Discrete Mathematics

Lecture Notes

Licence L2 — 2025–2026

Yaë Ulrich Gaba

"God made the integers; all else is the work of man."
— Leopold Kronecker

March 25, 2026

Preface

Discrete mathematics provides the theoretical backbone of computer science, combinatorics, cryptography, and many other fields of modern mathematics. Unlike continuous mathematics, which studies objects that vary smoothly, discrete mathematics is concerned with structures that are fundamentally separate and distinct: integers, graphs, logical statements, and algorithms.

These notes offer a rigorous yet accessible treatment of the core topics in discrete mathematics. Each chapter develops the theory from first principles, states and proves the main results carefully, and provides numerous worked examples and exercises.

Prerequisites. A basic familiarity with high-school algebra and an appetite for logical reasoning are the only prerequisites. No prior exposure to formal proof-writing is assumed; Chapter 2 is devoted entirely to proof techniques.

Structure. The course is organized as follows:

- Chapters 1–2 lay the logical and proof-theoretic foundations.
- Chapters 3–5 develop set theory, relations, functions, and combinatorics.
- Chapters 6–8 treat number theory, graph theory, and recurrences.
- Chapters 9–10 address Boolean algebra, automata, and further topics.

Throughout, the reader will find:

- Boxed definitions and theorems for easy reference.
- Detailed proofs with commentary on the strategy employed.
- TikZ diagrams illustrating key ideas.
- End-of-chapter exercises ranging from routine to challenging.

How to read these notes. Active engagement is essential. Attempt each example before reading the solution, and try the exercises before consulting any hints. Mathematical maturity is built through struggle, not spectation.

Notation and Conventions

We collect here the principal symbols and conventions used throughout these notes.

Symbol	**Meaning**
$\mathbb{N}$	The set of natural numbers $\{0, 1, 2, \dots\}$
$\mathbb{Z}$	The set of integers
$\mathbb{Q}$	The set of rational numbers
$\mathbb{R}$	The set of real numbers
$\mathbb{C}$	The set of complex numbers
$\mathcal{P}(A)$	The power set of A
$\lvert A\rvert$ or $\operatorname{card}(A)$	The cardinality of the set A
$\emptyset$	The empty set
$\subset$, $\subseteq$	Strict and non-strict set inclusion
$\cap$, $\cup$, $\setminus$	Intersection, union, set difference
$A \times B$	Cartesian product of A and B
$\neg$, $\wedge$, $\vee$	Logical NOT, AND, OR
$\Rightarrow$, $\Leftrightarrow$	Implication and biconditional
$\forall$, $\exists$	Universal and existential quantifiers
$n!$	Factorial of n
$\binom{n}{k}$	Binomial coefficient "n choose k"
$\lfloor x \rfloor$, $\lceil x \rceil$	Floor and ceiling of x
$a \mid b$	a divides b
$a \equiv b \pmod{n}$	a is congruent to b modulo n
$\square$ or $\square$	End of proof

Conventions.

1. We include 0 in the natural numbers: $\mathbb{N} = \{0, 1, 2, \dots\}$.
2. The notation $\{x \in S : P(x)\}$ denotes the subset of S satisfying property P.
3. All logarithms without an explicit base are taken to be base 2 (as is common in discrete mathematics and computer science).
4. The symbol $:=$ means "is defined to be."

Contents

Chapter 1

Propositional and Predicate Logic

Logic is the study of correct reasoning. In this chapter we develop the two main layers of formal logic used throughout mathematics: *propositional logic*, which deals with statements and their truth values, and *predicate logic*, which extends the framework to handle variables, properties, and quantification.

1.1 Propositions and Logical Connectives

Definition 1.1 (Proposition)**.** A **proposition** is a declarative sentence that is either *true* (T) or *false* (F), but not both.

Example 1.2. The following are propositions:

1. "$2 + 3 = 5$" (true).
2. "Every even number greater than 2 is the sum of two primes" (Goldbach's conjecture; either true or false, though currently unproven).
3. "$\sqrt{2}$ is irrational" (true).

The following are *not* propositions:

1. "What time is it?" (a question).
2. "$x + 1 = 3$" (truth value depends on x; this is a predicate, not a proposition).
3. "Do your homework!" (a command).

We denote propositions by lowercase letters $p, q, r, \ldots$ and build compound propositions using *logical connectives*.

Definition 1.3 (Logical connectives)**.** Let p and q be propositions. We define:

1. **Negation**: $\neg p$ is true when p is false, and false when p is true.
2. **Conjunction** (AND): $p \wedge q$ is true when both p and q are true.
3. **Disjunction** (OR): $p \vee q$ is true when at least one of p, q is true.
4. **Implication**: $p \Rightarrow q$ is false only when p is true and q is false.
5. **Biconditional**: $p \Leftrightarrow q$ is true when p and q have the same truth value.
6. **Exclusive or**: $p \oplus q$ is true when exactly one of p, q is true.

Remark 1.4. The implication $p \Rightarrow q$ is *vacuously true* whenever p is false. This convention may seem strange at first but is essential for mathematical reasoning. For instance, the statement "If n is a prime less than 2, then n is even" is true, because there is no prime less than 2.

1.2 Truth Tables

A *truth table* lists the truth value of a compound proposition for every possible combination of truth values of its components.

Example 1.5 (Truth table for basic connectives)**.**

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$p \oplus q$
T	T	F	T	T	T	T	F
T	F	F	F	T	F	F	T
F	T	T	F	T	T	F	T
F	F	T	F	F	T	T	F

Example 1.6 (Verifying a compound proposition)**.** Consider the proposition $(p \wedge q) \Rightarrow p$. We construct its truth table:

p	q	$p \wedge q$	$(p \wedge q) \Rightarrow p$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

Since the final column is always T, the proposition is a tautology.

1.3 Tautologies, Contradictions, and Logical Equivalence

Definition 1.7 (Tautology, contradiction, contingency)**.** A compound proposition is called:

1. a **tautology** if it is true for every assignment of truth values to its variables;
2. a **contradiction** if it is false for every assignment;
3. a **contingency** if it is neither a tautology nor a contradiction.

Definition 1.8 (Logical equivalence)**.** Two propositions α and β are **logically equivalent**, written $\alpha \equiv \beta$, if $\alpha \Leftrightarrow \beta$ is a tautology.

Theorem 1.9 (Key logical equivalences)**.** *Let p, q, r be propositions. Then:*

1. ***Double negation***: $\neg(\neg p) \equiv p$.
2. ***Commutativity***: $p \wedge q \equiv q \wedge p$; $\quad p \vee q \equiv q \vee p$.
3. ***Associativity***: $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$; $\quad (p \vee q) \vee r \equiv p \vee (q \vee r)$.
4. ***Distributivity***: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$; $\quad p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$.
5. ***Identity laws***: $p \wedge T \equiv p$; $\quad p \vee F \equiv p$.
6. ***Domination laws***: $p \vee T \equiv T$; $\quad p \wedge F \equiv F$.
7. ***Idempotent laws***: $p \wedge p \equiv p$; $\quad p \vee p \equiv p$.
8. ***Absorption laws***: $p \vee (p \wedge q) \equiv p$; $\quad p \wedge (p \vee q) \equiv p$.
9. ***Implication equivalence***: $p \Rightarrow q \equiv \neg p \vee q$.
10. ***Contrapositive***: $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$.

Proof. Each equivalence can be verified by constructing the appropriate truth table and checking that both sides yield the same column. We illustrate (9).

Proof of (9): Consider the truth table:

p	q	$p \Rightarrow q$	$\neg p$	$\neg p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Columns 3 and 5 are identical, so $p \Rightarrow q \equiv \neg p \vee q$. The remaining equivalences are verified analogously and left as exercises (Exercise 1.3). □

1.4 De Morgan's Laws

De Morgan's laws are among the most frequently used equivalences in mathematics and computer science. They describe how negation distributes over conjunction and disjunction.

Theorem 1.10 (De Morgan's laws for propositions)**.** *For any propositions p and q:*

1. $\neg(p \wedge q) \equiv \neg p \vee \neg q$.
2. $\neg(p \vee q) \equiv \neg p \wedge \neg q$.

Proof. We prove both by truth table.

Part (1):

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

Columns 4 and 7 coincide, establishing the equivalence.

Part (2): An analogous table (left to the reader) confirms $\neg(p \vee q) \equiv \neg p \wedge \neg q$. □

Remark 1.11. De Morgan's laws generalize to any finite number of propositions:

$$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv \neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n,$$

and similarly for $\vee$. This follows by induction on n (see Exercise 1.4).

1.5 Predicate Logic and Quantifiers

Propositional logic cannot express statements like "every integer greater than 1 has a prime factor." For this, we need *predicate logic*.

Definition 1.12 (Predicate)**.** A **predicate** (or **propositional function**) is an expression $P(x)$ involving a variable x that becomes a proposition when x is assigned a specific value from a **domain of discourse** D.

Example 1.13. Let $P(x)$: "$x^2 - 1 = 0$" with domain $D = \mathbb{Z}$. Then $P(1)$ is true, $P(-1)$ is true, $P(2)$ is false, and $P(0)$ is false.

Definition 1.14 (Universal and existential quantifiers)**.** Let $P(x)$ be a predicate with domain D.

1. The **universal quantification** $\forall x \in D,\ P(x)$ asserts that $P(x)$ is true for *every* x in D.
2. The **existential quantification** $\exists x \in D,\ P(x)$ asserts that $P(x)$ is true for *at least one* x in D.

Example 1.15. Let $D = \mathbb{Z}$.

1. $\forall x \in \mathbb{Z},\ x + 0 = x$ (true).
2. $\exists x \in \mathbb{Z},\ x^2 = 2$ (false, since $\sqrt{2} \notin \mathbb{Z}$).
3. $\forall n \in \mathbb{N},\ n(n+1)$ is even (true).

1.6 Negation of Quantified Statements

One of the most important skills in mathematics is correctly negating quantified statements.

Theorem 1.16 (De Morgan's laws for quantifiers)**.** *1.* $\neg\big(\forall x,\ P(x)\big) \equiv \exists x,\ \neg P(x)$.
2. $\neg\big(\exists x,\ P(x)\big) \equiv \forall x,\ \neg P(x)$.

Proof. (1) The statement $\forall x,\ P(x)$ is false exactly when there is some element x_0 in the domain for which $P(x_0)$ is false, i.e., $\neg P(x_0)$ is true. This is precisely the assertion $\exists x,\ \neg P(x)$.

(2) Similarly, $\exists x,\ P(x)$ is false exactly when *no* element satisfies P, i.e., every element satisfies $\neg P$. This gives $\forall x,\ \neg P(x)$. □

Example 1.17 (Negating a nested quantifier statement)**.** Negate the statement: "For every $\varepsilon > 0$, there exists $\delta > 0$ such that $|f(x) - L| < \varepsilon$ whenever $|x - a| < \delta$."

Solution. The statement has the form $\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x,\ (|x - a| < \delta \Rightarrow |f(x) - L| < \varepsilon)$.
Negating step by step:

$$\begin{aligned}
&\neg\Big[\forall \varepsilon > 0,\ \exists \delta > 0,\ \forall x,\ (|x - a| < \delta \Rightarrow |f(x) - L| < \varepsilon)\Big] \\
&\equiv \exists \varepsilon > 0,\ \neg\Big[\exists \delta > 0,\ \forall x,\ (|x - a| < \delta \Rightarrow |f(x) - L| < \varepsilon)\Big] \\
&\equiv \exists \varepsilon > 0,\ \forall \delta > 0,\ \neg\Big[\forall x,\ (|x - a| < \delta \Rightarrow |f(x) - L| < \varepsilon)\Big] \\
&\equiv \exists \varepsilon > 0,\ \forall \delta > 0,\ \exists x,\ \neg(|x - a| < \delta \Rightarrow |f(x) - L| < \varepsilon) \\
&\equiv \exists \varepsilon > 0,\ \forall \delta > 0,\ \exists x,\ \Big(|x - a| < \delta\ \wedge\ |f(x) - L| \geq \varepsilon\Big).
\end{aligned}$$

In words: "There exists $\varepsilon > 0$ such that for every $\delta > 0$ there is an x with $|x - a| < \delta$ and $|f(x) - L| \geq \varepsilon$."

1.7 Logic Diagrams

We can visualize the relationship between connectives and their truth conditions using TikZ diagrams.

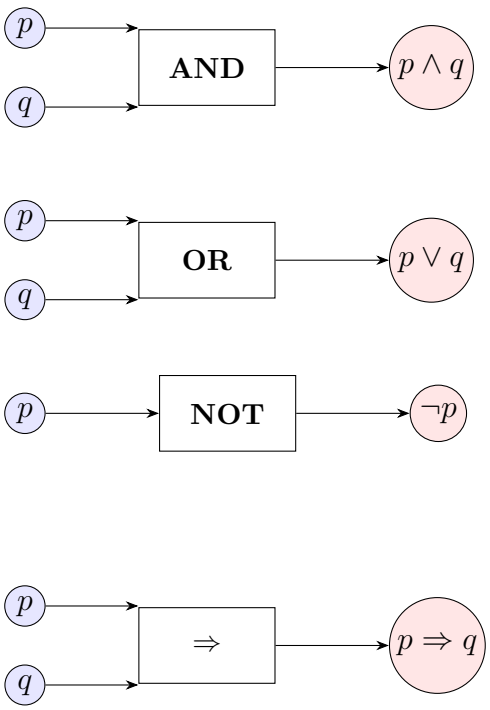


Figure 1.1: Schematic representation of basic logic gates.

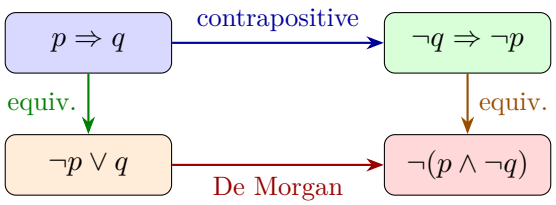


Figure 1.2: Equivalent forms of the implication $p \Rightarrow q$.

1.8 Exercises

Exercise 1.1. Classify each of the following as a proposition or not. If it is a proposition, determine its truth value.

(a) $3 + 7 = 10$.
(b) $x^2 \geq 0$.
(c) The moon is made of cheese.
(d) $\sqrt{16} = 4$.
(e) Close the door!
(f) Every prime number is odd.

Exercise 1.2. Construct truth tables for each of the following compound propositions:

(a) $(p \Rightarrow q) \wedge (q \Rightarrow p)$.
(b) $p \Rightarrow (q \Rightarrow p)$.
(c) $(p \vee q) \wedge (\neg p \vee r) \Rightarrow (q \vee r)$.

Exercise 1.3. Verify each of the equivalences in Theorem 1.9 by constructing truth tables.

Exercise 1.4. Use mathematical induction to prove the generalized De Morgan's law:

$$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \equiv \neg p_1 \vee \neg p_2 \vee \cdots \vee \neg p_n$$

for all $n \geq 2$.

Exercise 1.5. Negate each of the following statements, writing the result in positive form (i.e., push the negation inward as far as possible):

(a) $\forall x \in \mathbb{R},\ x^2 + 1 > 0$.
(b) $\exists n \in \mathbb{N},\ \forall m \in \mathbb{N},\ n \leq m$.
(c) $\forall \varepsilon > 0,\ \exists N \in \mathbb{N},\ \forall n \geq N,\ |a_n - L| < \varepsilon$.
(d) $\forall x \in \mathbb{R},\ (x > 0 \Rightarrow \exists y \in \mathbb{R},\ y^2 = x)$.

Exercise 1.6. Determine whether each of the following arguments is valid. Justify your answer using truth tables or known equivalences.

(a) $p \Rightarrow q$, $q \Rightarrow r$, therefore $p \Rightarrow r$ (hypothetical syllogism).
(b) $p \Rightarrow q$, $\neg q$, therefore $\neg p$ (modus tollens).
(c) $p \vee q$, $\neg p$, therefore q (disjunctive syllogism).
(d) $p \Rightarrow q$, q, therefore p (affirming the consequent).

Exercise 1.7. On an island, every inhabitant is either a *knight* (always tells the truth) or a *knave* (always lies). You meet two inhabitants, A and B.

(a) A says: "Both of us are knaves." What are A and B?
(b) A says: "I am a knave or B is a knight." What are A and B?

Hint: Translate each scenario into propositional logic and analyze.

1.9 Chapter Summary

- A **proposition** is a declarative sentence with a definite truth value.
- The main **logical connectives** are $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, and $\oplus$.
- A **tautology** is always true; a **contradiction** is always false.
- Two propositions are **logically equivalent** if they have the same truth table.
- **De Morgan's laws**: $\neg(p \wedge q) \equiv \neg p \vee \neg q$ and $\neg(p \vee q) \equiv \neg p \wedge \neg q$.
- A **predicate** $P(x)$ becomes a proposition when x is instantiated.
- The **universal quantifier** $\forall$ and **existential quantifier** $\exists$ bind variables in predicates.
- Negation swaps quantifiers: $\neg(\forall x,\ P(x)) \equiv \exists x,\ \neg P(x)$.

Chapter 2

Proof Techniques

A *proof* is a rigorous logical argument establishing the truth of a mathematical statement beyond any doubt. In this chapter we develop the main proof strategies: direct proof, proof by contradiction, proof by contrapositive, mathematical induction, and several additional techniques. Mastery of these methods is essential for all that follows.

2.1 Direct Proof

The most straightforward proof technique: to prove $p \Rightarrow q$, assume p is true and deduce, through a chain of logical steps, that q must also be true.

Definition 2.1 (Even and odd integers)**.** An integer n is **even** if $n = 2k$ for some integer k, and **odd** if $n = 2k + 1$ for some integer k.

Theorem 2.2. *The sum of two even integers is even.*

Proof. Let m and n be even integers. By definition, there exist integers a and b such that $m = 2a$ and $n = 2b$. Then

$$m + n = 2a + 2b = 2(a + b).$$

Since $a + b \in \mathbb{Z}$, the integer $m + n$ has the form $2k$ with $k = a + b$, so $m + n$ is even. □

Theorem 2.3. *The product of an even integer and an odd integer is even.*

Proof. Let m be even and n be odd. Write $m = 2a$ and $n = 2b + 1$ for integers a, b. Then

$$mn = 2a(2b + 1) = 2\Big(a(2b + 1)\Big).$$

Since $a(2b + 1) \in \mathbb{Z}$, the product mn is even. □

Example 2.4 (Direct proof: divisibility)**. Claim.** If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Suppose $a \mid b$ and $b \mid c$. Then there exist integers k and ℓ such that $b = ak$ and $c = b\ell$. Therefore,

$$c = b\ell = (ak)\ell = a(k\ell).$$

Since $k\ell \in \mathbb{Z}$, we conclude $a \mid c$. □

Example 2.5 (Direct proof: sum of consecutive integers)**. Claim.** For every positive integer n, the sum $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Proof. Let $S = 1 + 2 + \cdots + n$. Writing the sum in reverse order:

$$S = n + (n-1) + \cdots + 1.$$

Adding term by term:

$$2S = (1+n) + (2+n-1) + \cdots + (n+1) = n(n+1).$$

Hence $S = \frac{n(n+1)}{2}$. □

2.2 Proof by Contradiction

To prove a statement P, we assume $\neg P$ and derive a logical contradiction (a statement of the form $Q \wedge \neg Q$). Since a contradiction is always false, the assumption $\neg P$ must be false, so P is true.

Theorem 2.6. *$\sqrt{2}$ is irrational.*

Proof. Suppose, for the sake of contradiction, that $\sqrt{2}$ is rational. Then we can write $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, $b \neq 0$, and $\gcd(a, b) = 1$ (the fraction is in lowest terms).

Squaring both sides gives $2 = \frac{a^2}{b^2}$, so $a^2 = 2b^2$. This means a^2 is even, so a must be even (if a were odd, a^2 would be odd). Write $a = 2c$ for some integer c. Then

$$(2c)^2 = 2b^2 \implies 4c^2 = 2b^2 \implies b^2 = 2c^2.$$

So b^2 is even, hence b is even. But then both a and b are even, contradicting $\gcd(a, b) = 1$.

Therefore, $\sqrt{2}$ is irrational. □

Theorem 2.7. *There are infinitely many prime numbers.*

Proof. Suppose, for contradiction, that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$. Consider the integer

$$N = p_1 p_2 \cdots p_n + 1.$$

Since $N > 1$, it has a prime factor p. This prime p must be one of $p_1, \ldots, p_n$ (since these are all the primes). But $N \equiv 1 \pmod{p_i}$ for each i, so $p_i \nmid N$ for any i. This contradicts the fact that p divides N.

Therefore, there are infinitely many primes. □

Example 2.8 (Contradiction: no smallest positive rational)**. Claim.** There is no smallest positive rational number.

Proof. Suppose, for contradiction, that r is the smallest positive rational number.

Consider $\frac{r}{2}$. Since $r > 0$, we have $\frac{r}{2} > 0$, and since r is rational, $\frac{r}{2}$ is also rational. But $\frac{r}{2} < r$, contradicting the assumption that r is the smallest positive rational. Therefore, no such r exists. □

2.3 Proof by Contrapositive

To prove $p \Rightarrow q$, we can instead prove the logically equivalent statement $\neg q \Rightarrow \neg p$ (the contrapositive; see Theorem 1.9(10)). This is especially useful when the direct approach seems difficult but the negation of the conclusion provides a convenient starting point.

Theorem 2.9. *If n^2 is even, then n is even.*

Proof. We prove the contrapositive: if n is odd, then n^2 is odd.
Suppose n is odd. Then $n = 2k + 1$ for some integer k. Hence,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Since $2k^2 + 2k \in \mathbb{Z}$, the integer n^2 is odd. By the contrapositive, if n^2 is even, then n is even. □

Theorem 2.10. *For every integer n, if $3n - 1$ is even, then n is odd.*

Proof. We prove the contrapositive: if n is even, then $3n - 1$ is odd.
Suppose n is even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then

$$3n - 1 = 3(2k) - 1 = 6k - 1 = 2(3k - 1) + 1.$$

Since $3k - 1 \in \mathbb{Z}$, the integer $3n - 1$ is odd, as required. □

Example 2.11 (Contrapositive: rational square root)**. Claim.** Let n be a positive integer. If $\sqrt{n}$ is rational, then $\sqrt{n}$ is an integer.

Proof. We prove the contrapositive: if $\sqrt{n}$ is not an integer, then $\sqrt{n}$ is irrational.
Suppose $\sqrt{n}$ is not an integer, but assume for contradiction that $\sqrt{n}$ is rational. Write $\sqrt{n} = \frac{a}{b}$ with $\gcd(a, b) = 1$ and $b \geq 2$ (since $\sqrt{n}$ is not an integer). Then $n = \frac{a^2}{b^2}$, so $a^2 = nb^2$. Let p be a prime factor of b. Then $p^2 \mid b^2 \mid a^2$, so $p \mid a$, contradicting $\gcd(a, b) = 1$.
Hence, if $\sqrt{n}$ is not an integer, it is irrational. Equivalently, if $\sqrt{n}$ is rational, then $\sqrt{n}$ is an integer. □

2.4 Proof by Mathematical Induction

Mathematical induction is a fundamental proof technique for statements involving natural numbers. It exploits the well-ordered structure of $\mathbb{N}$.

Theorem 2.12 (Principle of Mathematical Induction (PMI))**.** *Let $P(n)$ be a predicate defined for integers $n \geq n_0$. If:*

1. ***Base case***: *$P(n_0)$ is true, and*
2. ***Inductive step***: *for every integer $k \geq n_0$, $P(k) \Rightarrow P(k+1)$,*

then $P(n)$ is true for all integers $n \geq n_0$.

Remark 2.13. Induction is often compared to a row of dominoes: the base case knocks over the first domino, and the inductive step ensures that each falling domino knocks over the next.

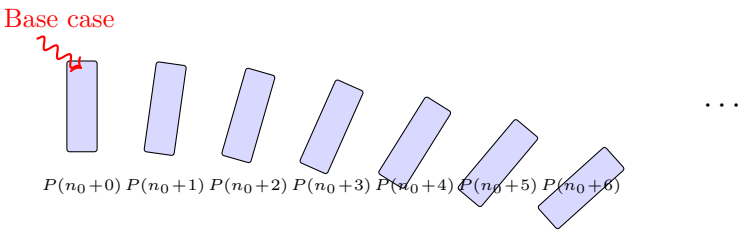


Figure 2.1: The domino analogy for mathematical induction.

