), but now $D(p)$ and $D(q)$ are defined using

$\{1,2,\dots,p^2q\}$. (Note that it is correct to work with $D(p)$ rather than $D(p^2)$, since we have to rule out divisibility by p, not p^2.) The same calculation as (a) now gives

$$\phi(pq^2) = pq^2 - \frac{pq^2}{p} - \frac{pq^2}{q} + \frac{pq^2}{pq} = pq^2\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{q}\Big).$$

The three prime case in (c) is similar to (a): you should find that

$$\phi(pqr) = pqr\Big(1-\frac{1}{p}\Big)\Big(1-\frac{1}{q}\Big)\Big(1-\frac{1}{r}\Big).$$

3.4 (a) This is similar to the second example in §3.3, replacing the ranks Ace, King, Queen and Jack with the suits spades $\spadesuit$, hearts $\heartsuit$, diamonds $\diamondsuit$ and clubs $\clubsuit$. As before, let Ω be all $\binom{52}{5}$ hands of five cards. Let $C_\spadesuit$ be the hands *we do not want to count* because they have no spades, and define $C_\heartsuit$, $C_\diamondsuit$ and $C_\clubsuit$ similarly. For example, $|C_\spadesuit| = \binom{52}{39}$ since there are 39 non-spades in the deck. By the Principle of Inclusion and Exclusion, the number of five card hands with at least one card of each suit is

$$\begin{aligned}
&|\overline{C_\spadesuit \cap C_\heartsuit \cap C_\diamondsuit \cap C_\clubsuit}| \\
&\quad = |\Omega| - |C_\spadesuit| - |C_\heartsuit| - |C_\diamondsuit| - |C_\clubsuit| + |C_\spadesuit \cap C_\heartsuit| + \cdots + |C_\diamondsuit \cap C_\clubsuit| \\
&\qquad - |C_\spadesuit \cap C_\heartsuit \cap C_\diamondsuit| - \cdots - |C_\heartsuit \cap C_\diamondsuit \cap C_\clubsuit| + |C_\spadesuit \cap C_\heartsuit \cap C_\diamondsuit \cap C_\clubsuit| \\
&\quad = \binom{52}{5} - 4\binom{39}{5} + 6\binom{26}{5} - 4\binom{13}{5} + \binom{0}{5} \\
&\quad = 682604.
\end{aligned}$$

(This is a bit over $\frac{1}{4}$ of all hands.)

For (b) we use the sets above and also C_A, C_K, C_Q, C_J from §3.3. As an example, consider $C_\mathrm{A} \cap C_\spadesuit \cap C_\heartsuit$. Its elements are the five card hands built from a reduced deck having no aces, spades or hearts. Using the Principle of Inclusion and Exclusion in the case $n = 2$, there are $52 - 4 - 26 + 2$ cards in the reduced deck. (The final $+2$ accounts for the aces of spades and hearts.) Therefore $|C_\mathrm{A} \cap C_\spadesuit \cap C_\heartsuit| = \binom{24}{5}$. More generally, a set A_I defined by taking r of the rank sets $C_\mathrm{A}, C_\mathrm{K}, C_\mathrm{Q}, C_\mathrm{J}$ and s of the suit sets $C_\spadesuit, C_\heartsuit, C_\diamondsuit, C_\clubsuit$ has size $\binom{52-13r-4s+rs}{5}$. Hence there are

$$\sum_{r=0}^{4}\sum_{s=0}^{4}(-1)^{r+s}\binom{4}{r}\binom{4}{s}\binom{52-13r-4s+rs}{5} = 2592$$

five card hands having at least one card of each suit and at least one Ace, King, Queen and Jack. (The sum has 25 terms, so is most easily evaluated using computer algebra.)

3.5 (a) A function $f : \{1,2,\dots,m\} \to \{1,2,\dots,n\}$ is uniquely determined by its values $f(1), f(2),\dots, f(m) \in \{1,2,\dots,n\}$. There are n possible choices for each $f(t)$. Hence, multiplying independent choices, we find that $|\Omega| = n^m$. For A_i we may not choose $f(t) = i$ so there are now $n-1$ choices and $|A_i| = (n-1)^m$.

(b) We have

$$A_I = \big\{ f \in \Omega : f(t) \notin I \text{ for any } t \in \{1,2\dots,m\} \big\}.$$

Generalizing the argument in (a), there are $n-|I|$ possible choices for each $f(t)$ so $|A_I| = (n-|I|)^m$.

(c) A function $f \in \Omega$ is surjective if and only if $f \notin A_1, f \notin A_2, \dots, f \notin A_n$. Equivalently, $f \in \overline{A_1 \cup A_2 \cup \cdots \cup A_n}$. By the Principle of Inclusion and Exclusion and (b) we get

$$\begin{aligned} |\overline{A_1 \cup A_2 \cup \cdots \cup A_n}| &= \sum_{I \subseteq \{1,2,\dots,n\}} (-1)^{|I|} |A_I| \\ &= \sum_{I \subseteq \{1,2,\dots,n\}} (-1)^{|I|} (n-|I|)^m \\ &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m \end{aligned}$$

as required.

(d) Given a placement of m numbered balls into n numbered urns, define $f \in \Omega$ by

$$f(t) = u \iff \text{ball number } t \text{ is put in urn number } u.$$

Conversely, each $f \in \Omega$ defines a corresponding ball-and-urn placement. The placements where every urn contains a ball are precisely those corresponding to surjective functions.

3.6 Let the factorizations of M and N into distinct primes be $M = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$ and $N = q_1^{f_1} q_2^{f_2} \dots q_r^{f_r}$. Since M and N are coprime, the p_i and q_j are distinct. Hence Proposition 3.4.4 implies that

$$\phi(MN) = \prod_{i=1}^{n} p_i^{e_i} \Big(1 - \frac{1}{p_i}\Big) \prod_{j=1}^{r} q_j^{f_j} \Big(1 - \frac{1}{q_j}\Big)$$

By another application of Proposition 3.4.4, this is $\phi(M)\phi(N)$. This multiplicativity property fails whenever M and N are not coprime. For example if p is prime then $\phi(p^2) = p^2(1-\frac{1}{p}) = p^2 - p$ whereas $\phi(p)^2 = (p-1)^2 = p^2 - 2p + 1$.

3.7 (a) The encryption of 7 is 7^9 mod 187, namely 129.

(b) Since $M = 187 = 11 \times 17$, we have $\phi(M) = (11-1)(17-1) = 160$. We must solve $9d \equiv 1$ mod 160. Using Euclid's Algorithm to express 1 as an integral linear combination of 9 and 160 we compute $160 = 17 \times 9 + 7$, $9 = 1 \times 7 + 2$ and $7 = 3 \times 2 + 1$, hence $1 = 7 - 3 \times 2 = 7 - 3 \times (9 - 1 \times 7) = 4 \times 7 - 3 \times 9 = 4 \times (160 - 17 \times 9) - 3 \times 9 = 4 \times 160 - 71 \times 9$. Since $-71 \equiv 89$ mod 160 we have $d = 89$.

(c) Using d, Alice decrypts 51 as 51^{89} mod 187, namely 85. (You can do this on a calculator by repeated squaring: write $89 = 2^6 + 2^4 + 2^3 + 1$ and compute 51^{2^3} by successively squaring 51 three times, reducing modulo 187 after each square, then square this to get 51^{2^4}, and so on.)

(d) Of course the primes are far too small. But even if p and q were of the size currently recommended by NCSC (National Cyber Security Centre, UK) and NIST (National Institute of Standards and Technology, USA) of about 2^{1024}, Eve the eavesdropper could use Alice's public key (n, a) to encrypt each of the possible messages to Alice, 0^a mod n, 1^a mod n, $\ldots$, 100^a mod n. If x^a mod n matches Bob's encrypted message, then Alice's exam mark is x. This attack is an inevitable feature of public key encryption, but can be avoided if Bob pads his message with sufficient unpredictable text. Another problem is that, since anyone can send a message to Alice using her public key, Alice has no way to be certain the message is from Bob. This problem is solved by asking Bob to 'sign' the encrypted message by *decrypting* it using *his* RSA private key. With these changes correctly implemented, the scheme is widely believed to be secure. (With some refinements, it is used whenever you pay for something online.)

3.8 We are given $M = pq$ and $\phi(M) = (p-1)(q-1) = pq - p - q + 1$. Let $s = M - \phi(M) + 1 = p + q$. Since $M = p(s-p) = q(s-q)$, the factors p and q are the roots of the quadratic equation $M = x(s-x)$, where the coefficients M and s are known.

3.9 (a) Since p is prime, and p does not divide x or y, p does not divide xy. (This is less obvious than it might sound, but follows from unique factorization.) If $xy \equiv r$ mod M then $xy = kpq + r$ for some $k \in \mathbb{N}_0$, and so p does not divide r. Similarly q does not divide r. Hence r is in U.

(b) Let $y, y' \in \{0, 1, \ldots, M-1\}$ and suppose that $f_x(y) = f_x(y')$. Then $xy \equiv xy'$ mod M, so $x(y - y') \equiv 0$ mod M. Hence p and q divide $x(y-y')$. But since $x \in U$ is coprime to p and q, pq must divide $y - y'$. Hence $y \equiv y'$ mod M, and so $y = y'$.

(c) By (a), each f_x restricts to a function from U to U. Since $1 \in U$ and an injective function on a finite set is surjective, there exists $x' \in U$ such that $f_x(x') = 1$. That is, $xx' \equiv 1 \bmod M$.

(d) By (a), U is closed under multiplication modulo M. The identity element is 1 and by (c) each element of U has an inverse. Multiplication is well known to be associative. Therefore U is a group. The order of U is $\phi(M)$, namely $(p-1)(q-1)$.

(e) Suppose that a is coprime to $\phi(M)$. There exists d such that $ad \equiv 1 \bmod \phi(M)$. Suppose that $ad = k\phi(M)+1$. By Lagrange's Theorem, $x^{\phi(M)} \equiv 1 \bmod M$ for all $x \in U$. Hence

$$(x^a)^d = x^{ad} = x^{k\phi(M)+1} = (x^{\phi(M)})^k x \equiv x \bmod M.$$

Similarly $(x^d)^a \equiv x \bmod M$. This shows that $x \mapsto x^d \bmod M$ is the inverse of $x \mapsto x^a \bmod M$. Given $\phi(M)$ we can compute d as in Exercise 3.7(b) using Euclid's Algorithm. No other method is known for computing d. In particular, by Exercise 3.7, computing $\phi(M)$ is equivalent to factoring M; when p and q are large (see the answer to Exercise 3.7(d) above), this is widely believed to be computationally infeasible.

3.10 (a) Using the Taylor series for the exponential function we have $\mathrm{e}^{cy} > c^2y^2/2$ for $y > 0$. Hence $y\mathrm{e}^{-cy} < 2/c^2y \to 0$ as $y \to \infty$.

(b) Using $\log\log M \le \log M$ and (a) with $y = \log M$, we get

$$\begin{aligned}\frac{\log M}{M}\log\log M &\le \frac{(\log M)^2}{M} = y^2\mathrm{e}^{-y} = (y\mathrm{e}^{-y/2})^2 \le (\tfrac{8}{y})^2 \to 0 \text{ as } y \to \infty,\\ \frac{M^{\log 2}}{M}\log\log M &\le \frac{\log M}{M^{1-\log 2}} = y\mathrm{e}^{-(1-\log 2)y} \le y\mathrm{e}^{-y/4} \le \tfrac{8}{y} \to 0 \text{ as } y \to \infty.\end{aligned}$$

Hence $\pi(M) \le 2M/\log\log M$ for all sufficiently large M.

(In fact the bounds above imply that $\pi(M) \le 2M/\log\log M$ for $\log M \ge 16$; then by checking the 'small' cases where $M < \mathrm{e}^{16} < 10^7$ on a computer, one gets the more explicit result that $\pi(M) \le 2M/\log\log M$ for all $M \ge 3$.)

