Chapter 1

Sets and Notation

1.1 Defining sets

Definition. A *set* is an unordered collection of distinct objects. The objects in a set are called the *elements,* or *members,* of the set. A set is said to *contain* its elements.

A set can be defined by simply listing its members inside curly braces. For example, the set $\{2, 4, 17, 23\}$ is the same as the set $\{17, 4, 23, 2\}$. To denote membership we use the $\in$ symbol, as in $4 \in \{2, 4, 17, 23\}$. On the other hand, non-membership is denoted as in $5 \notin \{2, 4, 17, 23\}$.

If we want to specify a long sequence that follows a pattern, we can use the ellipsis notation, meaning "fill in, using the same pattern". The ellipsis is often used after two or more members of the sequence, and before the last one, as follows: $\{1, 2, \ldots, n\}$. The pattern denoted by the ellipsis should be apparent at first sight! For instance, $\{1, \ldots, n\}$ is generally regarded as underspecified (that is, too ambiguous). Of course, even $\{1, 2, \ldots, n\}$ is still ambiguous—did we mean all integers between 1 and n, all powers of two up to n, or perhaps the set $\{1, 2, 25, n\}$?—but is generally sufficient, unless you really do mean all powers of two up to n, in which case $\{2^0, 2^1, 2^2, \ldots, 2^k\}$ for an appropriate k is a better choice. The ellipsis can also be used to define an infinite set, as in the following.

Definition. The set of *natural numbers* or *nonnegative integers*, denoted by $\mathbb{N}$, is defined as $\{0, 1, 2, \ldots\}$.

To avoid ambiguities it is often useful to use the *set builder* notation, which lists on the right side of the colon the property that any set element, specified on the left side of the colon, has to satisfy. Let's define the positive integers using the set builder notation:

$$\mathbb{N}^+ = \{x : x \in \mathbb{N} \text{ and } x > 0\}.$$

We can also write

$$\mathbb{N}^+ = \{x \in \mathbb{N} : x > 0\}.$$

This is a matter of taste. In general, use the form that will be easiest for the reader of your work to understand. Often it is the least "cluttered" one.

Ok, now onto the integers:

$$\mathbb{Z} = \{x : x \in \mathbb{N} \text{ or } -x \in \mathbb{N}\}.$$

Hmm, perhaps in this case it is actually better to write

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

Remember, when you write mathematics, you should keep your readers' perspective in mind. For now, we—the staff of this course—are your readers. In the future it might be your colleagues, supervisors, or the readers of your published work. In addition to being reasonably formal and unambiguous, your mathematical writing should be as clear and understandable to your intended readership as possible.

Here are the *rational numbers*:

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Instead of $a \in \mathbb{Z}, b \in \mathbb{Z}$, you can write $a, b \in \mathbb{Z}$, which is more concise and generally more readable. Don't go overboard, though, with writing something like $a, b \neq 0 \in \mathbb{Z}$, this is way too confusing and does not say what you want it to.

Finally, the set of *real numbers* is denoted by $\mathbb{R}$. All the reals that are not rational are called *irrational*. These include the familiar $\pi = 3.1415926...$, $e = 2.7182818...$, $\sqrt{2}$, and infinitely many others. (How do we know that these numbers are irrational, do you ask? Actually, we will see a proof of this for $\sqrt{2}$ shortly. The proofs for π and e require mathematical analysis and are outside our scope.)

On being formal. Were the above definitions formal enough? The answer is: it depends. For example, defining the natural numbers is an important and non-trivial accomplishment of mathematics. After all, what do these symbols "1", "2", "3", actually *mean*? These numbers can be formally defined in terms of sets. Even more involved is the formal definition of the reals, usually covered in a first mathematical analysis course.

Here we cannot afford to cover everything in complete detail, which would have to include, among other things, basic algebra and trigonometry. Furthermore, the vast majority of mathematical works, while considered to be "formal", gloss over details all the time. For example, you'll be hard-pressed to find a mathematical paper that goes through the trouble of justifying the equation $a^2 - b^2 = (a - b)(a + b)$. In effect, every mathematical paper or lecture assumes a shared knowledge base with its readers or listeners. It is extremely important for an author of mathematics, such as yourself during this course, to estimate this shared knowledge base correctly!

In CS103X we will assume most of high-school mathematics, including perhaps some AP math like single-variable calculus, as our shared knowledge base. Thus notions and techniques from this base will generally not be justified in lecture, and can be used freely in your homework and exams. Furthermore, once we develop certain

notation or prove some theorem in class, you can use these freely in your homework and exams, provided that you clearly cite the appropriate theorems. In writing and speaking mathematics, a delicate balance is maintained between being formal and not getting bogged down in minutia.[1] This balance usually becomes second-nature with experience. You should all get the hang of it by the end of the quarter.

1.2 Set operations

A is said to be a subset of B if and only if every element of A is also an element of B, in which case we write $A \subseteq B$. A is a *strict subset* of B if A is a subset of B and A is not equal to B, which is denoted by $A \subset B$. For example, $\{4, 23\} \subset \{2, 4, 17, 23\} \subseteq \{2, 4, 17, 23\}$.

Two sets A and B are considered equal if and only if they have the same elements. This is denoted by $A = B$. More formally, $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.

For two sets A and B, the operations of union, intersection, and difference are defined as follows:

$$\begin{aligned} A \cup B &= \{x : x \in A \text{ or } x \in B\} \\ A \cap B &= \{x : x \in A \text{ and } x \in B\} \\ A \setminus B &= \{x : x \in A \text{ and } x \notin B\} \end{aligned}$$

The $\cup$ and $\cap$ notation can be extended to the union and intersection of multiple sets. Given n sets $A_1, A_2, \ldots, A_n$, we can write

$$\bigcup_{i=1}^{n} A_i$$

for their union, and

$$\bigcap_{i=1}^{n} A_i$$

for their intersection. In fact, this notation is pretty flexible and the same union can be written as

$$\bigcup_{i=1}^{n} A_i = \bigcup_{1 \le i \le n} A_i = \bigcup_{i \in \{x \,:\, 1 \le x \le n\}} A_i.$$

Here is another example:

$$\bigcap_{\substack{i \in \{x \,:\, 1 \le x \le 10\} \\ i \text{ is prime}}} A_i = A_2 \cap A_3 \cap A_5 \cap A_7.$$

Given a set A, the *cardinality* of A, also known as the *size* of A, is simply the number of elements in A. The cardinality of A is denoted by $|A|$. For example, if $A = \{2, 4, 17, 23\}$, then $|A| = 4$.

[1] Of course, what is considered minutia differs from subfield to subfield, and from classroom to classroom.

1.3 More sets

The *empty set* is denoted by $\emptyset$. It is the unique set without elements. It holds that $\emptyset \subseteq A$ for any set A. Why? By definition, this holds if every element of $\emptyset$ is also an element of A. Since $\emptyset$ has no elements, all possible statements about the elements of $\emptyset$ are true! In particular, all elements of $\emptyset$ are also elements of A. If this is confusing don't worry, we will go into such matters more rigorously when we get to logic. (For now, you can ponder the following: If we know for a fact that there are no unicorns <Gasp!>, then it is definitely true that all unicorns have soft light-blue fur.)

A set can contain sets as its elements. For example, $\{\{2,4\},\{17\},23\}$ is a perfectly valid set with three elements, two of them sets. (The second element is a *singleton*, a set with one element.) Note that $\{2,4\} \in \{\{2,4\},\{17\},23\}$, but $\{2,4\} \subseteq \{2,4,17,23\}$, and that $17 \notin \{\{2,4\},\{17\},23\}$, but $\{17\} \in \{\{2,4\},\{17\},23\}$. Also, $\{\emptyset\}$ is *not* the empty set. (Think about it.)

The *power set* of a set A is the set of all subsets of A, and is denoted by 2^A. That is,

$$2^A = \{S : S \subseteq A\}.$$

For example, for $A = \{2,4,17,23\}$, we have

$$2^A = \Big\{\emptyset, \{2\}, \{4\}, \{17\}, \{23\}, \{2,4\}, \{2,17\}, \{2,23\}, \{4,17\}, \{4,23\}, \{17,23\}, \{2,4,17\}, \{2,4,23\}, \{2,17,23\}, \{4,17,23\}, \{2,4,17,23\}\Big\}.$$

The cardinality of this set is 16, and $16 = 2^4$. This is not a coincidence: As we shall see when we get to combinatorics and counting, for a set A with n elements, the cardinality of 2^A is 2^n. This is in fact the reason for the power set notation.

Chapter 2

Induction

2.1 Introducing induction

Suppose there is an infinite line of people, numbered $1, 2, 3, \ldots$, and every person has been instructed as follows: "If something is whispered in your ear, go ahead and whisper the same thing to the person in front of you (the one with the greater number)". Now, what will happen if we whisper a secret to person 1? 1 will tell it to 2, 2 will tell it to 3, 3 will tell it to 4, and ... everybody is going to learn the secret! Similarly, suppose we align an infinite number of dominoes, such that if some domino falls, the next one in line falls as well. What happens when we knock down the first domino? That's right, they all fall. This intuition is formalized in the principle of mathematical induction:

Induction Principle: Given a set A of positive integers, suppose the following hold:

- $1 \in A$.
- If $k \in A$ then $k + 1 \in A$.

Then *all* positive integers belong to A. (That is, $A = \mathbb{N}^+$.)

Here are two simple proofs that use the induction principle:

Theorem 2.1.1. *Every positive integer is either even or odd.*

Proof. By definition, we are required to prove that for every $n \in \mathbb{N}^+$, there exists some $l \in \mathbb{N}$, such that either $n = 2l$ or $n = 2l + 1$. The proof proceeds by induction. The claim holds for $n = 1$, since $1 = 2 \cdot 0 + 1$. Suppose the claim holds for $n = k$. That is, there exists $l \in \mathbb{N}$, such that $k = 2l$ or $k = 2l + 1$. We prove that the claim holds for $n = k + 1$. Indeed, if $k = 2l$ then $k + 1 = 2l + 1$, and if $k = 2l + 1$ then $k + 1 = 2(l + 1)$. Thus the claim holds for $n = k + 1$ and the proof by induction is complete. □

Theorem 2.1.2. *Every positive integer power of 3 is odd.*

Proof. By definition, we are required to prove that for every $n \in \mathbb{N}^+$, it holds that $3^n = 2l + 1$, for some $l \in \mathbb{N}$. The proof proceeds by induction. For $n = 1$, we have $3 = 2 \cdot 1 + 1$, so the claim holds. Suppose the claim holds for k, so $3^k = 2l + 1$, for some $l \in \mathbb{N}$. Then

$$3^{k+1} = 3 \cdot 3^k = 3(2l + 1) = 2(3l + 1) + 1,$$

and the claim also holds for $k + 1$. The proof by induction is complete. □

Proof tip: If you don't know how to get a proof started, look to the definitions, and state formally and precisely what it is that you need to prove. It might not be obvious how to prove that "Every positive integer power of 3 is odd", but a bit easier to proceed with proving that "for every $n \in \mathbb{N}^+$, it holds that $3^n = 2l + 1$, for some $l \in \mathbb{N}$." If you need to prove an implication (that is, a claim of the form "if ... then ..."), then formally state all the assumptions as well as what you need to prove that they imply. Comparing the two might lead to some insight.