Theorem 2.14. *For every positive integer n,*

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof. We proceed by induction on n.

Base case ($n = 1$): The left side is $1^2 = 1$ and the right side is $\frac{1 \cdot 2 \cdot 3}{6} = 1$. They agree.

Inductive step. Suppose the formula holds for some $k \geq 1$, i.e.,

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}. \qquad \text{(Inductive Hypothesis)}$$

We must show it holds for $k+1$:

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \left(\sum_{i=1}^{k} i^2\right) + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} \\
&= \frac{(k+1)\big[k(2k+1) + 6(k+1)\big]}{6} \\
&= \frac{(k+1)(2k^2+7k+6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} \\
&= \frac{(k+1)\Big((k+1)+1\Big)\Big(2(k+1)+1\Big)}{6}.
\end{aligned}$$

This is the formula with $n = k + 1$. By induction, the result holds for all $n \geq 1$. □

Theorem 2.15. ***(Bernoulli's inequality)*** *For every real number $x \geq -1$ and every positive integer n,*

$$(1 + x)^n \geq 1 + nx.$$

Proof. We use induction on n.

Base case ($n = 1$): $(1 + x)^1 = 1 + x = 1 + 1 \cdot x$. The inequality holds with equality.

Inductive step. Assume $(1 + x)^k \geq 1 + kx$ for some $k \geq 1$. Since $1 + x \geq 0$ (because $x \geq -1$), we may multiply both sides by $1 + x$:

$$\begin{aligned}(1 + x)^{k+1} &= (1 + x)^k \cdot (1 + x) \\ &\geq (1 + kx)(1 + x) \\ &= 1 + kx + x + kx^2 \\ &= 1 + (k + 1)x + kx^2 \\ &\geq 1 + (k + 1)x,\end{aligned}$$

where the last inequality uses $kx^2 \geq 0$. By induction, the result holds for all $n \geq 1$. □

Example 2.16 (Induction: divisibility)**. Claim.** For every non-negative integer n, $3 \mid (n^3 - n)$.

Proof. **Base case** ($n = 0$): $0^3 - 0 = 0$, and $3 \mid 0$.

Inductive step. Suppose $3 \mid (k^3 - k)$ for some $k \geq 0$. Then

$$\begin{aligned}(k + 1)^3 - (k + 1) &= k^3 + 3k^2 + 3k + 1 - k - 1 \\ &= (k^3 - k) + 3k^2 + 3k \\ &= (k^3 - k) + 3(k^2 + k).\end{aligned}$$

By the inductive hypothesis, $3 \mid (k^3 - k)$, and clearly $3 \mid 3(k^2 + k)$. Therefore $3 \mid \big[(k^3 - k) + 3(k^2 + k)\big] = (k + 1)^3 - (k + 1)$.
By induction, $3 \mid (n^3 - n)$ for all $n \geq 0$. □

2.5 Strong Induction

In *strong induction* (also called *complete induction*), the inductive hypothesis assumes $P(n_0), P(n_0 + 1), \ldots, P(k)$ are all true (not just $P(k)$) in order to prove $P(k + 1)$.

Theorem 2.17 (Principle of Strong Induction)**.** *Let $P(n)$ be a predicate defined for integers $n \geq n_0$. If:*

1. ***Base case**: $P(n_0)$ is true, and*
2. ***Inductive step**: for every $k \geq n_0$, $\big[P(n_0) \wedge P(n_0+1) \wedge \cdots \wedge P(k)\big] \Rightarrow P(k+1)$,*

then $P(n)$ is true for all $n \geq n_0$.

Remark 2.18. Strong induction is equivalent in power to ordinary (weak) induction; any proof by strong induction can be converted to one using weak induction (and vice versa). However, strong induction is often more natural when the proof of $P(k+1)$ requires information about values *earlier* than $P(k)$.

Theorem 2.19 (Fundamental Theorem of Arithmetic — existence part)**.** *Every integer $n \geq 2$ can be written as a product of primes.*

Proof. We use strong induction on n.

Base case ($n = 2$): The integer 2 is itself prime, so it is trivially a product of primes (a product with one factor).

Inductive step. Let $k \geq 2$ and assume that every integer m with $2 \leq m \leq k$ can be written as a product of primes. Consider $k+1$.

Case 1: $k+1$ is prime. Then $k+1$ is a product of primes.

Case 2: $k+1$ is composite. Then $k+1 = ab$ for some integers a, b with $2 \leq a, b \leq k$. By the strong inductive hypothesis, both a and b can be written as products of primes. Hence $k+1 = ab$ is also a product of primes.

By strong induction, every integer $n \geq 2$ is a product of primes. □

Example 2.20 (Strong induction: postage stamps)**. Claim.** Every integer amount of postage $n \geq 12$ cents can be formed using only 4-cent and 5-cent stamps.

Proof. **Base cases:**

- $n = 12$: $12 = 3 \times 4$.
- $n = 13$: $13 = 2 \times 4 + 1 \times 5$.
- $n = 14$: $14 = 1 \times 4 + 2 \times 5$.
- $n = 15$: $15 = 3 \times 5$.

Inductive step. Let $k \geq 15$ and assume the claim holds for all integers m with $12 \leq m \leq k$. We prove it for $k+1$.

Since $k+1 \geq 16$, we have $k+1-4 = k-3 \geq 12$. By the strong inductive hypothesis, $k-3$ can be formed using 4-cent and 5-cent stamps. Adding one more 4-cent stamp gives $k+1$ cents.

By strong induction, the claim holds for all $n \geq 12$. □

2.6 The Pigeonhole Principle

The pigeonhole principle is a deceptively simple counting argument with surprisingly powerful applications.

Theorem 2.21 (Pigeonhole Principle)**.** *If $n+1$ or more objects are placed into n containers, then at least one container holds two or more objects.*

Proof. We prove the contrapositive. Suppose every container holds at most one object. Then the total number of objects is at most $n \cdot 1 = n$. Hence, if the number of objects exceeds n, at least one container must hold at least two objects. □

Theorem 2.22 (Generalized Pigeonhole Principle)**.** *If N objects are placed into k containers, then at least one container holds at least $\lceil N/k \rceil$ objects.*

Proof. Suppose, for contradiction, that every container holds at most $\lceil N/k \rceil - 1$ objects. Then the total number of objects is at most

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k \cdot \frac{N}{k} = N,$$

where we used $\lceil N/k \rceil - 1 < N/k$. This contradicts the fact that there are N objects in total. □

Example 2.23 (Pigeonhole: birthdays)**.** In any group of 367 people, at least two must share the same birthday (since there are at most 366 possible birthdays, including February 29).

Example 2.24 (Pigeonhole: socks in the dark)**.** A drawer contains 10 black socks and 10 white socks. How many socks must you draw (in the dark) to guarantee a matching pair?
Solution. The "containers" are the 2 colors. By the pigeonhole principle, drawing 3 socks guarantees at least $\lceil 3/2 \rceil = 2$ socks of the same color.

Example 2.25 (Pigeonhole: subset sums)**. Claim.** Given any set of $n+1$ integers from $\{1, 2, \ldots, 2n\}$, there must be two elements in the set such that one divides the other.

Proof. Write each element a in the form $a = 2^s \cdot m$ where m is odd. The odd part m must be one of the n odd numbers $1, 3, 5, \ldots, 2n-1$ (the "containers"). Since there are $n+1$ elements and only n possible odd parts, by the pigeonhole principle two elements share the same odd part, say $a = 2^s m$ and $b = 2^t m$ with $s < t$. Then $a \mid b$. □

Example 2.26 (Pigeonhole: lattice points)**. Claim.** Among any five points chosen from the integer lattice $\mathbb{Z}^2$, some pair has a midpoint that is also a lattice point.

Proof. Each lattice point (x, y) can be classified by the parities of x and y: $(even, even)$, $(even, odd)$, $(odd, even)$, or (odd, odd). These give 4 classes. Among 5 points, by the pigeonhole principle, at least two belong to the same class, say (x_1, y_1) and (x_2, y_2) with $x_1 \equiv x_2 \pmod 2$ and $y_1 \equiv y_2 \pmod 2$. Their midpoint is

$$\left(\frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2}\right),$$

which has integer coordinates because $x_1 + x_2$ and $y_1 + y_2$ are both even. □

2.7 The Well-Ordering Principle

Theorem 2.27 (Well-Ordering Principle)**.** *Every non-empty subset of* $\mathbb{N}$ *has a least element.*

Remark 2.28. The Well-Ordering Principle is logically equivalent to the Principle of Mathematical Induction. We take the Well-Ordering Principle as an axiom (it follows from the Peano axioms for $\mathbb{N}$) and note that proofs using it have a distinctive flavour: one considers the set of counterexamples, argues it is non-empty if the statement fails, then derives a contradiction from the existence of a minimal counterexample.

Example 2.29 (Well-ordering proof: division algorithm)**. Claim (Division Algorithm).** For every integer a and positive integer d, there exist unique integers q (quotient) and r (remainder) such that $a = dq + r$ and $0 \leq r < d$.

Proof of existence. Consider the set

$$S = \{a - dk : k \in \mathbb{Z},\ a - dk \geq 0\}.$$

This set is non-empty: if $a \geq 0$, take $k = 0$; if $a < 0$, take $k = a$ (then $a - da = a(1 - d) \geq 0$ since $d \geq 1$ and $a < 0$).
Since $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, the Well-Ordering Principle guarantees that S has a least element $r = a - dq$ for some q.
We claim $r < d$. Suppose for contradiction that $r \geq d$. Then

$$a - d(q + 1) = r - d \geq 0,$$

so $r - d \in S$. But $r - d < r$, contradicting the minimality of r. Therefore $0 \leq r < d$, as required. □

Example 2.30 (Well-ordering proof: every positive integer ≥ 2 has a prime factor)**. Claim.** Every integer $n \geq 2$ has a prime factor.

Proof. Suppose the claim is false. Let $S = \{n \in \mathbb{Z} : n \geq 2$ and n has no prime factor$\}$. By assumption, S is non-empty. By the Well-Ordering Principle, S has a least element m.
Since $m \in S$, the integer m has no prime factor. In particular, m itself is not prime (since every prime is its own prime factor). So m is composite: $m = ab$ with $2 \leq a, b < m$. Since $a < m$ and m is the least element of S, the integer a has a prime factor p. But $p \mid a$ and $a \mid m$ imply $p \mid m$, contradicting $m \in S$.
Therefore $S = \emptyset$, and every integer $n \geq 2$ has a prime factor. □

2.8 Additional Examples and Techniques

We gather several more worked examples that combine the techniques introduced above.

Example 2.31 (Proof by cases)**. Claim.** For every integer n, the integer $n^2 + n$ is even.

Proof. We consider two cases.
Case 1: n is even. Write $n = 2k$. Then $n^2 + n = 4k^2 + 2k = 2(2k^2 + k)$, which is even.
Case 2: n is odd. Write $n = 2k + 1$. Then $n^2 + n = (2k + 1)^2 + (2k + 1) = 4k^2 + 4k + 1 + 2k + 1 = 4k^2 + 6k + 2 = 2(2k^2 + 3k + 1)$, which is even.
In both cases, $n^2 + n$ is even. □

Example 2.32 (Existence proof)**. Claim.** There exist irrational numbers a and b such that a^b is rational.

Proof. Consider $\sqrt{2}^{\sqrt{2}}$. This number is either rational or irrational.
Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Then take $a = b = \sqrt{2}$ (both irrational), and a^b is rational. Done.
Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Then take $a = \sqrt{2}^{\sqrt{2}}$ (irrational by assumption) and $b = \sqrt{2}$ (irrational). We get

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

which is rational.
In both cases, we have found irrational a, b with a^b rational. □

Example 2.33 (Uniqueness proof)**. Claim.** The additive identity in $\mathbb{Z}$ is unique: if $e \in \mathbb{Z}$ satisfies $n + e = n$ for all $n \in \mathbb{Z}$, then $e = 0$.

Proof. Suppose e and e' are both additive identities. Then $e = e + e' = e'$, where the first equality uses that e' is an identity and the second uses that e is an identity. □

Example 2.34 (Constructive proof: rational between any two reals)**. Claim.** Between any two distinct real numbers there is a rational number.

Proof. Let $a < b$ be real numbers. The Archimedean property guarantees the existence of a positive integer n such that $n(b-a) > 1$, i.e., $nb - na > 1$. Therefore, there exists an integer m with $na < m < nb$ (since the interval (na, nb) has length greater than 1). Dividing by n:

$$a < \frac{m}{n} < b.$$

The number $\frac{m}{n}$ is rational and lies strictly between a and b. □

2.9 Exercises

Exercise 2.1. Prove each of the following by direct proof:
(a) The sum of two odd integers is even.
(b) If n is odd, then n^2 is odd.

(c) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
(d) For all $n \in \mathbb{N}$, $n^3 - n$ is divisible by 6.

Exercise 2.2. Prove each of the following by contradiction:
(a) $\sqrt{3}$ is irrational.
(b) If n^2 is odd, then n is odd.
(c) There is no largest integer.
(d) The sum of a rational number and an irrational number is irrational.

Exercise 2.3. Prove each of the following by contrapositive:
(a) If n^2 is divisible by 3, then n is divisible by 3.
(b) If $x + y \geq 2$, then $x \geq 1$ or $y \geq 1$.
(c) If $n^3 + 5$ is odd, then n is even.

Exercise 2.4. Prove each of the following by mathematical induction:
(a) $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$ for all $n \geq 1$.
(b) $2^n > n^2$ for all $n \geq 5$.
(c) $n! > 2^n$ for all $n \geq 4$.
(d) $\displaystyle\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$ for all $n \geq 0$.

Exercise 2.5. Prove each of the following by strong induction:
(a) Every integer $n \geq 2$ is either prime or can be expressed as a product of two or more primes.
(b) Every positive integer can be represented as a sum of distinct powers of 2 (binary representation).
(c) The Fibonacci sequence, defined by $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$, satisfies $F_n < 2^n$ for all $n \geq 1$.

Exercise 2.6. Solve each of the following using the pigeonhole principle:
(a) Show that among any $n + 1$ integers chosen from $\{1, 2, \ldots, 2n\}$, there must be a pair of consecutive integers.
(b) Show that in any group of 6 people, there are either 3 mutual friends or 3 mutual strangers. *(Hint: consider the edges of K_6 colored with two colors.)*
(c) Prove that for every positive integer n, there is a multiple of n whose decimal representation consists entirely of 0s and 1s. *(Hint: consider the numbers $1, 11, 111, \ldots$)*
(d) Show that among any 52 integers, there exist two whose difference is divisible by 51.

Exercise 2.7. Use the Well-Ordering Principle to prove:
(a) There is no integer between 0 and 1.
(b) For every pair of positive integers a and b with $a \mid b$ and $b \mid a$, we have $a = b$.

Exercise 2.8. Prove or disprove each of the following (choose any appropriate method):
(a) For every integer n, $n^2 + n + 41$ is prime.
(b) If $a^2 \mid b^2$, then $a \mid b$ (where a, b are positive integers).
(c) For all positive reals x and y, $\frac{x+y}{2} \geq \sqrt{xy}$ (the AM–GM inequality).
(d) Every integer of the form $4k + 3$ has a prime factor of the form $4j + 3$.

2.10 Chapter Summary

- A **direct proof** of $p \Rightarrow q$ assumes p and derives q.
- A **proof by contradiction** assumes $\neg P$ and derives a contradiction, thereby establishing P.
- A **proof by contrapositive** of $p \Rightarrow q$ proves the equivalent statement $\neg q \Rightarrow \neg p$.
- **Mathematical induction** (weak) proves $P(n)$ for all $n \geq n_0$ by establishing a base case and an implication $P(k) \Rightarrow P(k+1)$.
- **Strong induction** allows the inductive hypothesis to assume $P(n_0), \ldots, P(k)$ when proving $P(k+1)$.
- The **Pigeonhole Principle**: if $n+1$ objects go into n boxes, some box contains at least two objects. The generalized version gives a lower bound of $\lceil N/k \rceil$.
- The **Well-Ordering Principle**: every non-empty subset of $\mathbb{N}$ has a least element. It is equivalent to induction.
- Other proof strategies include *proof by cases*, *existence proofs*, *uniqueness proofs*, and *constructive proofs*.

Chapter 3

Sets, Relations, and Functions

"A set is a Many that allows itself to be thought of as a One."
— Georg Cantor

Sets are the foundational language of modern mathematics. In this chapter we develop the core notions of set theory, explore relations (with special attention to equivalence relations and partial orders), and study functions as a particular type of relation. We conclude with a discussion of cardinality and Cantor's landmark diagonal argument.

3.1 Sets and subsets

Definition 3.1 (Set)**.** A *set* is an unordered collection of distinct objects, called the *elements* (or *members*) of the set. If x is an element of a set A we write $x \in A$; otherwise $x \notin A$.

A set may be specified by *roster notation*, $A = \{1, 2, 3\}$, or by *set-builder notation*, $A = \{x \in \mathbb{Z} : x^2 < 10\}$.

Definition 3.2 (Subset)**.** Let A and B be sets. We say A is a *subset* of B, written $A \subseteq B$, if every element of A belongs to B:

$$A \subseteq B \iff \big(\forall x,\ x \in A \implies x \in B\big).$$

If $A \subseteq B$ and $A \neq B$, we write $A \subsetneq B$ and call A a *proper subset* of B.

Definition 3.3 (Set equality)**.** Two sets A and B are *equal*, written $A = B$, if and only if $A \subseteq B$ and $B \subseteq A$.

Definition 3.4 (Empty set)**.** The *empty set*, denoted $\varnothing$, is the unique set with no elements. For every set A we have $\varnothing \subseteq A$.

3.2 Power set and Cartesian product

Definition 3.5 (Power set)**.** The *power set* of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A:

$$\mathcal{P}(A) = \{S : S \subseteq A\}.$$

Example 3.6. If $A = \{1, 2, 3\}$, then

$$\mathcal{P}(A) = \Big\{\varnothing,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\Big\}.$$

In particular $\operatorname{card}\mathcal{P}(A) = 2^3 = 8$.

Proposition 3.7. *If A is a finite set with* $\operatorname{card} A = n$*, then* $\operatorname{card}\mathcal{P}(A) = 2^n$.

Proof. Each subset of A is determined by, for each of the n elements, choosing whether to include it or not. There are 2 choices per element and the choices are independent, giving 2^n subsets in total. □

Definition 3.8 (Cartesian product)**.** The *Cartesian product* of sets A and B is

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

More generally, $A_1 \times A_2 \times \cdots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i \text{ for each } i\}$.

3.3 Set operations

Definition 3.9 (Union, intersection, difference, complement)**.** Let A and B be subsets of a universal set U.

(i) **Union:** $A \cup B = \{x : x \in A \text{ or } x \in B\}$.

(ii) **Intersection:** $A \cap B = \{x : x \in A \text{ and } x \in B\}$.

(iii) **Difference:** $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$.

(iv) **Complement:** $A^c = U \setminus A = \{x \in U : x \notin A\}$.

(v) **Symmetric difference:** $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Theorem 3.10 (De Morgan's Laws)**.** *Let A and B be subsets of a universal set U. Then:*

(i) $(A \cup B)^c = A^c \cap B^c$,

(ii) $(A \cap B)^c = A^c \cup B^c$.

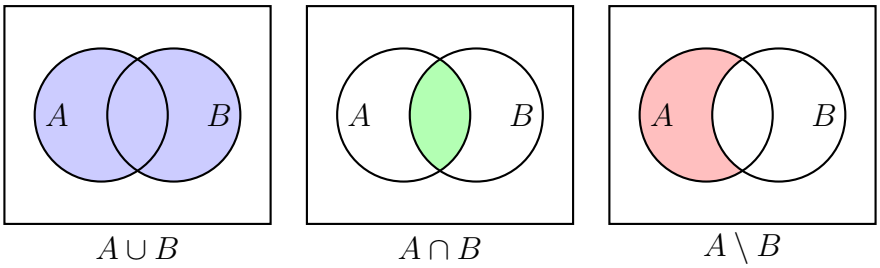


Figure 3.1: Venn diagrams for union, intersection, and set difference.

Proof. We prove (i); the proof of (ii) is analogous.

($\subseteq$) Let $x \in (A \cup B)^c$. Then $x \notin A \cup B$, which means $x \notin A$ and $x \notin B$. Hence $x \in A^c$ and $x \in B^c$, so $x \in A^c \cap B^c$.

($\supseteq$) Let $x \in A^c \cap B^c$. Then $x \notin A$ and $x \notin B$. Therefore $x \notin A \cup B$, i.e. $x \in (A \cup B)^c$.

Since each side is a subset of the other, equality holds. □

Remark 3.11. De Morgan's laws generalise to arbitrary families of sets: $\left(\bigcup_{i \in I} A_i\right)^c = \bigcap_{i \in I} A_i^c$ and $\left(\bigcap_{i \in I} A_i\right)^c = \bigcup_{i \in I} A_i^c$.

3.4 Relations

Definition 3.12 (Binary relation)**.** A *binary relation* R from a set A to a set B is a subset $R \subseteq A \times B$. We often write $a \, R \, b$ instead of $(a, b) \in R$. When $B = A$, we say R is a relation *on* A.

Definition 3.13 (Properties of relations)**.** Let R be a relation on a set A. We say R is:

(i) **reflexive** if $a \, R \, a$ for all $a \in A$;

(ii) **symmetric** if $a \, R \, b \implies b \, R \, a$;

(iii) **antisymmetric** if $a \, R \, b$ and $b \, R \, a$ imply $a = b$;

(iv) **transitive** if $a \, R \, b$ and $b \, R \, c$ imply $a \, R \, c$.

3.4.1 Equivalence relations and partitions

Definition 3.14 (Equivalence relation)**.** A relation $\sim$ on a set A is an *equivalence relation* if it is reflexive, symmetric, and transitive.

Definition 3.15 (Equivalence class)**.** Let $\sim$ be an equivalence relation on A and let $a \in A$. The *equivalence class* of a is

$$[a] = \{x \in A : x \sim a\}.$$

The set of all equivalence classes is called the *quotient set* and denoted $A/\sim$.

Definition 3.16 (Partition)**.** A *partition* of a set A is a collection $\mathcal{P}$ of non-empty, pairwise disjoint subsets of A whose union is A:

(i) $P \neq \varnothing$ for every $P \in \mathcal{P}$;

(ii) $P \cap Q = \varnothing$ for all $P, Q \in \mathcal{P}$ with $P \neq Q$;

(iii) $\bigcup_{P \in \mathcal{P}} P = A$.

Theorem 3.17 (Partition theorem)**.** *Let A be a non-empty set.*

(a) If $\sim$ is an equivalence relation on A, then the collection of equivalence classes $A/\sim$ is a partition of A.

(b) Conversely, if $\mathcal{P}$ is a partition of A, then the relation $\sim_{\mathcal{P}}$ defined by $a \sim_{\mathcal{P}} b$ if and only if a and b belong to the same block of $\mathcal{P}$ is an equivalence relation on A, and $A/\sim_{\mathcal{P}} = \mathcal{P}$.

Proof. **(a)** We verify the three conditions of a partition.

(i) For every $a \in A$, reflexivity gives $a \sim a$, so $a \in [a]$ and each class is non-empty.

(iii) Since every $a \in A$ belongs to $[a]$, we have $A = \bigcup_{a \in A} [a]$.

(ii) Suppose $[a] \cap [b] \neq \varnothing$; pick $c \in [a] \cap [b]$. Then $c \sim a$ and $c \sim b$. By symmetry, $a \sim c$, and by transitivity $a \sim b$. For any $x \in [a]$ we have $x \sim a \sim b$, so $x \in [b]$; hence $[a] \subseteq [b]$. By a symmetric argument $[b] \subseteq [a]$, giving $[a] = [b]$.

(b) Define $a \sim_{\mathcal{P}} b$ iff there exists $P \in \mathcal{P}$ with $a, b \in P$.

Reflexive: Since $\mathcal{P}$ covers A, every a belongs to some block, so $a \sim_{\mathcal{P}} a$.

Symmetric: If $a, b \in P$, then $b, a \in P$.

Transitive: If $a, b \in P$ and $b, c \in Q$, then $b \in P \cap Q$. Since blocks are pairwise disjoint, $P = Q$, so $a, c \in P$.