3.11 (a) Expanding the geometric series we get

$$\prod_{i=1}^{n}\Big(1-\frac{1}{p_i}\Big)^{-1} = \prod_{i=1}^{n}\Big(1+\frac{1}{p_i}+\frac{1}{p_i^2}+\cdots+\frac{1}{p_i^{e_i}}+\cdots\Big).$$

If $x \le p_n$ then x has a prime factorization $p_1^{e_1}p_2^{e_2}\ldots p_n^{e_n}$ for some $e_1, e_2, \ldots, e_n \in \mathbb{N}_0$. Hence $1/x$ is obtained by multiplying out the product, taking $1/p_i^{e_i}$ from the ith term for each i. It follows that the product is at least $\sum_{x=1}^{p_n}\frac{1}{x}$.

(b) We have

$$\int_x^{x+1} \frac{\mathrm{d}t}{t} \leq \int_x^{x+1} \frac{\mathrm{d}t}{x} \leq \frac{1}{x}$$

for each $x \in \mathbb{N}$. Hence

$$\int_1^S \frac{\mathrm{d}t}{t} \leq \sum_{x=1}^{S-1} \int_x^{x+1} \frac{\mathrm{d}t}{t} \leq \sum_{x=1}^{S-1} \frac{1}{x} \leq \sum_{x=1}^{S} \frac{1}{x}$$

as required.

(c) If there are finitely many primes then $\prod_p \left(1 - \frac{1}{p}\right)^{-1}$, where the product is over all primes, is finite and so converges. This contradicts (b). (Of course Corollary 3.4.6 and Exercise 3.10 give a stronger result: the argument here is an even shorter demonstration of the relevance of analytic methods to number theory.)

3.12 (a) Since $|1/m^z| = 1/m^{\operatorname{Re} z}$ and $\sum_{m=1}^{\infty} 1/m^r$ converges whenever $r > 1$ (for example, by the integral test), $\sum_{m=1}^{\infty} 1/m^z$ converges absolutely when $\operatorname{Re} z > 1$. When $z = 1$ the series diverges, by Exercise 3.11(b).

(b) Replacing p_i with p_i^z in Exercise 3.11(a) we get

$$\prod_{i=1}^{n} \left(1 - \frac{1}{p_i^z}\right)^{-1} = \sum \frac{1}{m^z}$$

where the sum is over all those $m \in \mathbb{N}$ divisible only by the primes $p_1, \ldots, p_n$. By (a), the right hand-side converges to $\sum_{m=1}^{\infty} 1/m^z$ as $n \to \infty$. This series converges absolutely, so the sum is independent of the order of terms. Therefore

$$\prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^z}\right)^{-1} = \sum_{m=1}^{\infty} \frac{1}{m^z}$$

as required.

(c) Using $\eta(z)$ to cancel summands $1/(2m+1)^z$ in $\zeta(z)$ we get

$$\zeta(z) - \eta(z) = 2 \sum_{m=1}^{\infty} \frac{1}{(2m)^z} = 2^{-(z-1)} \zeta(z).$$

Hence $\zeta(z)(1 - 2^{-(z-1)}) = \eta(z)$, as required.

(d) If $z \in \mathbb{R}$ and $z > 0$ then the terms $(-1)^m/m^z$ are alternating in sign and decreasing. Convergence of $\eta(z)$ follows from the alternating series test. Convergence for general z with $\operatorname{Re} z > 0$ can be proved by using the Generalized Binomial Theorem (Theorem 5.2.1) to write

$$(m + \tfrac{1}{2} + \ell)^{-z} = (m + \tfrac{1}{2})^{-z} \left(1 + \tfrac{\ell}{m+\frac{1}{2}}\right)^{-s} = (m + \tfrac{1}{2})^{-z} \left(1 + \tbinom{-z}{1} \tfrac{\ell}{m+\frac{1}{2}} + O(m^{-2})\right).$$

Now take $\ell = \pm\frac{1}{2}$ and $m = 2q-1$ to show that

$$(2q-1)^{-z}-(2q)^{-z}=(2q-\tfrac{1}{2})^{-z}\left(\tfrac{z}{2q-\frac{1}{2}}+O(q^{-2})\right)=z(2q-\tfrac{1}{2})^{-(z+1)}+O(q^{-(z+2)}).$$

The 'big-O'-notation used above is defined in §6.4. We saw in (a) that $\sum_{q=1}^{\infty} 1/q^{z+1}$ converges absolutely when $\mathrm{Re}\, z > 0$, hence $\eta(z)$ converges when $\mathrm{Re}\, z > 0$.

(A less ad-hoc proof uses Abel summation, one of the main techniques in analytic number theory; this method can also be applied directly to the ζ function to get the meromorphic continuation $\zeta(s) = \frac{s}{s-1} + \int_1^\infty \frac{\{x\}}{x^{s+1}}\,\mathrm{d}x$ to $\mathrm{Re}\, s > 0$; here $\{x\}$ denotes the fractional part of $x \in \mathbb{R}$.)

3.13 (a) Let $\Omega = \{1,2,\ldots,M\}$. Since $x \in \Omega$ is square-free if and only if x is not divisible by any of $p_1^2, p_2^2, \ldots, p_n^2$, we have

$$S = \overline{D(p_1^2) \cup D(p_2^2) \cup \ldots \cup D(p_n^2)}.$$

Thus $\pi_2(M) = |S|$ and by the Principle of Inclusion and Exclusion and Proposition 3.4.3,

$$\pi_2(M) = \sum_{I\subseteq\{1,2,\ldots,n\}} (-1)^{|I|} \left\lfloor \frac{M}{\prod_{i\in I} p_i^2} \right\rfloor.$$

If we repeat the approximation in the proof of Theorem 3.4.5 we get the same error term of 2^n. By the Prime Number Theorem, there are about $\sqrt{M}/\log\sqrt{M}$ primes less than or equal to $\sqrt{M}$, so the error term is roughly $2^{\sqrt{M}}$. This is far larger than M and $\pi_2(M)$. Instead, we observe that if $\prod_{i\in I} p_i > \sqrt{M}$ then the summand for I is zero. We can therefore drop all these summands, leaving at most $\sqrt{M}$ non-zero summands. Dividing by M and using the $\star$ notation from the question to denote that summands $\pm 1/d$ with $d > M$ are to be ignored, we get

$$\left| \frac{\pi_2(M)}{M} - \sum_{I\subseteq\{1,2,\ldots,n\}}^{\star} (-1)^{|I|} \frac{1}{\prod_{i\in I} p_i^2} \right| \le \frac{\sqrt{M}}{M}.$$

Writing the sum as a product, as in Theorem 3.4.5, gives

$$\left| \frac{\pi_2(M)}{M} - \prod_{i=1}^{n}{}^{\star} \left(1 - \frac{1}{p_i^2}\right) \right| \le \frac{1}{\sqrt{M}}.$$

where the $\star$ notation is as in the question. This proves (a).

(b) As M tends to infinity we sieve over more and more primes and every $\pm\frac{1}{d^2}$ for $d \in \mathbb{N}$ appears as an (unignored) term in the product. The right-hand side tends to 0. Therefore

$$\lim_{M\to\infty} \frac{\pi_2(M)}{M} = \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^2}\right).$$

By Exercise 3.12(a) it follows that $\lim_{M\to\infty} \frac{\pi_2(M)}{M} = \zeta(2)$.

(c) We were able to estimate $\pi_2(M)$ by sieving over all relevant primes relevant to $\pi_2(M)$ without introducing a large error term. This was impossible for $\pi(M)$. Therefore we get a more precise answer for $\pi_2(M)$ than $\pi(M)$. Correspondingly, $\prod_{i=1}^{n}\big(1-\frac{1}{p_i^2}\big)^{-1}$ converges to $\zeta(2)$ as $n\to\infty$, whereas, by Exercise 3.11(a),

$$\prod_{i=1}^{n}\Big(1-\frac{1}{p_i}\Big)^{-1} \to \infty \text{ as } n\to\infty.$$

(For this reason, the sieve used in this question is called the 'convergent sieve'.)

3.14 (a) Using the definition of $g_r(x)$ and then swapping the sums over $x\in\Omega$ and $I\subseteq\{1,2,\ldots,n\}$, we have

$$c_r = \sum_{x\in\Omega} g_r(x) = \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ |I|\le r}} \sum_{x\in\Omega} \begin{cases} (-1)^{|I|} & \text{if } x\in A_I \\ 0 & \text{otherwise} \end{cases} = \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ |I|\le r}} (-1)^{|I|}|A_I|$$

as claimed.

(b) By hypothesis, $x\in A_j$ if and only if $j\in J$. As seen in the proof of the Principle of Inclusion and Exclusion, x contributes to $|A_I|$ if and only if $I\subseteq J$. Therefore we can restrict the sum defining $f_r(x)$ to those I such that $I\subseteq J$ to get

$$g_r(x) = \sum_{\substack{I\subseteq J\\ |I|\le r}} (-1)^{|I|}.$$

Since there are $\binom{|J|}{k}$ k-subsets of J, the right-hand side is $\sum_{k=0}^{r}(-1)^k\binom{|J|}{k}$. By Lemma 2.2.2 the sum is $(-1)^r\binom{|J|-1}{r}$, hence $g_r(x) = (-1)^r\binom{|J|-1}{r}$ as required. By definition of m_x we have $m_x = |J|$. Therefore, summing over all $x\in\Omega$ we get

$$c_r = \sum_{x\in\Omega} g_r(x) = \sum_{x\in\Omega}(-1)^r\binom{m_x-1}{r}.$$

(c) Let $x\in\Omega$. If $x\in\overline{A_1\cup A_2\cup\ldots\cup A_n}$ then $m_x=0$. By the extended definition of binomial coefficients in §2.4, $\binom{-1}{0}=1$, therefore x contributes 1 to c_n. Otherwise $m_x\ge 1$ and $\binom{m_x-1}{r}=0$. Hence $c_n = |\overline{A_1\cup A_2\cup\ldots\cup A_n}|$; this is equivalent to Theorem 3.1.3.

(d) Generalizing (c), each $x\in\overline{A_1\cup A_2\cup\ldots\cup A_n}$ contributes 1 to c_r, and since r is even and so $(-1)^r\binom{m_x-1}{r}\ge 0$, the contribution from all other $x\in\Omega$ is non-negative. Hence $c_r\ge|\overline{A_1\cup A_2\cup\ldots\cup A_n}|$.

(e) This is very similar to (d).

(f) By (b) we have

$$c_r - c_{r+2} = \sum_{x \in \Omega} (-1)^r \left(\binom{m_x - 1}{r} - \binom{m_x - 1}{r+2} \right).$$

Since $r \geq (n-1)/2$ and $m_x \leq n-1$, it follows from Exercise 2.7 that $\binom{m_x-1}{r} \geq \binom{m_x-1}{r+2}$. Therefore $c_r - c_{r+2} \geq 0$ if r is even and $c_r - c_{r+2} \leq 0$ if r is odd, as required.

(g) ($\star$) The 'worst case' in (f) requires $\binom{n-1}{r} \geq \binom{n-1}{r+2}$. If $n = 2m$ is even then, by Exercise 2.7, $\binom{2m-1}{r} \geq \binom{2m-1}{r+2}$ if and only if $r \geq m-1$. If $n = 2m+1$ is odd then, again by Exercise 2.7, $\binom{2m}{r} \geq \binom{2m}{r+2}$ if and only if $r \geq m-1$. Therefore we may take $r \geq \lfloor n/2 \rfloor - 1$ in place of $(n-1)/2$. To show that no further improvement is possible, apply the Principle of Inclusion and Exclusion to the case where Ω is a singleton set, and $A_1, A_2, \ldots, A_n = \Omega$.