Proof technique: Induction. The induction principle is often used when we are trying to prove that some claim holds for all positive integers. As the above two proofs illustrate, when we use induction we do not need to explicitly refer to the set A from the statement of the induction principle. Generally, this set is the set of numbers for which the claim that we are trying to prove holds. In the first proof, it was the set of numbers n that are either even or odd. In the second proof, it was the set of numbers n for which 3^n is odd. Suppose we want to show that some claim holds for all positive integers. Here is a general template for proving this by induction:

(a) State the method of proof. For example, "The proof proceeds by induction."

(b) Prove the "induction basis". That is, prove that the number 1 satisfies the claim. (This step is often easy, but is crucially important, and should never be omitted!)

(c) Assume the "induction hypothesis". That is, state the assumption that the claim holds for some positive integer k.

(d) Prove, using the induction hypothesis, that the claim holds for $k+1$. The proof should consist of a chain of clear statements, each logically following from the previous ones combined with our shared knowledge base. The final statement in the chain should state that the claim holds for $k + 1$.

(e) Conclude the proof. For example, "This completes the proof by induction."

Theorem 2.1.3. *For every positive integer n,*

$$1 + 2 + \cdots + n = \frac{n(n + 1)}{2}.$$

Proof. The proof proceeds by induction. For $n = 1$, we have $1 = \frac{1 \cdot 2}{2}$ and the claim holds. Assume $1 + 2 + \cdots + k = k(k+1)/2$. Then

$$1+2+\cdots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2},$$

which proves the claim for $k + 1$ and completes the proof by induction. □

Sigma and Pi notations. Just as the $\bigcup$ symbol can be used to compactly express the union of many sets, the $\sum$ symbol can be used to express summations. For example,

$$1 + 2 + \cdots + n = \sum_{i=1}^{n} i = \sum_{1 \le i \le n} i = \sum_{i \in \{x \,:\, 1 \le x \le n\}} i.$$

You should not assume just because $\sum$ appears that there is an actual summation, or that there are any summands at all. For example, when $n = 1$, $\sum_{i=1}^{n} i = 1$, and when $n \le 0$, $\sum_{i=1}^{n} i = 0$!

Similarly, products can be expressed using the $\prod$ symbol, as in

$$2^0 \cdot 2^1 \cdot 2^2 \cdot \ldots \cdot 2^n = \prod_{i=0}^{n} 2^i.$$

One thing to be aware of is that the empty product is defined to equal 1, so

$$\prod_{i=3}^{1} i \quad = \quad \prod_{\substack{i \,\in\, \{2,4,10,14\} \\ i \text{ is odd}}} i \quad = \quad 1.$$

A single $\sum$ or $\prod$ symbol can also be used to describe the sum or product over more than one variable. For example,

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

2.2 Strong induction

Suppose that a property P holds for $n = 1$, and the following is true: If P holds for all integers between 1 and k, then it also holds for $k + 1$. Under these assumptions, P holds for all positive integers. This is the principle of strong induction. It differs from regular induction in that we can assume something stronger to derive the same conclusion. Namely, we can assume not only that P holds for k, but that in fact P holds for all positive integers up to k. We state the strong induction principle more formally, and then demonstrate its usefulness.

Strong Induction Principle: Given a set A of positive integers, suppose the following hold:

- $1 \in A$.
- If $\{1, 2, \ldots, k\} \subseteq A$ then $k + 1 \in A$.

Then all positive integers belong to A.

Definition. An integer $p > 1$ is said to be *prime* if the only positive divisors of p are 1 and p itself.

Theorem 2.2.1. *Every positive integer greater than* 1 *can be expressed as a product of primes.*

Proof. The proof proceeds by strong induction. Since 2 is a prime, the claim holds for 2. (Note how the induction basis in this case is 2, not 1, since we are proving a claim concerning all integers equal to or greater than 2.) Now assume the claim holds for all integers between 2 and k. If $k+1$ is a prime then the claim trivially holds. Otherwise it has a positive divisor a other than 1 and $k + 1$ itself. Thus, $k + 1 = a \cdot b$, with $2 \leq a, b \leq k$. Both a and b can be expressed as products of primes by the induction hypothesis. Their product can therefore also be thus expressed. This completes the proof by strong induction. □

The versatility of induction. We have seen in the proof of Theorem 2.2.1 that if we want to prove a statement concerning all positive integers equal to or greater than 2, we can use induction (or strong induction) with 2 as the base case. This holds for any positive integer in the place of 2. In fact, induction is an extremely versatile technique. For example, if we want to prove a property of all even positive integers, we can use 2 as the base case, and then prove that if the property holds for k, it will also hold for $k + 2$. Generally we will just assume that such variations are ok, there is no need to state a separate induction principle for each of these cases.

Fairly subtle variations of induction are often used. For example, if we can prove that a statement holds for 1 and 2, and that if it holds for k it will also hold for $k + 2$, we can safely conclude that the statement holds for all the positive integers. However, don't get carried away with variations that are simply incorrect, like using 1 as a base case, proving that if a statement holds for k then it also holds for $k + 2$, and then claiming its validity for all positive integers.

2.3 Why is the induction principle true?

Some of you might be surprised by the title question. Isn't it obvious? I mean, you know, the dominoes are aligned, you knock one down, they all fall. End of story. Right? Not quite.

"Common sense" often misleads us. You probably noticed this in daily life, and you're going to notice it a whole lot if you get into mathematics. Think of optical

illusions: we see, very clearly, what isn't really there. Our mind plays tricks on us too, just like our eyes sometimes do. So in mathematics, we are after proving everything. To be mathematically correct, every statement has to logically follow from previously known ones. So how do we prove the induction principle?

The answer lies in the previous paragraph. We said that every statement has to logically follow from other statements that we have proven previously. But this cannot go on forever, do you see? We have to start from some statements that we *assume* to be true. Such statements are called axioms. For example, why is it true that for any two natural numbers a, b, c, it holds that $a+(b+c) = (a+b)+c$? Because we assume it to be so, in order to build up the rest of mathematics from this and a small number of other such axioms.

This is also what we do with the induction principle: We accept it as an axiom. And if we accept the induction principle, strong induction can be proved from it, as you'll discover in the homework.

Chapter 3

More Proof Techniques

3.1 Proofs by contradiction

The following proof proceeds by contradiction. That is, we will assume that the claim we are trying to prove is wrong and reach a contradiction. If all the derivations along the way are correct, then the only thing that can be wrong is the assumption, which was that the claim we are trying to prove does not hold. This proves that the claim does hold.

Theorem 3.1.1. *$\sqrt{2}$ is irrational.*

Proof. We have seen previously that every integer is either even or odd. That is, for every $n \in \mathbb{Z}$ there exists $k \in \mathbb{Z}$, such that either $n = 2k$ or $n = 2k+1$. Now, if $n = 2k$ then $n^2 = (2k)^2 = 4k^2 = 2 \cdot (2k^2)$, which means that if n is even then n^2 is also even. On the other hand, if $n = 2k+1$ then $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2 \cdot (2k^2+2k)+1$, so if n is odd then n^2 is also odd.

We now proceed with a proof by contradiction. Assume that $\sqrt{2}$ is rational, that is, $\sqrt{2} \in \mathbb{Q}$. (This is the assumption that should lead to a contradiction.) By definition, this means that there exist two numbers $p, q \in \mathbb{Z}$, with $q \neq 0$, such that

$$\frac{p}{q} = \sqrt{2},$$

and thus

$$\left(\frac{p}{q}\right)^2 = 2.$$

We can assume that p and q have no common divisor, since all common divisors can be divided out to begin with. We have

$$p^2 = 2q^2.$$

This shows that p^2 is even, and consequently p must be even; that is, $p = 2k$ for some $k \in \mathbb{Z}$. Then

$$p^2 = 4k^2 = 2q^2,$$

so

$$2k^2 = q^2.$$

This shows that q^2 is even, and consequently that q is even. Thus both p and q are even, contradicting the fact that p and q have no common divisor. We have reached a contradiction, which completes the proof. □

Proof Technique: Proof by contradiction. Suppose we want to prove some statement A by contradiction. A common template for such proofs is as follows:

(a) State the method of proof. For example, "The proof proceeds by contradiction."

(b) State the assumption that should lead to the contradiction. For example, "Assume statement A does not hold."

(c) Proceed with a chain of clear statements, each logically following from the previous ones combined with our shared knowledge base. The final statement in the chain should be a contradiction, either of itself (as in, $0 \neq 0$), or of some previous statement in the chain, or of part of our shared knowledge base.

(d) Conclude the proof. For example, "We have reached a contradiction, which completes the proof."

Theorem 3.1.2. $\log_2 3$ *is irrational.*

Proof. The proof proceeds by contradiction. Assume that $\log_2 3$ is rational. By definition, there exist two numbers $p, q \in \mathbb{Z}$, with $q \neq 0$, such that

$$\log_2 3 = \frac{p}{q},$$

which means that

$$2^{\frac{p}{q}} = 3,$$

and thus

$$2^p = 3^q.$$

We can assume that $p, q > 0$. (Indeed, if $p/q > 0$ then we can just work with $|p|$ and $|q|$, and if $p/q \leq 0$ we reach a contradiction of the form $3 = 2^{p/q} \leq 2^0 = 1$.) Now, any positive integer power of 2 is even, because it has 2 as a divisor, so 2^p is even. On the other hand, a positive integer power of 3 is odd, as we've seen previously. We have reached a contradiction. □

3.2 Direct proofs

We should not forget perhaps the most intuitive proof technique of all: the direct one. Direct proofs start out with our shared knowledge base and, by a sequence of logical derivations, reach the conclusion that needs to be proved. Such proofs are often particularly ingenious and surprising.

Consider the following well-known puzzle question. Take the usual 8×8 chessboard and cut out two diagonally opposite corner squares. Can the remaining 62 squares be tiled by domino-shaped 2×1 tiles, each covering two adjacent squares of the board? (That is, each tile can be placed either horizontally or vertically, so as to precisely cover two squares of the board.)

Theorem 3.2.1. *A tiling as above is impossible.*

Proof. Every tile covers one white square and one black square. Thus in any tiling as above, the number of white squares covered is the same as the number of black ones. The two removed squares have the same color, hence the number of white squares left on the board is not the same as the number of black ones. So the remaining squares cannot be tiled. □

The above proof can also be phrased as a proof by contradiction, or even in terms of induction. However, even though such a phrasing might appear more formal, it is rather unnecessary, as the above proof is already logically sound (which is critical!), and better conveys the power (and dare I say, the beauty) of the argument.

Proof Technique: Direct proof. Here is a common template for direct proofs:

(a) Provide a chain of clear statements, each logically following from our shared knowledge base and the previous ones. The final statement in the chain should be the claim we need to prove.

(b) (Optional.) Conclude the proof. For example, "This completes the proof."

Chapter 4

Divisibility

4.1 The division algorithm

For the next few lectures we will exercise our ability to prove mathematical statements, using the fertile ground of number theory. In the process we will learn new proof techniques and tricks of trade. The number-theoretic concepts and results we will cover will be useful throughout your computer science studies, and, indeed, throughout your involvement with mathematics.

The following result is commonly known as the *division algorithm*, even though it is not an algorithm at all.

Theorem 4.1.1. *If a and b are integers and $b \neq 0$, then there is a unique pair of integers q and r, such that $a = qb + r$ and $0 \leq r < |b|$.*

Proof. We need to prove two things: that there is some such pair q, r (existence) and that this pair is unique (uniqueness).