Finally, the class $[a]$ equals the unique block containing a, so $A/\sim_{\mathcal{P}} = \mathcal{P}$. □

Example 3.18. Fix $n \geq 1$. The relation $\equiv \pmod{n}$ on $\mathbb{Z}$ is an equivalence relation. The equivalence classes are the residue classes $[0], [1], \ldots, [n-1]$, which partition $\mathbb{Z}$.

3.4.2 Partial orders and Hasse diagrams

Definition 3.19 (Partial order)**.** A relation $\preceq$ on a set A is a *partial order* if it is reflexive, antisymmetric, and transitive. The pair $(A, \preceq)$ is called a *partially ordered set* (or *poset*).

Example 3.20. On $\mathbb{N}^*$, the divisibility relation $a \mid b$ defines a partial order.

Definition 3.21 (Hasse diagram)**.** A *Hasse diagram* for a finite poset $(A, \preceq)$ is a graph in which:

(i) each element of A is a vertex;

(ii) if $a \prec b$ and there is no c with $a \prec c \prec b$ (i.e. b *covers* a), an edge is drawn from a upward to b;

(iii) edges implied by transitivity are omitted.

Example 3.22. The Hasse diagram of the divisors of 12, ordered by divisibility:

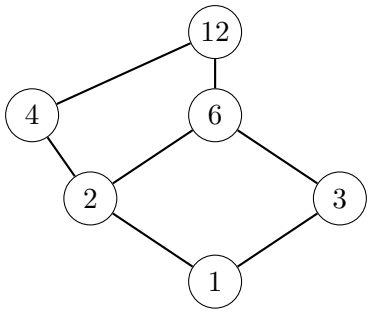


Figure 3.2: Hasse diagram for $(\{1, 2, 3, 4, 6, 12\}, \mid)$.

Definition 3.23 (Total order)**.** A partial order $\preceq$ on A is a *total* (or *linear*) order if for all $a, b \in A$, either $a \preceq b$ or $b \preceq a$. In this case $(A, \preceq)$ is called a *chain*.

Example 3.24. The usual $\leq$ on $\mathbb{R}$ is a total order. By contrast, divisibility on $\mathbb{N}^*$ is not total: neither $2 \mid 3$ nor $3 \mid 2$.

3.5 Functions

Definition 3.25 (Function)**.** A *function* (or *map*) $f \colon A \to B$ is a relation $f \subseteq A \times B$ such that for every $a \in A$ there exists exactly one $b \in B$ with $(a, b) \in f$. We write $b = f(a)$. The set A is the *domain*, and B is the *codomain*. The *image* (or *range*) of f is $\operatorname{im}(f) = \{f(a) : a \in A\}$.

Definition 3.26 (Injection, surjection, bijection)**.** Let $f \colon A \to B$.

(i) f is *injective* (one-to-one) if $f(a_1) = f(a_2) \implies a_1 = a_2$.

(ii) f is *surjective* (onto) if for every $b \in B$ there exists $a \in A$ with $f(a) = b$.

(iii) f is *bijective* if it is both injective and surjective.

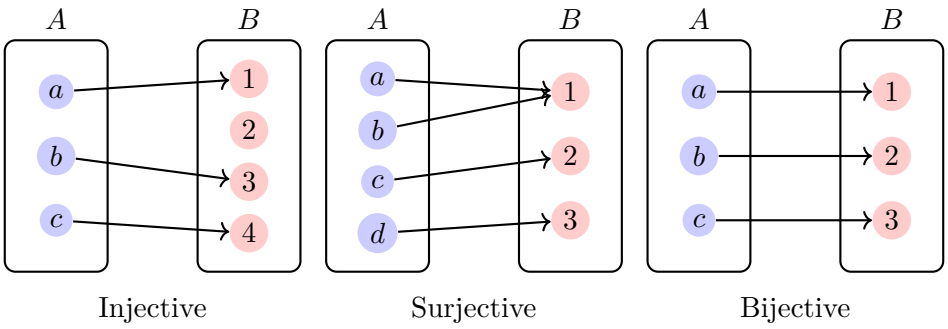


Figure 3.3: Diagrams illustrating injection, surjection, and bijection.

Definition 3.27 (Composition)**.** Given $f\colon A \to B$ and $g\colon B \to C$, the *composition* $g \circ f\colon A \to C$ is defined by $(g \circ f)(a) = g(f(a))$.

Proposition 3.28. *(i) If f and g are injective, then $g \circ f$ is injective.*

(ii) If f and g are surjective, then $g \circ f$ is surjective.

(iii) If f and g are bijective, then $g \circ f$ is bijective.

Proof. (i) Suppose $(g \circ f)(a_1) = (g \circ f)(a_2)$. Then $g(f(a_1)) = g(f(a_2))$. Since g is injective, $f(a_1) = f(a_2)$. Since f is injective, $a_1 = a_2$.

(ii) Let $c \in C$. Since g is surjective, there exists $b \in B$ with $g(b) = c$. Since f is surjective, there exists $a \in A$ with $f(a) = b$. Then $(g \circ f)(a) = g(b) = c$.

(iii) This follows immediately from (i) and (ii). □

Definition 3.29 (Inverse function)**.** Let $f\colon A \to B$ be a bijection. The *inverse* of f is the function $f^{-1}\colon B \to A$ defined by $f^{-1}(b) = a$ where a is the unique element of A satisfying $f(a) = b$.

Proposition 3.30. *A function $f\colon A \to B$ is bijective if and only if there exists a function $g\colon B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.*

Proof. ($\Rightarrow$) Take $g = f^{-1}$. For all $a \in A$, $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = a$, and for all $b \in B$, $(f \circ f^{-1})(b) = f(f^{-1}(b)) = b$.

($\Leftarrow$) Suppose such g exists. If $f(a_1) = f(a_2)$, apply g: $a_1 = g(f(a_1)) = g(f(a_2)) = a_2$, so f is injective. Given $b \in B$, set $a = g(b)$; then $f(a) = f(g(b)) = b$, so f is surjective. □

3.6 Cardinality

Definition 3.31 (Equinumerous sets)**.** Two sets A and B are *equinumerous*, written $\operatorname{card} A = \operatorname{card} B$, if there exists a bijection $f\colon A \to B$.

Definition 3.32 (Countable set)**.** A set A is *countably infinite* if $\operatorname{card} A = \operatorname{card} \mathbb{N}$, i.e. there exists a bijection $A \to \mathbb{N}$. A set is *countable* if it is finite or countably infinite. A set that is not countable is *uncountable*.

Proposition 3.33. *$\mathbb{Z}$ is countable.*

Proof. The function $f\colon \mathbb{N} \to \mathbb{Z}$ defined by

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ is even,} \\ -(n+1)/2 & \text{if } n \text{ is odd,} \end{cases}$$

is a bijection: the sequence of values is $0, -1, 1, -2, 2, -3, 3, \ldots$ □

Proposition 3.34. *$\mathbb{Q}$ is countable.*

Proof sketch. List the positive rationals by diagonalising the grid of fractions p/q (with $p, q \geq 1$), skipping those already encountered. This produces an enumeration of $\mathbb{Q}^+$; interleave with the negatives to enumerate all of $\mathbb{Q}$. □

Theorem 3.35 (Cantor's diagonal argument)**.** *The set $\mathbb{R}$ is uncountable. More precisely, the interval $(0, 1)$ is uncountable.*

Proof. Suppose for contradiction that $(0, 1)$ is countable. Then we can list its elements as $r_1, r_2, r_3, \ldots$, where each r_n has a decimal expansion

$$r_n = 0.d_{n1}\, d_{n2}\, d_{n3} \cdots$$

(choosing the non-terminating expansion when ambiguous).

Define a real number $r^* = 0.d_1^*\, d_2^*\, d_3^* \cdots$ by

$$d_k^* = \begin{cases} 3 & \text{if } d_{kk} \neq 3, \\ 7 & \text{if } d_{kk} = 3. \end{cases}$$

Then $r^* \in (0, 1)$ (it has no digits 0 or 9, so it lies strictly between 0 and 1 and its expansion does not terminate). For every $n \in \mathbb{N}^*$, the n-th digit of r^* differs from the n-th digit of r_n, so $r^* \neq r_n$. This contradicts the assumption that every element of $(0, 1)$ appears in the list. Therefore $(0, 1)$ is uncountable. □

Corollary 3.36. *$\mathcal{P}(\mathbb{N})$ is uncountable.*

Proof. The map $S \mapsto \sum_{n \in S} 2^{-(n+1)}$ gives an injection $\mathcal{P}(\mathbb{N}) \hookrightarrow [0, 1]$, and the argument above shows $\operatorname{card} \mathcal{P}(\mathbb{N}) = \operatorname{card} \mathbb{R} > \operatorname{card} \mathbb{N}$. □

Theorem 3.37 (Cantor)**.** *For any set A, there is no surjection $A \to \mathcal{P}(A)$. In particular* $\operatorname{card} A < \operatorname{card} \mathcal{P}(A)$.

Proof. Suppose for contradiction that $f\colon A \to \mathcal{P}(A)$ is surjective. Define $D = \{a \in A : a \notin f(a)\}$. Since $D \subseteq A$, we have $D \in \mathcal{P}(A)$, so by surjectivity there exists $d \in A$ with $f(d) = D$. Now ask: is $d \in D$?

If $d \in D$, then by definition of D, $d \notin f(d) = D$, a contradiction. If $d \notin D$, then $d \notin f(d)$ is false, i.e. $d \in f(d) = D$, again a contradiction. Hence no such surjection exists. □

3.7 Exercises

Exercise 3.1. Prove the following set identities for arbitrary sets A, B, C:

(a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (distributivity of $\cap$ over $\cup$).

(b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (distributivity of $\cup$ over $\cap$).

(c) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Exercise 3.2. Let $A = \mathbb{Z}$ and define $a \sim b$ iff $3 \mid (a - b)$.

(a) Prove that $\sim$ is an equivalence relation.

(b) List all the equivalence classes explicitly.

(c) Draw a diagram showing how the classes partition $\mathbb{Z}$.

Exercise 3.3. Draw the Hasse diagram of $(\mathcal{P}(\{a, b, c\}), \subseteq)$.

Exercise 3.4. Let A and B be finite sets with $\operatorname{card} A = m$ and $\operatorname{card} B = n$.

(a) Prove that if there exists an injection $A \hookrightarrow B$, then $m \leq n$.

(b) Prove that if there exists a surjection $A \twoheadrightarrow B$, then $m \geq n$.

(c) Prove that $\operatorname{card} A = \operatorname{card} B$ if and only if there exists a bijection $A \to B$.

Exercise 3.5. (Cantor–Bernstein–Schröder, statement only.) Suppose there exist injections $f\colon A \hookrightarrow B$ and $g\colon B \hookrightarrow A$. Use this to argue informally that $\operatorname{card} A = \operatorname{card} B$. (A full proof is beyond the scope of this course.)

Exercise 3.6. Prove that the set of irrational numbers $\mathbb{R} \setminus \mathbb{Q}$ is uncountable. *Hint:* if $\mathbb{Q}$ and $\mathbb{R} \setminus \mathbb{Q}$ were both countable, what would follow about $\mathbb{R}$?

Exercise 3.7. Let $f\colon A \to B$ and $g\colon B \to C$.

(a) Show that if $g \circ f$ is injective, then f is injective.

(b) Show that if $g \circ f$ is surjective, then g is surjective.

(c) Give an example where $g \circ f$ is bijective but neither f nor g is bijective.

3.8 Chapter summary

- A **set** is an unordered collection of distinct objects; key operations are union, intersection, difference, and complement.
- **De Morgan's laws** relate complements of unions and intersections.
- A **relation** on A is a subset of $A \times A$. Equivalence relations (reflexive, symmetric, transitive) produce partitions; partial orders (reflexive, antisymmetric, transitive) are visualised with Hasse diagrams.
- A **function** $f\colon A \to B$ is injective, surjective, or bijective; bijections have inverses.
- **Cantor's diagonal argument** proves $\mathbb{R}$ is uncountable, and Cantor's theorem shows $\operatorname{card} A < \operatorname{card} \mathcal{P}(A)$ for every set A.

Chapter 4

Combinatorics — Counting

"To count is to enumerate without repetition and without omission."
— traditional

Combinatorics is the art and science of counting. In this chapter we develop the fundamental counting principles, study permutations and combinations, prove the binomial theorem and Vandermonde's identity, and explore further topics such as multiset coefficients, stars and bars, and derangements.

4.1 Basic counting principles

Theorem 4.1 (Addition principle)**.** *If $A_1, A_2, \dots, A_k$ are pairwise disjoint finite sets, then*

$$\operatorname{card} A_1 \cup A_2 \cup \cdots \cup A_k = \operatorname{card} A_1 + \operatorname{card} A_2 + \cdots + \operatorname{card} A_k.$$

Theorem 4.2 (Multiplication principle)**.** *If a procedure consists of k successive stages, with n_i choices at stage i (independent of earlier choices), then the total number of outcomes is*

$$n_1 \cdot n_2 \cdots n_k.$$

Equivalently, $\operatorname{card} A_1 \times A_2 \times \cdots \times A_k = \operatorname{card} A_1 \cdot \operatorname{card} A_2 \cdots \operatorname{card} A_k$.

Example 4.3. A licence plate consists of 3 letters (from 26) followed by 4 digits (from 10). The number of distinct plates is $26^3 \times 10^4 = 175{,}760{,}000$.

Example 4.4. Re-deriving Proposition 3.7: each of the n elements of a set is either included or excluded from a subset, giving 2^n subsets by the multiplication principle.

4.2 Permutations

Definition 4.5 (Permutation)**.** A *permutation* of a set S is a bijection $\sigma\colon S \to S$. When $\operatorname{card} S = n$, the number of permutations of S is denoted $n!$ ("n factorial").

Proposition 4.6. *For $n \geq 1$, $n! = n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$. By convention, $0! = 1$.*

Proof. There are n choices for the image of the first element, $n-1$ for the second (since it must differ), and so on. By the multiplication principle the total is $n(n-1)(n-2)\cdots 1 = n!$. □

Definition 4.7 (k-permutation)**.** A *k-permutation* of a set of n elements is an ordered selection of k distinct elements. Their number is

$$P(n,k) = \frac{n!}{(n-k)!} = n(n-1)\cdots(n-k+1).$$

Example 4.8. In a race with 10 runners, the number of possible podium finishes (gold, silver, bronze) is $P(10,3) = 10 \cdot 9 \cdot 8 = 720$.

4.3 Combinations

Definition 4.9 (Binomial coefficient)**.** The number of ways to choose k elements from a set of n elements (without regard to order) is

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}, \qquad 0 \leq k \leq n.$$

We set $\binom{n}{k} = 0$ for $k < 0$ or $k > n$.

Proposition 4.10 (Symmetry)**.** $\displaystyle\binom{n}{k} = \binom{n}{n-k}$ *for all $0 \leq k \leq n$.*

Proof. $\displaystyle\binom{n}{n-k} = \frac{n!}{(n-k)!\,(n-(n-k))!} = \frac{n!}{(n-k)!\,k!} = \binom{n}{k}.$ □

Proposition 4.11 (Pascal's identity)**.** *For $1 \leq k \leq n$,*

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

Proof. Consider a distinguished element x in a set of n elements. Every k-element subset either contains x or not:

- those containing x: choose the remaining $k-1$ from $n-1$ elements: $\binom{n-1}{k-1}$ subsets;
- those not containing x: choose all k from $n-1$ elements: $\binom{n-1}{k}$ subsets.

By the addition principle the total is $\binom{n-1}{k-1} + \binom{n-1}{k}$. □

Example 4.12. A committee of 4 must be chosen from 10 people. The number of possible committees is $\binom{10}{4} = \frac{10!}{4!\,6!} = 210$.

Example 4.13. The number of lattice paths from $(0,0)$ to (m,n) using only unit steps right (R) and up (U) is $\binom{m+n}{n}$, since such a path is determined by choosing which n of the $m+n$ steps are U.

4.4 The binomial theorem

Theorem 4.14 (Binomial theorem)**.** *For any x, y and non-negative integer n,*

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

Proof. We proceed by induction on n.

Base case. For $n=0$: $(x+y)^0 = 1 = \binom{0}{0}x^0y^0$.

Inductive step. Suppose the identity holds for some $n \geq 0$. Then

$$\begin{aligned}(x+y)^{n+1} &= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k}.\end{aligned}$$

Re-index the first sum by setting $j = k+1$:

$$= \sum_{j=1}^{n+1}\binom{n}{j-1}x^j y^{n+1-j} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n+1-k}.$$

The $k = n+1$ term in the first sum contributes $\binom{n}{n}x^{n+1}y^0$, and the $k=0$ term in the second contributes $\binom{n}{0}x^0y^{n+1}$. For $1 \leq k \leq n$ the coefficients combine by Pascal's identity:

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

Hence $(x+y)^{n+1} = \sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{n+1-k}$, which completes the induction. □

Corollary 4.15. *Setting specific values in the binomial theorem:*

(i) $x = y = 1$*:* $\displaystyle\sum_{k=0}^{n}\binom{n}{k} = 2^n.$

(ii) $x = 1,\ y = -1$: $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$ *for* $n \geq 1$.

4.5 Vandermonde's identity

Theorem 4.16 (Vandermonde's identity)**.** *For non-negative integers* m, n, r *with* $r \leq m + n$,

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

Proof. **Combinatorial proof.** Consider a group of $m+n$ people divided into two teams: team A of m people and team B of n people. We wish to choose a committee of r people from the full group.

On the left side, this count is $\binom{m+n}{r}$.

On the right side, we classify committees by the number k of members drawn from team A. If k members come from A, then $r-k$ come from B. The number of such committees is $\binom{m}{k}\binom{n}{r-k}$. Summing over all valid k (from 0 to r, noting that $\binom{m}{k} = 0$ when $k > m$ and $\binom{n}{r-k} = 0$ when $r - k > n$) gives the right-hand side. □

Example 4.17. Setting $m = n = r$ gives: $\displaystyle\binom{2n}{n} = \sum_{k=0}^{n}\binom{n}{k}^2$.

4.6 Pascal's triangle

Pascal's triangle arranges the binomial coefficients in a triangular array where entry (n, k) is $\binom{n}{k}$ and each entry is the sum of the two entries above it (Pascal's identity, Proposition 4.11).

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}$$

Figure 4.1: Pascal's triangle, rows $n = 0$ through $n = 7$.

Remark 4.18. Several patterns are visible in Pascal's triangle:

(i) Each row is symmetric: $\binom{n}{k} = \binom{n}{n-k}$.

(ii) The entries on each edge are 1.

(iii) The sum of row n is 2^n.

(iv) The "hockey-stick" identity: $\sum_{i=0}^{r} \binom{n+i}{i} = \binom{n+r+1}{r}$.

4.7 Multiset coefficients and stars and bars

Definition 4.19 (Multiset)**.** A *multiset* is a collection of objects where repetition is allowed. A k-element multiset chosen from a set of n types is called a *k-combination with repetition.*

Theorem 4.20 (Stars and bars)**.** *The number of ways to choose k elements from n types with repetition allowed (equivalently, the number of solutions in non-negative integers to $x_1 + x_2 + \cdots + x_n = k$) is*

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

Proof. Represent a selection as a string of k stars ($*$) and $n-1$ bars ($|$). The stars represent the chosen items and the bars separate the n types. For example, with $n = 4$ types and $k = 6$, the string

$$** \mid * \mid \mid ***$$

encodes $x_1 = 2,\ x_2 = 1,\ x_3 = 0,\ x_4 = 3$.

Each valid string consists of $k + (n-1)$ symbols in total, and is uniquely determined by choosing which $n-1$ of these positions are bars (or equivalently, which k positions are stars). Hence the count is $\binom{k+n-1}{n-1} = \binom{n+k-1}{k}$. □

Example 4.21. A child wants to buy lollipops at a shop that stocks 4 flavours. If the child buys 6 lollipops, how many flavour combinations are possible?
Using stars and bars with $n = 4$ and $k = 6$: $\binom{4+6-1}{6} = \binom{9}{6} = 84$.

Example 4.22. Find the number of solutions in *positive* integers to $x_1 + x_2 + x_3 = 10$. Substitute $y_i = x_i - 1$ (so $y_i \geq 0$) to obtain $y_1 + y_2 + y_3 = 7$. By stars and bars, the answer is $\binom{7+3-1}{7} = \binom{9}{7} = 36$.

Proposition 4.23 (Multinomial coefficient)**.** *The number of ways to partition a set of n objects into groups of sizes $k_1, k_2, \ldots, k_r$ (with $k_1 + \cdots + k_r = n$) is the* multinomial

coefficient

$$\binom{n}{k_1, k_2, \ldots, k_r} = \frac{n!}{k_1!\, k_2! \cdots k_r!}.$$

Example 4.24. The number of distinct arrangements of the letters in MISSISSIPPI is

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

(There is 1 M, 4 I's, 4 S's, and 2 P's.)

4.8 Derangements

Definition 4.25 (Derangement)**.** A *derangement* of a set $\{1, 2, \ldots, n\}$ is a permutation σ with no fixed points, i.e. $\sigma(i) \neq i$ for all i. The number of derangements of n elements is denoted D_n.

Theorem 4.26.

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

In particular, D_n is the nearest integer to $n!/e$ for $n \geq 1$.

Proof. Let A_i be the set of permutations of $\{1, \ldots, n\}$ that fix i. By inclusion–exclusion,

$$D_n = n! - \operatorname{card} A_1 \cup A_2 \cup \cdots \cup A_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)!.$$

For any k-element subset $S \subseteq \{1, \ldots, n\}$, $\operatorname{card} \bigcap_{i \in S} A_i = (n-k)!$ (the remaining $n-k$ elements may be permuted freely). There are $\binom{n}{k}$ such subsets, so inclusion–exclusion gives

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \qquad \square$$

Example 4.27. Computing small values:

n	0	1	2	3	4	5	6	7
D_n	1	0	1	2	9	44	265	1854

As $n \to \infty$, the probability that a random permutation is a derangement converges to $1/e \approx 0.3679$.

Proposition 4.28 (Recurrence for derangements)**.** *For $n \geq 2$,*

$$D_n = (n-1)(D_{n-1} + D_{n-2}),$$

with $D_0 = 1$ and $D_1 = 0$.

Proof. Consider element 1. In a derangement, $\sigma(1) = j$ for some $j \in \{2, \dots, n\}$, giving $n-1$ choices. Two cases arise:

- *Case 1:* $\sigma(j) = 1$. Then elements 1 and j swap, and the remaining $n-2$ elements must be deranged: D_{n-2} ways.
- *Case 2:* $\sigma(j) \neq 1$. Define a permutation τ of $\{2, \dots, n\}$ by $\tau(i) = \sigma(i)$ for $i \neq j$ and $\tau(j) = \sigma(j)$. The condition $\sigma(j) \neq 1$ together with $\sigma(i) \neq i$ for $i \neq 1, j$ means τ is a derangement of $n-1$ elements: D_{n-1} ways.

By the addition and multiplication principles, $D_n = (n-1)(D_{n-1} + D_{n-2})$. □

4.9 Worked examples

Example 4.29 (Committees with restrictions)**.** From 8 men and 6 women, choose a committee of 5 that includes at least 2 women.
Solution. Count by the number w of women ($w \geq 2$):

$$\sum_{w=2}^{5} \binom{6}{w}\binom{8}{5-w} = \binom{6}{2}\binom{8}{3}+\binom{6}{3}\binom{8}{2}+\binom{6}{4}\binom{8}{1}+\binom{6}{5}\binom{8}{0} = 840+560+120+6 = 1526.$$

Example 4.30 (Distributing identical objects)**.** Distribute 15 identical balls into 4 distinct boxes such that each box has at least 2 balls.
Solution. Let x_i be the number of balls in box i. We need the number of solutions to $x_1 + x_2 + x_3 + x_4 = 15$ with each $x_i \geq 2$. Substitute $y_i = x_i - 2$:

$$y_1 + y_2 + y_3 + y_4 = 7, \qquad y_i \geq 0.$$

By stars and bars: $\binom{7+3}{3} = \binom{10}{3} = 120$.

Example 4.31 (Paths on a grid)**.** How many shortest lattice paths go from $(0,0)$ to $(5,4)$ passing through $(2,2)$?
Solution. A path through $(2,2)$ splits into two independent segments: $(0,0) \to (2,2)$ and $(2,2) \to (5,4)$. The counts are $\binom{4}{2} = 6$ and $\binom{5}{2} = 10$, giving $6 \times 10 = 60$ paths.