3.15 (a) Suppose that $x \in \Omega$ lies in exactly r of the sets $A_1, A_2, \ldots, A_n$. If $r = 0$ then x never contributes to the right-hand side. If $r = 1$ and $x \in A_i$ then x contributes to the right-hand side if and only if $I = \{i\}$, with coefficient $(-1)^0 e_1$. We must therefore take $e_1 = 1$. If $r = 2$ and $x \in A_i$ and $x \in A_j$ then x contributes to the right-hand side if and only if I is a non-empty subset of $\{i, j\}$; the coefficient is $(-1)^0 e_1 + (-1)^0 e_1 + (-1)^1 e_2 = 1 + 1 - e_2$. We must therefore take $e_2 = 2$. Continuing this line of reasoning suggests that the number of elements of Ω lying in exactly one of the sets $A_1, A_2, \ldots, A_r$ is

$$\sum_{k=1}^{n} (-1)^{k-1} k \sum_{\substack{I \subseteq \{1,2,\ldots,n| \\ |I| = k}} |A_I|.$$

Having guessed the formula it is not hard to prove it by the usual method. Suppose that $x \in \Omega$ lies in A_j if and only if $j \in J$. The contribution from x to the right-hand side is then

$$\sum_{I \subseteq J} (-1)^{|I|-1} |I| = \sum_{k=1}^{|J|} (-1)^{k-1} k \binom{|J|}{k}.$$

By Exercise 2.1 we have $k\binom{|J|}{k} = |J|\binom{|J|-1}{k-1}$. Hence, by Corollary 2.2.8(ii), the right-hand side is

$$|J| \sum_{k=1}^{|J|} (-1)^{k-1} \binom{|J|-1}{k-1} = \begin{cases} 1 & \text{if } |J| = 1 \\ 0 & \text{otherwise,} \end{cases}$$

as required.

(b) The argument used to discover the formula in (a) generalizes to suggest that the number of elements of Ω lying in exactly t of the sets $A_1, A_2, \ldots, A_r$ is

$$\sum_{k=t}^{n} (-1)^{k-t} \binom{k}{t} \sum_{\substack{I \subseteq \{1,2,\ldots,n\} \\ |I|=k}} |A_I|.$$

We now prove this. Suppose that $x \in \Omega$ lies in A_j if and only if $j \in J$. Then the contribution from x to the right-hand side is

$$\sum_{I \subseteq J} (-1)^{|I|-t} \binom{|I|}{t} = \sum_{k=t}^{|J|} (-1)^{k-t} \binom{k}{t} \binom{|J|}{k}.$$

By Lemma 2.2.4, $\binom{k}{t}\binom{|J|}{k} = \binom{|J|}{t}\binom{|J|-t}{k-t}$. Hence, by Corollary 2.2.8(ii), the right-hand side is

$$\binom{|J|}{t} \sum_{k=t}^{|J|} (-1)^{k-t} \binom{|J|-t}{k-t} = \begin{cases} 1 & \text{if } |J| = t \\ 0 & \text{otherwise,} \end{cases}$$

as required.

(c) Define the sets A_i as in §3.2, so A_i is the set of permutations of $\{1,2,\ldots,n\}$ that fix i. We saw in this section that $|A_I| = (n-|I|)!$. Therefore, by (b), the number of permutations with exactly t fixed points is

$$\sum_{k=t}^{n} (-1)^{k-t} \binom{k}{t} \binom{n}{k} (n-k)! = \sum_{k=t}^{n} (-1)^{k-t} \frac{n!}{(k-t)!t!}.$$

This is $\frac{n!}{t!}\left(1 - \frac{1}{1!} + \cdots + \frac{(-1)^{n-t}}{(n-t)!}\right)$, as seen in Exercise 1.10.

3.16 This is left to you as an extended exercise on the method of counting contributions.

3.17 (a) Since $1_X(x) = 1$ if $x \in X$ and $1_X(x) = 0$ if $x \notin X$, we have $\sum_{x\in\Omega} 1_X(x) = |X|$.

(b) Again by definition of 1_X, we have $1_B(x)1_C(x) = 1 \iff 1_B(x) = 1$ and $1_C(x) = 1 \iff x \in B$ and $x \in C \iff x \in B \cap C \iff 1_{B\cap C}(x) = 1$. Therefore $1_B 1_C = 1_{B\cap C}$.

(c) As in (b), we check that the two sides agree on all $x \in \Omega$. Suppose that $x \in A_1 \cup A_2 \cup \cdots \cup A_n$. Then $x \in A_j$ for some j and $(1_\Omega - 1_{A_j})(x) = 1 - 1 = 0$. If $x \notin A_1 \cup A_2 \cup \cdots \cup A_n$ then $(1_\Omega - 1_{A_j})(x) = 1$ for all j. Hence

$$x \in \overline{A_1 \cup A_2 \cup \cdots \cup A_n} \iff (1_\Omega - 1_{A_1})(1_\Omega - 1_{A_2}) \ldots (1_\Omega - 1_{A_n})(x) = 1$$

and so $1_{\overline{A_1 \cup A_2 \cup \cdots \cup A_n}} = (1_\Omega - 1_{A_1})(1_\Omega - 1_{A_2}) \ldots (1_\Omega - 1_{A_n})$.

(d) Multiplying out the right hand side above we get $(-1)^{|I|} 1_{A_{i_1}} \ldots 1_{A_{i_k}}$ by taking

-1_{A_i} from the term $1_\Omega - 1_{A_i}$ if $i \in I$ and 1_Ω if $i \notin I$. If $I = \varnothing$ we always take 1_Ω and get $1_\Omega = 1_{A_\varnothing}$. Otherwise, by (a), repeatedly applied, we have $1_{A_{i_1}} 1_{A_{i_2}} \ldots 1_{A_{i_k}} = 1_{A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}} = 1_{A_I}$. Hence the right-hand side is $\sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} 1_{A_I}$, as required.

(e) Summing the result of (d) over all $x \in \Omega$ we get

$$\begin{aligned} \sum_{x \in \Omega} 1_{\overline{A_1 \cup A_2 \cup \cdots \cup A_n}}(x) &= \sum_{x \in \Omega} \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} 1_{A_I}(x) \\ &= \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} \sum_{x \in \Omega} 1_{A_I}(x) \\ &= \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{I|} |A_I| \end{aligned}$$

where the final equality uses (a).

3.18 (a) Following the hint, we let Ω be the collection of r-subsets of $\{1, \ldots, m + n\}$ and aim to count the r-subsets not meeting $\{m+1, \ldots, m+n\}$. Let A_i be those subsets *we do not want to count* because they contain $m+i$. Then $\overline{A_1 \cup A_2 \cup \ldots \cup A_n}$ is the collection of r-subsets of $\{1, \ldots, m\}$. By the Principle of Inclusion and Exclusion, we have

$$\binom{m}{r} = \sum_{I \subseteq \{1,2,\ldots,n\}} (-1)^{|I|} |A_I|.$$

An r-subset is in A_I if and only if it contains $m+i$ for each $i \in I$. This leaves $r - |I|$ elements that can be chosen freely. Hence $|A_I| = \binom{n+m-|I|}{r-|I|}$. As we have often seen, the sizes of the sets A_I depends only on $|I|$. Hence the formula above from the Principle of Inclusion and Exclusion simplifies to

$$\binom{m}{r} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{n+m-k}{r-k}$$

as required.

(b) Here the challenge is finding a suitable set to count. Considering how k varies and the terms $\binom{2n-2k}{n-s-2k}$, one guess is that we should let Ω be the collection of all $(n-s)$-subsets of a set of size $2n$. If you reason from the case $k = 1$ that each A_i should contain exactly $\binom{2n-2}{n-2-s}$ of these $(n-s)$-subsets, you may find the solution outlined below.

Let A_i be those $(n-s)$-subsets of $\{1, 2, \ldots, 2n\}$ that contain $\{2i, 2i+1\}$. Then $\overline{A_1 \cup A_2 \cup \ldots \cup A_n}$ is those $(n-s)$-subsets having at most one element of each of $\{1,2\}$, $\{3,4\}$, $\ldots$, $\{2n-1, 2n\}$. There are $2^{n-s}\binom{n}{n-s}$ such subsets. Since A_I is those

$(n-s)$-subsets of $\{1,2,\ldots,2n\}$ that contain the $2k$ elements $\bigcup_{i\in I}\{2i,2i+1\}$, we have $|A_I| = \binom{2n-2k}{n-s-2k}$. Hence, by the Principle of Inclusion and Exclusion,

$$2^{n-s}\binom{n}{n-s} = \sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{2n-2k}{n-s-2k}.$$

Since $\binom{n}{n-s} = \binom{n}{s}$, by Lemma 2.1.5, this is equivalent to the identity. Rewriting $\binom{2n-2k}{n-s-2k}$ as $\binom{2n-2k}{n+s}$, changing the the summation variable to $n-k$ and applying Lemma 2.1.5 to $\binom{n}{n-k}$ we get $\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{2k}{n+s} = (-1)^n 2^{n-s}\binom{n}{s}$.

(c) Let $S = \{1,2,\ldots,n\}\times\{1,2,\ldots,m\}$ and let Ω be the set of all $(n+1)$-subsets of S. Say that $X\in\Omega$ is *admissible* if for all $i\in\{1,2,\ldots,n\}$ there exists $r\in\{1,2,\ldots,m\}$ such that $(i,r)\in X$. Let a be the number of admissible subsets. For each $i\in\{1,2,\ldots,n\}$ let

$$A_i = \big\{X\in\Omega : (i,r)\not\in X \text{ for any } r\in\{1,\ldots,m\}\big\}.$$

Thus A_i is those subsets that are inadmissible (and *we do not want to count*) because they contain no pair with first entry i. By the Principle of Inclusion and Exclusion

$$a = |\overline{A_1\cup A_2\cup\cdots\cup A_n}| = \sum_{I\subseteq\{1,2,\ldots,n\}}(-1)^{|I|}|A_I|$$

For any $I\subseteq\{1,\ldots,n\}$ we have

$$A_I = \big\{X\in\Omega : X\subseteq(\{1,\ldots,n\}\backslash I)\times\{1,\ldots,m\}\big\}.$$

Therefore $|A_I| = \binom{(n-|I|)m}{n+1}$. Summing over $I\subseteq\{1,\ldots,k\}$ according to their size k we get

$$a = \sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{(n-k)m}{n+1}.$$

On the other hand, we can construct an admissible $(n+1)$-subset of S by choosing $(1,r_1),\ldots,(n,r_n)\in S$ in m^n ways, and then choosing any remaining element of S in $mn-n$ ways. This double counts each admissible subset X since if $(i,r)\in X$ and $(i,r')\in X$ are distinct then either (i,r) or (i,r') could have been the final element chosen. Therefore

$$a = \frac{m^n(mn-n)}{2} = \frac{n}{2}\big(m^{n+1}-m^n\big).$$

The identity follows by equating the two expressions for a.

3.19 As suggested, let Ω be the set of functions $f:\{1,2,\ldots,n\}\to\{1,2,\ldots,n\}$ having no fixed points. Let A_i be those functions *we do not want to count* because i is not in their range. The set of derangements is then $\overline{A_1\cup A_2\cup\ldots\cup A_n}$. To construct

$f \in A_i$ we have $n-2$ choices for $f(x)$ for each $x \neq i$, and $n-1$ choices for $f(i)$. Therefore $|A_i| = (n-2)^{n-1}(n-1)$. More generally, if $|I| = k$ then

$$|A_I| = (n-k-1)^k (n-k)^{n-k}.$$

Since there are $\binom{n}{k}$ subsets I of size k, it follows from the Principle of Inclusion and Exclusion that

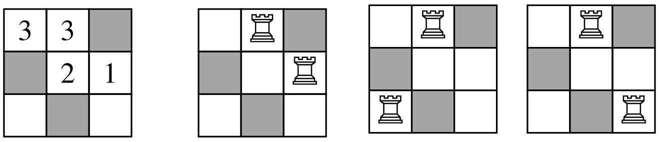
$$d_n = \sum_{k=0}^{n} \binom{n}{k} (n-k-1)^k (n-k)^{n-k}.$$

Here we started with a set of fixed-point-free functions, and threw out those that were not injective (and so were not permutations); by comparison, in §3.2 we started with a set of permutations and threw out those that had a fixed point.