Let's begin with existence. First we show that there is a pair $q, r \in \mathbb{Z}$ that satisfies $a = qb + r$ for some $r \geq 0$. This is easy after some playing around: Take $q = -|ab|/b$ and $r = a + |ab|$. Since $|b| \geq 1$, it holds that $r \geq 0$. Now we need to show that such $q, r \in \mathbb{Z}$ exist with r in addition being smaller than $|b|$. For this, consider the set S of all $r \in \mathbb{N}$ that satisfy $a = qb + r$ for some $q \in \mathbb{Z}$. We've just shown that S is nonempty, so it must have a smallest element, call it r_0. We have $a = q_0 b + r_0$. If $r_0 < |b|$ we're done. Otherwise, we have $a = (q_0 b + |b|) + (r_0 - |b|)$, which means that $r_0 - |b|$ is a smaller element of S than r_0, leading to a contradiction. This completes the existence proof.

To prove uniqueness, suppose that $a = qb + r = sb + t$, with $0 \leq r, t < |b|$. Thus $(q - s)b + (r - t) = 0$. Since $0 \leq r, t < |b|$, we have $|r - t| < |b|$, hence $|(q - s)b| < |b|$ and $|q - s| < 1$. Since q and s are integers, this implies $q = s$. From this we have $r = t$ and the uniqueness proof is complete. □

Proof tip: When we need to prove that some mathematical object exists and is unique, it is useful to approach in two stages. First prove that at least one such object exists. This can be done either by directly constructing an object and demonstrating

that it fulfills the requirements, or by assuming that no such object exists and reaching a contradiction. Then show that any two such objects must be the same.

The Well-Ordering Principle. In proving the division algorithm, we considered a certain set $S \subseteq \mathbb{N}$ and argued that since it is nonempty, it must have a smallest element. Why is this true? As with induction, we accept this proposition as an axiom. In general, the "well-ordering principle" states that *any nonempty set of natural numbers must have a smallest element.* As you will prove in the homework, the well-ordering principle is equivalent to the principles of induction and strong induction.

4.2 Remainders

A more algorithmic view of Theorem 4.1.1 is as follows: If we divide the equation

$$a = qb + r$$

by b we get

$$\frac{a}{b} = q + \frac{r}{b}.$$

Since $0 \leq r < |b|$, we get that if $b > 0$, then $0 \leq \frac{r}{b} < 1$ and thus $q = \left\lfloor \frac{a}{b} \right\rfloor$, the greatest integer less than or equal to $\frac{a}{b}$. If $b < 0$, then $0 \geq \frac{r}{b} > -1$ and thus $q = \left\lceil \frac{a}{b} \right\rceil$, the least integer greater or equal to $\frac{a}{b}$. This can be used to calculate q, from which we can derive r.

In Theorem 4.1.1, we call q the *quotient* and r the *remainder*. We use the notation $r = a \text{ rem } b$ to denote that r is the remainder when a is divided by b. There is no need for a special notation for quotient, since we can just use $\left\lfloor \frac{a}{b} \right\rfloor$ and $\left\lceil \frac{a}{b} \right\rceil$, depending on the sign of b.

Definition: If a and b are such that $a \text{ rem } b = 0$ we say that a is a *multiple* of b, or that b *divides* a (or is a *divisor* of a). Note that this holds when there exists some integer q, such that $a = qb$. In particular, every integer divides 0, and every integer is a multiple of 1. When b divides a we write $b|a$, and when b does not divide a we write $b \not| a$.

Definition: An integer u is called a *linear combination* of a set of integers $a_1, a_2, \ldots, a_n$ if and only if there exist integer coefficients $c_1, c_2, \ldots, c_n$ that satisfy

$$u = \sum_{i=1}^{n} c_i a_i.$$

Theorem 4.2.1. *Properties of divisibility:*

(a) If $b|a$ and $c|b$ then $c|a$.

(b) If $b|a$ and $a \neq 0$ then $|b| \leq |a|$.

(c) If b divides each of $a_1, a_2, \ldots, a_n$, then b divides all linear combinations of $a_1, a_2, \ldots, a_n$.

(d) $a|b$ and $b|a$ if and only if $a = \pm b$.

Proof. We prove the properties in turn:

(a) Since $b|a$, there exists an integer q, such that $a = qb$. Similarly, there exists an integer r, such that $b = rc$. Thus $a = qb = qrc$. Since qr is an integer, it holds that $c|a$.

(b) Since $b|a$, there exists an integer q, such that $a = qb$. This implies $|a| = |q| \cdot |b|$. Assume for the sake of contradiction that $a \neq 0$ but $|b| > |a|$. Then $|q| \cdot |b| < |b|$. Since $|b| > |a| > 0$, we can divide by $|b|$ to get $|q| < 1$, implying $q = 0$. Thus $a = qb = 0$, which is a contradiction.

(c) Consider a linear combination $u = \sum_{i=1}^{n} c_i a_i$. Since $b|a_i$, there exists an integer q_i, such that $a_i = q_i b$, for all $1 \leq i \leq n$. Thus

$$u = \sum_{i=1}^{n} c_i a_i = \sum_{i=1}^{n} c_i q_i b = b \cdot \sum_{i=1}^{n} c_i q_i.$$

Since $\sum_{i=1}^{n} c_i q_i$ is an integer, we have $b|u$.

(d) For the "if" statement, note that if $a = \pm b$ then $b = qa$ and $a = qb$, for $q = \pm 1$, so $a|b$ and $b|a$. To prove the "only if" statement, assume that $a|b$ and $b|a$. This implies the existence of integers q and r, such that $b = qa$ and $a = rb$. Thus $b = qrb$. If $b = 0$ then $a = 0$ and the claim that $a = \pm b$ holds. Otherwise we can divide by b to get $qr = 1$. Note that in this case $q, r \neq 0$. Part (b) of the theorem implies that $|q| \leq 1$ and $|r| \leq 1$. Thus $q, r = \pm 1$ and the claim that $a = \pm b$ follows.

□

Proof tip: Often we need to prove that a proposition A holds if and only if some other proposition B holds. Such an "if and only if" (sometimes abbreviated as "iff") statement is really composed of two implications, each of which needs to be proved. It is often useful to decouple these and prove them separately. First prove that "If A then B," and then prove that "If B then A." Another strategy is to prove that "If A then B" and "If not A then not B."

4.3 Greatest common divisors

If $d|a$ and $d|b$ then d is a *common divisor* of a and b. For example, 1 is a common divisor of any pair a, b. If a and b are not both 0 then, by Theorem 4.2.1(b), any

common divisor of a and b is not greater than $\max(|a|, |b|)$. Thus the set of common divisors of a and b has a largest element, called the *greatest common divisor* of a and b, or $\gcd(a, b)$. This is the integer d that satisfies the following two criteria:

- $d|a$ and $d|b$.
- If $c|a$ and $c|b$ then $c \leq d$.

Note that when $a = b = 0$, there is no greatest common divisor, since any integer divides 0. When a and b are not both 0, we often want to compute $\gcd(a, b)$ efficiently. Note that the set of divisors of a and $-a$ is the same, and similarly for b and $-b$. Furthermore, if $a = 0$ then $\gcd(a, b) = b$, and if $a = b$ then $\gcd(a, b) = a = b$. Thus it suffices to concentrate on the case $a > b > 0$, without loss of generality.

Since $1 \leq \gcd(a, b) \leq b$, we can just test all integers between 1 and b and choose the largest one that divides both a and b. However, there is a much more efficient way to find greatest common divisors, called Euclid's algorithm. This algorithm, one of the earliest in recorded history, is based on the following lemma.

Lemma 4.3.1. *If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.*

Proof. By Theorem 4.2.1(c), all common divisors of b and r also divide a, since a is a linear combination of b and r. Thus a common divisor of b and r is also a common divisor of a and b. Similarly, since $r = a - qb$, a common divisor of a and b also divides r, so it is a common divisor of b and r. Thus a, b and b, r have the same set of common divisors, and in particular the same greatest common divisor. □

With this lemma in our toolbelt, Euclid's algorithm is easy to describe. To find $\gcd(a, b)$, use the division algorithm (Theorem 4.1.1) to represent $a = qb + r$, where $0 \leq r < b$. (Remember that we are assuming that $a > b > 0$.) If $r = 0$ then $b|a$ and $\gcd(a, b) = b$. Otherwise $\gcd(a, b) = \gcd(b, r)$ and $b > r > 0$. We can thus repeat the above procedure recursively with the pair b, r. Every recursive call strictly reduces both numbers in the pair, so after at most b steps the algorithm will terminate with a valid greatest common divisor of a and b. You will formally prove the correctness of the algorithm in the homework.

4.4 Greatest common divisors and linear combinations

We have seen that a common divisor of a and b divides any linear combination of a and b. Now we will prove a surprising property known as *Bezout's identity* that shows that the greatest common divisor of a and b is itself a linear combination of a and b.

Theorem 4.4.1. *For two integers a and b that are not both 0, $\gcd(a, b)$ is a linear combination of a and b.*

Proof. As above, we can concentrate on the case $a > b > 0$. The proof proceeds by strong induction on the value of a. In the base case, $a = 2$, $b = 1$, and $\gcd(a, b) = 1 = 0 \cdot a + 1 \cdot b$. Assume that the theorem holds for all pairs a, b with $0 < b < a \leq k$. Consider a pair a', b' with $0 < b' < a' = k + 1$. If $b' | a'$ then $\gcd(a', b') = b'$ and the theorem trivially holds. Otherwise use the division algorithm to express $a' = qb' + r$, where $0 < r < b'$. By the induction hypothesis, there exist coefficients u and v, such that $\gcd(b', r) = ub' + vr$. Lemma 4.3.1 shows that $\gcd(a', b') = \gcd(b', r)$, therefore $\gcd(a', b') = ub' + vr = ub' + v(a' - qb') = va' + (u - vq)b'$. This shows that $\gcd(a', b')$ is a linear combination of a' and b' and completes the proof by induction. □

Bezout's identity implies that the set of linear combinations of a and b is the same as the set of multiples of their greatest common divisor (!):

Corollary 4.4.2. *An integer z is a linear combination of a and b if and only if it is a multiple of $\gcd(a, b)$. In particular, $\gcd(a, b)$ is the least positive linear combination of a and b.*

Proof. By Theorem 4.2.1(c), since $\gcd(a, b)$ divides both a and b, it divides any linear combination z of a and b, and thus z is a multiple of $\gcd(a, b)$. On the other hand, we know by Bezout's identity that there are coefficients u and v, such that $\gcd(a, b) = ua + vb$, so if $z = c \cdot \gcd(a, b)$, then $z = c(ua + vb) = (cu)a + (cu)v$. □

Chapter 5

Prime Numbers

5.1 The fundamental theorem of arithmetic

Definition: An integer $p > 1$ is said to be *prime* if its only positive divisors are 1 and p itself. All other integers greater than 1 are called composite.

A composite number n can be written as a product $n = ab$ of two strictly smaller numbers $1 < a, b < n$. Note that, by convention, 1 is neither prime nor composite. Here are all primes below 100:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Given a prime p and another integer a, either a is a multiple of p or $\gcd(p, a) = 1$. Indeed, $\gcd(p, a)$ divides p, so it must be either 1 or p, and since $\gcd(p, a)$ also divides a then either $\gcd(p, a) = 1$ or a is a multiple of p. This can be used to prove a very important property of primes:

Theorem 5.1.1. *Let p be a prime.*

(a) Given two integers a and b, if $p|ab$ then either $p|a$ or $p|b$.