Example 4.32 (Application of the binomial theorem)**.** Find the coefficient of x^7 in $(2x-3)^{10}$.
Solution. By the binomial theorem,

$$(2x-3)^{10} = \sum_{k=0}^{10} \binom{10}{k}(2x)^k(-3)^{10-k}.$$

The x^7 term is $\binom{10}{7}(2)^7(-3)^3 = 120 \cdot 128 \cdot (-27) = -414{,}720$.

Example 4.33 (Hat problem (derangements))**.** Ten guests check their hats. If the hats are returned randomly, what is the probability that nobody receives their own hat?
Solution. This is a derangement problem. The probability is

$$\frac{D_{10}}{10!} = \sum_{k=0}^{10} \frac{(-1)^k}{k!} \approx \frac{1}{e} \approx 0.3679.$$

4.10 Exercises

Exercise 4.1. How many 5-letter "words" (sequences of letters) can be formed from the English alphabet if:

(a) repetition is allowed?

(b) no letter may be repeated?

(c) the word must begin with a vowel and end with a consonant, with repetition allowed?

Exercise 4.2. How many binary strings of length 12 contain exactly 5 ones?

Exercise 4.3. Use the binomial theorem to prove that $\sum_{k=0}^{n} k\binom{n}{k} = n \cdot 2^{n-1}$.
Hint: differentiate $(1+x)^n$ and set $x = 1$.

Exercise 4.4. Find the number of solutions in non-negative integers to $x_1+x_2+x_3+x_4 = 20$ with $x_1 \leq 6$.
Hint: total solutions minus those with $x_1 \geq 7$.

Exercise 4.5. Verify the recurrence $D_n = (n-1)(D_{n-1} + D_{n-2})$ for $n = 4$ and $n = 5$ by listing all derangements of $\{1, 2, 3, 4\}$.

Exercise 4.6. Use Vandermonde's identity to evaluate $\sum_{k=0}^{5} \binom{10}{k}\binom{15}{5-k}$.

Exercise 4.7. (a) How many distinct arrangements are there of the letters in ARRANGEMENT?

(b) In how many of these do the two R's appear next to each other?

Exercise 4.8. A club of 20 members must choose a president, a secretary, and a committee of 5 (which may include the president and secretary). In how many ways can this be done?

Exercise 4.9. Prove that $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$ using Vandermonde's identity.

Exercise 4.10. Show that $D_n = nD_{n-1} + (-1)^n$ for $n \geq 1$.
Hint: use the explicit formula $D_n = n! \sum_{k=0}^{n} (-1)^k/k!$.

4.11 Chapter summary

- The **addition** and **multiplication** principles are the cornerstones of counting.
- **Permutations**: $n!$ ways to arrange n objects; $P(n,k)$ for k-permutations.
- **Combinations**: $\binom{n}{k}$ counts unordered selections; the **binomial theorem** $(x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k}$.
- **Vandermonde's identity**: $\binom{m+n}{r} = \sum_k \binom{m}{k}\binom{n}{r-k}$.
- **Stars and bars**: the number of non-negative integer solutions to $x_1 + \cdots + x_n = k$ is $\binom{n+k-1}{k}$.
- **Derangements**: $D_n = n! \sum_{k=0}^{n} (-1)^k/k! \approx n!/e$.

Chapter 5

Inclusion-Exclusion and Advanced Counting

In the previous chapters we developed the basic tools of enumerative combinatorics: the addition and multiplication principles, permutations, combinations, and the binomial theorem. These tools are remarkably powerful, yet they share a common limitation: they work best when the objects being counted fall into *disjoint* categories. In practice, the sets we wish to count frequently overlap, and we must account for the elements that belong to several sets at once.

The **principle of inclusion-exclusion** provides a systematic way to handle such overlaps. It generalises the familiar identity $\operatorname{card} A \cup B = \operatorname{card} A + \operatorname{card} B - \operatorname{card} A \cap B$ to an arbitrary finite union, and it leads to elegant formulas for counting surjections, computing the Euler totient function, and enumerating derangements.

We then turn to two further themes in advanced counting: *Stirling numbers* and *integer partitions*, which refine the art of distributing objects into groups.

5.1 Inclusion-Exclusion for Two and Three Sets

Theorem 5.1 (Inclusion-Exclusion for Two Sets)**.** *Let A and B be finite sets. Then*

$$\operatorname{card} A \cup B \;=\; \operatorname{card} A + \operatorname{card} B - \operatorname{card} A \cap B.$$

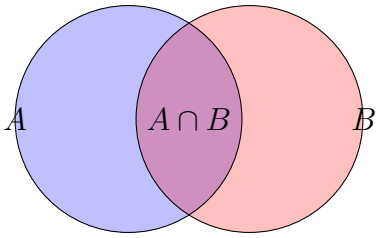
Proof. Every element of $A \cup B$ belongs to at least one of A and B. Write $A \cup B$ as the disjoint union

$$A \cup B \;=\; (A \setminus B) \;\cup\; (A \cap B) \;\cup\; (B \setminus A).$$

Hence $\operatorname{card} A \cup B = \operatorname{card} A \setminus B + \operatorname{card} A \cap B + \operatorname{card} B \setminus A$. Since $\operatorname{card} A = \operatorname{card} A \setminus B + \operatorname{card} A \cap B$ and $\operatorname{card} B = \operatorname{card} B \setminus A + \operatorname{card} A \cap B$, adding gives

$$\operatorname{card} A + \operatorname{card} B = \operatorname{card} A \setminus B + 2 \operatorname{card} A \cap B + \operatorname{card} B \setminus A = \operatorname{card} A \cup B + \operatorname{card} A \cap B,$$

and the result follows. □



$$\operatorname{card} A \cup B = \operatorname{card} A + \operatorname{card} B - \operatorname{card} A \cap B$$

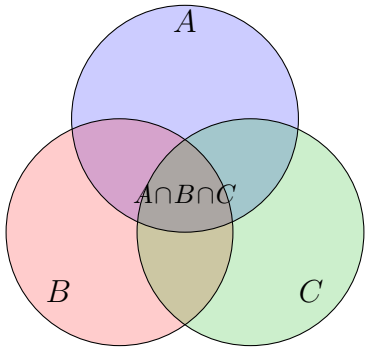
Theorem 5.2 (Inclusion-Exclusion for Three Sets)**.** *Let A, B, and C be finite sets. Then*

$$\begin{aligned}\operatorname{card} A \cup B \cup C = \operatorname{card} A + \operatorname{card} B + \operatorname{card} C \\ - \operatorname{card} A \cap B - \operatorname{card} A \cap C - \operatorname{card} B \cap C \\ + \operatorname{card} A \cap B \cap C.\end{aligned}$$

Proof. Apply the two-set formula twice:

$$\begin{aligned}\operatorname{card} A \cup B \cup C &= \operatorname{card} (A \cup B) \cup C \\ &= \operatorname{card} A \cup B + \operatorname{card} C - \operatorname{card} (A \cup B) \cap C \\ &= \operatorname{card} A \cup B + \operatorname{card} C - \operatorname{card} (A \cap C) \cup (B \cap C).\end{aligned}$$

Expanding $\operatorname{card} A \cup B$ and $\operatorname{card} (A \cap C) \cup (B \cap C)$ via Theorem 5.1 and noting that $(A \cap C) \cap (B \cap C) = A \cap B \cap C$ yields the result. □



Example 5.3. In a class of 100 students, 40 study French, 35 study German, and 20 study Spanish. Furthermore, 12 study both French and German, 8 study both French and Spanish, 6 study both German and Spanish, and 2 study all three languages. How many students study at least one of the three languages?
Let F, G, S denote the respective sets. By inclusion-exclusion,

$$\operatorname{card} F \cup G \cup S = 40 + 35 + 20 - 12 - 8 - 6 + 2 = 71.$$

Hence $100 - 71 = 29$ students study none of these languages.

5.2 The General Principle

Theorem 5.4 (General Inclusion-Exclusion)**.** *Let $A_1, A_2, \dots, A_n$ be finite subsets of a finite set U. Then*

$$\operatorname{card} *\bigcup_{i=1}^{n} A_i \;=\; \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < \cdots < i_k \le n} \operatorname{card} A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}.$$

Equivalently, writing $S_k = \sum_{1 \le i_1 < \cdots < i_k \le n} \operatorname{card} A_{i_1} \cap \cdots \cap A_{i_k}$,

$$\operatorname{card} *\bigcup_{i=1}^{n} A_i = S_1 - S_2 + S_3 - \cdots + (-1)^{n+1} S_n.$$

Proof. We show that each element $x \in \bigcup_{i=1}^{n} A_i$ is counted exactly once on the right-hand side. Suppose x belongs to exactly $m \ge 1$ of the sets $A_1, \dots, A_n$. Then x is counted once in each $\binom{m}{k}$ of the intersections of size k, so the right-hand side counts x a total of

$$\sum_{k=1}^{m} (-1)^{k+1} \binom{m}{k} = -\sum_{k=1}^{m} (-1)^{k} \binom{m}{k} = -\left[\sum_{k=0}^{m} (-1)^{k} \binom{m}{k} - 1 \right] = -(0 - 1) = 1,$$

where we used the binomial theorem: $\sum_{k=0}^{m} (-1)^k \binom{m}{k} = (1-1)^m = 0$ for $m \ge 1$. Hence every element of the union is counted exactly once. □

Remark 5.5. It is often more convenient to count the *complement*. If $A_1, \dots, A_n \subseteq U$, then

$$\operatorname{card} *U \setminus \bigcup_{i=1}^{n} A_i = \operatorname{card} U - S_1 + S_2 - S_3 + \cdots + (-1)^n S_n,$$

where S_k is defined as above. This form is especially useful when we want to count elements of U that belong to *none* of the A_i.

5.3 Counting Surjections

Theorem 5.6 (Number of Surjections)**.** *The number of surjections from a set of n elements onto a set of m elements (with $n \ge m$) is*

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

Proof. Let $X = \{x_1, \dots, x_n\}$ and $Y = \{y_1, \dots, y_m\}$, and let U be the set of all functions $f \colon X \to Y$, so $\operatorname{card} U = m^n$. For each $j \in \{1, \dots, m\}$, let A_j be the set of functions that *miss* y_j, i.e. $A_j = \{f \in U : y_j \notin f(X)\}$. A function is surjective if and only if it lies in none of the A_j, so

$$\operatorname{Surj}(n, m) = \operatorname{card} *U \setminus \bigcup_{j=1}^{m} A_j.$$

For any k-element subset $\{j_1, \dots, j_k\} \subseteq \{1, \dots, m\}$, the set $A_{j_1} \cap \cdots \cap A_{j_k}$ consists of functions whose range avoids k specified elements, hence $\operatorname{card} A_{j_1} \cap \cdots \cap A_{j_k} = (m-k)^n$. Since there are $\binom{m}{k}$ such subsets, inclusion-exclusion (Remark 5.5) gives

$$\operatorname{Surj}(n, m) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n. \qquad \square$$

Example 5.7. The number of surjections from $\{1, 2, 3, 4\}$ onto $\{a, b, c\}$ is

$$\binom{3}{0}3^4 - \binom{3}{1}2^4 + \binom{3}{2}1^4 - \binom{3}{3}0^4 = 81 - 48 + 3 - 0 = 36.$$

5.4 Euler's Totient Function

Definition 5.8 (Euler's Totient Function)**.** For a positive integer n, the **Euler totient function** $\varphi(n)$ counts the number of integers k with $1 \le k \le n$ and $\gcd(k, n) = 1$.

Theorem 5.9 (Product Formula for φ)**.** *If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ is the prime factorisation of $n \ge 2$, then*

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Proof. Let $U = \{1, 2, \dots, n\}$ and, for each i, let A_i be the set of elements of U divisible by p_i. Then $\varphi(n) = \operatorname{card} U \setminus \bigcup_{i=1}^{r} A_i$. We have $\operatorname{card} A_i = n/p_i$ and, more generally, for any subset $\{i_1, \dots, i_k\} \subseteq \{1, \dots, r\}$,

$$\operatorname{card} A_{i_1} \cap \cdots \cap A_{i_k} = \frac{n}{p_{i_1} \cdots p_{i_k}},$$

since the p_i are distinct primes. By inclusion-exclusion,

$$\begin{aligned} \varphi(n) &= \sum_{k=0}^{r} (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le r} \frac{n}{p_{i_1} \cdots p_{i_k}} \\ &= n \sum_{k=0}^{r} (-1)^k \sum_{1 \le i_1 < \cdots < i_k \le r} \frac{1}{p_{i_1} \cdots p_{i_k}} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right), \end{aligned}$$

where the last step expands the product. $\square$

Example 5.10. For $n = 60 = 2^2 \cdot 3 \cdot 5$,

$$\varphi(60) = 60\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right)\left(1 - \tfrac{1}{5}\right) = 60 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{4}{5} = 16.$$

5.5 Derangements

Definition 5.11 (Derangement)**.** A **derangement** of $\{1, 2, \ldots, n\}$ is a permutation σ such that $\sigma(i) \neq i$ for all i. The number of derangements of an n-element set is denoted D_n.

Theorem 5.12 (Derangement Formula)**.**

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

In particular, $D_n/n! \to 1/e$ as $n \to \infty$, so approximately a fraction $1/e \approx 36.8\%$ of all permutations are derangements.

Proof. Let U be the set of all permutations of $\{1, \ldots, n\}$ and let $A_i = \{\sigma \in U : \sigma(i) = i\}$ be the set of permutations that fix i. A derangement is a permutation in none of the A_i, so $D_n = \operatorname{card} U \setminus \bigcup_{i=1}^{n} A_i$.

For any k-element subset $\{i_1, \ldots, i_k\}$, the permutations fixing all of $i_1, \ldots, i_k$ form a set of size $(n-k)!$. There are $\binom{n}{k}$ such subsets. By inclusion-exclusion,

$$D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \qquad \square$$

Example 5.13. The first several values of D_n are:

n	0	1	2	3	4	5	6
D_n	1	0	1	2	9	44	265

For instance, $D_4 = 4!(1 - 1 + \frac{1}{2} - \frac{1}{6} + \frac{1}{24}) = 24 \cdot \frac{3}{8} = 9$.

Remark 5.14. Derangements also satisfy the recurrence

$$D_n = (n-1)(D_{n-1} + D_{n-2}), \quad n \geq 2,$$

with $D_0 = 1$ and $D_1 = 0$. To see this, consider where element 1 is sent: say $\sigma(1) = j \neq 1$. If $\sigma(j) = 1$ (a "swap"), the remaining $n-2$ elements must be deranged, giving D_{n-2}. If $\sigma(j) \neq 1$, we must derange $\{1, \ldots, n\} \setminus \{1\}$ with the constraint $\sigma(j) \neq 1$, which is equivalent to a derangement of $n-1$ elements, giving D_{n-1}. Since there are $n-1$ choices for j, the recurrence follows.

Exercise 5.1. (Hat-Check Problem.) At a party, n guests each check a hat. On leaving, the hats are returned at random. What is the probability that no guest receives their own hat? Show that this probability is $D_n/n!$ and compute it for $n = 5$.

5.6 Stirling Numbers of the Second Kind

Definition 5.15 (Stirling Number of the Second Kind)**.** The **Stirling number of the second kind** $S(n,k)$ (also written $\left\{ {n \atop k} \right\}$) is the number of ways to partition a set of n elements into exactly k non-empty subsets.

Proposition 5.16 (Explicit Formula)**.**

$$S(n,k) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

Proof. The number of surjections from an n-set to a k-set is $\mathrm{Surj}(n,k) = \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n$ by Theorem 5.6. Each partition into k non-empty blocks can be labelled in $k!$ ways to give a surjection, so $\mathrm{Surj}(n,k) = k!\, S(n,k)$. □

Proposition 5.17 (Recurrence)**.** *For $n, k \geq 1$,*

$$S(n,k) = k\, S(n-1,k) + S(n-1,k-1),$$

with $S(0,0) = 1$ and $S(n,0) = S(0,k) = 0$ for $n,k \geq 1$.

Proof. Consider element n. Either it forms a singleton block ($S(n-1,k-1)$ ways to partition the remaining $n-1$ elements into $k-1$ blocks), or it is added to one of the k existing blocks of a partition of $\{1,\dots,n-1\}$ into k blocks ($k\, S(n-1,k)$ ways). □

Example 5.18. A table of Stirling numbers $S(n,k)$ for small values:

$n \setminus k$	0	1	2	3	4	5
0	1					
1	0	1				
2	0	1	1			
3	0	1	3	1		
4	0	1	7	6	1	
5	0	1	15	25	10	1

5.7 Bell Numbers

Definition 5.19 (Bell Number)**.** The **Bell number** B_n is the total number of partitions of a set of n elements:

$$B_n = \sum_{k=0}^{n} S(n,k).$$

Proposition 5.20 (Bell Recurrence)**.**

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k, \quad B_0 = 1.$$

Proof. Consider element $n+1$. The block containing $n+1$ has k other elements (chosen in $\binom{n}{k}$ ways), and the remaining $n-k$ elements are partitioned in B_{n-k} ways. Summing over k and re-indexing gives the result. □

Example 5.21. The first few Bell numbers are: $B_0 = 1$, $B_1 = 1$, $B_2 = 2$, $B_3 = 5$, $B_4 = 15$, $B_5 = 52$, $B_6 = 203$.

5.8 Integer Partitions

Definition 5.22 (Integer Partition)**.** A **partition** of a positive integer n is a way of writing n as a sum of positive integers, where the order of the summands does not matter. Each summand is called a **part**. The number of partitions of n is denoted $p(n)$.

Example 5.23. The partitions of 5 are:

$$5, \quad 4+1, \quad 3+2, \quad 3+1+1, \quad 2+2+1, \quad 2+1+1+1, \quad 1+1+1+1+1,$$

so $p(5) = 7$.

Notation 5.24. We write a partition as $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_\ell)$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_\ell \geq 1$ and $\lambda_1 + \cdots + \lambda_\ell = n$. The number ℓ is the **length** of λ.

Theorem 5.25 (Generating Function for $p(n)$)**.**

$$\sum_{n=0}^{\infty} p(n)\, x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}.$$

Proof. Each factor $\frac{1}{1-x^k} = 1 + x^k + x^{2k} + \cdots$ encodes choosing how many parts equal to k appear. Multiplying over all $k \geq 1$ and collecting the coefficient of x^n counts the number of partitions of n. □

Theorem 5.26 (Euler's Distinct–Odd Theorem)**.** *The number of partitions of n into* distinct *parts equals the number of partitions of n into* odd *parts.*

Proof. The generating function for distinct-part partitions is $\prod_{k=1}^{\infty}(1+x^k)$, and for odd-part partitions it is $\prod_{k=0}^{\infty} \frac{1}{1-x^{2k+1}}$. We verify they are equal:

$$\prod_{k=1}^{\infty}(1+x^k) = \prod_{k=1}^{\infty} \frac{1-x^{2k}}{1-x^k} = \frac{\prod_{k=1}^{\infty}(1-x^{2k})}{\prod_{k=1}^{\infty}(1-x^k)} = \frac{1}{\prod_{j \text{ odd}}(1-x^j)},$$

since the even factors cancel. $\square$

5.9 Exercises

Exercise 5.2. How many integers in $\{1, 2, \dots, 1000\}$ are divisible by neither 3, 5, nor 7?

Exercise 5.3. Compute the number of surjections from $\{1, \dots, 5\}$ onto $\{a, b, c\}$.

Exercise 5.4. Prove that $\sum_{d \mid n} \varphi(d) = n$ for every positive integer n.

Exercise 5.5. Show that D_n is the nearest integer to $n!/e$ for all $n \geq 1$.

Exercise 5.6. Prove that $\sum_{k=0}^{n} S(n,k)\, x^{\underline{k}} = x^n$, where $x^{\underline{k}} = x(x-1)\cdots(x-k+1)$ is the falling factorial.

Exercise 5.7. The **Bell triangle** is constructed by placing $B_0 = 1$ at the top and filling each row so that each entry is the sum of its left and upper-left neighbours. Construct rows 0 through 5 and verify that the left-most entry in each row gives B_n.

Exercise 5.8. List all partitions of 8 into distinct parts and all partitions of 8 into odd parts, thereby verifying Euler's theorem for $n = 8$.

Exercise 5.9. (Problème des Ménages.) n married couples sit around a circular table so that men and women alternate and no husband sits next to his wife. Using inclusion-exclusion, show that the number of such seatings is

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

5.10 Chapter Summary

- **Inclusion-exclusion** (Theorem 5.4) computes $\operatorname{card} \bigcup A_i$ by alternately adding and subtracting the sizes of intersections.
- **Surjections:** $\operatorname{Surj}(n,m) = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n$ (Theorem 5.6).
- **Euler's totient:** $\varphi(n) = n \prod_{p \mid n} (1 - 1/p)$ (Theorem 5.9).
- **Derangements:** $D_n = n! \sum_{k=0}^{n} (-1)^k / k!$ (Theorem 5.12).
- **Stirling numbers** $S(n,k)$ count set partitions into k blocks; they satisfy $S(n,k) = kS(n-1,k) + S(n-1,k-1)$.
- **Bell numbers** $B_n = \sum_k S(n,k)$ count all set partitions; they satisfy $B_{n+1} = \sum_k \binom{n}{k} B_k$.
- **Integer partitions:** the generating function $\prod_{k \geq 1} (1 - x^k)^{-1}$ encodes $p(n)$; distinct-part partitions are equinumerous with odd-part partitions.

Chapter 6

Ordinary and Exponential Generating Functions

Generating functions are one of the most versatile tools in combinatorics. The idea is deceptively simple: encode a sequence $(a_0, a_1, a_2, \dots)$ as the coefficients of a formal power series, and then use the algebraic and analytic properties of the series to extract information about the sequence.

George Pólya called generating functions "a clothesline on which we hang up a sequence of numbers for display." Herb Wilf more vividly wrote that a generating function is "a device somewhat similar to a bag: instead of carrying many little objects, we put them all in a bag, and then we have only one object to carry."

In this chapter we study two principal types:

- **Ordinary generating functions (OGFs)**, suited to problems of selection and combination;
- **Exponential generating functions (EGFs)**, suited to problems of arrangement and permutation.

6.1 Formal Power Series

Before we do combinatorics, we set up the algebraic framework in which generating functions live.

Definition 6.1 (Formal Power Series)**.** A **formal power series** over a commutative ring R is a sequence $(a_0, a_1, a_2, \dots)$ of elements of R, written

$$f(x) = \sum_{n=0}^{\infty} a_n x^n.$$

The set of all such series is denoted $R[[x]]$.

Definition 6.2 (Operations on Formal Power Series)**.** Let $f(x) = \sum a_n x^n$ and $g(x) = \sum b_n x^n$ be elements of $R[[x]]$.

(i) **Addition:** $f + g = \sum_{n \geq 0} (a_n + b_n) x^n$.

(ii) **Multiplication:** $f \cdot g = \sum_{n\geq 0} c_n x^n$ where $c_n = \sum_{k=0}^{n} a_k b_{n-k}$ (the *Cauchy product*).

(iii) **Coefficient extraction:** We write $[x^n]f(x) = a_n$.

Proposition 6.3 (Multiplicative Inverses)**.** *A formal power series $f(x) = \sum a_n x^n \in R[[x]]$ has a multiplicative inverse if and only if a_0 is a unit in R. When R is a field, this means $a_0 \neq 0$.*

Proof. Suppose $f(x)g(x) = 1$ with $g(x) = \sum b_n x^n$. Comparing constant terms gives $a_0 b_0 = 1$, so a_0 must be a unit. Conversely, if a_0 is a unit, define $b_0 = a_0^{-1}$ and recursively

$$b_n = -a_0^{-1} \sum_{k=1}^{n} a_k b_{n-k}, \quad n \geq 1.$$

One verifies that $f(x)g(x) = 1$. □

Remark 6.4. In the theory of formal power series, *convergence is irrelevant*. We never substitute a numerical value for x; the variable x is merely a bookkeeping device. This makes the algebra entirely rigorous without any appeal to analysis. Of course, when the series also converges (e.g. for $|x| < R$), we gain additional tools from analysis.

6.2 Ordinary Generating Functions

Definition 6.5 (OGF)**.** The **ordinary generating function** (OGF) of a sequence $(a_n)_{n\geq 0}$ is

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

6.2.1 Basic OGFs

We collect some standard OGFs that will be used repeatedly.