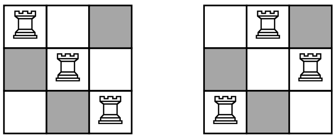
4. Rook polynomials

Exercise 4.1.2 A single rook is always non-attacking so $r_1(B)$ is the number of squares in B. Since there is a unique rook placement with no rooks, $r_0(B) = 1$ for any board B.

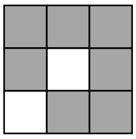
Exercise 4.1.3 By the previous exercise $r_0(B) = 1$ and $r_1(B) = 6$. The non-attacking placements with two rooks are enumerated according to the position of the highest rook in the left diagram below. For instance, the three placements with the highest rook in the box in the middle of the top row are shown to the right.



Therefore $r_2(B) = 9$. The two diagrams below show that $r_B(3) = 2$. Hence $f_B(z) = 1 + 6z + 9z^2 + 2z^3$.



Exercise 4.1.4 By Exercise 4.1.3, there are 9 placements of 2 rooks and 2 placements of 3 rooks not having a rook in the top-left corner. If there is a rook in this corner then the remaining rooks are on the board of unshaded squares in the margin. Hence $r_2(B) = 9 + 2 = 11$ and $r_3(3) = 2 + 1 = 3$ and so $f_B(z) = 1 + 7z + 11z^2 + 3z^3$.



Exercise 4.3.4 Applying Lemma 4.2.1 to B_n, using the square in the top-right corner as instructed, we get

$$\begin{aligned}
f_{B_n}(z) &= f_{S_{2n-1}}(z) + z f_{S_{2(n-1)-1}}(z) \\
&= \sum_{k=0}^{n} \binom{2n-k}{k} z^k + z \sum_{k=0}^{n} \binom{2(n-1)-k}{k} z^k \\
&= 1 + \sum_{k=1}^{n} \left(\binom{2n-k}{k} + \binom{2n-k-1}{k-1} \right) z^k \\
&= 1 + \sum_{k=1}^{n} \binom{2n-k}{k} (1 + \frac{k}{2n-k}) z^k \\
&= 1 + \sum_{k=1}^{n} \binom{2n-k}{k} \frac{2n}{2n-k} z^k
\end{aligned}$$

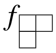
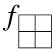
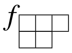
where the fourth equality uses the identity $(2n-k)\binom{2n-k-1}{k-1} = k\binom{2n}{k}$; this is an instance of Exercise 2.1.

Exercise 4.3.7 Since $g_\ell(z)$ is the rook polynomial of the board $B_{2\ell}$, the coefficient of z^k in $z^{n-\ell} g_\ell$ is $r_{k-(n-\ell)}(B_{2\ell})$ for each $k \in \{n-\ell, \dots, n\}$. Therefore Corollary 4.3.3 implies that

$$\begin{aligned}
r_n(\overline{B}) &= \sum_{\ell=0}^{n} a_\ell \sum_{k=n-\ell}^{n} (-1)^k r_{k-(n-\ell)}(B_{2\ell})(n-k)! \\
&= \sum_{\ell=0}^{n} a_\ell \sum_{j=0}^{\ell} (-1)^{j+(n-\ell)} r_j(B_{2\ell})(\ell-j)! \\
&= \sum_{\ell=0}^{n} a_\ell (-1)^{n-\ell} r_\ell(\overline{B}_{2\ell}) \\
&= \sum_{\ell=0}^{n} (-1)^{n-\ell} u_\ell
\end{aligned}$$

where the third inequality uses Corollary 4.3.3 applied to $B_{2\ell}$.

End of chapter exercises

4.1 Using Exercise 4.1.2 and a direct count of the number of placements of 2 rooks we get f$(z) = 1 + 3z + z^2$, f$(z) = 1 + 4z + 2z^2$, f$(z) = 1 + 5z + 4z^2$. The final board could also be done by a direct count, or by the method in Exercise 4.1.3, but instead we apply Lemma 4.2.1 to the square in the bottom-left corner. Deleting this square gives the third board, while deleting its entire row and column gives the first board. Hence

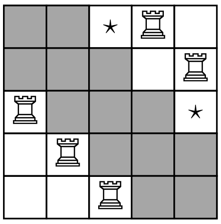
$$\begin{aligned} f_{\substack{\square\square\square\\ \square\square\\ \square}}(z) &= f_{\substack{\square\square\square\\ \square\square}}(z) + z f_{\substack{\square\square\\ \square}}(z) \\ &= 1+5z+4z^2+z(1+3z+z^2) \\ &= 1+6z+7z^2+z^3. \end{aligned}$$

4.2 To put k non-attacking rooks on the $m \times n$ grid we can choose k rows in $\binom{m}{k}$ ways and k columns in $\binom{n}{k}$ ways. We must then put k rooks on the $k \times k$ subboard of squares in the chosen rows and column; by the bijection between non-attacking rook placements and permutations seen in Example 4.1.6, this can be done in $k!$ ways. Therefore the coefficient of z^k is $\binom{m}{k}\binom{n}{k}k!$, as required.

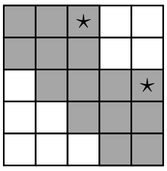
4.3 (a) As seen in Example 4.1.6, there is a bijection between permutations of $\{1,2,3,4,5\}$ and ways to place five non-attacking rooks on the squares of a 5×5 grid: a permutation σ corresponds to the rook placement with rooks in positions $(i, \sigma(i))$ for each $i \in \{1,2,3,4,5\}$. Derangements correspond to rook placements with no rooks on the diagonal. Moreover

- $\sigma(i) \neq i+1$ if $1 \leq i \leq 4$ rules out the squares $(1,2),(2,3),(3,4),(4,5)$, below the diagonal,
- $\sigma(i) \neq i-1$ if $2 \leq i \leq 5$ rules out the squares $(2,1),(3,2),(4,3),(5,4)$ above the diagonal.

Therefore derangements in T are in bijection with non-attacking rook placements of 5 rooks on the board of unshaded squares. For example, the permutation σ defined by $\sigma(1) = 3$, $\sigma(2) = 4$, $\sigma(3) = 5$, $\sigma(4) = 2$, $\sigma(5) = 1$ corresponds to the non-attacking placement shown below.



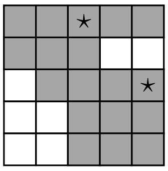
(b) Suppose that neither starred square is occupied. Then all rooks lie in the unshaded squares below.



No square in the bottom-left subboard lies in the same row or column as a square in the top-right subboard. Hence, by Lemma 4.2.2 and Exercise 4.1, the contribution to the rook polynomial from this case is

$$\begin{aligned}f_{\begin{smallmatrix}\square&\square\\\square&\square\end{smallmatrix}}(z)f_{\begin{smallmatrix}\square&&\\\square&\square&\\\square&\square&\square\end{smallmatrix}}(z)&=(1+4z+2z^2)(1+6z+7z^2+z^3)\\&=1+10z+33z^2+41z^3+18z^4+2z^5.\end{aligned}$$

If the only starred square occupied is the one in position $(1,3)$ then all other rooks are on the unshaded squares below.



Taking into account that one rook is already placed, the contribution to the rook polynomial is

$$\begin{aligned}zf_{\begin{smallmatrix}\square&\square\end{smallmatrix}}(z)f_{\begin{smallmatrix}\square&\\\square&\square\\\square&\square\end{smallmatrix}}(z)&=z(1+2z)(1+5z+4z^2)\\&=z+7z^2+14z^3+8z^4.\end{aligned}$$

By symmetry we get the same contribution to the rook polynomial if the other starred square is the only occupied starred square. Finally, as stated in the question, if both starred squares are occupied, the contribution to the rook polynomial is

$$\begin{aligned}z^2f_{\square}(z)f_{\begin{smallmatrix}\square&\square\\\square&\square\end{smallmatrix}}(z)&=z^2(1+z)(1+4z+2z^2)\\&=z^2+5z^3+6z^4+2z^5.\end{aligned}$$

Adding up these four contributions shows that the rook polynomial of the original board is

$$\begin{aligned}&(1+10z+33z^2+41z^3+18z^4+2z^5)+2(z+7z^2+14z^3+8z^4)\\&\qquad+(z^2+5z^3+6z^4+2z^5)=1+12z+48z^2+74z^3+40z^4+4z^5.\end{aligned}$$

(c) By Corollary 4.3.3, the number of placements of five non-attacking rooks on the shaded squares forming the complement $\overline{B}$ of B is

$$\begin{aligned}&5!r_0(B)-4!r_1(B)+3!r_2(B)-2!r_3(B)+1!r_4(B)-0!r_5(B)\\&\qquad=120-288+288-148+40-4=8.\end{aligned}$$

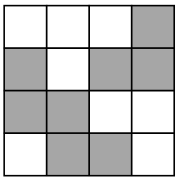
(d) ($\star$) Let A_i be the set of non-attacking placements of four rooks on the 5×5 grid in which there is a rook in row x and this rook is on a square in B. The sum $\sum_{I\subseteq\{1,\ldots,n\}:|I|=k}|A_I|$ of the sizes of all intersections of exactly k of the A_i is the number of ways to put down k red rooks on squares in B and $4-k$ blue rooks anywhere on the grid. By the argument in Lemma 6.9, this quantity is $\binom{5-k}{4-k}^2(4-k)!\,r_k(B)$. Hence using 2(b) we find that there are

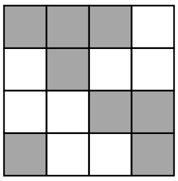
$$\begin{aligned}\binom{5}{4}^2 4!\,r_0(B) - \binom{4}{3}^2 3!\,r_1(B) + \binom{3}{2}^2 2!\,r_2(B) - \binom{2}{1}^2 1!\,r_3(B) + \binom{1}{0}^2 0!\,r_4(B)\\ = 5^2.24.1 - 4^2.6.12 + 3^2.2.48 - 2^2.1.74 + 40\\ = 600 - 1152 + 864 - 296 + 40 = 56\end{aligned}$$

ways to put four non-attacking rooks on the shaded squares.

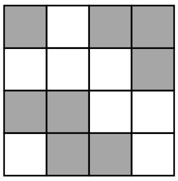
4.4 (a) If we take a board with a non-attacking rook placement and swap two rows then each row still has at most one rook in it, as does each column. Hence the rook placement on the new board is still non-attacking. Since any row permutation can be obtained by repeated swapping of rows, this shows that permuting the rows does not change the rook polynomial. Similarly for columns.

(b) The board B in Example 4.1.5 is formed from the unshaded squares in the diagram left below.

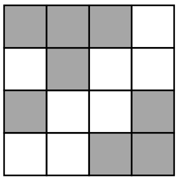




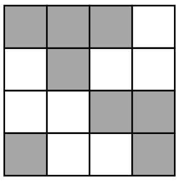
We aim to permute the rows and column of B to obtain its complement $\overline{B}$, shown right above. Note that the rows of B have, from top to bottom, 3, 1, 2 and 2 unshaded squares. So the only chance is to swap rows 1 and 2. This gives the board below.



Then we must move column 4 to column 2, since this is the only column to have a shaded square in row 2. Swapping these columns we get the board below.

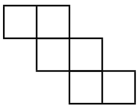


Finally swapping rows 3 and 4 gives $\overline{B}$, shown below.



Hence, by (a), B and $\overline{B}$ have the same rook polynomial.

4.5 (a) Using Exercise 4.1.2 and the method of Exercise 4.1.3 it is routine to show that $f_{S_1}(zz) = 1+z$, $f_{S_2}(z) = 1+2z$, $f_{S_3}(z) = 1+3z+z^2$, $f_{S_4}(z) = 1+4z+3z^2$. The rook polynomial $f_{S_5}(z) = 1+5z+6z^2+z^3$ was found at the start of the chapter.