(b) Given k integers $a_1, a_2, \ldots, a_k$, if $p| \prod_{i=1}^{k} a_i$ then $p|a_i$ for some $1 \leq i \leq k$.

Proof.

(a) If $p|a$ we are done. Otherwise $\gcd(p, a) = 1$ and by Bezout's identity there exist linear coefficients u and v for which $1 = ua + vp$. Multiplying both sides by b we get $b = uab + vpb$. Since p divides ab, p divides the whole sum $uab + vpb$. Therefore $p|b$.

(b) The proof proceeds by induction. The case $k = 1$ is trivial and $k = 2$ is handled in part (a). So we assume that the claim holds for some $k > 1$ and prove that it also holds for $k + 1$. Given that $p| \prod_{i=1}^{k+1} a_i$, we put $b = \prod_{i=1}^{k} a_i$. Since $p|ba_{k+1}$, part (a) implies that either $p|a_{k+1}$ or $p|b$. In both cases the claim holds, in the latter case by the induction hypothesis. This completes the proof by induction.

□

Theorem 5.1.1 can be used to derive a fundamental theorem of number theory. It is so fundamental it has "fundamental" in its name.

Theorem 5.1.2 (Fundamental Theorem of Arithmetic)**.** *Every positive integer can be represented in a unique way as a product of primes,*

$$n = p_1 p_2 \cdots p_k \qquad (p_1 \leq p_2 \leq \ldots \leq p_k).$$

Proof. We first prove existence and then uniqueness. Actually, we already proved existence in one of the previous lectures as an illustration of strong induction, but give the prove here again for completeness. So, to prove that every integer can be represented as a product of primes we use strong induction. The base case $n = 1$ holds because the *empty product*, as we previously discussed, is defined to equal 1. The induction hypothesis assumes that for some $n > 1$, all positive integers $k < n$ can be represented as a product of primes. If n is prime, then it is trivially a product of primes. Otherwise it can be written as $n = ab$, for $1 < a, b < n$. By the induction hypothesis, both a and b are products of primes, so their product n is also a product of primes. This proves existence.

The proof that the above representation is unique proceeds by contradiction. Assume then that there exists some positive integer that can be represented as a product of primes in (at least) two ways. By the well-ordering principle, there is a smallest such integer n. It holds that $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, where $p_1 \leq p_2 \leq \ldots \leq p_k$, $q_1 \leq q_2 \leq \ldots \leq q_l$, and $p_i \neq q_i$ for some i. By Theorem 5.1.1(b), since $p_i | q_1 q_2 \cdots q_l$, there must exist some q_j for which $p_i | q_j$. Since q_j is prime and $p_i > 1$, this can only occur when $p_i = q_j$. Thus we can eliminate p_i and q_j from the equation $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ and get two distinct representations of the positive integer number n/p_i as a product of primes. This contradicts the assumption that n is the smallest positive integer with this property, and concludes the proof of uniqueness. □

5.2 The infinity of primes

Here is another fundamental result with a proof from Euclid's *Elements*:

Theorem 5.2.1. *There are infinitely many primes.*

Proof. Assume for the sake of contradiction that there is only a finite set of primes, $p_1, p_2, \ldots, p_n$. Consider the number

$$p = p_1 p_2 \ldots p_n + 1.$$

By Theorem 5.1.2, p has a prime divisor, which has to be p_i, for some $1 \leq i \leq n$. Since p_i divides both p and $p_1 p_2 \ldots p_n$, it also divides $p - p_1 p_2 \ldots p_n = 1$. However, this is impossible since $p_i > 1$. This contradiction proves the theorem. □

Let's get some more mileage out of Euclid's proof. The results below show that not only do the primes never stop, but the number of primes $p \leq x$ is at least a certain natural function of x, namely at least $\log \log x$. (Here the base of the logarithm is 2.)

Theorem 5.2.2. *The n-th prime p_n satisfies $p_n \leq 2^{2^{n-1}}$ for all $n \geq 1$.*

Proof. We proceed using strong induction. For the base case, the first prime is $2 = 2^{2^0}$. Assume that the claim holds for all primes p_1 through p_k. Consider $p = p_1 p_2 \dots p_k + 1$. As in the above proof, p has a prime factor that is not one of the first k primes. This prime factor is thus at least as large as p_{k+1}, which implies

$$\begin{aligned} p_{k+1} \leq p = p_1 p_2 \dots p_k + 1 &\leq 2^{2^0} 2^{2^1} \cdots 2^{2^{k-1}} + 1 \\ &= 2^{1+2+4+\dots+2^{k-1}} + 1 \\ &= 2^{2^k - 1} + 1 \\ &= \frac{1}{2} 2^{2^k} + 1 \\ &\leq 2^{2^k}. \end{aligned}$$

This is precisely the induction step we needed, and concludes the proof by strong induction. □

Denote by $\pi(x)$ the number of primes $p \leq x$.

Corollary 5.2.3. *For $x \geq 2$, $\pi(x) \geq \lfloor \log \log x \rfloor + 1$.*

Proof. Plugging $n = \lfloor \log \log x \rfloor + 1$ into Theorem 5.2.2 implies that the n-th prime is at most x. Thus there are at least n primes below x. □

For general education, you should know that this is by far not the best possible estimate. A celebrated achievement in number theory is the Prime Number Theorem due to Hadamard and de la Vallée Poussin, which states that $x/\ln x$ (here we use the natural logarithm) is the "right" bound, in the sense that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} \to 1.$$

Chapter 6

Modular Arithmetic

6.1 Congruences

We usually associate arithmetic with the infinite set of integer numbers. However, *modular arithmetic* on finite sets is commonly used in our daily life. As an example, if it is now 1 am and we let 1000 hours pass, what time will it be? We can use the division algorithm to see that $1000 = 41 \times 24 + 16$ and conclude that adding 1000 hours is like adding 16 hours, since the clock returns to the same position every 24 hours. So after 1000 hours it will be 5 pm (17 hours after midnight).

There are many examples in which it is natural and useful to limit our number system to a finite range of integers, such as 0 through $n-1$, for some n. This number system is denoted by $\mathbb{Z}_n$. Days of the week, hours of the day, minutes in an hour are all familiar examples of finite number systems, as are numbers in microprocessor registers, commonly limited to 32 binary digits.

Modular arithmetic allows us to add, subtract, multiply, and sometimes divide numbers while staying within the finite set $\mathbb{Z}_n$. The number n is called the *modulus*. A central notion in modular arithmetic is *congruence*. We say that two integers are congruent modulo n if they leave the same remainder when divided by n. Here is the formal definition:

Definition: Two integers $a, b \in \mathbb{Z}$ are said to be *congruent modulo* n, written as $a \equiv_n b$ or $a \equiv b \pmod{n}$, if and only if they leave the same remainder when divided by n, that is, $a \text{ rem } n = b \text{ rem } n$.

This definition captures our intuition that the day of the week will be the same whether we let 10, 17, or 80 days pass. There is an equivalent definition of congruence that is often useful in proofs:

Lemma 6.1.1. *$a \equiv_n b$ if and only if $n|(a-b)$.*

Proof. If $a \equiv_n b$ then $a \text{ rem } n = b \text{ rem } n$. Put $r = a \text{ rem } n = b \text{ rem } n$. Then there exist two integers q_1 and q_2, such that $a = q_1 n + r$ and $b = q_2 n + r$. Subtracting the second equation from the first, we get $a - b = (q_1 - q_2)n$ and $n|(a-b)$.

On the other hand, if $n|(a-b)$ then there exists an integer d, such that $a - b = nd$. By the division algorithm, there exist integers $q_1, q_2 \in \mathbb{Z}$, and $0 \leq r_1, r_2 < n$, such

that $a = q_1 n + r_1$ and $b = q_2 n + r_2$. Thus $(q_1 - q_2)n + (r_1 - r_2) = nd$, and $r_1 - r_2 = (q_2 - q_1 + d)n$. Thus $n|(r_1 - r_2)$. However, $|r_1 - r_2| < n$, so necessarily $r_1 - r_2 = 0$, which implies that $a \text{ rem } n = b \text{ rem } n$, and $a \equiv_n b$. □

You should use the definition to verify that for any $a, b, c \in \mathbb{Z}$,

- $a \equiv_n a$. (Reflexivity.)
- If $a \equiv_n b$ then $b \equiv_n a$. (Symmetry.)
- If $a \equiv_n b$ and $b \equiv_n c$ then $a \equiv_n c$. (Transitivity.)

The operations of addition, subtraction, and multiplication on $\mathbb{Z}_n$ are defined by first doing the corresponding operation in $\mathbb{Z}$ and then taking the remainder modulo n. That is, if we denote these respective operations by $+_n$, $-_n$, and $\cdot_n$, then

$$\begin{aligned} a +_n b &= (a + b) \text{ rem } n \\ a -_n b &= (a - b) \text{ rem } n \\ a \cdot_n b &= (ab) \text{ rem } n \end{aligned}$$

Exponentiation is defined through repeated multiplication.

Lemma 6.1.2. *Properties of congruence:*

(a) $(a \text{ rem } n) \text{ rem } n = a \text{ rem } n$

(b) $(a \text{ rem } n) \equiv_n a$

(c) $(ab) \text{ rem } n = (a \text{ rem } n)(b \text{ rem } n) \text{ rem } n$

(d) $(a \text{ rem } n)(b \text{ rem } n) \equiv_n ab$

(e) $\prod_{i=1}^{k} (a_i \text{ rem } n) \equiv_n \prod_{i=1}^{k} a_i$

(f) If $a_1 \equiv_n a_2$ *and* $b_1 \equiv_n b_2$ *then*

$$\begin{aligned} a_1 + b_1 &\equiv_n a_2 + b_2 \\ a_1 - b_1 &\equiv_n a_2 - b_2 \\ a_1 b_1 &\equiv_n a_2 b_2 \end{aligned}$$

Proof. (b) is just a restatement of (a). To prove these we need to show that $n|(a - (a \text{ rem } n))$. Put $r = a \text{ rem } n$. By the division algorithm, there exists $q \in \mathbb{Z}$, such that $a = qn + r$. Thus $a - r = qn$, which implies that $n|a - r$ and concludes the proof.

(d) is a restatement of (c), and (e) can be proved from (d) by induction. To prove (c) we need to show that $n|(ab - (a \text{ rem } n)(b \text{ rem } n))$. Use the division algorithm to represent $a = q_1 n + r_1$ and $b = q_2 n + r_2$. Then

$$ab - (a \text{ rem } n)(b \text{ rem } n) = (q_1 n + r_1)(q_2 n + r_2) - r_1 r_2 = (q_1 q_2 n + r_1 q_2 + q_1 r_2)n,$$

which implies the claim.