Proposition 6.6 (Catalogue of OGFs)**.** *(i)* $\dfrac{1}{1-x} = \sum_{n\geq 0} x^n$ *(constant sequence $a_n = 1$).*

(ii) $\dfrac{1}{(1-x)^2} = \sum_{n\geq 0} (n+1)x^n.$

(iii) $\dfrac{1}{(1-x)^k} = \sum_{n\geq 0} \binom{n+k-1}{k-1} x^n$ *for $k \geq 1$.*

(iv) $\dfrac{x}{(1-x)^2} = \sum_{n\geq 0} n\, x^n.$

(v) $(1+x)^m = \sum_{n=0}^{m} \binom{m}{n} x^n$ *for* $m \in \mathbb{N}$.

(vi) $\dfrac{1}{1-x-x^2}$ *is the OGF of the Fibonacci numbers (see Section 6.3.1).*

6.2.2 Operations on OGFs

Proposition 6.7 (OGF Operations). *Let* $A(x) = \sum a_n x^n$ *and* $B(x) = \sum b_n x^n$.

(i) ***Scaling:*** $A(cx) = \sum a_n c^n x^n$.

(ii) ***Right shift:*** $x^k A(x) = \sum_{n \geq k} a_{n-k} x^n$.

(iii) ***Differentiation:*** $A'(x) = \sum_{n \geq 0} (n+1) a_{n+1} x^n$.

(iv) ***Convolution:*** $A(x)B(x) = \sum_{n \geq 0} c_n x^n$ *where* $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

(v) ***Partial sums:*** $\frac{A(x)}{1-x} = \sum_{n \geq 0} \Big(\sum_{k=0}^{n} a_k \Big) x^n$.

6.3 Solving Recurrences with OGFs

Generating functions provide a systematic three-step method for solving linear recurrences with constant coefficients:

1. Multiply the recurrence by x^n and sum over all valid n to obtain a functional equation for the OGF.
2. Solve algebraically for the OGF.
3. Extract coefficients using partial fractions or known series.

6.3.1 Worked Example: Fibonacci Numbers

Theorem 6.8 (OGF of Fibonacci Numbers). *Define* (F_n) *by* $F_0 = 0$, $F_1 = 1$, *and* $F_n = F_{n-1} + F_{n-2}$ *for* $n \geq 2$. *Then*

$$F(x) = \sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2}.$$

Proof. Let $F(x) = \sum_{n \geq 0} F_n x^n$. Multiplying $F_n = F_{n-1} + F_{n-2}$ by x^n and summing for $n \geq 2$:

$$\sum_{n \geq 2} F_n x^n = \sum_{n \geq 2} F_{n-1} x^n + \sum_{n \geq 2} F_{n-2} x^n.$$

The left side is $F(x) - F_0 - F_1 x = F(x) - x$. The right side is $x(F(x) - F_0) + x^2 F(x) = xF(x) + x^2 F(x)$. Hence

$$F(x) - x = xF(x) + x^2 F(x) \implies F(x)(1-x-x^2) = x \implies F(x) = \frac{x}{1-x-x^2}. \qquad \square$$

Corollary 6.9 (Binet's Formula)**.** *Let* $\phi = (1+\sqrt{5})/2$ *and* $\hat{\phi} = (1-\sqrt{5})/2$*. Then*

$$F_n = \frac{\phi^n - \hat{\phi}^n}{\sqrt{5}}.$$

Proof. Factor $1 - x - x^2 = -(x - 1/\phi)(x - 1/\hat{\phi})$ and decompose $F(x)$ into partial fractions:

$$F(x) = \frac{x}{1-x-x^2} = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\phi x} - \frac{1}{1-\hat{\phi}x}\right).$$

Expanding each geometric series and extracting $[x^n]$ gives the result. □

6.4 Catalan Numbers

Definition 6.10 (Catalan Numbers)**.** The **Catalan numbers** C_n are defined by $C_0 = 1$ and the recurrence

$$C_{n+1} = \sum_{k=0}^{n} C_k\, C_{n-k}, \quad n \geq 0.$$

Theorem 6.11 (OGF and Closed Form for Catalan Numbers)**.** *The OGF* $C(x) = \sum_{n\geq 0} C_n x^n$ *satisfies*

$$C(x) = \frac{1 - \sqrt{1-4x}}{2x},$$

and the closed form is

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Proof. The recurrence $C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}$ says that the sequence $(C_1, C_2, \dots)$ is the Cauchy product of $(C_0, C_1, \dots)$ with itself. In terms of generating functions,

$$\frac{C(x) - 1}{x} = C(x)^2,$$

i.e. $xC(x)^2 - C(x) + 1 = 0$. By the quadratic formula,

$$C(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Since $C(0) = C_0 = 1$, we need the branch with the minus sign (the plus sign gives $C(x) \to \infty$ as $x \to 0$).

For the closed form, use the generalised binomial theorem:

$$\sqrt{1-4x} = \sum_{n=0}^{\infty} \binom{1/2}{n} (-4x)^n.$$

One computes $\binom{1/2}{n}(-4)^n = \frac{(-1)^{n-1}\cdot 2}{n}\binom{2(n-1)}{n-1}$ for $n \geq 1$. After simplification,

$$C(x) = \sum_{n=0}^{\infty} \frac{1}{n+1}\binom{2n}{n} x^n.$$

□

Example 6.12. The first several Catalan numbers: $C_0 = 1$, $C_1 = 1$, $C_2 = 2$, $C_3 = 5$, $C_4 = 14$, $C_5 = 42$, $C_6 = 132$.

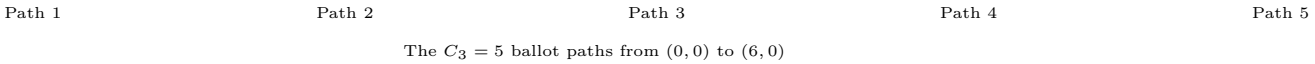
Remark 6.13 (Catalan Interpretations). The Catalan number C_n counts, among many other things:

(i) the number of **ballot paths** (lattice paths from $(0,0)$ to $(2n,0)$ using steps $(1,1)$ and $(1,-1)$ that never go below the x-axis);

(ii) the number of ways to **triangulate** a convex $(n+2)$-gon;

(iii) the number of strings of n pairs of **matched parentheses**;

(iv) the number of **full binary trees** with n internal nodes.



The $C_3 = 5$ ballot paths from $(0,0)$ to $(6,0)$

6.5 Exponential Generating Functions

When we count *labelled* structures (permutations, arrangements, labelled graphs), the natural generating function weights the nth term by $1/n!$ instead of 1.

Definition 6.14 (EGF)**.** The **exponential generating function** (EGF) of a sequence $(a_n)_{n\geq 0}$ is

$$\hat{A}(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Proposition 6.15 (Basic EGFs)**.** *(i)* $e^x = \sum_{n\geq 0} \frac{x^n}{n!}$ *(sequence* $a_n = 1$*).*

(ii) $e^{cx} = \sum_{n\geq 0} c^n \frac{x^n}{n!}$ *(sequence* $a_n = c^n$*).*

(iii) $\frac{1}{1-x} = \sum_{n\geq 0} n! \frac{x^n}{n!}$ *(sequence* $a_n = n!$*, i.e. permutations).*

(iv) $-\ln(1-x) = \sum_{n\geq 1} (n-1)! \dfrac{x^n}{n!}$ *(sequence* $a_n = (n-1)!$ *for* $n \geq 1$*, i.e. cyclic permutations).*

6.5.1 The Exponential Formula

The key property of EGFs is that *multiplication corresponds to shuffling labels.*

Theorem 6.16 (Product of EGFs)**.** *If* $\hat{A}(x) = \sum a_n x^n/n!$ *and* $\hat{B}(x) = \sum b_n x^n/n!$*,*

then

$$\hat{A}(x)\,\hat{B}(x) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\binom{n}{k}a_k\,b_{n-k}\right)\frac{x^n}{n!}.$$

Thus the coefficient of $x^n/n!$ in the product counts ways to split $\{1,\dots,n\}$ into an ordered pair (S,T) with $\operatorname{card} S = k$ and $\operatorname{card} T = n-k$, place an "A-structure" on S and a "B-structure" on T, summed over all k.

Proof. Direct computation of the Cauchy product:

$$\hat{A}(x)\hat{B}(x) = \sum_{n\geq 0}\sum_{k=0}^{n}\frac{a_k}{k!}\cdot\frac{b_{n-k}}{(n-k)!}\,x^n = \sum_{n\geq 0}\frac{1}{n!}\sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}\,x^n. \qquad \square$$

6.6 Permutations and Derangements via EGF

Example 6.17 (EGF for Permutations)**.** The number of permutations of an n-set is $n!$, so the EGF is

$$\sum_{n=0}^{\infty} n!\,\frac{x^n}{n!} = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

Theorem 6.18 (EGF for Derangements)**.** *The EGF for the derangement numbers D_n is*

$$\hat{D}(x) = \sum_{n=0}^{\infty} D_n\frac{x^n}{n!} = \frac{e^{-x}}{1-x}.$$

Proof. From Theorem 5.12, $D_n = n!\sum_{k=0}^{n}(-1)^k/k!$. This is the binomial convolution $D_n = \sum_{k=0}^{n}\binom{n}{k}(-1)^k(n-k)!$, which by Theorem 6.16 corresponds to

$$\hat{D}(x) = e^{-x}\cdot\frac{1}{1-x}. \qquad \square$$

Remark 6.19. Alternatively, write $D_n/n! = \sum_{k=0}^{n}(-1)^k/k!$ and recognise that $D_n/n! \to e^{-1}$ as $n\to\infty$. In fact, $\hat{D}(x) = e^{-x}/(1-x)$ gives the elegant interpretation: a permutation is a derangement times a set of fixed points. That is, we partition $\{1,\dots,n\}$ into a set of fixed points (whose EGF is e^x) and a derangement on the rest. Since the EGF for all permutations is $1/(1-x)$, we get $1/(1-x) = e^x\hat{D}(x)$.

6.7 Bell Numbers via EGF

Theorem 6.20 (EGF for Bell Numbers)**.**

$$\sum_{n=0}^{\infty} B_n\frac{x^n}{n!} = e^{e^x-1}.$$

Proof. A partition of $\{1, \dots, n\}$ is a set of non-empty subsets (the blocks). The EGF for a single non-empty subset ("at least one element") is $e^x - 1$. By the compositional formula for EGFs (the "exponential formula"), the EGF for *sets of non-empty subsets* is

$$\exp\Big(e^x - 1\Big).$$

□

Remark 6.21. Expanding $e^{e^x-1} = e^{-1}\sum_{k=0}^{\infty} \frac{e^{kx}}{k!}$ and extracting $[x^n/n!]$ gives **Dobiński's formula**:

$$B_n = \frac{1}{e}\sum_{k=0}^{\infty} \frac{k^n}{k!}.$$

This remarkable identity expresses B_n as a convergent infinite sum.

6.8 Worked Example: A General Recurrence

Example 6.22 (Solving $a_n = 5a_{n-1} - 6a_{n-2}$)**.** Let $a_0 = 1$, $a_1 = 4$, and $a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$. Find a closed form for a_n.
Step 1. Let $A(x) = \sum a_n x^n$. Multiply the recurrence by x^n and sum for $n \geq 2$:

$$A(x) - 1 - 4x = 5x(A(x) - 1) - 6x^2 A(x).$$

Solving: $A(x)(1 - 5x + 6x^2) = 1 - x$, so

$$A(x) = \frac{1 - x}{1 - 5x + 6x^2} = \frac{1 - x}{(1 - 2x)(1 - 3x)}.$$

Step 2. Partial fractions: write $\frac{1-x}{(1-2x)(1-3x)} = \frac{\alpha}{1-2x} + \frac{\beta}{1-3x}$. Setting $x = 1/2$: $\alpha = (1-1/2)/(1-3/2) = (1/2)/(-1/2) = -1$. Setting $x = 1/3$: $\beta = (1-1/3)/(1-2/3) = (2/3)/(1/3) = 2$. Hence

$$A(x) = \frac{-1}{1 - 2x} + \frac{2}{1 - 3x} = -\sum_{n\geq 0} 2^n x^n + 2\sum_{n\geq 0} 3^n x^n.$$

Step 3. Extract coefficients: $a_n = 2 \cdot 3^n - 2^n$. We verify: $a_0 = 2 - 1 = 1$, $a_1 = 6 - 2 = 4$, $a_2 = 18 - 4 = 14 = 5(4) - 6(1) = 14$.✓

6.9 Worked Example: Derangements Revisited

Example 6.23 (Derangement OGF from the Recurrence)**.** The recurrence $D_n = (n-1)(D_{n-1} + D_{n-2})$ (Remark 5.14) does not have constant coefficients, so the OGF approach is less direct. Instead, we use the EGF.
From $D_n = n!\sum_{k=0}^{n}(-1)^k/k!$, define $d_n = D_n/n!$. Then $d_n = \sum_{k=0}^{n}(-1)^k/k!$, so $d_n - d_{n-1} = (-1)^n/n!$. The EGF $\hat{D}(x) = \sum d_n n! \frac{x^n}{n!} = \sum D_n x^n/n!$ but it is more illuminating to note:

The relation $D_n = nD_{n-1} + (-1)^n$ gives

$$\frac{D_n}{n!} = \frac{D_{n-1}}{(n-1)!} \cdot \frac{1}{n} \cdot n + \frac{(-1)^n}{n!}$$

which simplifies to $\frac{D_n}{n!} - \frac{D_{n-1}}{(n-1)!} = \frac{(-1)^n}{n!}$. Summing from $n = 1$ to N:

$$\frac{D_N}{N!} = \sum_{n=0}^{N} \frac{(-1)^n}{n!},$$

confirming $\hat{D}(x) = e^{-x}/(1-x)$ once more.

6.10 Composition and the Exponential Formula

Theorem 6.24 (Exponential Formula)**.** *Let $\hat{C}(x) = \sum_{n\geq 1} c_n\, x^n/n!$ be the EGF of a class of connected (or indecomposable) labelled structures, with $c_0 = 0$. Then the EGF for* sets of such structures *is*

$$\hat{A}(x) = \exp\Big(\hat{C}(x)\Big) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}.$$

Conversely, $\hat{C}(x) = \ln \hat{A}(x)$.

Example 6.25. A permutation is a set of cycles. The EGF for a single cycle of length $n \geq 1$ is $(n-1)!\, x^n/n! = x^n/n$, so

$$\hat{C}(x) = \sum_{n=1}^{\infty} \frac{x^n}{n} = -\ln(1-x).$$

The exponential formula gives

$$\exp\Big(-\ln(1-x)\Big) = \frac{1}{1-x},$$

which is indeed the EGF for $n!$ (the number of permutations).

Example 6.26. An **involution** is a permutation σ with $\sigma^2 = \mathrm{id}$, i.e. every cycle has length 1 or 2. The EGF for fixed points (cycles of length 1) is x, and for transpositions (cycles of length 2) it is $x^2/2$. So the EGF for involutions is

$$\exp\Big(x + \frac{x^2}{2}\Big).$$

Writing $I_n = [x^n/n!] \exp(x + x^2/2)$, we get $I_0 = 1$, $I_1 = 1$, $I_2 = 2$, $I_3 = 4$, $I_4 = 10$, $I_5 = 26$.

6.11 Further Applications

6.11.1 Counting with Restrictions

Example 6.27 (Compositions with Restricted Parts)**.** A **composition** of n into parts from a set $S \subseteq \mathbb{N}_{\geq 1}$ is an ordered tuple $(s_1, \ldots, s_k)$ with $s_i \in S$ and $s_1 + \cdots + s_k = n$. The OGF for the number of such compositions is

$$\frac{1}{1 - \sum_{s \in S} x^s}.$$

For instance, if $S = \{1, 2\}$, the OGF is $\frac{1}{1-x-x^2}$, giving the Fibonacci numbers as the number of compositions of n into parts 1 and 2 (offset by one).

6.11.2 The Snake Oil Method

Example 6.28 (A Binomial Identity)**.** We prove the **Vandermonde identity**

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

using generating functions. The left side is the coefficient of x^r in $(1+x)^m(1+x)^n = (1+x)^{m+n}$, which is $\binom{m+n}{r}$.

6.12 Exercises

Exercise 6.1. Find a closed form for $\sum_{n=0}^{\infty} n^2 x^n$ by differentiating $\sum x^n = 1/(1-x)$.

Exercise 6.2. Solve the recurrence $a_n = 3a_{n-1} - 2a_{n-2}$ with $a_0 = 0$, $a_1 = 1$ using OGFs.

Exercise 6.3. Show directly (without generating functions) that the number of valid strings of n pairs of parentheses satisfies the Catalan recurrence.

Exercise 6.4. (Reflection Principle.) Show that the number of lattice paths from $(0,0)$ to $(2n,0)$ with steps $(1,1)$ and $(1,-1)$ that touch or cross the x-axis negatively is $\binom{2n}{n-1}$, and deduce $C_n = \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}$.

Exercise 6.5. Using EGFs, show that the number of permutations of $\{1, \ldots, n\}$ with exactly k fixed points is $\binom{n}{k} D_{n-k}$.

Exercise 6.6. Let $g_n = 2^{\binom{n}{2}}$ be the number of labelled graphs on n vertices, and let c_n be the number of *connected* labelled graphs. Using the exponential formula, write down the relation between $\sum g_n x^n/n!$ and $\sum c_n x^n/n!$, and compute c_1, c_2, c_3, c_4.

Exercise 6.7. Show that the OGF for the number of partitions of n into distinct parts is $\prod_{k=1}^{\infty}(1+x^k)$, and expand it to find the coefficients up to $n = 10$.

Exercise 6.8. Use the OGF of the Fibonacci numbers to prove that $\sum_{k=0}^{n} F_k F_{n-k} = \frac{1}{5}\Big((2n+1)F_n + 2nF_{n-1}\Big)$. *Hint:* square $F(x) = x/(1-x-x^2)$ and use partial fractions.

Exercise 6.9. Verify the EGF e^{e^x-1} for Bell numbers by expanding through $n = 5$ and checking against the known values $B_0 = 1, \ldots, B_5 = 52$.

Exercise 6.10. Show that the number of involutions satisfies $I_n = I_{n-1} + (n-1)I_{n-2}$ for $n \geq 2$, with $I_0 = I_1 = 1$. Derive this both combinatorially and from the EGF $\exp(x + x^2/2)$.

6.13 Chapter Summary

- A **formal power series** $\sum a_n x^n \in R[[x]]$ encodes a sequence; convergence is not required. The ring $R[[x]]$ admits inverses whenever a_0 is a unit.
- **Ordinary generating functions** $A(x) = \sum a_n x^n$ are the tool of choice for selections (subsets, multisets, compositions, partitions). Key operations: convolution encodes sums of indices; partial fractions extract coefficients.
- **Exponential generating functions** $\hat{A}(x) = \sum a_n x^n/n!$ are suited to labelled structures. Their product encodes binomial convolution, i.e. shuffling labels.
- **Fibonacci numbers:** $F(x) = x/(1 - x - x^2)$; Binet's formula follows from partial fractions (Theorem 6.8, Corollary 6.9).
- **Catalan numbers:** $C(x) = (1 - \sqrt{1-4x})/(2x)$; closed form $C_n = \binom{2n}{n}/(n+1)$ (Theorem 6.11).
- **Derangements:** EGF is $e^{-x}/(1-x)$ (Theorem 6.18).
- **Bell numbers:** EGF is e^{e^x-1} (Theorem 6.20); Dobiński's formula gives $B_n = e^{-1}\sum k^n/k!$.
- The **exponential formula** (Theorem 6.24): if $\hat{C}(x)$ is the EGF of connected structures, then $\exp(\hat{C}(x))$ is the EGF for sets of such structures.

Chapter 7

Recurrences

A *recurrence relation* (or simply a *recurrence*) defines each term of a sequence in terms of one or more preceding terms together with an initial condition (or several). Recurrences appear naturally in counting problems, algorithm analysis, and many other areas of discrete mathematics. In this chapter we develop systematic methods for solving them.

7.1 Basic Notions

Definition 7.1 (Recurrence relation)**.** A *recurrence relation* for a sequence $(a_n)_{n \geq 0}$ is an equation that expresses a_n in terms of one or more of the previous terms $a_{n-1}, a_{n-2}, \ldots$ for all n greater than or equal to some fixed integer n_0. The values $a_0, a_1, \ldots, a_{n_0-1}$ that are specified independently are called *initial conditions*.

Example 7.2 (Simple recurrence)**.** The relation $a_n = 2a_{n-1}$ with $a_0 = 3$ defines the sequence $3, 6, 12, 24, \ldots$ Its closed-form solution is $a_n = 3 \cdot 2^n$.

The *order* of a recurrence is the difference between the largest and smallest indices that appear. For instance $a_n = a_{n-1} + a_{n-2}$ has order 2.

7.2 Linear Homogeneous Recurrences

Definition 7.3 (Linear homogeneous recurrence with constant coefficients)**.** A recurrence of the form

$$a_n = c_1\, a_{n-1} + c_2\, a_{n-2} + \cdots + c_k\, a_{n-k}, \qquad c_k \neq 0,$$

where $c_1, \ldots, c_k$ are constants, is called a *linear homogeneous recurrence with constant coefficients* (LHCC) of order k.

7.2.1 The characteristic equation

The key idea is to guess a solution of the form $a_n = r^n$ for some constant $r \neq 0$. Substituting into the recurrence yields

$$r^n = c_1\, r^{n-1} + c_2\, r^{n-2} + \cdots + c_k\, r^{n-k}.$$

Dividing through by r^{n-k} gives the *characteristic equation*

$$r^k - c_1\, r^{k-1} - c_2\, r^{k-2} - \cdots - c_k = 0. \tag{7.1}$$

Theorem 7.4 (Solution of a second-order LHCC)**.** *Consider the recurrence $a_n = c_1\, a_{n-1} + c_2\, a_{n-2}$ with characteristic equation $r^2 - c_1\, r - c_2 = 0$.*

1. *If the characteristic equation has two distinct roots $r_1 \neq r_2$, then the general solution is*
$$a_n = \alpha\, r_1^n + \beta\, r_2^n,$$
where α, β are determined by the initial conditions.

2. *If the characteristic equation has a repeated root $r_1 = r_2 = r_0$, then the general solution is*
$$a_n = (\alpha + \beta\, n)\, r_0^n.$$

Proof. **Case 1.** Since r_1 and r_2 are roots of the characteristic equation, both (r_1^n) and (r_2^n) satisfy the recurrence. Because the recurrence is linear and homogeneous, any linear combination $a_n = \alpha\, r_1^n + \beta\, r_2^n$ also satisfies it. We need to show that every solution has this form. Given initial conditions a_0, a_1, we must solve

$$\alpha + \beta = a_0, \qquad \alpha\, r_1 + \beta\, r_2 = a_1.$$

The determinant of this system is $r_2 - r_1 \neq 0$ (since the roots are distinct), so there is a unique solution for α, β. Because the recurrence together with initial conditions determines the sequence uniquely, this must be the solution.

Case 2. When $r_1 = r_2 = r_0$ we have $r_0 = c_1/2$ and $c_2 = -r_0^2$. One checks directly that $a_n = n\, r_0^n$ satisfies the recurrence:

$$c_1\,(n-1)\, r_0^{n-1} + c_2\,(n-2)\, r_0^{n-2} = r_0^{n-2}\big[2r_0(n-1) - r_0^2(n-2)\big]\, r_0^{n-2}$$

simplifies to $n\, r_0^n$ after using $c_1 = 2r_0$ and $c_2 = -r_0^2$. Hence $\{r_0^n, n\, r_0^n\}$ form a basis, and the general solution is $a_n = (\alpha + \beta\, n)\, r_0^n$. □

Theorem 7.5 (General LHCC of order k)**.** *If the characteristic equation (7.1) has t distinct roots $r_1, \ldots, r_t$ with multiplicities $m_1, \ldots, m_t$ (so that $m_1 + \cdots + m_t = k$), then the general solution is*

$$a_n = \sum_{i=1}^{t} \left(\alpha_{i,0} + \alpha_{i,1}\, n + \cdots + \alpha_{i,m_i-1}\, n^{m_i-1}\right) r_i^n,$$

where the k constants $\alpha_{i,j}$ are determined by the k initial conditions.