(b) Applying Lemma 4.2.1 to the bottom right square in S_6 (shown in the margin) we get

$$\begin{aligned} f_{S_6}(z) &= f_{S_5}(z) + zf_{S_4}(z) \\ &= 1+5z+6z^2+z^3+z(1+4z+3z^2) \\ &= 1+6z+10z^2+4z^3. \end{aligned}$$

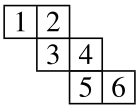
(c) Looking at the Pascal's Triangle on page 23 one can spot the coefficients in f_5 and f_6 on the southwest to northeast diagonals. For instance, the coefficients of f_6 are $1 = \binom{7}{0}$, $6 = \binom{6}{1}$, $10 = \binom{5}{2}$, $4 = \binom{4}{3}$. This suggests the conjecture that $r_{S_n}(k) = \binom{n-k+1}{k}$.

(d) The routine proof uses Lemma 4.2.1 to split the board on the bottom-left square. As seen in (b), removing this square gives S_{m-1}, while removing this square and all squares in its row and column gives S_{m-2}. Therefore by the lemma and induction we have

$$\begin{aligned} f_{S_m}(z) &= f_{S_{m-1}}(z) + zf_{S_{m-2}}(z) \\ &= \sum_k \binom{(m-1)-k+1}{k} z^k + z\sum_k \binom{(m-2)-k+1}{k} z^k \\ &= \sum_k \binom{m-k}{k} z^k + \sum_k \binom{m-k-1}{k} z^{k+1} \\ &= \sum_k \left(\binom{m-k}{k} + \binom{m-k}{k-1} \right) z^k \\ &= \sum_k \binom{m-k+1}{k} z^k \end{aligned}$$

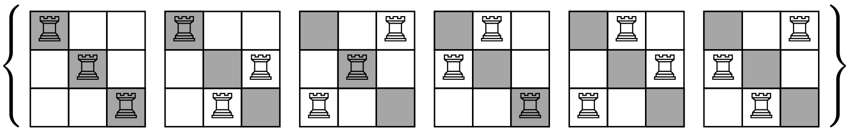
where the final step uses the Fundamental Recurrence (Lemma 2.1.7). The base cases $f_{S_1}(z) = 1+z$ and $f_{S_2}(z) = 1+2z$ are easily checked.

Alternatively, observe that if we number the squares in the staircase board S_m from

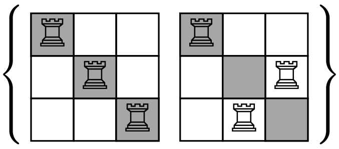


1 at the top-left to m in the bottom-right, as shown by the diagram in the margin for S_6, then a rook placement on S_m is non-attacking if and only if no two rooks lie on consecutively numbered suqares. Therefore there is a bijection between non-attacking placements of k rooks on S_m and placements of k lions into m cages as in Exercise 2.4. By this exercise, there are $\binom{m-k+1}{k}$ placements.

4.6 As usual $A_\varnothing$ is the universe set Ω of all non-attacking placements of 3 rooks on the 3×3 grid; as seen in Example 4.1.6 these correspond to the $3! = 6$ permutations of $\{1,2,3\}$:

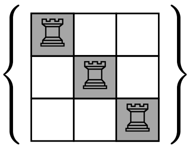
$A_\varnothing =$

.

This is also the set $\mathscr{C}_0$, since no rooks need to be coloured. As expected $|\mathscr{C}_0| = r_0(B)3! = 6$. By definition $A_{\{1\}}$ consists of those non-attacking rook placements where the rook on row 1 is on B; since the only shaded square in row 1 is in column 1, we have

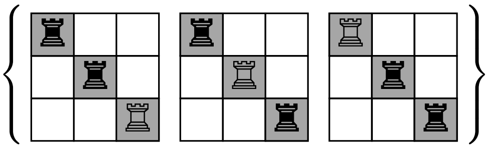
$A_{\{1\}} =$

.

Similarly $A_{\{2\}}$ consists of the two placements with a rook on the middle square, and $A_{\{3\}}$ of the two placements with a rook on the bottom-right square. Therefore the set $\mathscr{C}_1$ is as stated in the question

The set $A_{\{1,2\}}$ consists of those non-attacking rook placements where the rooks on rows 1 and row 2 are on B; there is a unique such placement and

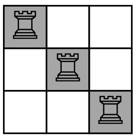
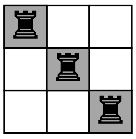
$A_{\{1,2\}} = A_{\{1,3\}} = A_{\{2,3\}} =$

.

These equal sets are distinguished in the proof of Lemma 4.3.2 by colouring rooks, giving

$\mathscr{C}_2 =$

.

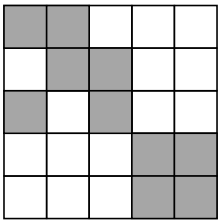
Hence $|\mathscr{C}_2| = 3$ agreeing with $|A_{\{1,2\}}| + |A_{\{1,3\}}| + |A_{\{2,3\}}| = 1 + 1 + 1 = 3$ and

$r_2(B)(3-2)! = 3 \times 1! = 3$. Finally

$A_{\{1,2,3\}} = \Bigg\{$  $\Bigg\}$, $\mathscr{C}_3 = \Bigg\{$  $\Bigg\}$.

Hence $|\mathscr{C}_3| = 1$ agreeing with $|A_{\{1,2,3\}}| = 1$ and $r_3(B)(3-3)! = 1 \times 0! = 1$.

4.7 Let B be the board of *shaded* square shown below



(a) By Lemma 4.2.2, we have

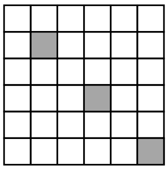
$$f_B(z) = (1+6z+9z^2+2z^3)(1+4z+2z^2) = 1+10z+35z^2+50z^3+26z^4+4z^5.$$

Hence, by Corollary 4.3.3, the number of ways to put five non-attacking rooks on $\overline{B}$ is $5! - 10 \times 4! + 35 \times 3! - 50 \times 2! + 26 \times 1! - 4 \times 0! = 12$.

(b) Suppose we put down five non-attacking rooks on $\overline{B}$, in positions $(1, j_1)$, $(2, j_2)$, $(3, j_3)$, $(4, j_4)$, $(5, j_5)$. Then $j_1 \notin \{1,2\}$, $j_2 \notin \{2,3\}$, $j_3 \notin \{1,3\}$, $j_4 \notin \{4,5\}$ and $j_5 \notin \{4,5\}$ and j_1, j_2, j_3, j_4, J_5 are distinct. Therefore we can extend the Latin rectangle to a $3 \times n$ Latin rectangle with third row $j_1 j_2 j_3 j_4 j_5$. Conversely, any allowable third row corresponds to a way to put five non-attacking rooks on $\overline{B}$. Therefore there are 12 extensions to a $3 \times n$ Latin rectangle.

(c) Since $f_B(z) = g_3(z)g_2(z) = g_5(z) + z^4 g_1(z)$ by Proposition 4.3.6, it follows from Exercise 4.3.7 that $r_5(\overline{B}) = u_5 + u_1$.

4.8 Let B be the board of *shaded* squares below.



By the bijection seen in Example 4.1.6, the permutations of $\{1,2,3,4,5,6\}$ with no even fixed point are in bijection with non-attacking placements of 6 rooks on $\overline{B}$.

The rook polynomial of B is $(1+z)^3 = 1+3z+3z^2+z^3$. Hence, by Corollary 4.3.3, the number of such permutations is

$$r_6(\overline{B}) = 6! - 5! \times 3 + 4! \times 3 - 3! = 720 - 360 + 72 - 6 = 426.$$

4.9 (a) The following MATHEMATICA code implements Lemma 4.2.1.

```
RookPolynomial[{}] := 1
DS[{i_, j_}, bs__] := DeleteCases[bs, {i, j}]
ES[{i_, j_}, bs__]
        := DeleteCases[bs, {iP_, jP_} /; Or[iP == i, jP == j]]
RookPolynomial[{{i_, j_}, bs___}]
        :=      RookPolynomial[DS[{i, j}, List[bs]]]
            + z*RookPolynomial[ES[{i, j}, List[bs]]]
```

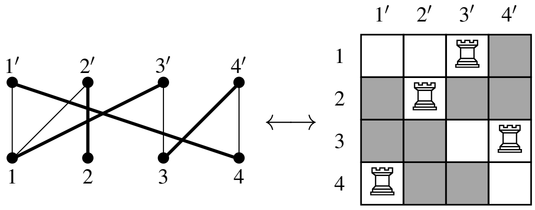
For example `RookPolynomial[{{1,1},{1,2},{2,1},{2,2}}]` evaluates to $1+4z+2z^2$. The 'helper' functions `DS` and `ES` create the boards D and E required in Lemma 4.2.1. In the main function, the *pattern* `{{i_, j_}, bs___}` matches an arbitrary non-empty list of squares, binding `i` and `j` to the position of the first square and `bs` to the remaining squares. After this `bs` is stored as a MATHEMATICA sequence, suitable for use as the collection of arguments to a function; it has to be converted back to a list by the `List` function in the recursive step.

(b), (c) MATHEMATICA code for these refined algorithms may be downloaded from the author's website (see page 4). An alternative implementation in the functional programming language HASKELL is also available.

(d) Using the algorithm in (c) that applies Lemma 4.2.2 where possible, the rook polynomial of the 'coffee' board is computed in 86 seconds on a 2015 MacBook Pro in MATHEMATICA. The compiled Haskell code takes 12 seconds. The simpler algorithms in (a) and (b) cannot compute this rook polynomial in a reasonable time.

4.10 (a) The summand $\prod_{i=1}^{n} M_{i\sigma(i)}$ in per M is 0 unless $M_{i\sigma(i)} = 1$ for all i; if this condition holds the summand is 1. Therefore the permanent counts the number of ways to put n non-attacking rooks on the $n \times n$ grid so that every rook is in a square (i, j) such that $M_{ij} = 1$. This is the coefficient of z^n in $f_B(z)$.

(b) Choose notation so that $H(B)$ has bipartition $\{1,\dots,n\} \cup \{1',\dots,n'\}$ where vertices $\{1,\dots,n\}$ to the rows and vertices $\{1',\dots,n'\}$ correspond to the columns. For instance, replacing Profs. W, X, Y, Z with $1', 2', 3', 4'$, the example graph and matching are shown on the left below.



There is a bijection between placements of n non-attacking rooks on B and matchings in $H(B)$ in which we choose the edge $\{i, j'\}$ if and only if there is a rook on the square (i, j). The non-attacking rook placement corresponding to the matching in the example is shown on the right above. Hence, by (a), per $M(B)$ is the number of matchings in $H(B)$.

(c) A board B contained in the $n \times n$ grid given as a list of squares can be turned into the $n \times n$ matrix $M(B)$ with 0, 1 entries in time $O(n^2)$. Similarly one can go turn such a matrix into a board, also in time $O(n^2)$. The problems of finding the coefficient of z^n in $f_B(z)$ and computing per $M(B)$ are therefore polynomial time equivalent. By Valiant's result, both are in #P, the complexity class of counting the number of accepting states of a non-deterministic Turing Machine that promises to run in polynomial time.

Perhaps surprisingly, it is possible to decide in polynomial time if $f_B(z)$ is non-zero. This is most easily seen using (b): there are algorithms that run in time polynomial in n and return either a complete matching in the graph $H(B)$, or a subset $X \subseteq \{1, 2, \ldots, n\}$ such that X has strictly fewer than $|X|$ neighbours in $\{1', \ldots, n'\}$. See for instance the algorithmic proof of Hall's Marriage Theorem on page 27 of Bryant (1993). Alternatively one can apply the Ford–Fulkerson Algorithm (which you might have seen used to prove the Max-flow Min-cut Theorem) to the network version of $H(B)$.