We now prove (f). We know that $n|(a_1 - a_2)$ and $n|(b_1 - b_2)$. That is, there exist integers q and s, such that $a_1 - a_2 = qn$ and $b_1 - b_2 = sn$. Adding these equations gives $(a_1 + b_1) - (a_2 + b_2) = (q + s)n$, which yields the first part of the claim. Subtracting similarly gives the second part. Writing $a_1 = a_2 + qn$ and $b_1 = b_2 + sn$ and multiplying the equations gives

$$\begin{aligned} a_1 b_1 &= a_2 b_2 + b_2 qn + a_2 sn + qsn^2 \\ a_1 b_1 - a_2 b_2 &= (b_2 q + a_2 s + qsn)n, \end{aligned}$$

which yields the third part. □

6.2 Modular division

You might have noticed that we defined addition, subtraction, and multiplication, but not division. This might not be surprising, since the division operation is not defined for the integers in general: There is no integer that corresponds to 5 divided by 4, for instance. (In other words, there is no $x \in \mathbb{Z}$, such that $4x = 5$.) This distinguishes $\mathbb{Z}$ from sets like $\mathbb{Q}$ or $\mathbb{R}$ that are *closed under division*.

Division in $\mathbb{Z}_n$ appears even more unruly. For example, in $\mathbb{Z}_6$, the equation $2x = 4$ is satisfied by both $x = 2$ and $x = 5$, while the equation $2x = 3$ has no solutions. So the notion of "b divided by a" can be undefined or even ambiguous in $\mathbb{Z}_n$. In particular, we cannot generally cancel a multiplier from both sides of a congruence, that is, if $ab \equiv_n ac$ we cannot reason that $b \equiv_n c$. To take the above illustration, $2 \cdot 2 \equiv_6 2 \cdot 5$, but $2 \not\equiv_6 5$.

Quite remarkably, however, the division operation is well-defined when n is a prime p. Thus $\mathbb{Z}_p$ is in a sense as well-behaved as the real numbers, despite being a finite set! After a small digression that explores what "well-behaved" actually means here, we will state an even more general result on modular division.

Digression (notions from abstract algebra): There is a way to precisely state what we mean by "well-behaved" above. Jumping the gun, I'll say that $\mathbb{Z}_p$ is a *field*, not just a *ring*. Now let me tell you what this means. The notion of a ring in algebra is meant to abstract our intuition concerning the essential properties of the integers. Given a set S equipped with two operations, $+$ (addition) and $\cdot$ (multiplication), we say that S is a ring if the following all hold for any $a, b, c \in S$:

- $a + b \in S$ and $a \cdot b \in S$.
- $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- $a + b = b + a$ and $a \cdot b = b \cdot a$.
- $a \cdot (b + c) = a \cdot b + a \cdot c$.
- There exists an *additive identity* element $0 \in S$ that satisfies $a + 0 = a$ and a *multiplicative identity* element $1 \in S$ that satisfies $a \cdot 1 = a$ for all $a \in S$.

- For every $a \in S$ there exists an *additive inverse* $-a \in S$ for which $a + (-a) = 0$.

All the number systems we have encountered so far are rings, including $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{Z}_n$. However, some of them possess additional structure that allows the division operation. Namely, a ring is said to be a *field* if, in addition to the above, the following holds

- For every $a \in S$, such that $a \neq 0$, there exists a *multiplicative inverse* $a^{-1} \in S$ for which $a \cdot a^{-1} = 1$.

The number systems $\mathbb{R}$ and $\mathbb{Q}$, as well as $\mathbb{Z}_p$ when p is prime, are fields. In fields the division operation is well-defined, and $b/a = b \cdot a^{-1}$, as can be verified by plugging $x = b \cdot a^{-1}$ into the equation $ax = b$. A field with a finite number of elements is called a *Galois field*, after the French mathematician Evariste Galois. (A feisty young man who died in a duel at the age of 20, *after* making significant enough contributions to mathematics to have a whole field (sic) named in his honor!) Anyway, now that we know what fields are, let's see why $\mathbb{Z}_p$ is one. In fact, we prove something more general:

Theorem 6.2.1. *If a and n are coprime then there exists exactly one $x \in \mathbb{Z}_n$ for which $ax \equiv_n b$, for any $b \in \mathbb{Z}$.*

Proof. We need to prove existence and uniqueness of x as described in the theorem. $ax \equiv_n b$ if and only if there exists $q \in \mathbb{Z}$, such that $ax - b = nq$, or $ax - nq = b$. Now, since $\gcd(a, n) = 1$, any integer, including b, is a linear combination of a and n. This proves existence.

To prove uniqueness, assume that for $x, y \in \mathbb{Z}_n$ it holds that $ax \equiv_n b$ and $ay \equiv_n b$. Thus $ax - ay \equiv_n 0$, or $n|a(x-y)$. As you proved in one of the homework assignments, since n and a are coprime, this implies that $n|(x-y)$, and therefore that $x - y \equiv_n 0$. Thus $x \equiv_n y$, which proves uniqueness. □

Corollary 6.2.2. *For a prime p and any $a, b \in \mathbb{Z}$, such that $a \not\equiv_p 0$, there exists exactly one $x \in \mathbb{Z}_p$ for which $ax \equiv_p b$.*

The fact that division is well-defined in $\mathbb{Z}_p$ when p is prime also means that cancelations become valid. Thus if $a \not\equiv_p 0$ and $ab \equiv_p ac$ we can safely conclude that $b \equiv_p c$.

We now know that b/a is well-defined in $\mathbb{Z}_p$, but how do we find it? That is, how do we find $x \in \mathbb{Z}_p$, for which $ax \equiv_p b$. This question is particularly important when p is large and it takes too long to simply enumerate all the elements of $\mathbb{Z}_p$. Fortunately, the following result, known as *Fermat's Little Theorem*, can help us:

Theorem 6.2.3. *For a prime p and any $a \not\equiv_p 0$,*

$$a^{p-1} \equiv_p 1.$$

Proof. Consider the set S, defined as $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$. None of these $p - 1$ integers are congruent modulo p, since we have seen that if $ia \equiv_p ja$ then $i \equiv_p j$.

However, each element of S is congruent to some element of $\mathbb{Z}_p$. Since there are $p-1$ elements in S and $p-1$ nonzero elements in $\mathbb{Z}_p$, the elements of S must be congruent to each of $1, 2, \ldots, (p-1)$ in some order. Therefore,

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv_p 1a \cdot 2a \cdot \cdots \cdot (p-1)a,$$

or

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv_p 1 \cdot 2 \cdot \cdots \cdot (p-1) \cdot a^{p-1}.$$

We can cancel each of $1, 2, \ldots, (p-1)$ from both sides of the congruence, obtaining $a^{p-1} \equiv_p 1$. □

Fermat's Little Theorem allows us to quickly perform division in $\mathbb{Z}_p$. The element $x \in \mathbb{Z}_p$ for which $ax \equiv_p b$ is simply $(a^{p-2}b \text{ rem } p)$.

Chapter 7

Relations and Functions

7.1 Ordered pairs

The definition of a set explicitly disregards the order of the set elements, all that matters is who's in, not who's in first. However, sometimes the order is important. This leads to the notion of an *ordered pair* of two elements x and y, denoted (x, y). The crucial property is:

$$(x, y) = (u, v) \text{ if and only if } x = u \text{ and } y = v.$$

This notion can be extended naturally to define an *ordered n-tuple* as the ordered counterpart of a set with n elements.

Give two sets A and B, their *cartesian product* $A \times B$ is the set of all ordered pairs (x, y), such that $x \in A$ and $y \in B$:

$$A \times B = \{(x, y) : x \in A, y \in B\}.$$

Here is a useful special case:

$$A^2 = A \times A = \{(x, y) : x, y \in A\}.$$

And here is a general definition: $A^1 = A$, and for $n \geq 2$,

$$A^n = \big\{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in A\big\}.$$

For example, $\mathbb{R}^2$ is the familiar cartesian plane, and $\mathbb{R}^n$ is often referred to as the n-dimensional Euclidean space. If we omit the parentheses and the commas, $\{a, b\}^4$ is comprised of child babble and a 70s pop band:

$$\{aaaa, baba, abab, baaa, baab, aaab, aaba, abaa, abba, bbaa, bbba, bbbb, aabb, abbb, babb, bbab\}.$$

Proposition 7.1.1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$

Proof. Recall that for two sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$.

Consider any element $(u, v) \in (A \cup B) \times C$. By definition, $u \in A \cup B$ and $v \in C$. Thus, $u \in A$ or $u \in B$. If $u \in A$ then $(u, v) \in A \times C$ and if $u \in B$ then $(u, v) \in B \times C$.

Thus (u, v) is in $A \times C$ or in $B \times C$, and $(u, v) \in (A \times C) \cup (B \times C)$. This proves that $(A \cup B) \times C \subseteq (A \times C) \cup (B \times C)$.

Now consider any element $(u, v) \in (A \times C) \cup (B \times C)$. This implies that $(u, v) \in A \times C$ or $(u, v) \in B \times C$. In the first case $u \in A$ and $v \in C$ and in the second case $u \in B$ and $v \in C$. Thus $u \in A \cup B$ and $v \in C$, which implies $(u, v) \in (A \cup B) \times C$. $\square$

7.2 Relations

Given a set A, a *relation on* A is some property that is either true or false for any ordered pair $(x, y) \in A^2$. For example, "greater than" is a relation on $\mathbb{Z}$, denoted by $>$. It is true for the pair $(3, 2)$, but false for the pairs $(2, 2)$ and $(2, 3)$. In more generality,

Definition 7.2.1. *Given sets A and B, a* relation between A and B *is a subset of $A \times B$.*

By this definition, a relation R is simply a specification of which pairs are related by R, that is, which pairs the relation R is true for. For the relation $>$ on the set $\{1, 2, 3\}$,

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

This notation might look weird because we do not often regard the symbol "$>$" as a meaningful entity in itself. It is, at least from the vantage point of the foundations of mathematics: This symbol is a particular relation.

The common usage of the symbol "$>$" (as in $3 > 2$) is an instance of a useful notational convention: For a relation R, $(a, b) \in R$ can also be specified as aRb. Thus, in the above example, $(2, 1) \in >$ can be written as $2 > 1$. How convenient!

Common mathematical relations that will concern us include $<$, $>$, $\leq$, $\geq$, $=$, $\neq$, $|$, $\equiv_n$, $\subset$, $\subseteq$, etc. For example, the relation $=$ on the set $\mathbb{Z}$ is precisely the set $\{(n, n) : n \in \mathbb{Z}\}$ and the relation $\leq$ on $\mathbb{R}$ is the set $\{(x, x + |y|) : x, y \in \mathbb{R}\}$.

The concept of a relation is as general as the concept of a set, and is not limited to strictly mathematical settings. For instance, we can define the relation *likes* between the set {Anna,Britney,Caitlyn} and the set {Austin,Brian,Carlos}, such that

likes = $\big\{$(Britney,Austin),(Caitlyn,Austin),(Britney, Carlos),(Anna,Austin),(Caitlyn,Brian)$\big\}$.

In this setting we can write *Britney likes Austin*.

7.3 Kinds of relations

A relation R on a set A is called

- *reflexive* if for all $a \in A$, aRa.
- *symmetric* if for all $a, b \in A$, aRb implies bRa.
- *antisymmetric* if for all $a, b \in A$, aRb and bRa implies $a = b$.
- *transitive* if for all $a, b, c \in A$, aRb and bRc implies aRc.

Equivalence relations. A relation that is reflexive, symmetric, and transitive is called an *equivalence relation*. Clearly, the common relation $=$ on the set $\mathbb{R}$, say, is an equivalence relation. Also, we have seen earlier that the congruence relation $\equiv_n$ on the set $\mathbb{Z}$ is reflexive, symmetric, and transitive, thus it is also an equivalence relation. The similarity relation on the set of triangles in the plane is another example.