Example 7.6 (Distinct roots)**.** Solve $a_n = 5a_{n-1} - 6a_{n-2}$, with $a_0 = 1$, $a_1 = 4$.
The characteristic equation is $r^2 - 5r + 6 = 0$, whose roots are $r_1 = 2$ and $r_2 = 3$. Thus $a_n = \alpha \cdot 2^n + \beta \cdot 3^n$. The initial conditions give

$$\alpha + \beta = 1, \qquad 2\alpha + 3\beta = 4 \implies \alpha = -1,\ \beta = 2.$$

Hence $a_n = -2^n + 2 \cdot 3^n = 2 \cdot 3^n - 2^n$.

Example 7.7 (Repeated root)**.** Solve $a_n = 4a_{n-1} - 4a_{n-2}$, with $a_0 = 1$, $a_1 = 6$.
The characteristic equation $r^2 - 4r + 4 = 0$ has the double root $r_0 = 2$. So $a_n = (\alpha + \beta n)\, 2^n$. From $a_0 = 1$ we get $\alpha = 1$; from $a_1 = 6$ we get $2(\alpha + \beta) = 6$, so $\beta = 2$. Therefore $a_n = (1 + 2n)\, 2^n$.

7.3 Non-Homogeneous Linear Recurrences

Definition 7.8 (Non-homogeneous linear recurrence)**.** A recurrence of the form

$$a_n = c_1\, a_{n-1} + \cdots + c_k\, a_{n-k} + f(n),$$

where $f(n) \not\equiv 0$, is called a *non-homogeneous* linear recurrence.

The general solution equals the general solution of the associated homogeneous recurrence *plus* any particular solution of the non-homogeneous recurrence:

$$a_n = a_n^{(\mathrm{h})} + a_n^{(\mathrm{p})}. \tag{7.2}$$

Theorem 7.9 (Method of undetermined coefficients)**.** *If the non-homogeneous term has the form $f(n) = (b_d\, n^d + \cdots + b_0)\, s^n$ for constants b_i, s, then one may seek a particular solution of the form*

$$a_n^{(\mathrm{p})} = n^m\, (B_d\, n^d + \cdots + B_0)\, s^n,$$

where m is the multiplicity of s as a root of the characteristic equation (set $m = 0$ if s is not a root).

Example 7.10 (Non-homogeneous recurrence)**.** Solve $a_n = 3a_{n-1} + 4^n$, with $a_0 = 1$.
Homogeneous part. The characteristic equation of $a_n = 3a_{n-1}$ is $r - 3 = 0$, so $a_n^{(\mathrm{h})} = \alpha \cdot 3^n$.
Particular solution. Since $f(n) = 4^n$ and $s = 4$ is not a root, we try $a_n^{(\mathrm{p})} = A \cdot 4^n$. Substituting: $A \cdot 4^n = 3A \cdot 4^{n-1} + 4^n$. Dividing by 4^{n-1}: $4A = 3A + 4$, giving $A = 4$.
General solution. $a_n = \alpha \cdot 3^n + 4 \cdot 4^n = \alpha \cdot 3^n + 4^{n+1}$. From $a_0 = 1$: $\alpha + 4 = 1$, so $\alpha = -3$. Thus $a_n = -3^{n+1} + 4^{n+1}$.

7.4 The Fibonacci Sequence and Binet's Formula

Definition 7.11 (Fibonacci sequence)**.** The *Fibonacci sequence* $(F_n)_{n\geq 0}$ is defined by

$$F_0 = 0, \qquad F_1 = 1, \qquad F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

Its first terms are $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$

Theorem 7.12 (Binet's formula)**.** *For every $n \geq 0$,*

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}},$$

where $\varphi = \dfrac{1+\sqrt{5}}{2}$ *(the* golden ratio*) and* $\psi = \dfrac{1-\sqrt{5}}{2}$.

Proof. The characteristic equation of $F_n = F_{n-1} + F_{n-2}$ is $r^2 - r - 1 = 0$, whose roots are

$$\varphi = \frac{1+\sqrt{5}}{2}, \qquad \psi = \frac{1-\sqrt{5}}{2}.$$

By Theorem 7.4 the general solution is $F_n = \alpha\,\varphi^n + \beta\,\psi^n$. The initial conditions give the system

$$\alpha + \beta = 0, \qquad \alpha\,\varphi + \beta\,\psi = 1.$$

From the first equation $\beta = -\alpha$. Substituting into the second:

$$\alpha(\varphi - \psi) = 1 \implies \alpha = \frac{1}{\varphi - \psi} = \frac{1}{\sqrt{5}}.$$

Therefore $\beta = -1/\sqrt{5}$, and $F_n = \dfrac{\varphi^n - \psi^n}{\sqrt{5}}$. □

Remark 7.13. Since $|\psi| = \left|(1-\sqrt{5})/2\right| \approx 0.618 < 1$, the term $\psi^n/\sqrt{5} \to 0$ as $n \to \infty$. Hence F_n is the nearest integer to $\varphi^n/\sqrt{5}$ for all $n \geq 0$.

7.5 Classic Recurrences

7.5.1 The Tower of Hanoi

The Tower of Hanoi puzzle asks for the minimum number of moves T_n needed to transfer n disks from one peg to another, moving one disk at a time and never placing a larger disk on a smaller one.

Proposition 7.14 (Tower of Hanoi recurrence)**.** *The sequence (T_n) satisfies*

$$T_0 = 0, \qquad T_n = 2\,T_{n-1} + 1 \quad (n \geq 1).$$

Its closed form is $T_n = 2^n - 1$.

Proof. To move n disks from peg A to peg C:

1. Move the top $n-1$ disks from A to B (T_{n-1} moves).
2. Move disk n from A to C (1 move).
3. Move the $n-1$ disks from B to C (T_{n-1} moves).

This gives $T_n = 2T_{n-1} + 1$.

For the closed form, observe that this is a non-homogeneous first-order recurrence. Setting $S_n = T_n + 1$ yields $S_n = 2S_{n-1}$ with $S_0 = 1$, so $S_n = 2^n$ and $T_n = 2^n - 1$. □

7.5.2 Catalan numbers

Definition 7.15 (Catalan numbers)**.** The n-th *Catalan number* is

$$C_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n \geq 0.$$

The first values are $1, 1, 2, 5, 14, 42, 132, 429, \ldots$

Proposition 7.16 (Catalan recurrence)**.** *The Catalan numbers satisfy*

$$C_0 = 1, \qquad C_{n+1} = \sum_{i=0}^{n} C_i\, C_{n-i} \quad (n \geq 0).$$

Equivalently, $C_{n+1} = \dfrac{2(2n+1)}{n+2}\, C_n$.

Proof. Consider the number of ways to fully parenthesise a product of $n+2$ factors. Splitting after the i-th factor (for $i = 1, \ldots, n+1$) gives $C_i \cdot C_{n+1-i}$ arrangements for the left and right parts. Summing and reindexing yields the convolution.

For the ratio formula, divide the closed form for C_{n+1} by that for C_n:

$$\frac{C_{n+1}}{C_n} = \frac{1}{n+2}\binom{2n+2}{n+1} \cdot \frac{n+1}{\binom{2n}{n}} = \frac{n+1}{n+2} \cdot \frac{(2n+2)!/(n+1)!^2}{(2n)!/n!^2} = \frac{2(2n+1)}{n+2}.$$ □

Remark 7.17. Catalan numbers count many combinatorial objects, including: the number of Dyck paths of length $2n$, the number of different triangulations of a convex $(n+2)$-gon, and the number of full binary trees with $n+1$ leaves.

7.6 The Master Theorem

Many divide-and-conquer algorithms yield recurrences of the form $T(n) = a\,T(n/b) + f(n)$. The master theorem gives their asymptotic behaviour in three cases.

Theorem 7.18 (Master theorem)**.** *Let $a \geq 1$, $b > 1$ be constants, and let $f(n)$ be a non-negative function. Define $T(n)$ by*

$$T(n) = a\,T\!\left(\frac{n}{b}\right) + f(n),$$

with $T(1) = \Theta(1)$. Let $c = \log_b a$. Then:

1. *If $f(n) = O(n^{c-\epsilon})$ for some $\epsilon > 0$, then $T(n) = \Theta(n^c)$.*
2. *If $f(n) = \Theta(n^c \log^k n)$ for some $k \geq 0$, then $T(n) = \Theta(n^c \log^{k+1} n)$.*
3. *If $f(n) = \Omega(n^{c+\epsilon})$ for some $\epsilon > 0$, and if $a\,f(n/b) \leq \delta\, f(n)$ for some $\delta < 1$ and all sufficiently large n, then $T(n) = \Theta(f(n))$.*

Example 7.19 (Merge sort)**.** Merge sort satisfies $T(n) = 2T(n/2) + \Theta(n)$. Here $a = 2$, $b = 2$, $c = \log_2 2 = 1$, and $f(n) = \Theta(n) = \Theta(n^c)$. Case 2 with $k = 0$ gives $T(n) = \Theta(n \log n)$.

Example 7.20 (Binary search)**.** Binary search satisfies $T(n) = T(n/2) + \Theta(1)$. Here $a = 1$, $b = 2$, $c = \log_2 1 = 0$, and $f(n) = \Theta(1) = \Theta(n^0)$. Case 2 with $k = 0$ gives $T(n) = \Theta(\log n)$.

Example 7.21 (Strassen's algorithm)**.** Strassen's matrix multiplication satisfies $T(n) = 7T(n/2) + \Theta(n^2)$. Here $c = \log_2 7 \approx 2.807$, and $f(n) = \Theta(n^2) = O(n^{c-\epsilon})$ with $\epsilon \approx 0.807$. Case 1 gives $T(n) = \Theta(n^{\log_2 7})$.

7.7 Solving Recurrences via Generating Functions

Generating functions provide a powerful algebraic approach to solving recurrences, especially when the characteristic-equation method is cumbersome.

Definition 7.22 (Ordinary generating function)**.** The *ordinary generating function* (OGF) of a sequence $(a_n)_{n \geq 0}$ is the formal power series

$$A(x) = \sum_{n=0}^{\infty} a_n\, x^n.$$

Strategy. Given a recurrence for (a_n):

1. Multiply both sides by x^n and sum over the valid range of n.
2. Express each sum in terms of $A(x)$.
3. Solve the resulting equation for $A(x)$.
4. Extract a_n by expanding $A(x)$ in partial fractions or by recognising known series.

Example 7.23 (Fibonacci via generating functions)**.** We derive the OGF of the Fibonacci sequence. Starting from $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$, multiply by x^n and sum:

$$\sum_{n=2}^{\infty} F_n x^n = \sum_{n=2}^{\infty} F_{n-1} x^n + \sum_{n=2}^{\infty} F_{n-2} x^n.$$

The left side is $F(x) - F_0 - F_1 x = F(x) - x$. The right side is $x\big(F(x) - F_0\big) + x^2 F(x) = x\,F(x) + x^2 F(x)$. Therefore

$$F(x) - x = x\,F(x) + x^2 F(x) \implies F(x) = \frac{x}{1 - x - x^2}.$$

Partial-fraction decomposition with roots φ, ψ of $1 - x - x^2 = 0$ recovers Binet's formula.

Example 7.24 (Catalan OGF)**.** Let $C(x) = \sum_{n \geq 0} C_n x^n$. The convolution recurrence $C_{n+1} = \sum_{i=0}^{n} C_i C_{n-i}$ translates to

$$\frac{C(x) - 1}{x} = C(x)^2 \implies x\,C(x)^2 - C(x) + 1 = 0.$$

By the quadratic formula,

$$C(x) = \frac{1 - \sqrt{1 - 4x}}{2x}.$$

(We choose the minus sign so that $C(0) = 1$.) Expanding $(1-4x)^{1/2}$ via the generalised binomial theorem yields the closed form $C_n = \frac{1}{n+1}\binom{2n}{n}$.

7.8 Exercises

Exercise 7.1. Solve the recurrence $a_n = 7a_{n-1} - 10a_{n-2}$ with $a_0 = 2$ and $a_1 = 1$.

Exercise 7.2. Solve $a_n = 6a_{n-1} - 9a_{n-2}$ with $a_0 = 0$ and $a_1 = 3$.

Exercise 7.3. Find a closed-form solution for $a_n = 2a_{n-1} + 3^n$ with $a_0 = 1$.

Exercise 7.4. The *Tribonacci numbers* are defined by $T_0 = 0$, $T_1 = 0$, $T_2 = 1$, and $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ for $n \geq 3$. Write down the characteristic equation and find its roots numerically.

Exercise 7.5. Use the master theorem to determine the asymptotic behaviour of $T(n) = 4T(n/2) + n$.

Exercise 7.6. Use the master theorem for $T(n) = 2T(n/4) + \sqrt{n}$.

Exercise 7.7. Find the ordinary generating function for the sequence defined by $a_n = 3a_{n-1}$, $a_0 = 2$. Verify by expanding as a power series.

Exercise 7.8. Prove by induction that the Tower of Hanoi requires at least $2^n - 1$ moves (i.e. the solution is optimal).

Exercise 7.9. Show that the Catalan numbers satisfy $C_n = \dfrac{4n-2}{n+1} C_{n-1}$ for $n \geq 1$, starting from $C_0 = 1$.

Exercise 7.10. A staircase has n steps. You can climb 1 or 2 steps at a time. Let s_n be the number of distinct ways to climb the staircase. Set up and solve the recurrence for s_n.

7.9 Chapter Summary

1. A **linear homogeneous recurrence with constant coefficients** is solved via the **characteristic equation**. Distinct roots give rise to exponential terms; repeated roots introduce polynomial factors.

2. A **non-homogeneous** recurrence is solved by combining the general homogeneous solution with a particular solution found by undetermined coefficients.

3. **Binet's formula** gives a closed form for the Fibonacci numbers using the golden ratio.

4. Classic recurrences include the **Tower of Hanoi** ($T_n = 2^n - 1$) and the **Catalan numbers** ($C_n = \frac{1}{n+1}\binom{2n}{n}$).

5. The **master theorem** gives asymptotic solutions to divide-and-conquer recurrences $T(n) = aT(n/b) + f(n)$.

6. **Generating functions** translate recurrences into algebraic equations for formal power series, from which closed forms can be extracted.

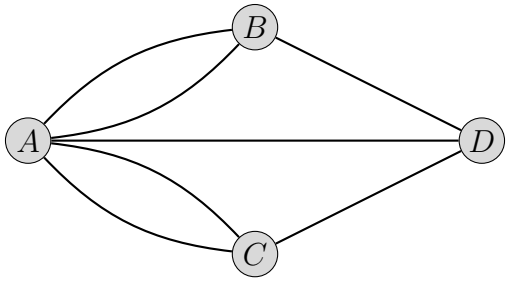
Chapter 8

Graph Theory — Basics

Graph theory is one of the most widely applicable branches of discrete mathematics, with uses ranging from network design and social-network analysis to chemistry, linguistics, and theoretical computer science. We begin with the historical problem that sparked the subject, then develop the fundamental definitions and results.

8.1 The Königsberg Bridge Problem

In 1736, Leonhard Euler considered whether one could walk through the city of Königsberg (now Kaliningrad) crossing each of its seven bridges exactly once and return to the starting point. He proved that no such walk exists by modelling the landmasses as *vertices* and the bridges as *edges*, creating what is regarded as the first theorem in graph theory.



8.2 Fundamental Definitions

Definition 8.1 (Graph)**.** A *graph* $G = (V, E)$ consists of a finite non-empty set V of *vertices* (also called *nodes*) and a set E of *edges*, where each edge is associated with an unordered pair of vertices.

Definition 8.2 (Adjacency and incidence)**.** Two vertices $u, v \in V$ are *adjacent* if there is an edge $e = \{u, v\} \in E$. In this case e is *incident* with both u and v, and u and v are called the *endpoints* of e.

Definition 8.3 (Loop and multi-edge)**.** An edge whose two endpoints coincide is called a *loop*. Two or more edges with the same pair of endpoints are called *multi-edges*

(or *parallel edges*).

8.3 Types of Graphs

Definition 8.4 (Simple graph)**.** A *simple graph* is a graph with no loops and no multi-edges. Every edge is uniquely determined by its pair of distinct endpoints, so we may identify E with a subset of $\binom{V}{2}$.

Definition 8.5 (Multigraph)**.** A *multigraph* allows multi-edges (but usually not loops). The Königsberg graph above is a multigraph.

Definition 8.6 (Directed graph)**.** A *directed graph* (or *digraph*) $G = (V, A)$ consists of a set V of vertices and a set A of *arcs* (directed edges), where each arc is an ordered pair (u, v) with u the *tail* and v the *head*.

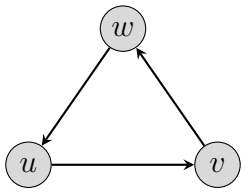


Figure 8.1: A directed graph on three vertices.

Definition 8.7 (Weighted graph)**.** A *weighted graph* is a graph in which each edge e is assigned a numerical value $w(e)$, called its *weight*.

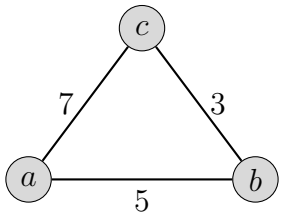


Figure 8.2: A weighted graph.

8.4 Graph Representations

8.4.1 Adjacency matrix

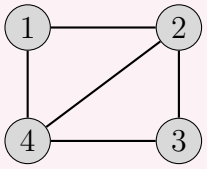
Definition 8.8 (Adjacency matrix)**.** Let G be a simple graph with vertices $v_1, \ldots, v_n$.

Its *adjacency matrix* is the $n \times n$ matrix $\mathbf{A}$ with

$$A_{ij} = \begin{cases} 1 & \text{if } \{v_i, v_j\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

For a simple undirected graph, $\mathbf{A}$ is symmetric with zeros on the diagonal.

Example 8.9 (Adjacency matrix)**.** Consider the following graph and its adjacency matrix.



$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

8.4.2 Incidence matrix

Definition 8.10 (Incidence matrix)**.** Let G have n vertices and m edges. The *incidence matrix* is the $n \times m$ matrix $\mathbf{B}$ where

$$B_{ij} = \begin{cases} 1 & \text{if vertex } v_i \text{ is an endpoint of edge } e_j, \\ 0 & \text{otherwise.} \end{cases}$$

Each column of $\mathbf{B}$ has exactly two ones (for a simple graph without loops).

8.4.3 Adjacency list

Definition 8.11 (Adjacency list)**.** An *adjacency list* representation stores, for each vertex v, the list of all vertices adjacent to v. This representation is often more space-efficient than an adjacency matrix for sparse graphs.

Example 8.12 (Adjacency list)**.** For the graph in Example 8.9:

$$\begin{aligned} &1 : \{2, 4\}, \\ &2 : \{1, 3, 4\}, \\ &3 : \{2, 4\}, \\ &4 : \{1, 2, 3\}. \end{aligned}$$

Remark 8.13. For a graph with n vertices and m edges, the adjacency matrix uses $\Theta(n^2)$ space, while the adjacency list uses $\Theta(n+m)$ space. Checking whether a specific edge exists takes $O(1)$ time with the matrix but $O(\deg v)$ time with the list.

8.5 Vertex Degree and the Handshaking Lemma

Definition 8.14 (Degree)**.** The *degree* of a vertex v in a graph G, denoted $\deg(v)$, is the number of edges incident with v (with loops counted twice). A vertex of degree 0 is called *isolated*.

Theorem 8.15 (Handshaking lemma)**.** *In any graph $G = (V, E)$,*

$$\sum_{v \in V} \deg(v) = 2 \operatorname{card} E. \tag{8.1}$$

Proof. Each edge $e = \{u, v\}$ contributes exactly 1 to $\deg(u)$ and 1 to $\deg(v)$, hence 2 to the total sum. Summing over all edges gives the result. □

Corollary 8.16. *In any graph, the number of vertices with odd degree is even.*

Proof. Let V_{odd} and V_{even} denote the sets of vertices of odd and even degree, respectively. By Theorem 8.15,

$$\sum_{v \in V_{\text{odd}}} \deg(v) + \sum_{v \in V_{\text{even}}} \deg(v) = 2 \operatorname{card} E.$$

The second sum is even (each term is even), and $2 \operatorname{card} E$ is even, so the first sum must be even. Since each term in the first sum is odd, the number of terms must be even. □

Definition 8.17 (In-degree and out-degree)**.** In a digraph, the *in-degree* $\deg^-(v)$ of vertex v is the number of arcs with head v, and the *out-degree* $\deg^+(v)$ is the number of arcs with tail v. For every digraph,

$$\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = \operatorname{card} A.$$

8.6 Walks, Paths, and Cycles

Definition 8.18 (Walk)**.** A *walk* in a graph G is a sequence of vertices $v_0, v_1, \ldots, v_k$ such that $\{v_{i-1}, v_i\} \in E$ for each $i = 1, \ldots, k$. The number k is the *length* of the walk.

Definition 8.19 (Trail and path)**.** A walk in which all *edges* are distinct is called a *trail*. A walk in which all *vertices* are distinct is called a *path*. (Every path is a trail, but not conversely.)

Definition 8.20 (Cycle)**.** A *cycle* (or *closed path*) is a walk $v_0, v_1, \ldots, v_k$ with $v_0 = v_k$, $k \geq 3$, and all vertices $v_0, v_1, \ldots, v_{k-1}$ distinct.

Definition 8.21 (Connectivity)**.** A graph G is *connected* if for every pair of vertices u, v there exists a path from u to v. A maximal connected subgraph of G is called a *connected component*.

Proposition 8.22. *A connected graph on n vertices has at least $n-1$ edges.*

Proof. We proceed by induction on n. The base case $n = 1$ is immediate (zero edges suffice). For the inductive step, let G be connected with $n \geq 2$ vertices. Choose a vertex v and consider the graph $G' = G - v$. If G' has c connected components, then G' has at least $n - 1 - c$ edges by induction applied to each component. Since G is connected, v must be adjacent to at least one vertex in each component of G', contributing at least c additional edges. Thus $\operatorname{card} E(G) \geq (n - 1 - c) + c = n - 1$. □

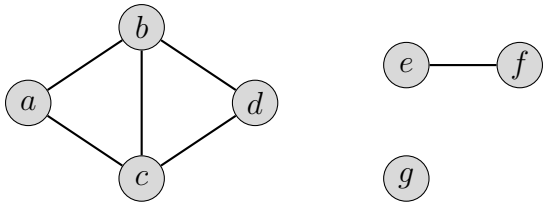
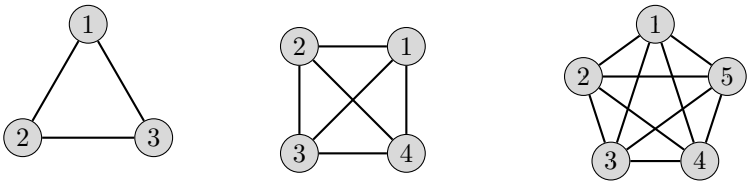


Figure 8.3: A graph with three connected components.

8.7 Important Families of Graphs

8.7.1 Complete graphs K_n

Definition 8.23 (Complete graph)**.** The *complete graph* K_n is the simple graph on n vertices in which every pair of distinct vertices is joined by an edge. It has $\binom{n}{2} = \frac{n(n-1)}{2}$ edges.



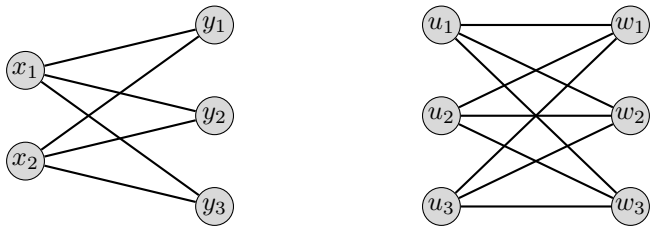
K_3 K_4 K_5

Figure 8.4: Complete graphs K_3, K_4, and K_5.

8.7.2 Complete bipartite graphs $K_{m,n}$

Definition 8.24 (Bipartite graph)**.** A graph $G = (V, E)$ is *bipartite* if V can be partitioned into two disjoint sets X and Y such that every edge has one endpoint in X and one in Y.

Definition 8.25 (Complete bipartite graph)**.** The *complete bipartite graph* $K_{m,n}$ has parts of sizes m and n, with every vertex in one part adjacent to every vertex in the other. It has mn edges.