Therefore, unless $\mathrm{P} = \mathrm{NP}$, it is strictly harder to compute the coefficient of z^n in $f_B(z)$ than to decide if it is non-zero.

4.11 (a) By Exercise 4.2, the rook polynomial of the $n-1 \times n$ grid is $\sum_{k=0}^{n} \binom{n-1}{k}\binom{n}{k}k!$. Hence

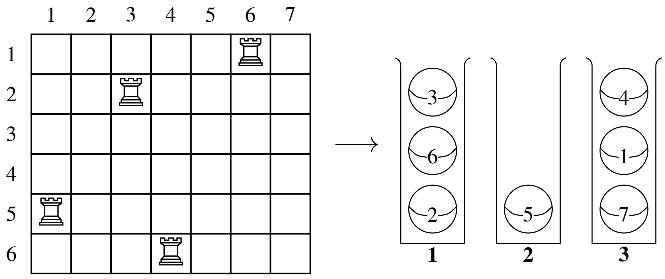
$$\left]\begin{matrix} n \\ k \end{matrix}\right[= \binom{n-1}{n-k}\binom{n}{n-k}(n-k)! = \binom{n-1}{k-1}\frac{n!}{k!}$$

as required.

(b) By Exercise 2.5, swapping the roles of k and n, there are $\binom{n-1}{k-1}$ solutions to the equation $u_1 + u_2 + \cdots + u_k = n$ with $u_r \in \mathbb{N}$ for each r. Fix such a solution. We then choose a permutation $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ and put balls $\sigma(1), \ldots, \sigma(u_1)$ into tube 1, balls $\sigma(u_1 + 1), \ldots, \sigma(u_1 + u_2)$ into tube 2, and so on. This shows that there are $\binom{n-1}{k-1}n!$ ways to put n labelled balls into k labelled tubes. By (a), this number is $k!\left]{n \atop k}\right[$.

(c) Given a placement of n labelled balls into k unlabelled tubes so that each tube is non-empty, we can distinguish the tubes using the balls at their bottoms, and so label them in $k!$ ways. This gives a placement of n labelled balls into k labelled urns; by (b) there are $k!\left]{n \atop k}\right[$ such placements. Hence the number of placements into unlabelled tubes is $\left]{n \atop k}\right[$.

(d) ($\star$) A non-attacking placement of $n-k$ rooks on the $(n-1)\times n$ grid has exactly k empty columns. Suppose that columns $c_1,\dots,c_k$ are empty. Put balls $c_1,\dots,$ c_k at the bottom of the k tubes; this labels the tubes $1,2,\dots,k$. Now scanning from row 1 downwards, find the column of each rook, and put the corresponding ball in tube 1, stopping at the first empty row. Then continue with tube 2, and so on. Since there are $k-1$ empty rows we make k scans; these specify the remaining balls in each of the k urns. An example with $n=7$ and $k=3$ is shown below.



Note that the second scan finishes immediately since row 4 is empty. Therefore tube 2 contains only ball number 5.

Constructing the inverse map from ball-and-tube placements to rook placements is left as an exercise: for a detailed solution see pages 15 and 16 of Butler *et al.* (n.d.).

4.12 (a) Clearly $h_t(B)\binom{t}{k}$ is the number of ways to put n non-attacking rooks on the $n\times n$ grid so that exactly t on B and then to colour k of the rooks on B black. Alternatively, we can construct such a coloured rook placement by first putting k non-attacking black rooks on B and then $n-k$ white rooks on the rest of the grid, so that all n rooks are non-attacking. As seen in the proof of Lemma 4.3.2, we can do this in $r_k(B)(n-k)!$ ways.

(b) By the Binomial Theorem,

$$\sum_{t=0}^{n} h_t(B)(1+z)^t = \sum_{t=0}^{n}\sum_{k=0}^{t} h_t(B)\binom{t}{k}z^k.$$

The coefficient of z^k on the right-hand side is $\sum_t h_t(B)\binom{t}{k}$; by (a) this is $r_k(B)(n-k)!$. This proves the first identity. Now substitute $w = z-1$ to get the second.

(c) Substituting $w = 0$ the left-hand side is replaced with its constant term $h_0(B)$, so we have

$$h_0(B) = \sum_{k=0}^{n} r_k(B)(n-k)!(-1)^k$$

as first proved in Corollary 4.3.3.

(d) Let B be the board of diagonal square in the $n \times n$ grid. By the usual correspondence seen in Example 4.1.6 between non-attacking rook placements and permutation, the hit number $h_t(B)$ is the number of permutations of $\{1,2,\ldots,n\}$ with precisely t fixed points, namely $a_n(t)$. Since $r_k(B) = \binom{n}{k}$, it follows from (b) in the previous question that

$$\sum_{t=0}^{n} h_t(B)w^t = \sum_{k=0}^{n} \binom{n}{k}(n-k)!(w-1)^k.$$

Taking the coefficient of w^t on the right-hand side, we get

$$a_n(t) = \sum_{k=0}^{n} \binom{n}{k}(n-k)!(-1)^{t-k}\binom{k}{t} = \frac{n!}{t!}\sum_{k=t}^{n} \frac{(-1)^{t-k}}{(t-k)!}$$

where the final equality uses $\binom{n}{k}\binom{k}{t}(n-k)! = \frac{n!}{t!(k-t)!}$.

(e) Let B_n be the board contained in the $n \times n$ grid used to solve the Problème des Ménages used in §4.3. By Exercise 4.12(b), we have

$$\sum_{t=0}^{n} h_t(B)w^t = \sum_{k=0}^{n} r_k(B)(n-k)!(w-1)^k.$$

By Exercise 4.3.4, $r_k(B) = \binom{2n-k}{k}\frac{2n}{2n-k}$. Hence taking the coefficient of w^t as in the previous exercise, we get

$$h_t(B) = \sum_{k=t}^{n} \binom{2n-k}{k}(n-k)!\binom{k}{t}(-1)^{k-t}.$$

Now following the argument in §4.3, we seat the men in $n!$ ways in the odd-numbered seats, and the women in $h_t(B)$ ways in the even numbered seats, thus putting t couples into adjacent seats. Multiplying by 2 as before to count the placements with men in even-numbered seats we get $2n!\sum_{k=t}^{n}\binom{2n-k}{k}(n-k)!\binom{k}{t}(-1)^{k-t}$ placements.

4.13 Let A_i be those placements of m non-attacking rooks on the $n \times n$ grid that *we do not want to count* because there is a rook in row i and this rook is on B.

Generalizing the colouring argument used to prove Lemma 4.3.2, suppose that we put k non-attacking black rooks on B. We then have $\binom{n-k}{m-k}^2(m-k)!$ ways to put $m-k$ white rooks on the grid so that all m rooks are non-attacking. Therefore

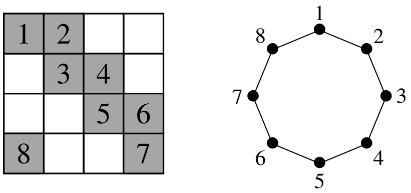
$$\sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\|I|=k}} |A_I| = r_k(B)\binom{n-k}{m-k}^2(m-k)!$$

and using the Principle of Inclusion and Exclusion as in the proof of Corollary 4.3.3, we get

$$r_m(\overline{B}) = \sum_{k=0}^{m}(-1)^k r_k(B)\binom{n-k}{m-k}^2(m-k)!$$

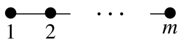
as required.

4.14 (a) Label the squares of B_n by the numbers $1,2,\ldots,2m-1,2m$ from top-left to bottom row, as shown on the left below for B_4. Then $r_k(B_n)$ is the number of ways to put k rooks on the squares of B_n so that no two rooks are on squares with consecutive numbers. (Regard $2m+1$ as 1.)



Labelling the vertices of the graph C_{2n} as shown on the right above for C_8, it is clear the number of such placements is $r_k(C_{2n})$.

(b) A similar argument to (a) shows that the graph corresponding to the staircase board S_m is the line with m vertices, shown below.



Therefore, splitting placements of k rooks on C_m according to whether or not there is a rook on vertex m, we count $r_k(S_{m-1})$ placements with no rook on vertex m, and $r_{k-1}(S_{m-3})$ placements with a rook on vertex m (and so no rook on either vertex 1 or vertex $m-1$). Hence $r_k(C_m) = r_k(S_{m-1}) + r_{k-1}(S_{m-3})$ and so $f_{C_m}(z) = f_{S_{m-1}}(z) + zf_{S_{m-3}}(z)$, as seen earlier for B_{2m} using Lemma 4.2.1. The calculation in Exercise 4.3.4 now shows that $f_{C_m}(z) = \sum_{k=0}^{m}\binom{m-k}{k}\frac{m}{m-k}z^k$.

(c) It is equivalent to show that $r_k(C_{m-1}) + r_{k-1}(C_{m-2}) = r_k(C_m)$. By (b), the left-hand side is

$$\begin{aligned}\binom{m-1-k}{k}\frac{m-1}{m-1-k}+\binom{m-1-k}{k-1}\frac{m-2}{m-1-k}\\ &=\binom{m-k}{k}\frac{1}{m-1-k}\Big(\frac{(m-2k)(m-1)}{m-k}+\frac{k(m-2)}{m-k}\Big)\\ &=\binom{m-k}{k}\frac{m}{m-k}\Big(\frac{(m-2k)(m-1)+k(m-2)}{m(m-1-k)}\Big)\\ &=\binom{m-k}{k}\frac{m}{m-k}\end{aligned}$$

which is $r_k(C_m)$ by another application of (b). As mentioned in the question, there is a much more enlightening proof using Exercise 4.18(e): if u is any vertex of C_m then C_m/u is C_{m-1} and $C_m//u$ is C_{m-2}, and so, by this exercise, $p_m(z) = p_{m-1}(z) + zp_{m-2}(z)$.

(d) Using the given polynomials we have $p_2(z)^2 = (1+2z)^2 = 1+4z+4z^2 = (1+4z+2z^2)+2z^2 = p_4(z)+z^2p_0(z)$ and $p_3(z)p_2(z) = (1+3z)(1+2z) = 1+5z+6z^2 = (1+5z+5z^2)+z^2 = p_5(z)+z^3p_1(z)$. Using (c) to get the first and last equalities below, and the inductive hypothesis for the second, we have

$$\begin{aligned}p_m(z)p_2(z) &= p_{m-1}(z)p_2(z)+zp_{m-2}p_2(z)\\ &= p_{m+1}(z)+z^2p_{m-3}(z)+zp_m(z)+z^3p_{m-4}(z)\\ &= p_{m+1}(z)+zp_m(z)+z^2\big(p_{m-3}(z)+zp_{m-4}(z)\big)\\ &= p_{m+2}(z)+z^2p_{m-2}(z)\end{aligned}$$

as required.