Equivalence relations are special in that they naturally partition the underlying set into *equivalence classes*. For example, the relation $\equiv_2$ partitions the integers into even and odd ones. These are, respectively, the integers that are related (by $\equiv_2$) to 0, and the ones related to 1. Let's formalize these concepts.

Definition 7.3.1. *A* partition *of a set A is a set $\mathcal{X} \subseteq 2^A \setminus \{\emptyset\}$, such that*

(a) Each $a \in A$ belongs to some $S \in \mathcal{X}$.

(b) If $S, T \in \mathcal{X}$, either $S = T$ or $S \cap T = \emptyset$.

Stated differently, this definition says that the set A is the union of the members of $\mathcal{X}$, and these members are disjoint. Now, given an equivalence relation R on A, the *equivalence class* of $a \in A$ is defined as

$$R[a] = \{b \in A : aRb\}.$$

Theorem 7.3.2. *Let R be an equivalence relation on a set A. Then $\{R[a] : a \in A\}$ is a partition of A.*

Proof. Consider an equivalence relation R on A. Due to reflexivity, every element $a \in A$ belongs to $R[a]$, which implies (a). Now, consider two equivalence classes $R[a]$ and $R[b]$. If aRb, then for any $c \in R[a]$, by transitivity and symmetry, bRc and $c \in R[b]$. This shows $R[a] \subseteq R[b]$. We can symmetrically argue that $R[b] \subseteq R[a]$, which together implies $R[a] = R[b]$.

Otherwise, if $a \not R b$ then consider some $c \in R[a]$. If $c \in R[b]$ then aRc and bRc, which imply, by transitivity and reflexivity, aRb, leading to a contradiction. Thus no element of $R[a]$ belongs to $R[b]$ and $R[a] \cap R[b] = \emptyset$. This shows (b) and concludes the theorem. □

Order relations. A relation that is reflexive, antisymmetric, and transitive is called a *partial order*. The relations $\leq$, $\geq$, and $|$ on the set $\mathbb{Z}$, as well as the relation $\subseteq$ on the powerset 2^A of any set A, are familiar partial orders. Note that a pair of elements can be *incomparable* with respect to a partial order. For example, $|$ is a partial order on $\mathbb{Z}$, but $2 \not| 3$ and $3 \not| 2$. A set A with a partial order on A is called a *partially ordered set*, or, more commonly, a *poset*.

A relation R on a set A is a *total order* if it is a partial order and satisfies the following additional condition:

- For all $a, b \in A$, either aRb or bRa (or both).

For example, the relations $\geq$ and $\leq$ are total orders on $\mathbb{R}$, but $|$ is not a total order on $\mathbb{Z}$. Finally, a *strict order* on A is a relation R that satisfies the following two conditions:

- For all $a, b, c \in A$, aRb and bRc implies aRc. (Transitivity.)

- Given $a, b \in A$, exactly one of the following holds (and not the other two): aRb, bRa, $a = b$.

The familiar $<$ and $>$ relations (on $\mathbb{R}$, say) are examples of strict orders.

7.4 Creating relations

There are a few ways to define new relations from existing ones, and we describe two important such ways below.

Restrictions of relations. Here is one notion that is sometimes useful: Given a relation R on a set A, and a subset $S \subseteq A$, we can use R to define a relation on S called the *restriction* of R to S. Denoted by $R|_S$, it is defined as

$$R|_S = \big\{(a, b) \in R : a, b \in S\big\}.$$

Compositions of relations. For three sets A, B, C, consider a relation R between A and B, and a relation S between B and C. The *composition of R and S* is a relation T between A and C, defined as follows: aTc if and only if there exists some $b \in B$, such that aRb and bSc. The composition of R and S is commonly denoted by $R \circ S$.

Note that by this definition, the composition of relations on the same set A is always well-defined. In particular, given a relation R on A we can recursively define $R^1 = R$ and $R^n = R^{n-1} \circ R$ for all $n \geq 2$. Now consider the infinite union

$$T = \bigcup_{i \in \mathbb{N}^+} R^i.$$

This relation T is called the *transitive closure* of R.

Proposition 7.4.1. *Important properties of transitive closure:*

(a) T is transitive.

(b) T is the smallest transitive relation that contains R. (That is, if U is a transitive relation on A and $R \subseteq U$, then $T \subseteq U$.)

(c) If $|A| = n$ then

$$T = \bigcup_{i=1}^{n} R^i.$$

7.5 Functions

The general concept of a function in mathematics is defined very similarly to relations. In fact, as far as the definitions go, functions *are* relations, of a special type:

Definition 7.5.1. *Given two sets A and B, a function $f : A \to B$ is a subset of $A \times B$ such that*

(a) If $x \in A$, there exists $y \in B$ such that $(x, y) \in f$.

(b) If $(x, y) \in f$ and $(x, z) \in f$ then $y = z$.

A function is sometimes called a *map* or *mapping*. The set A in the above definition is the *domain* and B is the *codomain* of f.

A function $f : A \to B$ is effectively a special kind of relation between A and B, which relates every $x \in A$ to *exactly one* element of B. That element is denoted by $f(x)$.

If the above definition is followed rigidly, particular functions should be defined by specifying all the pairs $(x, f(x))$. This is often cumbersome and unnecessary, and we will mostly continue describing a function from A to B as we did before: as a rule for picking an element $f(x) \in B$ for every element $x \in A$. As in, "Consider a function $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x^2$ for all $x \in \mathbb{R}$."

Kinds of Functions. For a function $f : A \to B$, the set $f(A) = \{f(x) : x \in A\}$ is called the *range* of f. The range is a subset of the codomain but may be different from it. If $f(A) = B$ then we say that f is *onto*. More precisely, a function $f : A \to B$ is a *surjection* (or *surjective*), or *onto* if each element of B is of the form $f(x)$ for at least one $x \in A$.

Today is the day of weird names, so: A function $f : A \to B$ is an *injection* (or *injective*), or *one-to-one* if for all $x, y \in A$, $f(x) = f(y)$ implies $x = y$. Put differently, $f : A \to B$ is one-to-one if each element of B is of the form $f(x)$ for at most one $x \in A$.

As if this wasn't enough: A function $f : A \to B$ is a *bijection* (or *bijective*), or a *one-to-one correspondence* if it is both one-to-one and onto. Alternatively, $f : A \to B$ is a bijection if each element of B is of the form $f(x)$ for exactly one $x \in A$.

Compositions and Inverse Functions. Given two functions $f : A \to B$ and $g : B \to C$ we can define a new function $g \circ f : A \to C$ by $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

One useful function that can be defined for any set A is the *identity function* $i_A : A \to A$, defined by $i_A(x) = x$ for all $x \in A$. We can use identity functions to define *inverse functions*. Specifically, if $f : A \to B$ is a bijection, then its inverse $f^{-1} : B \to A$ is defined so that $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$. Of course, we haven't shown that f^{-1} even exists or that it is unique, but these properties do hold, assuming that $f : A \to B$ is a bijection. (This assumption is necessary.)

Another result that is sometimes used is the following: If $f : A \to B$ and $g : B \to C$ are bijections then $g \circ f : A \to C$ is a bijection, and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

We omit the proof.

Bijections and cardinality. Bijections allow us to rigorously define when two sets are of the same cardinality:

Definition 7.5.2. *Two sets A and B have the same number of elements if and only if there exists a bijection $f : A \to B$.*

Chapter 8

Mathematical Logic

Perhaps the most distinguishing characteristic of mathematics is its reliance on logic. Explicit training in mathematical logic is essential to a mature understanding of mathematics. Familiarity with the concepts of logic is also a prerequisite to studying a number of central areas of computer science, including databases, compilers, and complexity theory.

8.1 Propositions and predicates

A *proposition* is a statement that is either true or false. For example, "It will rain tomorrow" and "It will not rain tomorrow" are propositions, but "It will probably rain tomorrow" is not, pending a more precise definition of "probably".

A *predicate* is a statement that contains a variable, such that for any specific value of the variable the statement is a proposition. Usually the allowed values for the variable will come from a specific set, sometimes called the *universe* of the variable, which will be either explicitly mentioned or clear from context. A simple example of a predicate is $x \geq 2$ for $x \in \mathbb{R}$. Clearly, for any real value of x, this statement is either true or false. We denote predicates in a similar way to functions, as in $P(x)$. In fact, the connection to functions runs deep: A predicate $P(x)$ can be considered a function, $P : \mathcal{U} \to \{0, 1\}$, where $\mathcal{U}$ is the universe of the variable x, 1 represents truth, and 0 represents falsehood.

A predicate may have more than one variable, in which case we speak of predicates in two variables, three variables, and so on, denoted as $Q(x, y)$, $S(x, y, z)$, etc.

8.2 Quantifiers

Given a predicate $P(x)$ that is defined for all elements in a set A, we can reason about whether $P(x)$ is true for all $x \in A$, or if it's at least true for some $x \in A$. We can state propositions to this effect using the *universal quantifier* $\forall$ and the *existential quantifier* $\exists$.

- $\forall x \in A : P(x)$ is true if and only if $P(x)$ is true for all $x \in A$. This proposition can be read "For all $x \in A$, $P(x)$."

- $\exists x \in A : P(x)$ is true if and only if $P(x)$ is true for at least one $x \in A$. This proposition can be read "There exists $x \in A$ such that $P(x)$."

Given a predicate in more than one variable we can quantify each (or some) of the variables. For example, the statement "For every real x and y, it holds that $x^2 - y^2 = (x - y)(x + y)$" can be formalized as

$$\forall x, y \in \mathbb{R} : x^2 - y^2 = (x - y)(x + y).$$

Somewhat more interestingly, the statement "There is no greatest integer" might be formulated as

$$\forall n \in \mathbb{Z}\ \exists m \in \mathbb{Z} : m > n.$$

It is crucial to remember that the meaning of a statement may change if the existential and universal quantifiers are exchanged. For example, $\exists m \in \mathbb{Z}\ \forall n \in \mathbb{Z} : m > n$ means "There is an integer strictly greater than all integers." This is not only contrary to the spirit of the original statement, but is patently wrong as it asserts in particular that there is an integer that is strictly greater than itself.

Exchanging the order of two quantifiers of the same type (either universal or existential) does not change the truth value of a statement. We do not prove this here.

8.3 Negations

Given a proposition P, the *negation* of P is the proposition "P is false". It is true if P is false, and false if P is true. The negation of P is denoted by $\neg P$, read as "not P." If we know the meaning of P, such as when P stands for "It will rain tomorrow," the proposition $\neg P$ can be stated more naturally than "not P," as in "It will not rain tomorrow." The truth-value of $\neg P$ can be represented by the following *truth table*:

P	$\neg P$
true	false
false	true

A truth table simply lists the truth values of particular statements in all possible cases. Something interesting can be observed in we consider the truth values of $\neg\neg Q$, which can be obtained by using the above table once with $P = Q$ and once with $P = \neg Q$:

Q	$\neg Q$	$\neg\neg Q$
true	false	true
false	true	false

We see that the statements Q and $\neg\neg Q$ have the same truth values. In this case we say that the two statements are *equivalent*, and write $Q \Leftrightarrow \neg\neg Q$. If $A \Leftrightarrow B$ we can freely use B in the place of A, or A instead of B in our logical derivations.