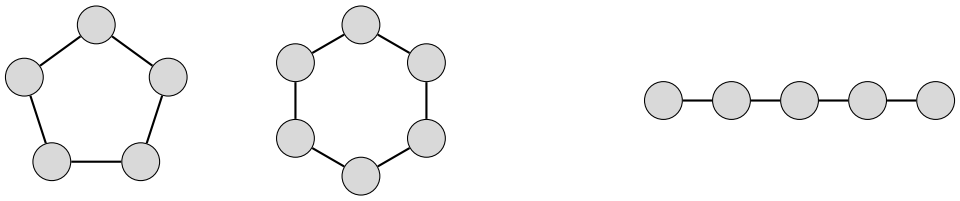


$K_{2,3}$ $K_{3,3}$

Figure 8.5: Complete bipartite graphs $K_{2,3}$ and $K_{3,3}$.

8.7.3 Cycle graphs C_n and path graphs P_n

Definition 8.26 (Cycle graph and path graph)**.** The *cycle graph* C_n ($n \geq 3$) is the graph consisting of a single cycle on n vertices. The *path graph* P_n ($n \geq 1$) is obtained from C_n by removing one edge (equivalently, it is a path with n vertices and $n-1$ edges).



C_5 C_6 P_5

Figure 8.6: Cycle graphs C_5, C_6 and path graph P_5.

8.7.4 The Petersen graph

Definition 8.27 (Petersen graph)**.** The *Petersen graph* is a 3-regular graph on 10 vertices and 15 edges. It serves as a counterexample to many optimistic conjectures in graph theory.

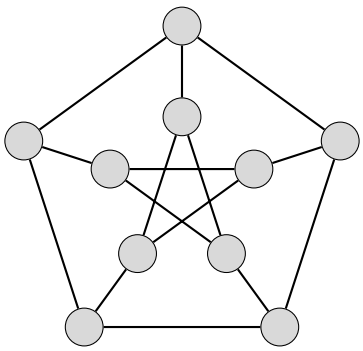


Figure 8.7: The Petersen graph.

Proposition 8.28. *The Petersen graph is*

1. *3-regular (every vertex has degree 3),*
2. *connected,*
3. *has girth 5 (the shortest cycle has length 5),*
4. *has diameter 2 (every two vertices are at distance at most 2),*
5. *not Hamiltonian (there is no cycle visiting every vertex exactly once).*

8.8 More Graph Illustrations

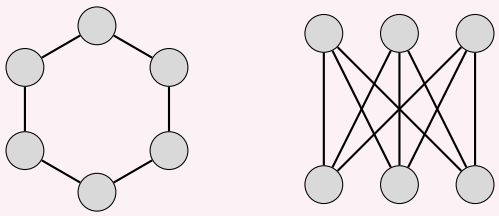
Visualising graphs is essential for building intuition. Here we collect further examples.

Example 8.29 (A graph and its complement)**.** The *complement* $\overline{G}$ of a simple graph $G = (V, E)$ is the graph on the same vertex set where $\{u, v\} \in E(\overline{G})$ if and only if $\{u, v\} \notin E(G)$.

G $\qquad$ $\overline{G}$

Together, G and $\overline{G}$ have all $\binom{4}{2} = 6$ possible edges.

Example 8.30 (Regular graphs)**.** A graph is *k-regular* if every vertex has degree k.



2-regular $\qquad$ 3-regular

Example 8.31 (The cube graph Q_3)**.** The 3-*dimensional cube graph* (or hypercube) Q_3 has 8 vertices labelled by binary strings of length 3, with two vertices adjacent if and only if their labels differ in exactly one bit.

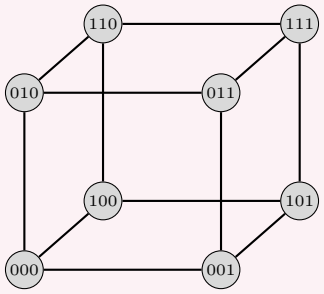


Figure 8.8: The cube graph Q_3.

Example 8.32 (A tree)**.** A *tree* is a connected acyclic graph. Every tree on n vertices has exactly $n - 1$ edges.

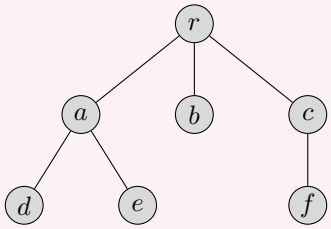


Figure 8.9: A rooted tree with root r.

8.9 Subgraphs and Graph Isomorphism

Definition 8.33 (Subgraph)**.** A graph $H = (V', E')$ is a *subgraph* of $G = (V, E)$ if $V' \subseteq V$ and $E' \subseteq E$. If $V' = V$, then H is a *spanning subgraph*.

Definition 8.34 (Induced subgraph)**.** Given $S \subseteq V$, the subgraph *induced* by S, denoted $G[S]$, has vertex set S and includes all edges of G whose both endpoints lie in S.

Definition 8.35 (Graph isomorphism)**.** Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are *isomorphic*, written $G_1 \cong G_2$, if there exists a bijection $\phi\colon V_1 \to V_2$ such that

$$\{u, v\} \in E_1 \iff \{\phi(u), \phi(v)\} \in E_2.$$

Remark 8.36. Isomorphic graphs share all structural properties: number of vertices, number of edges, degree sequence, connectivity, etc. These serve as *isomorphism invariants*: if any invariant differs, the graphs are not isomorphic. However, matching invariants does not guarantee isomorphism.

8.10 Exercises

Exercise 8.1. Draw the graphs K_6 and $K_{2,4}$. How many edges does each have?

Exercise 8.2. Write the adjacency matrix and an adjacency list for the cycle graph C_5 (label the vertices $1, 2, 3, 4, 5$).

Exercise 8.3. A graph has 6 vertices with degree sequence $(3, 3, 3, 3, 2, 2)$. How many edges does it have? Draw one such graph.

Exercise 8.4. Prove that a graph is bipartite if and only if it contains no odd cycle.

Exercise 8.5. Show that K_n has $\frac{n!}{2n}$ distinct Hamiltonian cycles for $n \geq 3$.

Exercise 8.6. For which values of n is the cycle graph C_n bipartite?

Exercise 8.7. A graph G is *self-complementary* if $G \cong \overline{G}$. Show that a self-complementary graph on n vertices has exactly $\binom{n}{2}/2$ edges. For which values of n is this an integer?

Exercise 8.8. Let G be a simple graph on n vertices. Show that if G has more than $\binom{n-1}{2}$ edges, then G is connected.

Exercise 8.9. Determine the number of vertices, edges, and the degree sequence of the Petersen graph directly from its definition. Verify the handshaking lemma.

Exercise 8.10. The *n-dimensional hypercube* Q_n has 2^n vertices labelled by binary strings of length n, with two vertices adjacent when their labels differ in exactly one position.

1. How many edges does Q_n have?
2. What is the degree of each vertex?
3. Show that Q_n is bipartite.

Exercise 8.11. Draw the Petersen graph and identify a Hamiltonian path (visiting all 10 vertices exactly once). Explain why no Hamiltonian *cycle* exists.

Exercise 8.12. Let G be a connected graph with exactly two vertices of odd degree. Show that G has an Eulerian trail (a trail using every edge exactly once) whose endpoints are the two odd-degree vertices.

8.11 Chapter Summary

1. A **graph** $G = (V, E)$ consists of vertices and edges. Variations include simple graphs, multigraphs, digraphs, and weighted graphs.
2. Graphs can be represented by an **adjacency matrix**, **incidence matrix**, or **adjacency list**, each with different space and time trade-offs.
3. The **handshaking lemma** states that $\sum_v \deg(v) = 2 \operatorname{card} E$, implying that the number of odd-degree vertices is always even.
4. A **walk** is a sequence of adjacent vertices; a **path** has no repeated vertices; a **cycle** is a closed path. A graph is **connected** if every pair of vertices is linked by a path.

5. Important graph families include the complete graphs K_n, the complete bipartite graphs $K_{m,n}$, the cycle graphs C_n, the path graphs P_n, and the **Petersen graph**.

6. **Isomorphic** graphs are structurally identical; invariants such as the degree sequence help distinguish non-isomorphic graphs.

Chapter 9

Trees, Eulerian and Hamiltonian Graphs

Trees are among the simplest yet most important structures in graph theory and computer science. They appear naturally in hierarchical data, search algorithms, network design, and combinatorial enumeration. In this chapter we characterize trees, study spanning trees and minimum-weight spanning trees, explore Eulerian and Hamiltonian graphs, and present the classical theorems of Dirac and Ore.

9.1 Trees: Definitions and Characterization

Definition 9.1 (Tree)**.** A *tree* is a connected acyclic graph. A *forest* is an acyclic graph (not necessarily connected); each connected component of a forest is a tree.

Definition 9.2 (Leaf)**.** A vertex of degree 1 in a tree is called a *leaf* (or *pendant vertex*).

Lemma 9.3. *Every tree with at least two vertices has at least two leaves.*

Proof. Let T be a tree on $n \geq 2$ vertices. Take a longest path $v_0, v_1, \ldots, v_k$ in T. Since T is acyclic, v_0 cannot be adjacent to any v_i with $i \geq 2$ (otherwise a cycle would form), and by maximality of the path v_0 has no neighbor outside the path. Hence $\deg(v_0) = 1$. The same argument applies to v_k. □

Theorem 9.4 (Characterization of trees)**.** *Let G be a graph on n vertices. The following are equivalent:*

1. *G is a tree (connected and acyclic).*
2. *G is connected and has exactly $n - 1$ edges.*
3. *G is acyclic and has exactly $n - 1$ edges.*
4. *For every pair of vertices u, v there is a unique path from u to v.*

5. *G is connected, but removing any edge disconnects it.*

6. *G is acyclic, but adding any edge creates exactly one cycle.*

Proof. We prove the cycle of implications $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1)$ and then show $(1) \Leftrightarrow (4) \Leftrightarrow (5) \Leftrightarrow (6)$.

$(1) \Rightarrow (2)$: By induction on n. For $n = 1$ the tree has $0 = n - 1$ edges. Suppose every tree on fewer than $n \geq 2$ vertices has $n - 2$ edges. By Lemma 9.3, G has a leaf v. Removing v and its incident edge gives a tree G' on $n - 1$ vertices, which by induction has $n - 2$ edges. Hence G has $n - 1$ edges. Since G is a tree it is connected.

$(2) \Rightarrow (3)$: Suppose G is connected with $n - 1$ edges but contains a cycle C. Removing an edge of C keeps G connected (both endpoints remain linked via the rest of the cycle) but yields a connected graph on n vertices with $n - 2$ edges. Repeating the argument as long as cycles remain we eventually reach a connected acyclic graph (a tree) on n vertices with fewer than $n - 1$ edges, contradicting $(1) \Rightarrow (2)$.

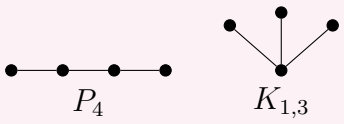
$(3) \Rightarrow (1)$: Suppose G is acyclic with $n - 1$ edges. Let G have k components $T_1, \ldots, T_k$ with n_i vertices each. Each T_i is a tree (connected and acyclic), so has $n_i - 1$ edges. The total number of edges is $\sum(n_i - 1) = n - k$. But G has $n - 1$ edges, so $k = 1$ and G is connected.

$(1) \Leftrightarrow (4)$: In a connected graph, a path between every pair exists. If two distinct paths joined u to v, their union would contain a cycle, contradicting acyclicity. Conversely, unique paths imply connectivity and acyclicity.

$(1) \Leftrightarrow (5)$: A tree is connected. If removing edge $\{u, v\}$ leaves the graph connected, an alternative u–v path together with the edge $\{u, v\}$ would form a cycle. Conversely, a connected graph in which every edge is a bridge is acyclic.

$(1) \Leftrightarrow (6)$: A tree is acyclic. Adding edge $\{u, v\}$ creates a cycle using the unique u–v path. Conversely, an acyclic graph where every non-edge addition creates exactly one cycle is connected (if u, v were in different components, adding $\{u, v\}$ would create no cycle). □

Example 9.5 (Small trees)**.** Up to isomorphism, there is one tree on $1, 2, 3$ vertices, two trees on 4 vertices (the path P_4 and the star $K_{1,3}$), and three trees on 5 vertices.



9.2 Spanning Trees

Definition 9.6 (Spanning tree)**.** A *spanning tree* of a connected graph G is a subgraph that is a tree and includes every vertex of G.

Proposition 9.7. *Every connected graph has a spanning tree.*

Proof. If G is connected and contains a cycle, remove an edge of that cycle; the resulting graph is still connected. Repeat until no cycle remains. The result is a connected acyclic spanning subgraph, hence a spanning tree. □

9.2.1 Cayley's Formula

Theorem 9.8 (Cayley, 1889)**.** *The number of labeled trees on the vertex set* $\{1, 2, \ldots, n\}$ *is* n^{n-2}.

We state without proof the classical result, noting that elegant proofs exist via Prüfer sequences and the matrix-tree theorem.

Example 9.9. For $n = 3$ there are $3^{3-2} = 3$ labeled trees on $\{1, 2, 3\}$: the edges are $\{1, 2\}, \{2, 3\}$; or $\{1, 3\}, \{2, 3\}$; or $\{1, 2\}, \{1, 3\}$.

9.3 Minimum Spanning Trees

Let $G = (V, E)$ be a connected graph with edge-weight function $w \colon E \to \mathbb{R}$. A *minimum spanning tree* (MST) is a spanning tree T that minimizes $\sum_{e \in E(T)} w(e)$.

9.3.1 Kruskal's Algorithm

1. Sort the edges in non-decreasing order of weight.
2. Initialize $T = \emptyset$.
3. For each edge e (in sorted order): add e to T if it does not create a cycle.
4. Return T.

Theorem 9.10. *Kruskal's algorithm produces a minimum spanning tree.*

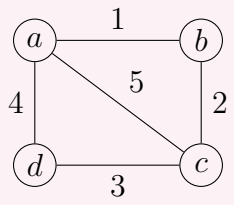
Proof sketch. At each step the lightest available edge that does not create a cycle is added. By the cut property (every lightest edge crossing a cut belongs to some MST), each chosen edge belongs to an MST. Since we select exactly $n - 1$ edges and form a spanning tree, the result is an MST. □

9.3.2 Prim's Algorithm

1. Start with an arbitrary vertex v_0; set $S = \{v_0\}$, $T = \emptyset$.
2. While $S \neq V$: among all edges with one endpoint in S and the other in $V \setminus S$, choose one of minimum weight, say $\{u, v\}$ with $u \in S$. Add v to S and $\{u, v\}$ to T.
3. Return T.

Theorem 9.11. *Prim's algorithm produces a minimum spanning tree.*

Example 9.12 (MST computation)**.** Consider the weighted graph below. Both Kruskal's and Prim's algorithms yield the MST with edges $\{a, b\}, \{b, c\}, \{c, d\}$ of total weight 6.



9.4 Eulerian Graphs

Definition 9.13 (Euler circuit and Euler path)**.** An *Euler circuit* in a graph G is a closed walk that traverses every edge exactly once. An *Euler path* is a walk that traverses every edge exactly once (not necessarily closed). A graph possessing an Euler circuit is called *Eulerian*.

Theorem 9.14 (Euler, 1736)**.** *A connected graph G has an Euler circuit if and only if every vertex of G has even degree. It has an Euler path (but no Euler circuit) if and only if it has exactly two vertices of odd degree.*

Proof. ($\Rightarrow$) If G has an Euler circuit, each visit to a vertex uses one edge to enter and one to leave, contributing 2 to the degree. Hence every vertex has even degree.

($\Leftarrow$) We proceed by strong induction on $|E(G)|$. If $|E(G)| = 0$ the empty walk suffices. Otherwise, since every vertex has even degree ≥ 2, G contains a cycle C (start at any vertex and walk without repeating a vertex; since every visited vertex has even degree, we must eventually return). Remove the edges of C from G to obtain G'. Every vertex of G' still has even degree. Each connected component of G' with edges is Eulerian by induction. We splice: walk along C, and whenever we reach a vertex that starts a component of G' with edges, we detour through that component's Euler circuit before continuing along C. The result is an Euler circuit of G.

For the Euler path statement: if G has exactly two odd-degree vertices u and v, add edge $\{u, v\}$ to make all degrees even; find an Euler circuit; remove $\{u, v\}$ to obtain an Euler path from u to v. □

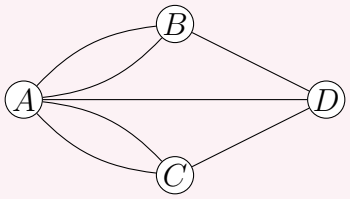
9.4.1 Fleury's Algorithm

Given an Eulerian graph G:

1. Start at any vertex.
2. At each step, choose an edge to traverse. Prefer a non-bridge edge (i.e., do not cross a bridge unless no other option exists).
3. Remove the traversed edge. Repeat until all edges are traversed.

Remark 9.15. Fleury's algorithm, while elegant, runs in $O(|E|^2)$ time because of bridge-checking. Hierholzer's algorithm achieves $O(|E|)$.

Example 9.16 (Königsberg bridges)**.** The original Königsberg bridge graph has four vertices with degrees $3, 3, 3, 5$ — all odd. Hence it has neither an Euler path nor an Euler circuit, which was Euler's celebrated 1736 result.



9.5 Hamiltonian Graphs

Definition 9.17 (Hamilton cycle and Hamilton path)**.** A *Hamilton cycle* in a graph G is a cycle that visits every vertex exactly once. A *Hamilton path* visits every vertex exactly once. A graph possessing a Hamilton cycle is called *Hamiltonian*.

Remark 9.18. Unlike the Eulerian case, no simple necessary and sufficient condition for the existence of a Hamilton cycle is known. In fact, deciding whether a graph is Hamiltonian is NP-complete.

Theorem 9.19 (Dirac, 1952)**.** *If G is a simple graph on $n \geq 3$ vertices such that $\deg(v) \geq n/2$ for every vertex v, then G is Hamiltonian.*

Proof. Suppose for contradiction that G satisfies the degree condition but is not Hamiltonian. Add edges to G one at a time (choosing non-adjacent pairs) until obtaining a graph G^* that is not Hamiltonian but adding any further edge would create a Hamilton cycle. Such a maximal non-Hamiltonian graph G^* still satisfies $\deg(v) \geq n/2$.

Let u, v be non-adjacent in G^*. Then $G^* + \{u, v\}$ has a Hamilton cycle, which must use the edge $\{u, v\}$. Hence G^* has a Hamilton path $v = v_1, v_2, \ldots, v_n = u$.

Define the sets:

$$S = \{i : v_i \text{ is adjacent to } u\}, \qquad T = \{i : v_{i+1} \text{ is adjacent to } v\}.$$

Then $|S| \geq n/2$ and $|T| \geq n/2$, and both $S, T \subseteq \{1, \ldots, n-1\}$. By pigeonhole, there exists $i \in S \cap T$. Then v_i is adjacent to $u = v_n$ and v_{i+1} is adjacent to $v = v_1$. The cycle

$$v_1, v_2, \ldots, v_i, v_n, v_{n-1}, \ldots, v_{i+1}, v_1$$

is a Hamilton cycle in G^*, a contradiction. □

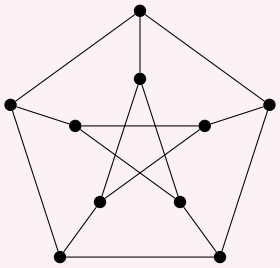
Theorem 9.20 (Ore, 1960)**.** *If G is a simple graph on $n \geq 3$ vertices such that for every pair of non-adjacent vertices u, v we have $\deg(u) + \deg(v) \geq n$, then G is Hamiltonian.*

Proof. The proof is virtually identical to Dirac's. We form the maximal non-Hamiltonian graph G^* and obtain a Hamilton path $v_1, v_2, \ldots, v_n$ with v_1, v_n non-adjacent. Ore's condition gives $\deg(v_1) + \deg(v_n) \geq n$. The same pigeonhole argument as above yields a Hamilton cycle, contradicting maximality. □

Corollary 9.21. *Dirac's theorem follows from Ore's theorem.*

Proof. If $\deg(v) \geq n/2$ for all v, then $\deg(u) + \deg(v) \geq n$ for every pair u, v, so Ore's condition is satisfied. □

Example 9.22 (Hamiltonian vs. non-Hamiltonian)**.** The Petersen graph is 3-regular on 10 vertices. Since $3 < 10/2 = 5$, Dirac's theorem does not apply, and indeed the Petersen graph is not Hamiltonian (though it does have a Hamilton path).



9.6 Exercises

Exercise 9.1. Prove that a forest on n vertices and k components has exactly $n - k$ edges.

Exercise 9.2. Use Prüfer sequences to show that the complete graph K_n has n^{n-2} spanning trees.

Exercise 9.3. Apply Kruskal's algorithm to the complete graph K_4 with edge weights $w(1,2) = 3$, $w(1,3) = 1$, $w(1,4) = 6$, $w(2,3) = 4$, $w(2,4) = 2$, $w(3,4) = 5$. List the edges in the order they are added.

Exercise 9.4. Let G be a connected graph with exactly $2k$ vertices of odd degree ($k \geq 1$). Show that the edges of G can be partitioned into exactly k edge-disjoint paths (none of which is closed).

Exercise 9.5. Show that the n-dimensional hypercube graph Q_n is Hamiltonian for $n \geq 2$.

Exercise 9.6. Let G be a simple graph on 7 vertices such that every vertex has degree at least 4. Prove that G is Hamiltonian using Ore's theorem.

Chapter 10

Coloring, Planarity, and Bipartite Graphs

Graph coloring, planarity, and bipartiteness are central themes in graph theory with wide-ranging applications in scheduling, map design, register allocation, and combinatorial optimization.

10.1 Vertex Coloring

Definition 10.1 (Proper coloring, chromatic number)**.** A *proper k-coloring* of a graph $G = (V, E)$ is a function $c\colon V \to \{1, 2, \dots, k\}$ such that $c(u) \neq c(v)$ whenever $\{u, v\} \in E$. The *chromatic number* $\chi(G)$ is the smallest k for which G admits a proper k-coloring.

Example 10.2.

- $\chi(K_n) = n$.
- $\chi(C_{2k}) = 2$ and $\chi(C_{2k+1}) = 3$ for $k \geq 1$.
- A graph is bipartite if and only if $\chi(G) \leq 2$.

10.1.1 Greedy Coloring

Proposition 10.3 (Greedy bound)**.** *For any graph G, $\chi(G) \leq \Delta(G) + 1$, where $\Delta(G)$ is the maximum degree.*

Proof. Order the vertices $v_1, \dots, v_n$ arbitrarily. Assign to v_i the smallest color not used by its already-colored neighbors. Since v_i has at most $\Delta(G)$ neighbors, at most $\Delta(G)$ colors are forbidden, and a color among $\{1, \dots, \Delta(G) + 1\}$ is always available. □

Theorem 10.4 (Brooks, 1941)**.** *If G is a connected graph that is neither a complete graph nor an odd cycle, then $\chi(G) \leq \Delta(G)$.*

Remark 10.5 (Four Color Theorem). Every planar graph is 4-colorable. This was proved by Appel and Haken (1976) with extensive computer assistance, and later verified by Robertson, Sanders, Seymour, and Thomas (1997).

10.2 Chromatic Polynomial

Definition 10.6 (Chromatic polynomial)**.** The *chromatic polynomial* $P(G, k)$ counts the number of proper k-colorings of G. It is a polynomial in k.

Example 10.7. For a tree T on n vertices, $P(T, k) = k(k-1)^{n-1}$.

Proof. Root the tree. The root has k choices. Each subsequent vertex (processed parent before children) has $k-1$ choices (any color except its parent's). □

10.2.1 Deletion–Contraction

Theorem 10.8 (Deletion–Contraction)**.** *For any edge $e = \{u, v\}$ of G:*

$$P(G, k) = P(G - e,\ k) - P(G/e,\ k),$$

where $G - e$ is obtained by deleting e and G/e by contracting e (merging u and v and removing resulting multi-edges).