(e) We have $\widetilde{g}_n(w)\widetilde{g}_1(w) = w^n g_n(-w^{-1})wg_1(-w^{-1}) = w^{n+1}p_{2n}(-w^{-1})p_2(-w^{-1})$. By (d) this is

$$\begin{aligned}w^{n+1}\big(p_{2(n+1)}(-w^{-1})+(-w^{-1})^2p_{2(n-1)}(-w^{-1})\big)\\ &= w^{n+1}g_{n+1}(-w^{-1})+w^{n-1}g_{n-1}(-w^{-1})\\ &= \widetilde{g}_{n+1}(w)+\widetilde{g}_{n-1}(w).\end{aligned}$$

(f) Since $\widetilde{g}_1(w) = w-2$ generates the polynomial ring $\mathbb{C}[w]$, there is a unique ring homomorphism $\mathbb{C}[w] \to \mathbb{C}[t^{-1},t]$ that sends $w-2$ to $t^{-1}+t$ and satisfies $\theta\big(h(w)(w-2)\big) = \theta\big(h(w)\big)\theta(w-2)$ for all $h(w) \in \mathbb{C}[w]$. Suppose, inductively, that $\theta\big(\widetilde{g}_m(w)\big) = t^{-m}+t^m$ for $m \leq n$. Then

$$\begin{aligned}\theta\big(\widetilde{g}_n(w)(w-2)\big) &= \theta\big(\widetilde{g}_n(w)\big)\theta(w-2)\\ &= (t^{-n}+t^n)(t^{-1}+t) = t^{-(n+1)}+t^{n+1}+t^{-(n-1)}+t^{n-1}.\end{aligned}$$

By (e), the left-hand side is $\theta\big(\widetilde{g}_{n+1}(w)+\widetilde{g}_{n-1}(w)\big)$, and since θ is a ring homomorphism, this is $\theta\big(\widetilde{g}_{n+1}(w)\big)+\theta\big(\widetilde{g}_{n-1}(w)\big)$. Since $\theta\big(\widetilde{g}_{n-1}(w)\big)=t^{-(n-1)}+t^{n-1}$, it follows that $\theta\big(\widetilde{g}_{n+1}(w)\big)=t^{-(n+1)}+t^{n+1}$, as required for the inductive step. Since a polynomial of degree d in $\mathbb{C}[w]$ is sent to a polynomial in $\mathbb{C}[t^{-1},t]$ with leading term t^d, the homomorphism θ is injective.

(g) Since θ is a ring homomorphism,

$$\theta\big(\widetilde{g}_n(w)^2\big)=\theta\big(\widetilde{g}_n(w)\big)^2=(t^{-n}+t^n)^2=t^{-2n}+2+t^{2n}=\theta\big(\widetilde{g}_{2n}(w)+w\big).$$

Since θ is injective, it follows that $\widetilde{g}_n(w)^2=\widetilde{g}_{2n}(w)+2$, or equivalently, that

$$\big(w^n g_n(-w^{-1})\big)^2=w^{2n}g_{2n}(-w^{-1})+2.$$

Replacing $-w^{-1}$ with z we get $\big((-z^{-1})^n g_n(z)\big)^2=(-z^{-1})^{2n}g_{2n}(z)+2$. Multiplying through by z^{2n} we get $g_n(z)^2=g_{2n}(z)+2z^{2n}$.

(h) This follows in the same way as (g), using the identity

$$(t^{-\ell}+t^{\ell})(t^{-m}+t^m)=t^{-(\ell+m)}+t^{\ell+m}+t^{-(\ell-m)}+t^{\ell-m}.$$

(i) ($\star$) Label the vertices of C_{2n} by $1,2,\ldots,2n$ as shown in (a) for the case $n=4$. Let $k<n$. Given a placement of k rooks on the vertices of C_{2n} with no two rooks adjacent, there exists $j\le n$ such that neither j nor $j+n$ has a rook. Choose j minimal with this property, and split the cycle into two n-cycles with vertices $1,2,\ldots,j,j+n+1,\ldots,2n$ and $j+1,\ldots,j+n$, keeping rooks on their chosen vertices. Construction of the inverse map is left as an exercise: see Ilya Bogdanov's answer to MathOverflow Question 364978. Since $r_{B_m}(m)=2$ for all $m\in\mathbb{N}$, this bijection does all the work needed to prove that $g_n(z)^2=g_{2n}(z)+2$.

4.15 (a) Since $n=2c_2+\cdots+nc_n$, we have

$$\begin{aligned}w^n f_B(-w^{-1})&=w^n g_2(-w^{-1})^{c_2}\ldots g_n(-w^{-1})^{c_n}\\&=\big(w^2g_2(-w^{-1})\big)^{c_2}\ldots\big(w^ng_n(-w^{-1})\big)^{c_n}=\widetilde{g}_2^{c_2}\ldots\widetilde{g}_n^{c_n}.\end{aligned}$$

(b) The coefficient of t^m in the right-hand side is the number of ways to write

$$m=2c_2^+-2c_2^-+3c_3^+-3c_3^-+\cdots+nc_n^++nc_n^-$$

where $c_k^++c_k^-=c_k$ for each k. Since $kc_k^+-kc_k^-$ has the same parity as $kc_k^++kc_k^-=kc_k$, and $2c_2+\cdots+nc_n=n$, if t^m has a non-zero coefficient then $-n\le m\le n$ and m and n have the same parity.

(c) Applying the ring homomorphism θ from Exercise 4.14(f) we get

$$\begin{aligned}\theta\big(w^nf_B(-w^{-1})\big)&=\theta\big(\widetilde{g}_2(w)\big)^{c_2}\ldots\theta\big(\widetilde{g}_n(w)\big)^{c_n}\\&=(t^{-2}+t^2)^{c_2}\ldots(t^{-n}+t^n)^{c_n}=\sum_{0\le\ell\le n/2}b_\ell(t^{-(n-2\ell)}+t^{n-2\ell}).\end{aligned}$$

Since θ is injective and $\theta\left(\sum_{0\le \ell\le n/2} b_\ell \widetilde{g}_{n-2\ell}(w)\right)$ is equal to the right-hand side, we have $w^n f_B(-w^{-1}) = \sum_{0\le \ell \le n/2} b_\ell \widetilde{g}_{n-2\ell}(w)$. Now replace w with $-z^{-1}$ and use $\widetilde{g}_{n-2\ell}(w) = w^{n-2\ell} g_{n-2\ell}(-w^{-1})$ to get

$$(-z^{-1})^n f_B(z) = \sum_{0\le \ell\le n/2} (-z)^{n-2\ell} b_\ell g_{n-2\ell}(z).$$

Finally multiplying through by $(-z)^n$ gives $f_B(z) = \sum_{0\le\ell\le n/2} b_\ell z^{2\ell} g_{n-2\ell}(z)$.

(d) Apply Exercise 4.3.7 to (c) to get $r_n(\overline{B}) = \sum_{0\le \ell\le n/2} b_\ell u_{n-2\ell}$.

(f) Let B be the board contained in the $mc \times mc$ grid used in the proof of Proposition 4.3.8. By (d) we have $r_{mc}(\overline{B}) = \sum_{0\le\ell\le mc/2} b_\ell u_{mc-2\ell}$ where the coefficients b_ℓ are defined by

$$(t^{-m}+t^m)^c = \sum_{0\le \ell\le mc} b_\ell (t^{-(n-2\ell)} + t^{n-2\ell}).$$

By the Binomial Theorem, the left-hand side is

$$\sum_{k=0}^{c} \binom{c}{k} t^{-mc} t^{m(c-k)} = \sum_{k=0}^{c} \binom{c}{k} (t^{-m(c-2k)} + t^{m(c-2k)}).$$

Comparing coefficients, we see that $r_{mc}(\overline{B}) = \sum_{0\le k\le c/2} \binom{c}{k} u_{m(c-2k)}$ as required.

4.16 (a) Since

$$(t^{-2}+t^2)(t^{-3}+t^3)(t^{-4}+t^4) = (t^{-1}+t)+(t^{-3}+t^3)+(t^{-5}+t^5)+(t^{-9}+t^9)$$

it follows from Exercise 4.15(d) that $f_B(z) = z^8 g_1(z) + z^6 g_3(z) + z^4 g_5(z) + g_9(z)$ and $r_9(\overline{B}) = u_1 + u_3 + u_5 + u_9$.

(b) Since $(t^{-1}+t)(t^{-2}+t^2)(t^{-3}+t^3)(t^{-4}+t^4) = 2(t^{-2}+t^2)+2(t^{-4}+t^4)+(t^{-6}+t^6)+(t^{-8}+t^8)+(t^{-10}+t^{10})$ the generalization of Exercise 4.15(d) to products involving $g_1(z)$ implies that

$$(1+2z)f_B(z) = 2z^8 g_2(z) + 2z^6 g_4(z) + 4z^4 g_6(z) + z^2 g_8(z) + g_{10}(z).$$

Since $f_{\square}(z) = 1+z = (1+2z)-z$ and, by Lemma 4.2.2, $f_C(z) = (1+z)f_B(z)$, we have

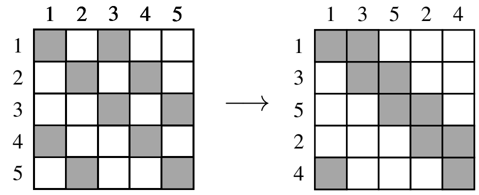
$$\begin{aligned} f_C(z) = (1+2z)f_B(z) - zf_B(z) = {}& -z^9 g_1(z) + 2z^8 g_2(z) - z^7 g_3(z) \\ & + 2z^6 g_4(z) - z^5 g_5(z) + z^4 g_6(z) + z^2 g_8(z) - z g_9(z) + g_{10}(z). \end{aligned}$$

Hence by Exercise 4.3.7, noting the signs, we get $r_{10}(\overline{B}) = u_1 + 2u_2 + u_3 + 2u_4 + u_5 + u_6 + u_8 + u_9 + u_{10}$.

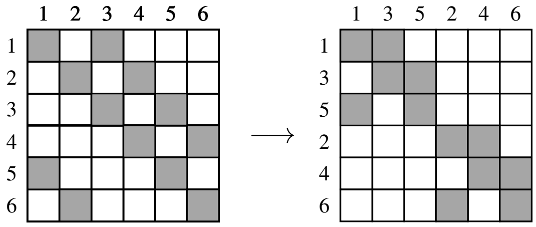
4.17 (a) A permutation $\phi : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ is discordant with both σ and τ if and only if $\phi(i) \notin \{\sigma(i),\tau(i)\}$ for each i, and so, if and only if $\sigma^{-1}\phi(i) \notin \{i,\sigma^{-1}\tau(i)\}$. Therefore the function sending ϕ to $\sigma^{-1}\phi$ is a bijection between permutations discordant with both σ and τ and permutations discordant with both the identity and $\sigma^{-1}\tau$.

(b) Let $\sigma : \{1,2\ldots,n\} \to \{1,2,\ldots,n\}$ be the n-cycle defined by $\sigma(1) = 2, \sigma(2) = 3, \ldots, \sigma(n) = 1$. Placements of n non-attacking rooks on D_n correspond to permutations discordant with both σ and σ^{-1}. By (a), such permutations are in bijection with permutations discordant with both the identity and σ^2. Let B be the board of diagonal squares in the $n \times n$ grid and all squares $\big(i,\sigma^2(i)\big)$.

If $n = 2m+1$ is odd then σ^2 is the n-cycle $(1,3,\ldots,2m+1,2,\ldots,2m)$. Hence the rows and columns of B can be reordered, as shown below for the case $n = 5$, so that B becomes the board B_n used in the Problème des Ménages. (This reordering is generalized in the proof of Lemma 9.4.1.)



If $n = 2m$ is even then $\sigma^2 = (1,3,\ldots,2m-1)(2,4,\ldots,2m)$ written in disjoint cycle notation. Hence the rows and columns of B can be reordered, as shown below for the case $n = 6$, so that B is two disjoint copies of the board B_m.



Therefore $f_B(z) = g_m(z)^2$. By Proposition 4.3.6, $f_B(z) = g_{2m}(z) + z^{2m}g_0(z)$ and so, by Exercise 4.3.7, $r_n(\overline{B}) = u_n + u_0 = u_n + 2$.

4.18 (a) The independence polynomials are $1+4z+3z^2+z^3$, $1+4z+3x^2$, $1+4z+2z^2$, $1+5z+5z^2$ and $1+5z+4z^2+z^3$, respectively.

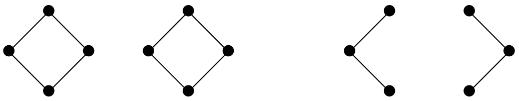
(b) Given a vertex $u \in G$, let $G\backslash u$ be G with u (and its incident edges) deleted, and let $G-u$ be G with u and all the vertices adjacent to u deleted. Then $f_G(z) = f_{G\backslash u}(z) + zf_{G-u}$.