Negation gets really interesting when the negated proposition is quantified. Then we can assert that

$$\begin{aligned} \neg\forall x \in A : P(x) &\Leftrightarrow \exists x \in A : \neg P(x) \\ \neg\exists x \in A : P(x) &\Leftrightarrow \forall x \in A : \neg P(x) \end{aligned}$$

These can be interpreted as the claim that if $P(x)$ is not true for all $x \in A$ then it is false for some $x \in A$ and vice versa, and the claim that if $P(x)$ is not false for any $x \in A$ then it is true for all $x \in A$ and vice versa. What this means, in particular, is that if we want to disprove a statement that asserts something for all $x \in A$, it is sufficient to demonstrate *one* such x for which the statement does not hold. On the other hand, if we need to disprove a statement that asserts the existence of an $x \in A$ with a certain property, we actually need to show that for *all* such x this property does not hold.

Looked at another way, the above equivalences imply that if we negate a quantified statement, the negation can be "pushed" all the way inside, so that no negated quantifiers are left. Indeed, leaving any negated quantifiers is often considered a mark of poor style. Here is how how this elimination is done in a particular example:

$$\begin{aligned} \neg\forall n \in \mathbb{Z}\ \exists m \in \mathbb{Z} : m > n &\Leftrightarrow \\ \exists n \in \mathbb{Z}\ \neg\exists m \in \mathbb{Z} : m > n &\Leftrightarrow \\ \exists n \in \mathbb{Z}\ \forall m \in \mathbb{Z} : m \leq n & \end{aligned}$$

This can be read as "There exists an integer that is greater or equal to any other integer," which is the proper negation of the original statement.

8.4 Logical connectives

The symbol $\neg$ is an example of a *connective*. Other connectives combine two propositions (or predicates) into one. The most common are $\wedge$, $\vee$, $\oplus$, $\rightarrow$ and $\leftrightarrow$. $P \wedge Q$ is read as "P and Q"; $P \vee Q$ as "P or Q"; $P \oplus Q$ as "P xor Q"; $P \rightarrow Q$ as "P implies Q" or "if P then Q"; and $P \leftrightarrow Q$ as "P if and only if Q". The truth-value of these *compound propositions* (sometimes called *sentences*) depends on the truth values of P and Q (which are said to be the *terms* of these sentences), in a way that is made precise in the truth-table below.

We will not concern ourselves much with the $\oplus$ and $\leftrightarrow$ connectives, as they are encountered somewhat less frequently.

One interesting thing about the above table is that the proposition $P \rightarrow Q$ is false only when P is true and Q is false. This is what we would expect: If P is true but Q is false then, clearly, P does not imply Q. The important thing to remember is that if

P	Q	$P \wedge Q$	$P \vee Q$	$P \oplus Q$	$P \to Q$	$P \leftrightarrow Q$
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

P is false, then $P \to Q$ is true. One way this can be justified is by remembering that we expect a proposition to be either false or true. Now, $P \to Q$ being false says that P does not imply Q, which means precisely that P is true but Q is still false. In all other cases we expect $P \to Q$ to be true. (Did I succeed in turning something obvious into a confusing mess? Well, we all know what is paved with good intentions...)

Now, there is another statement involving P and Q that is false precisely when P is true and Q is false. It is, of course, $\neg P \vee Q$. As the following truth table demonstrates, the proposition $\neg P \vee Q$ is equivalent to $P \to Q$:

P	Q	$P \to Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

This means something rather interesting: We can replace a proposition that involves implication by an equivalent one that instead has negation ($\neg$) and disjunction ($\vee$). Also, since $P \to Q$ is false only when P is true and Q is false, the proposition $\neg(P \to Q)$ is equivalent to $P \wedge \neg Q$:

$$\neg(P \to Q) \Leftrightarrow P \wedge \neg Q.$$

This means that in a negated implication, the negation can be "pushed inside", somewhat like with quantifiers. In fact, similar equivalences exist for other negated compound statements, as can be verified using truth tables (do it!):

$$\begin{aligned} \neg(P \vee Q) &\Leftrightarrow \neg P \wedge \neg Q \\ \neg(P \wedge Q) &\Leftrightarrow \neg P \vee \neg Q \end{aligned}$$

These are the famous *DeMorgan's laws*. What they mean is that we can eliminate negated compounds (sounds like a military operation, doesn't it?) just as we can eliminate negated quantifiers.

Here is another important logical equivalence: The implication $P \to Q$ is equivalent to the *contrapositive* implication $\neg Q \to \neg P$:

$$(P \to Q) \Leftrightarrow (\neg Q \to \neg P).$$

This is demonstrated by the following truth table:

P	Q	$P \to Q$	$\neg Q$	$\neg P$	$\neg Q \to \neg P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Indeed, an implication of the form "If P then Q" is sometimes proved by assuming that Q does not hold and showing that under this assumption P does not hold. This is called a proof by contrapositive. (Despite the similarity, it is different from a proof by contradiction.)

8.5 Tautologies and logical inference

A sentence that is true regardless of the values of its terms is called a *tautology*, while a statement that is always false is a *contradiction*. Another terminology says that tautologies are *valid* statements and contradictions are *unsatisfiable* statements. All other statements are said to be *satisfiable*, meaning they can be either true or false.

Easy examples of a tautology and a contradiction are provided by $P \vee \neg P$ and $P \wedge \neg P$, as demonstrated by the following truth table:

P	$\neg P$	$P \vee \neg P$	$P \wedge \neg P$
T	F	T	F
F	T	T	F

Note that by our definition of logical equivalence, all tautologies are equivalent. It is sometimes useful to keep a "special" proposition $\mathcal{T}$ that is always true, and a proposition $\mathcal{F}$ that is always false. Thus any tautology is equivalent to $\mathcal{T}$ and any contradiction is equivalent to $\mathcal{F}$.

Here is another tautology: $(P \wedge Q) \to P$:

P	Q	$P \wedge Q$	$(P \wedge Q) \to P$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

The statement $(P \wedge Q) \to P$ is read "P and Q implies P". The fact that this is a tautology means that the implication is always true. Namely, if we know the truth of $P \wedge Q$, we can legitimately conclude the truth of P. In such cases the symbol $\Rightarrow$ is used, and we can write $(P \wedge Q) \Rightarrow P$. There is a crucial difference between $(P \wedge Q) \to P$ and $(P \wedge Q) \Rightarrow P$. The former is a single statement, while the latter indicates a relationship between two statements. Such a relationship is called an *inference rule*. A similar inference rule, $P \Rightarrow P \vee Q$ can be established analogously.

In general, any tautology of the form $A \rightarrow B$ can be used to "manufacture" the inference rule $A \Rightarrow B$ that says that if we know A we can conclude B. Similarly, a tautology of the form $A \leftrightarrow B$ can be converted into the equivalence $A \Leftrightarrow B$, which can be regarded as two inference rules, $A \Rightarrow B$ and $B \Rightarrow A$. A particularly important inference rule is called *modus ponens*, and says that if we know that P and $P \rightarrow Q$ are both true, we can conclude that Q is true. It follows from the tautology $(P \wedge (P \rightarrow Q)) \rightarrow Q$:

P	Q	$P \rightarrow Q$	$P \wedge (P \rightarrow Q)$	$(P \wedge (P \rightarrow Q)) \rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

We've already seen a number of inference rules above, like $(P \rightarrow Q) \Leftrightarrow (\neg Q \rightarrow \neg P)$, without calling them that. Here are three others, all corresponding to tautologies that you are invited to verify using truth tables:

$$\begin{aligned} (\neg P \rightarrow \mathcal{F}) &\Leftrightarrow P \\ (P \leftrightarrow Q) &\Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P) \\ (P \leftrightarrow Q) &\Leftrightarrow (P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q) \end{aligned}$$

These three rules are of particular importance. The first formally establishes the validity of proofs by contradiction, and the second and third provide two means for proving "if and only if" statements. We've been using these all along, but now we know why they are justified.

Chapter 9

Counting

9.1 Fundamental principles

The subject of *enumerative combinatorics* is counting. Generally, there is some set A and we wish to calculate the size $|A|$ of A. Here are some sample problems:

- How many ways are there to seat n couples at a round table, such that each couple sits together?
- How many ways are there to express a positive integer n as a sum of positive integers?

There are a number of basic principles that we can use to solve such problems.

The sum principle: Consider n sets A_i, for $1 \leq i \leq n$, that are *pairwise disjoint*, namely $A_i \cap A_j = \emptyset$ for all $i \neq j$. Then

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i| .$$

For example, if there are n ways to pick an object from the first pile and m ways to pick on object from the second pile, there are $n+m$ ways to pick an object altogether.

The product principle: If we need to do n things one after the other, and there are c_1 ways to do the first, c_2 ways to do the second, and so on, the number of possible courses of action is $\prod_{i=1}^{n} c_i$. For example, the number of possible three-letter words in which a letter appears at most once that can be constructed using the English alphabet is $26 \cdot 25 \cdot 24$: There are 26 possibilities for the first letter, then 25 possibilities for the second, and finally 24 possibilities for the third.

The bijection principle: As we have seen, there exists a bijection from A to B if and only if the size of A equals the size of B. Thus, one way to count the number of elements in a set A is to show that there is a bijection from A to some other set B

and to count the number of elements in B. Often there is no need to explicitly specify the bijection and prove that it is such: At this point in the course, you can omit some low-level details from the written proofs in your homework solutions, *as long as you are certain that you could reproduce these details if asked to do so.* For example, you can simply state and use the observation that the number of ways to seat n people in a row is the same as the number of ways to order the integers $1, 2, \ldots, n$, which is the same as the number of n-element sequences that can be constructed from the integers $1, 2, \ldots, n$ (without repetition), which is the same as the number of bijections $f : A \to A$, for $A = \{1, 2, \ldots, n\}$. You should always make sure that you yourself fully understand why such equalities hold whenever you use them! Obviously, if you don't, you'll end up relying on equalities that are simply not true, which is not such a great idea. If in doubt, write down a complete proof to make sure your reasoning is correct.

9.2 Basic counting problems

Choosing an ordered sequence of distinct objects with repetition. How many ways are there to pick an ordered sequence of k objects from a pool with n types of objects, when repetitions are allowed? (That is, we can pick an object of the same type more than once.) Well, by the product principle, there are n options for the first object, n options for the second, and so on. Overall we get n^k possible sequences. What follows is a somewhat more formal argument by induction. Observe that the number of sequences as above is the same as the number of functions from a set of k elements to a set of n elements. (Make sure you understand this.)

Theorem 9.2.1. *Given sets A and B, such that $|A| = k$ and $|B| = n$, the number of functions $f : A \to B$ is n^k.*

Proof. Induction on k. If $k = 0$ the set A has no elements and there is only one mapping from A to B, the empty mapping. (Recall that a function $f : A \to B$ is a subset of $A \times B$, and if $A = \emptyset$ then $A \times B = \emptyset$.) We suppose the claim holds for $|A| = m$ and treat the case $|A| = m + 1$. Consider some element $a \in A$. To specify a function $f : A \to B$ we can specify $f(a) \in B$ and a mapping $f' : A \setminus \{a\} \to B$. There are n possible values of $f(a) \in B$, and for each of these there are n^m mappings f' by the induction hypothesis. This results in n^{m+1} mappings f and completes the proof by induction. □

Choosing an ordered sequence of distinct objects *without* repetition. How many ways are there to pick an ordered sequence of k objects from a set of n objects when only one copy of each object is available, so there can be no repetitions? Again we can use the product principle. Observe that the first object in the sequence can be chosen from n distinct objects. Once the first one is picked, there are only $n - 1$ possibilities for the second object. After that there are $n - 2$ objects to choose from,

and so on. Overall we get that the desired quantity is

$$n(n-1)\cdots(n-k+1) = \prod_{i=0}^{k-1}(n-i).$$

This is called a *falling factorial* and denoted by $(n)_k$ or $n^{\underline{k}}$. We again provide a more formal proof by induction, observing that the number of ways to pick an ordered sequence of k objects from a collection of n distinct ones without replacement is equal to the number of *one-to-one* functions $f : A \to B$, where $|A| = k$ and $|B| = n$.