Proof. The colorings of $G - e$ can be split into two classes: those where $c(u) \neq c(v)$, which number $P(G, k)$, and those where $c(u) = c(v)$, which are in bijection with colorings of G/e (the merged vertex receives the common color). Hence $P(G - e, k) = P(G, k) + P(G/e, k)$. □

Example 10.9. For the cycle C_4, contracting an edge gives C_3 and deleting it gives P_4:

$$P(C_4, k) = P(P_4, k) - P(C_3, k) = k(k-1)^3 - k(k-1)(k-2) = (k-1)^4 + (k-1).$$

10.3 Planar Graphs

Definition 10.10 (Planar graph)**.** A graph is *planar* if it can be drawn in the plane with no edge crossings. Such a drawing is called a *planar embedding*. The connected regions of the complement of the drawing are called *faces*.

Theorem 10.11 (Euler's formula for planar graphs)**.** *If G is a connected planar graph with V vertices, E edges, and F faces (including the outer face), then*

$$V - E + F = 2.$$

Proof. By induction on E. If $E = 0$, then $V = 1$ and $F = 1$ (only the outer face), so $1 - 0 + 1 = 2$.

If G is a tree, then $E = V - 1$ and $F = 1$, so $V - (V - 1) + 1 = 2$.

If G contains a cycle, let e be an edge on a cycle. Removing e merges two faces into one, so F decreases by 1 while V stays the same and E decreases by 1. By induction on the smaller graph, $V - (E - 1) + (F - 1) = 2$, which gives $V - E + F = 2$. □

Corollary 10.12. *If G is a simple connected planar graph with $V \geq 3$ vertices, then $E \leq 3V - 6$.*

Proof. Each face is bounded by at least 3 edges, and each edge borders at most 2 faces, so $2E \geq 3F$. Thus $F \leq 2E/3$. Substituting into Euler's formula: $2 = V - E + F \leq V - E + 2E/3 = V - E/3$, giving $E \leq 3V - 6$. □

Corollary 10.13. *If G is a simple connected planar graph with $V \geq 3$ and no triangles, then $E \leq 2V - 4$.*

Proof. Without triangles, each face is bounded by at least 4 edges, so $2E \geq 4F$, hence $F \leq E/2$. Then $2 = V - E + F \leq V - E/2$, giving $E \leq 2V - 4$. □

Theorem 10.14 (K_5 is non-planar)**.** *The complete graph K_5 is not planar.*

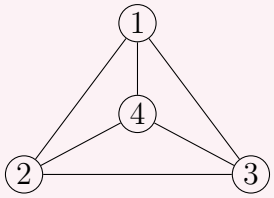
Proof. K_5 has $V = 5$ and $E = 10$. But $3V - 6 = 9 < 10 = E$, violating Corollary 10.12. □

Theorem 10.15 ($K_{3,3}$ is non-planar)**.** *The complete bipartite graph $K_{3,3}$ is not planar.*

Proof. $K_{3,3}$ has $V = 6$ and $E = 9$. Since $K_{3,3}$ is bipartite it contains no triangles, so Corollary 10.13 applies: $E \leq 2V - 4 = 8 < 9 = E$, a contradiction. □

Theorem 10.16 (Kuratowski, 1930)**.** *A graph is planar if and only if it contains no subdivision of K_5 or $K_{3,3}$ as a subgraph.*

Example 10.17 (Planar embedding of K_4)**.**



$V = 4,\ E = 6,\ F = 4$

$4 - 6 + 4 = 2$ ✓

10.4 Bipartite Graphs

Definition 10.18 (Bipartite graph)**.** A graph $G = (V, E)$ is *bipartite* if V can be partitioned into two sets A and B such that every edge has one endpoint in A and one in B.

Theorem 10.19 (Odd-cycle characterization)**.** *A graph is bipartite if and only if it contains no odd cycle.*

Proof. ($\Rightarrow$) In a bipartite graph with parts A, B, any walk alternates between A and B. A cycle that starts in A must return to A, requiring an even number of steps.

($\Leftarrow$) Suppose G has no odd cycle. We may assume G is connected (handle components independently). Fix a vertex s and define

$$A = \{v \in V : d(s, v) \text{ is even}\}, \qquad B = \{v \in V : d(s, v) \text{ is odd}\},$$

where $d(s, v)$ is the distance from s to v. We claim every edge joins a vertex in A to one in B. Suppose $\{u, v\} \in E$ with $u, v \in A$ (both at even distance from s). Then a shortest s–u path, the edge $\{u, v\}$, and a shortest v–s path form a closed walk of odd length, which must contain an odd cycle, contradicting our hypothesis. A symmetric argument handles $u, v \in B$. □

10.5 Matchings

Definition 10.20 (Matching)**.** A *matching* in a graph G is a set of pairwise disjoint edges. A matching is *perfect* if it covers every vertex.

Theorem 10.21 (König, 1931)**.** *In a bipartite graph, the maximum size of a matching equals the minimum size of a vertex cover.*

Theorem 10.22 (Hall's marriage theorem)**.** *Let $G = (A \cup B, E)$ be a bipartite graph. There exists a matching that covers every vertex in A if and only if for every $S \subseteq A$,*

$$|N(S)| \geq |S|,$$

where $N(S) = \{b \in B : \{a, b\} \in E \text{ for some } a \in S\}$ is the neighborhood of S.

Proof. ($\Rightarrow$) If a matching covers A, then for every $S \subseteq A$ the matched partners of S lie in $N(S)$, so $|N(S)| \geq |S|$.

($\Leftarrow$) By induction on $|A|$. If $|A| = 1$ the condition $|N(S)| \geq 1$ ensures A has a neighbor, and the single edge is a matching.

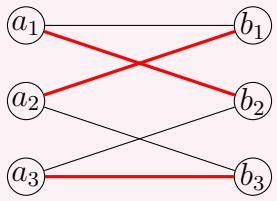
Case 1: $|N(S)| \geq |S| + 1$ for every non-empty proper subset $S \subsetneq A$. Pick any $a \in A$ and any neighbor $b \in N(a)$. Match a to b. In the graph $G' = G - (a, b)$ (removing a, b and their edges), for any $S' \subseteq A \setminus \{a\}$: $|N_{G'}(S')| \geq |N_G(S')| - 1 \geq (|S'| + 1) - 1 = |S'|$. By induction, G' has a matching covering $A \setminus \{a\}$.

Case 2: There exists a non-empty proper subset $S \subsetneq A$ with $|N(S)| = |S|$. By induction, the subgraph induced by $S \cup N(S)$ has a matching M_1 covering S. Now consider the subgraph G'' induced by $(A \setminus S) \cup (B \setminus N(S))$. For any $T \subseteq A \setminus S$:

$$|N_{G''}(T)| = |N_G(S \cup T)| - |N(S)| \geq |S \cup T| - |S| = |T|\,.$$

By induction, G'' has a matching M_2 covering $A \setminus S$. Then $M_1 \cup M_2$ covers all of A. $\square$

Example 10.23 (Matching in a bipartite graph)**.**



Perfect matching in red

10.6 Exercises

Exercise 10.1. Show that the chromatic number of the Petersen graph is 3.

Exercise 10.2. Compute the chromatic polynomial $P(C_n, k)$ for the cycle C_n using deletion–contraction.

Exercise 10.3. Verify Euler's formula $V - E + F = 2$ for the cube graph Q_3 drawn in the plane.

Exercise 10.4. Show that $K_{2,3}$ is planar by giving an explicit planar embedding.

Exercise 10.5. A dormitory has n students, each listing 3 acceptable rooms from among n rooms. If every set of k students collectively list at least k acceptable rooms, show that every student can be assigned an acceptable room.

Exercise 10.6. In the bipartite graph of Example 10.23, find a minimum vertex cover and verify König's theorem.

Exercise 10.7. Let $G = (A \cup B, E)$ be a bipartite graph where every vertex in A has degree $d \geq 1$ and every vertex in B has degree at most d. Prove that G has a matching covering A.

Chapter 11

Introduction to Coding Theory

Digital communication channels are inherently noisy. Coding theory provides mathematical tools to detect and correct errors introduced during transmission or storage. This chapter introduces the basic concepts of error-correcting codes, with emphasis on linear codes and the elegant family of Hamming codes.

11.1 Basic Concepts

We work over the binary field $\mathbb{F}_2 = \{0, 1\}$ with arithmetic modulo 2. A *binary code* of length n is a subset $\mathcal{C} \subseteq \mathbb{F}_2^n$. Each element of $\mathcal{C}$ is a *codeword*.

Definition 11.1 (Hamming distance)**.** The *Hamming distance* $d(\mathbf{x}, \mathbf{y})$ between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ is the number of positions in which they differ:

$$d(\mathbf{x}, \mathbf{y}) = \operatorname{card}\{i : x_i \neq y_i\}.$$

Definition 11.2 (Hamming weight)**.** The *Hamming weight* $\operatorname{wt}(\mathbf{x})$ of a vector $\mathbf{x}$ is $d(\mathbf{x}, \mathbf{0})$, the number of nonzero entries.

Proposition 11.3. *The Hamming distance is a metric on $\mathbb{F}_2^n$.*

Definition 11.4 (Minimum distance)**.** The *minimum distance* of a code $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathcal{C},\ \mathbf{x} \neq \mathbf{y}\}.$$

An (n, M, d)-code has length n, M codewords, and minimum distance d.

Theorem 11.5 (Error detection and correction)**.** *A code with minimum distance d can:*

1. *detect up to $d - 1$ errors,*
2. *correct up to $\lfloor (d-1)/2 \rfloor$ errors.*

Proof. (1) If at most $d-1$ errors occur, the received word differs from the sent codeword in at most $d-1$ positions, hence is not a codeword (since all codewords are at distance $\geq d$).

(2) If at most $t = \lfloor (d-1)/2 \rfloor$ errors occur, the received word $\mathbf{r}$ is within distance t of the sent codeword $\mathbf{c}$. For any other codeword $\mathbf{c}'$:

$$d(\mathbf{c}, \mathbf{c}') \leq d(\mathbf{c}, \mathbf{r}) + d(\mathbf{r}, \mathbf{c}') \implies d(\mathbf{r}, \mathbf{c}') \geq d - t > t.$$

So $\mathbf{c}$ is the unique closest codeword to $\mathbf{r}$. □

Example 11.6 (Repetition code)**.** The binary repetition code of length n is $\mathcal{C} = \{00\cdots0,\ 11\cdots1\}$ with $d = n$. It can correct $\lfloor (n-1)/2 \rfloor$ errors but has very low rate $(1/n)$.

11.2 Linear Codes

Definition 11.7 (Linear code)**.** A *linear code* $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_2^n$. We say $\mathcal{C}$ is an $[n,k]$-code, or $[n,k,d]$-code if the minimum distance is d.

Proposition 11.8. *For a linear code, the minimum distance equals the minimum weight of a nonzero codeword:*

$$d(\mathcal{C}) = \min\{\mathrm{wt}(\mathbf{c}) : \mathbf{c} \in \mathcal{C},\ \mathbf{c} \neq \mathbf{0}\}.$$

Proof. Since $\mathcal{C}$ is a subspace, $\mathbf{x} - \mathbf{y} \in \mathcal{C}$ for all $\mathbf{x}, \mathbf{y} \in \mathcal{C}$. Over $\mathbb{F}_2$, $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} + \mathbf{y})$, so the minimum distance is the minimum weight of a nonzero codeword. □

11.2.1 Generator and Parity-Check Matrices

Definition 11.9 (Generator matrix)**.** A *generator matrix* of an $[n,k]$-code $\mathcal{C}$ is a $k \times n$ matrix G whose rows form a basis of $\mathcal{C}$. Thus $\mathcal{C} = \left\{\mathbf{u}G : \mathbf{u} \in \mathbb{F}_2^k\right\}$.

Definition 11.10 (Systematic form)**.** A generator matrix is in *systematic form* (or *standard form*) if $G = [I_k \mid A]$, where I_k is the $k \times k$ identity and A is a $k \times (n-k)$ matrix.

Definition 11.11 (Parity-check matrix)**.** A *parity-check matrix* of an $[n,k]$-code is an $(n-k) \times n$ matrix H such that $\mathcal{C} = \left\{\mathbf{x} \in \mathbb{F}_2^n : H\mathbf{x}^T = \mathbf{0}\right\}$.

Proposition 11.12. *If $G = [I_k \mid A]$ is a generator matrix in systematic form, then $H = [-A^T \mid I_{n-k}]$ is a parity-check matrix. Over $\mathbb{F}_2$, $-A^T = A^T$, so $H = [A^T \mid I_{n-k}]$.*

Proof. We verify $GH^T = 0$: $[I_k \mid A][A \mid I_{n-k}]^T = A + A = 0$ over $\mathbb{F}_2$. Since H has rank $n-k$, the null space of H is k-dimensional, hence equals $\mathcal{C}$. □

Theorem 11.13 (Minimum distance from parity-check matrix)**.** *The minimum distance of a linear code with parity-check matrix H equals the minimum number of linearly dependent columns of H.*

Proof. A codeword $\mathbf{c}$ satisfies $H\mathbf{c}^T = \mathbf{0}$, meaning the columns of H indexed by the support of $\mathbf{c}$ sum to zero. Thus $\mathrm{wt}(\mathbf{c})$ equals the number of columns in a linear dependence. The minimum weight (hence minimum distance) is the smallest such dependence. □

11.2.2 Syndrome Decoding

Definition 11.14 (Syndrome)**.** The *syndrome* of a received vector $\mathbf{r} \in \mathbb{F}_2^n$ is $\mathbf{s} = H\mathbf{r}^T \in \mathbb{F}_2^{n-k}$.

Proposition 11.15. *Two vectors have the same syndrome if and only if they are in the same coset of $\mathcal{C}$ in $\mathbb{F}_2^n$.*

Proof. $H\mathbf{r}_1^T = H\mathbf{r}_2^T$ iff $H(\mathbf{r}_1 - \mathbf{r}_2)^T = \mathbf{0}$ iff $\mathbf{r}_1 - \mathbf{r}_2 \in \mathcal{C}$. □

The syndrome decoding procedure:

1. Precompute a *syndrome table*: for each syndrome $\mathbf{s}$, store the *coset leader* (minimum-weight vector in the coset).
2. Given received $\mathbf{r}$, compute $\mathbf{s} = H\mathbf{r}^T$.
3. Look up the coset leader $\mathbf{e}$ for syndrome $\mathbf{s}$.
4. Decode as $\hat{\mathbf{c}} = \mathbf{r} - \mathbf{e} = \mathbf{r} + \mathbf{e}$ (over $\mathbb{F}_2$).

Example 11.16. Consider the $[6, 3, 3]$-code with generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

The parity-check matrix is

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

If $\mathbf{r} = (1, 1, 0, 1, 1, 1)$ is received, the syndrome is $H\mathbf{r}^T = (1, 0, 0)^T$. The coset leader with this syndrome is $\mathbf{e} = (0, 0, 1, 0, 0, 0)$, so we decode $\hat{\mathbf{c}} = (1, 1, 1, 1, 1, 1)$.

11.3 Hamming Codes

Definition 11.17 (Hamming code)**.** For an integer $r \geq 2$, the *Hamming code* $\mathrm{Ham}(r, 2)$ is the $[2^r - 1,\, 2^r - 1 - r,\, 3]$-code whose parity-check matrix H has as columns all nonzero vectors in $\mathbb{F}_2^r$ (in any order).

Theorem 11.18. *The Hamming code* $\mathrm{Ham}(r, 2)$ *has the following properties:*

1. *It is a* $[2^r - 1,\, 2^r - 1 - r,\, 3]$*-code.*
2. *It can correct any single error.*
3. *It is a* perfect code*: every vector in* $\mathbb{F}_2^n$ *is within Hamming distance* 1 *of exactly one codeword.*

Proof. (1) The matrix H is $r \times (2^r - 1)$ with rank r (it contains I_r as a submatrix). So the code has dimension $(2^r - 1) - r$. Any two columns of H are distinct nonzero vectors, hence linearly independent (over $\mathbb{F}_2$, two distinct nonzero vectors are independent). Thus no codeword has weight 1 or 2, and $d \geq 3$. Since H has $2^r - 1 \geq 3$ columns, some three are dependent, so $d = 3$.

(2) With $d = 3$, the code corrects $\lfloor (3 - 1)/2 \rfloor = 1$ error.

(3) The number of vectors within distance 1 of a codeword is $1 + n = 1 + (2^r - 1) = 2^r$. The total number of such balls is $|\mathcal{C}| \cdot 2^r = 2^{2^r - 1 - r} \cdot 2^r = 2^{2^r - 1}$, which equals $|\mathbb{F}_2^n|$. Hence the balls partition $\mathbb{F}_2^n$: the code is perfect. □

Example 11.19 (Hamming(7,4))**.** For $r = 3$, we get the $[7, 4, 3]$-Hamming code. A standard parity-check matrix is

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

where column j is the binary representation of j (for $j = 1, \ldots, 7$). The syndrome $H\mathbf{r}^T$ of a single-error vector directly gives the binary index of the error position.

Remark 11.20 (Decoding Hamming codes). If the syndrome is $\mathbf{0}$, no error is detected. Otherwise, the syndrome (read as a binary number) gives the position of the single error, which is then flipped. This makes Hamming code decoding exceptionally simple.

Example 11.21 (Hamming(7,4) decoding)**.** Suppose we send codeword $\mathbf{c} = (1, 0, 1, 1, 0, 0, 1)$ and receive $\mathbf{r} = (1, 0, 1, 1, 0, 1, 1)$ (error in position 6). The syndrome is

$$H\mathbf{r}^T = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = (110)_2 = 6.$$

We flip bit 6 to recover $\hat{\mathbf{c}} = (1, 0, 1, 1, 0, 0, 1) = \mathbf{c}$.

11.4 The Singleton and Hamming Bounds

Theorem 11.22 (Singleton bound)**.** *An (n, M, d)-code satisfies $M \leq 2^{n-d+1}$. Equivalently, for an $[n, k, d]$-linear code, $k \leq n - d + 1$.*

Proof. Project each codeword onto the first $n - d + 1$ coordinates. Any two distinct codewords that agree on these coordinates must differ only in the last $d - 1$ coordinates, giving distance at most $d - 1 < d$, a contradiction. Hence the projection is injective: $M \leq 2^{n-d+1}$. □

Theorem 11.23 (Hamming bound (sphere-packing bound))**.** *An (n, M, d)-code with $d = 2t + 1$ satisfies*

$$M \cdot \sum_{i=0}^{t} \binom{n}{i} \leq 2^n.$$

Codes achieving equality are perfect*.*

Proof. The balls of radius t centered at distinct codewords are disjoint (since any two codewords are at distance $\geq 2t + 1$). Each ball contains $\sum_{i=0}^{t} \binom{n}{i}$ vectors. All balls lie within $\mathbb{F}_2^n$, which has 2^n elements. □

11.5 Reed–Solomon Codes: A Brief Mention

Reed–Solomon codes, introduced by Irving Reed and Gustave Solomon in 1960, are among the most widely deployed error-correcting codes. They operate over larger finite fields $\mathbb{F}_q$ (typically $q = 2^m$) and achieve the Singleton bound with equality, making them *maximum distance separable* (MDS) codes.

A Reed–Solomon code of length $n = q - 1$ and dimension k encodes a message polynomial $m(x)$ of degree $< k$ as the vector of evaluations $(m(\alpha_1), \ldots, m(\alpha_n))$, where $\alpha_1, \ldots, \alpha_n$ are the nonzero elements of $\mathbb{F}_q$. The minimum distance is $d = n - k + 1$.

Remark 11.24. Reed–Solomon codes are used in compact discs, QR codes, deep-space communication (Voyager, Mars rovers), and digital television (DVB). Their algebraic structure enables efficient decoding algorithms such as the Berlekamp–Massey algorithm.

11.6 Exercises

Exercise 11.1. Verify that the Hamming distance is a metric (prove the triangle inequality).

Exercise 11.2. The $[n, n - 1, 2]$ single-parity-check code consists of all binary vectors of even weight. Find its generator and parity-check matrices.

Exercise 11.3. Write down the parity-check matrix for $\mathrm{Ham}(4, 2)$, a $[15, 11, 3]$-code. How many codewords does it have?

Exercise 11.4. For the $[7, 4, 3]$-Hamming code, construct the complete syndrome table and decode the received vectors $\mathbf{r}_1 = (1, 1, 0, 0, 1, 0, 1)$ and $\mathbf{r}_2 = (0, 1, 1, 1, 0, 1, 0)$.

Exercise 11.5. Show that the only binary perfect e-error-correcting codes (for $e \geq 1$) are the Hamming codes ($e = 1$), the binary Golay code ($e = 3$, $n = 23$), and the repetition codes of odd length. (You may quote the classification theorem without proof.)

Exercise 11.6. Show that the $[n, 1, n]$ repetition code and the $[n, n-1, 2]$ parity-check code both meet the Singleton bound.

Exercise 11.7. The *dual code* $\mathcal{C}^\perp$ of an $[n, k]$-code $\mathcal{C}$ is the set of all vectors orthogonal to every codeword. Show that $\mathcal{C}^\perp$ is an $[n, n-k]$-code and that $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Exercise 11.8. The *weight enumerator* of a code $\mathcal{C}$ is the polynomial $W_\mathcal{C}(x, y) = \sum_{\mathbf{c}\in\mathcal{C}} x^{n-\mathrm{wt}(\mathbf{c})} y^{\mathrm{wt}(\mathbf{c})}$. Compute $W_\mathcal{C}(x, y)$ for the $[7, 4, 3]$-Hamming code.

Appendix A

Combinatorial Identities

The following table collects important combinatorial identities that appear throughout this course. In each identity, n and k are non-negative integers with $0 \le k \le n$ unless otherwise stated, and x, y may be real or complex numbers as appropriate.

Identity	**Name / Comment**
$\binom{n}{k} = \binom{n}{n-k}$	Symmetry of binomial coefficients
$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$	Pascal's identity
$\sum_{k=0}^{n} \binom{n}{k} = 2^n$	Sum of binomial coefficients
$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$	Alternating sum ($n \ge 1$)
$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$	Binomial theorem
$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}$	Vandermonde's identity
$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$	Special case of Vandermonde ($m = n = r$)
$\binom{n}{k}\binom{k}{j} = \binom{n}{j}\binom{n-j}{k-j}$	Absorption / triple binomial
$k\binom{n}{k} = n\binom{n-1}{k-1}$	Absorption identity
$\sum_{k=0}^{n} k\binom{n}{k} = n\,2^{n-1}$	Weighted sum
$\sum_{j=k}^{n} \binom{j}{k} = \binom{n+1}{k+1}$	Hockey-stick / Christmas-stocking identity
$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k}$	Upper negation

Identity	Name / Comment
$\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$	Stars and bars (multiset coefficient)
$\sum_{k=0}^{n} k^2 \binom{n}{k} = n(n+1)2^{n-2}$ (for $n \geq 2$)	Second moment
$\sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n$	Binomial series (finite)
$\sum_{k=0}^{\infty} \binom{n+k}{k} x^k = \frac{1}{(1-x)^{n+1}}$	Negative binomial series ($\lvert x\rvert < 1$)
$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$	Number of derangements
$\lvert A_1 \cup \cdots \cup A_n\rvert = \sum_{k=1}^{n} (-1)^{k+1} \sum_{I \subseteq [n],\, \lvert I\rvert = k} \left\lvert \bigcap_{i \in I} A_i \right\rvert$	Inclusion–exclusion principle
$\sum_{d \mid n} \varphi(d) = n$	Euler totient sum
$S(n,k) = kS(n-1,k) + S(n-1,k-1)$	Stirling numbers of the second kind recurrence
$p(n) = \sum_{k \geq 1} (-1)^{k+1} \big(p(n - \omega_k) + p(n - \bar{\omega}_k)\big)$	Euler's pentagonal recurrence for partitions

Here $\omega_k = k(3k-1)/2$ and $\bar{\omega}_k = k(3k+1)/2$ are generalized pentagonal numbers, φ is Euler's totient function, $S(n,k)$ denotes a Stirling number of the second kind, and $p(n)$ is the number of integer partitions of n.

Bibliography

[1] K. H. Rosen, *Discrete Mathematics and Its Applications*, 8th ed., McGraw-Hill, 2019.

[2] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed., Addison-Wesley, 1994.

[3] L. Lovász, *Combinatorial Problems and Exercises*, 2nd ed., AMS Chelsea Publishing, 2007.

[4] R. Diestel, *Graph Theory*, 5th ed., Graduate Texts in Mathematics, vol. 173, Springer, 2017.

[5] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, 1994.

[6] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge University Press, 2001.

Index