The proof of Lemma 4.2.1 generalizes routinely: for instance, deleting u and its adjacent vertices defines a bijection between non-attacking placements of k rooks on G with a rook on u and non-attacking placements of $k-1$ rooks on $G-u$.

(c) Suppose that G can be partitioned into subsets H and H' so that no vertex in H is adjacent to a vertex of H'. Then $r_k(G) = \sum_{\ell=0}^{k} r_\ell(H) r_{k-\ell}(H')$ and $f_G(z) = f_H(z) f_{H'}(z)$.

The proof of Lemma 4.2.2 generalizes almost word-for-word; again this is a special case of Theorem 8.0.1.

(d) Applying (b) to vertex u we define the graphs $G\backslash u$ and $G-u$ shown below.



By (c) we have $f_{G\backslash u}(z) = (1+4z+2z^2)^2$. and $f_{G-u}(z) = (1+3z)^2$. Therefore

$$f_G(z) = (1+4z+2z^2)^2 + z(1+3z)^2 = 1+9z+26z^2+25z^3+4z^4.$$

(e) We give a bijective proof. Given a non-attacking placement of rooks on G, there are five cases for the vertices t, u, v. If at most one rook is on these vertices, and vertex u is unoccupied, then send the placement to the corresponding placement on G/u, as shown in the table on the left below.

$t \in G$	$u \in G$	$v \in G$	$t \in G/u$	$v \in G/u$
.	.	.	.	.
♖	.	.	♖	.
.	.	♖	.	♖

$t \in G$	$u \in G$	$v \in G$	$u' \in G/\!/u$
.	♖	.	.
♖	.	♖	♖

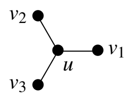
If there is a rook on u (and so no rook on t or v), remove this rook to get a non-attacking placement on $G/\!/u$; if there are rooks on both t and v (and so no rook on u), remove both these rooks and put a rook on the vertex, u' say, identifying t and v in $G/\!/u$. Since there were rooks on t and v, the new placement on $G/\!/u$ is non-attacking. As seen in the table on the right above, in both cases the number of rooks is reduced by one.

It is clear from the tables that this procedure is bijective, therefore

$$f_G(z) = f_{G/u}(z) + z f_{G/\!/u}(z)$$

as required.

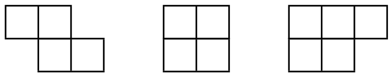
(f) Let $G(B)$ have vertices all boxes $(i,j) \in G$ and edges between all two boxes in the same row or column. Then non-attacking placements of k rooks on B are in bijection with placements of k rooks on G, with no two rooks on adjacent vertices. Hence $r_k(B) = r_k\big(G(B)\big)$ and $f_B(z) = f_{G(B)}(z)$.



(g) Label the vertices of the first graph as shown in the margin. If G is the graph of a board then each of the vertices v_1, v_2, v_3 is either in the same row or column as u. Hence two of these vertices are in the same row or column as u, and so should have an edge between them. Therefore G is not the graph of a board.

Neither is any cycle graph C_m for odd m. Since there are no triangles in C_m, steps along distinct edges must alternative moves along rows and down columns. A sequence of such moves returning to the starting point must have even length.

The remaining graphs are the graphs of the boards below.



(h) ($\star$) As a hint, part of the argument for (g) generalizes to show that each vertex is in at most two non-trivial cliques.

4.19 Let $c_j(\sigma)$ be the number of cycles of length j in the permutation σ.

(a) Let $B(\sigma)$ be the board with squares in positions $\big(i, \sigma(i)\big)$ for $i \in \{1, 2, \ldots, n\}$. Permuting the rows and columns of $B(\sigma)$ so that whenever $\big(i, \sigma(i), \ldots, \sigma^{m-1}(i)\big)$ is a cycle of σ, with i minimal, the rows and columns appear in the order i, $\sigma(i)$, $\ldots$, $\sigma^{m-1}(i)$ turns $B(\sigma)$ into the board formed by $c_j(\sigma)$ diagonally disjoint copies of the board B_{2j} in the Probléme des Ménages. Hence, by Lemma 4.2.2, the rook polynomial of B is $g_2(z)^{c_2} \ldots g_n(z)^{c_n}$. Now use Exercise 4.15(d).

(b) Polyá's Cycle Index Formula states that

$$\sum_{n=0}^{\infty} \frac{z^n}{n!} \sum_{\sigma \in \mathrm{Sym}_n} x_1^{c_1(\sigma)} \ldots x_n^{c_n(\sigma)} = \prod_{j=1}^{\infty} \exp\big(\frac{x_j}{j} z^j\big).$$

Specialize by setting $x_1 = 0$ and $x_j = t^{-j} + t^j$ to get

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{z^n}{n!} \sum_{\sigma \in \mathscr{D}_n} (t^{-2}+t^2)^{c_2(\sigma)} \ldots (t^{-n}+t^n)^{c_n(\sigma)} &= \prod_{j=1}^{\infty} \exp\big(\frac{t^{-j}+t^j}{j} z^j\big) \\ &= \exp\Big(\sum_{j=1}^{\infty} \frac{(z/t)^j}{j}\Big) \exp\Big(\sum_{j=1}^{\infty} \frac{(zt)^j}{j}\Big) \\ &= F(z/t)F(zt)\end{aligned}$$

where the final step uses that $F(z)$ is the specialization of Polyá's Cycle Index Formula by setting $x_1 = 0$ and $x_j = 1$ for $j \in \mathbb{N}$, and so $F(w) = \prod_{j=1}^{\infty} \exp \frac{w^j}{j}$. By (a), the left-hand side is

$$\sum_{n=0}^{\infty}\frac{z^n}{n!}\sum_{\sigma\in\mathscr{D}_n}\sum_{0\le\ell\le n/2}b_{n-2\ell}(t^{-(n-2\sigma)}+t^{n-2\sigma}).$$

(c) This follows from (a): note that formally replacing $t^{-0}+t^0$ with $u_0=2$ is correct, but this means that the zeroth power t^0 is replaced with $v_0=1$.

(d) Since $F(w)=\sum_{n=0}^{\infty}d_n\frac{w^n}{n!}$, we have

$$F(z/t)F(zt)=\sum_{n=0}^{\infty}\Big(\sum_{\ell=0}^{n}d_\ell d_{n-\ell}\binom{n}{\ell}t^{n-2\ell}\Big)\frac{z^n}{n!}.$$

Therefore if $0\le\ell\le n/2$, the coefficient of $z^nt^{n-2\ell}/n!$ in the right-hand side of (b) is $\sum_{\ell=0}^{n}d_\ell d_{n-\ell}\binom{n}{\ell}$. By (c), formally replacing each $t^{n-2\ell}$ with $v_{n-2\ell}$ gives the exponential generating function for $3\times n$ Latin rectangles with first row 1, 2, ..., n. The number of such Latin rectangles is therefore $\sum_{\ell=0}^{n}\binom{n}{\ell}d_\ell d_{n-\ell}v_{n-2\ell}$

Appendix 5

End notes

Introduction

Whitehead: *"Combinatorics is the slums of topology"* is reported in *Combinatorics entering the third millennium*, Peter J. Cameron, fourth draft, September 2011, `www.maths.qmul.ac.uk/~pjc/preprints/histcomb.pdf`.

Gelfand: *"The older I get, the more I believe that at the bottom of most deep mathematical problems there is a combinatorial problem."*, lecture to Courant Institute (1990), as reported in `www-history.mcs.st-and.ac.uk/Quotations/Gelfand.html`.

1. Derangements

Exercise 1.11: the misattribution of Burnside's Lemma is discussed in Peter M. Neumann, *A lemma that is not Burnside's*, The Mathematical Scientist, **4** (1979) 133–141.

Exercise 1.14, Amer. Math. Monthly **118** (2011) 463, Problem 11573, proposed by Rob Pratt, SAS Institute, Cary, NC.

2. Binomial coefficients

Al-Karaji: `www-history.mcs.st-and.ac.uk/Biographies/Al-Karaji.html`.

Exercise 2.10: Graham *et al.* (1994) (5.18).

Exercise 2.15(a): Jennifer J. Quinn, *Tonight! Epic math battles: counting vs. matching*, Math Horizon (February 2015).

Exercise 2.22: A. C. Dixon, *On the sum of the cubes of the coefficients in a certain expansion by the binomial theorem*, Messenger of Mathematics **20** (1891) 79–80.

Interlude I: The Egg Dropping Problem

Jacobi: *"man muss immer umkehren"* is reported in Edward B. Van Vleck, *Current tendencies of mathematical research*, Bull. Amer. Math. Soc. **23** (1916), 1–13. For a historical account of the early development of elliptic functions (first defined by their inverses, the elliptic integrals), see Chapter 12 of J. Stillwell, *Mathematics and its history*, Undergraduate Texts in Mathematics, Springer 2010 (2nd edition). An expository article on the egg dropping problem is Michael Boardman, *The Egg-Drop Numbers*, Mathematics Magazine **77** (2004), 368–372.

3. Principle of Inclusion and Exclusion

Eratothenes (c. 275–194 BC) was librarian at the Great Library of Alexandria. In Eratosthenes' original version of the sieve, only odd numbers were considered. He is credited with his sieve by the later writer Nicomachus of Gerasa in his *Introduction to Arithmetic* (Book II). In the example in Hoche's edition, I. 13. 2, page 31 (see `archive.org/details/nicomachigerasen00nicouoft/page/n6`), γ, ε, ζ, θ and $\iota\alpha$ stand for 3, 5, 7, 9, and 11. The square for θ is marked γ, to indicate that 3 divides 9.

4. Rook Polynomials

The exposition of the Problème des Ménages and Exercise 4.14 are based on Chapter 8 of Riordan (2002). The formula for the number of $3 \times n$ Latin rectangles in Exercise 4.17 [which will be part of the text in §9.4] was first proved by Riordan in Riordan (1946).

C. Solutions to exercises

Clay tokens, early numeracy and literacy: `http://sites.utexas.edu/dsb/tokens/tokens-and-writing-the-cognitive-development/`.

Figure A.1.1: `https://commons.wikimedia.org/wiki/File:Clay_accounting_tokens_Susa_Louvre_n2.jpg`, public domain.

References

Beasley, John D. 1989. *The mathematics of games*. Recreations in Mathematics, vol. 5. The Clarendon Press, Oxford University Press, New York.

Bryant, Victor. 1993. *Aspects of combinatorics*. Cambridge University Press, Cambridge. A wide-ranging introduction.

Butler, Fred, Mahir, Can, Haglund, Jim and Remmel, Jeffrey B. Rook Theory Notes. 57 pages.

de Bruijn, N. G. 1981. *Asymptotic methods in analysis*. third edn. Dover Publications, Inc., New York.

Erdős, P. 1942. On an elementary proof of some asymptotic formulas in the theory of partitions. *Ann. of Math. (2)*, **43**, 437–450.

Graham, Ronald L., Knuth, Donald E. and Patashnik, Oren. 1994. *Concrete Mathematics*. Addison Wesley.

Loehr, Nicholas A. 2011. *Bijective combinatorics*. Discrete Mathematics and its Applications (Boca Raton). Boca Raton, FL: CRC Press.

Riordan, John. 1946. Three-line latin rectangles. II. *Amer. Math. Monthly*, **53**, 18–20.

Riordan, John. 2002. *An introduction to combinatorial analysis*. Dover Publications, Inc., Mineola, NY. Reprint of the 1958 original [Wiley, New York; MR0096594 (20 #3077)].

van Lint, J. H. and Wilson, R. M. 2001. *A course in combinatorics*. Second edn. Cambridge University Press, Cambridge.

Wildon, Mark. 2008. Counting partitions on the abacus. *Ramanujan J.*, **17**(3), 355–367.

Wilf, Herbert S. 2006. *generatingfunctionology*. 3rd edn. A. K. Peters.

Index