Theorem 9.2.2. *Given sets A and B, such that $|A| = k$ and $|B| = n$, the number of* one-to-one *functions $f : A \to B$ is $(n)_k$.*

Proof. Induction on k. When $|A| = 0$, there is one mapping f as described, the empty mapping, and $(n)_k$ is the empty product, equal to 1. Suppose the claim holds for $|A| = m$ and consider the case $|A| = m + 1$. Fix an element $a \in A$. To specify f we specify $f(a)$ and a mapping $f' : A \setminus \{a\} \to B$. There are n possible values for $f(a) \in B$. Consider a specific such value $f(a) = b$. Since f is one-to-one, no element of $A \setminus \{a\}$ can be mapped to b. Thus f' has to be a one-to-one-mapping from $A \setminus \{a\}$ to $B \setminus \{b\}$. By the induction hypothesis, the number of such mappings is $(n-1)_m$. The number of possible mappings f is thus $n \cdot (n-1)_m = (n)_{m+1}$. □

Permutations. How many ways are there to arrange n people in a row? How many ordered n-tuples are there of integers from the set $\{1, 2, \ldots, n\}$? Haw many distinct rearrangements are there of the integers $1, 2, \ldots, n$? How many bijections are there from the set $\{1, 2, \ldots, n\}$ to itself? The answer to these questions is the same, and follows from Theorem 9.2.2. A bijection from a set A to itself is called a *permutation* of A. The number of permutations of the set $\{1, 2, \ldots, n\}$ is precisely the number of one-to-one functions from this set to itself, and this number is $(n)_n = n \cdot (n-1) \cdots 2 \cdot 1$. This quantity is called "n factorial" and is denoted by $n!$. We can now observe that

$$(n)_k = \frac{n!}{(n-k)!}.$$

It is important to remember that $0! = 1$, since $0!$ is the empty product. Here is a list of values of $n!$ for $0 \leq n \leq 10$:

$$1, 1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800$$

Seating at a round table. We've arranged n people in a row, now it's time to sit them down. So how many ways are there to seat n people at a round table? Let's be precise about what we mean: Two seating arrangements are considered identical if every person has the same neighbor to her right. In other words, rotations around the table do not matter. Here is how this problem can be tackled: Fix one person a and sit her down anywhere. This now fixes $n-1$ possible positions for the others: "first person to the right of a", "second person to the right of a", and so on until "$(n-1)$-st person to the right of a". The number of ways to arrange the others in these $n-1$ positions is $(n-1)!$, which is also the answer to the original question.

Choosing an *unordered* collection of distinct objects *without* repetition. How many ways are there to pick a *set* of k objects from a set of n objects? Since we are picking a set, we do not care about order, and there are no repetitions. Notice that every such set can be ordered in $k!$ ways. That is, each set corresponds to $k!$ distinct ordered k-tuples. Now, we know that the number of ordered k-tuples that can be picked from a collection of n distinct objects is $(n)_k$. Thus if we denote by X the number of sets of cardinality k that can be picked from a collection of n distinct objects, we get

$$\begin{aligned} X \cdot k! &= (n)_k \\ X &= \frac{(n)_k}{k!} \\ X &= \frac{n!}{k!(n-k)!}. \end{aligned}$$

This quantity X is denoted by $\binom{n}{k}$, read "n choose k". This is such an important quantity that we emphasize it again: The number of k-element subsets of an n-element set is $\binom{n}{k}$, defined as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}.$$

We can see that $\binom{n}{0} = \binom{n}{n} = 1$, and we define $\binom{n}{k} = 0$ when $k > n$ or $k < 0$.

The number of subsets. We have seen that the number of k-element subsets of an n-element set is $\binom{n}{k}$. How many subsets of an n-element set are there overall, of any size? Yes, it is time to prove the neat formula we've been using all along:

Theorem 9.2.3. *For a set A,*

$$\left|2^A\right| = 2^{|A|}.$$

Proof. By induction. When $|A| = 0$, $A = \emptyset$. Hence, A has only one subset (itself) and the formula holds since $2^0 = 1$. Assume the formula holds when $|A| = k$ and consider the case $|A| = k + 1$. Fix an element $a \in A$. A subset of A either contains a or not. The subsets of A that do not contain a are simply subsets of $A \setminus \{a\}$ and their number is 2^k by the induction hypothesis. On the other hand, each subset of A that does contain a is of the form $\{a\} \cup X$, for $X \subseteq A \setminus \{a\}$. Thus there is a bijective mapping between subsets of A that contain a and subsets of $A \setminus \{a\}$. The number of such subsets is again 2^k. Overall we get that the number of subsets of A is $2^k + 2^k = 2^{k+1}$, which completes the proof by induction. □

Here is another instructive way to prove Theorem 9.2.3: Consider the set of functions $f : A \to \{0, 1\}$. These functions assign a value of 0 or 1 to every element of A. In this way, such a function f uniquely specifies a subset of A. Namely, the elements x for which $f(x) = 1$ are the elements that belong to the subset of A specified by f. This defines a bijection between such functions f and subsets of A. By Theorem 9.2.1, the number of functions f from A to $\{0, 1\}$ is $2^{|A|}$, which proves Theorem 9.2.3.

We can use Theorem 9.2.3 to derive an interesting identity. We now know that the overall number of subsets of an n-element set is 2^n. Previously we have seen that the number of k-element subsets of an n-element set is $\binom{n}{k}$. By the sum principle, we get

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n.$$

Choosing an *unordered* collection of distinct objects *with* repetition. How many ways are there to pick a collection of k objects from a pool with n types of objects, when repetitions are allowed? We can reason as follows: The number of ways to pick k objects from a pool with n types of objects is the same as the number of ways to put k balls into n bins. Imagine these bins aligned in a row. A "configuration" of k balls in n bins can be specified as a sequence of $n-1$ "|" symbols and k "*" symbols, as in

$$**||*|***|$$

This sequence encodes the configuration where $k = 6$ and $n = 5$, and there are two balls in bin number 1, one ball in bin number 3, and three balls in bin number 4. How many such configurations are there? A configuration is uniquely specified by the positions of the k "*" symbols. Thus specifying a configuration amounts to choosing which of the $n + k - 1$ symbols are going to be "*". This simply means we need to choose a k-element subset from a set of size $n + k - 1$. The number of ways to pick a collection of k objects from a pool of n types of objects with repetitions is thus

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

Chapter 10

Binomial Coefficients

10.1 Basic properties

Recall that $\binom{n}{k}$ is the number of k-element subsets of an n-element set, and

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}.$$

The quantities $\binom{n}{k}$ are called *binomial coefficients* because of their role in the *Binomial Theorem*, apparently known to the 11th century Persian scholar Omar Khayyam. Before we state and prove the theorem let us consider some important identities that involve binomial coefficients. One that follows immediately from the algebraic definition is

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

This also has a nice combinatorial interpretation: Choosing a k-element subset B from an n-element set uniquely identifies the complement $A \setminus B$ of B in A, which is an $(n-k)$-subset of A. This defines a bijection between k-element and $(n-k)$-element subsets of A, which implies the identity.

Another relation between binomial coefficients is called *Pascal's rule*, although it was known centuries before Pascal's time in the Middle East and India:

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

This can be easily proved algebraically:

$$\begin{aligned}\binom{n}{k-1}+\binom{n}{k} &= \frac{n!}{(k-1)!(n+1-k)!}+\frac{n!}{k!(n-k)!}\\ &= \frac{n!k}{k!(n+1-k)!}+\frac{n!(n+1-k)}{k!(n+1-k)!}\\ &= \frac{n!k+n!(n+1-k)}{k!(n+1-k)!}\\ &= \frac{(n+1)!}{k!(n+1-k)!}\\ &= \binom{n+1}{k}.\end{aligned}$$

Pascal's rule also has a combinatorial interpretation: $\binom{n+1}{k}$ is the number of k-element subsets of an n-element set A. Fix an element $a \in A$. A subset of A either contains a or it doesn't. k-element subsets of A that do not contain a are in fact k-element subsets of $A \setminus \{a\}$ and their number is $\binom{n}{k}$. k-element subsets of A that do contain a bijectively correspond to $(k-1)$-element subsets of $A \setminus \{a\}$, the number of which is $\binom{n}{k-1}$. The identity follows.

Another illuminating identity is the *Vandermonde convolution*:

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

We only give a combinatorial argument for this one. We are counting the number of ways to choose an l-element subset of an $(m+n)$-element set A. Fix an m-element subset $B \subseteq A$. Any l-element subset S of A has k elements from B and $l-k$ elements from $A \setminus B$, for some $0 \leq k \leq l$. For a particular value of k, the number of k-element subsets of B that can be part of S is $\binom{m}{k}$ and the number of $(l-k)$-element subsets of $A \setminus B$ is $\binom{n}{l-k}$. We can now use the sum principle to sum over the possible values of k and obtain the identity. An interesting special case is

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

It follows from the Vandermonde convolution by taking $l = m = n$ and remembering that $\binom{n}{k} = \binom{n}{n-k}$.

10.2 Binomial theorem

Theorem 10.2.1. *For $n \in \mathbb{N}$ and $x, y \in \mathbb{R}$,*

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

Proof. By induction on n. When $n = 0$ both sides evaluate to 1. Assume the claim holds for $n = m$ and consider the case $n = m + 1$.

$$
\begin{aligned}
(x+y)^{m+1} &= (x+y)\cdot(x+y)^m && (10.1)\\
&= (x+y)\cdot\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k} && (10.2)\\
&= x\cdot\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k} + y\cdot\sum_{k=0}^{m}\binom{m}{k}x^k y^{m-k} && (10.3)\\
&= \sum_{k=0}^{m}\binom{m}{k}x^{k+1} y^{m-k} + \sum_{k=0}^{m}\binom{m}{k}x^k y^{m+1-k} && (10.4)\\
&= \sum_{k=1}^{m+1}\binom{m}{k-1}x^k y^{m+1-k} + \sum_{k=0}^{m}\binom{m}{k}x^k y^{m+1-k} && (10.5)\\
&= \left(x^{m+1} + \sum_{k=1}^{m}\binom{m}{k-1}x^k y^{m+1-k}\right) + \left(y^{m+1} + \sum_{k=1}^{m}\binom{m}{k}x^k y^{m+1-k}\right) && (10.6)\\
&= x^{m+1} + y^{m+1} + \sum_{k=1}^{m}\left(\binom{m}{k-1} + \binom{m}{k}\right)x^k y^{m+1-k} && (10.7)\\
&= x^{m+1} + y^{m+1} + \sum_{k=1}^{m}\binom{m+1}{k}x^k y^{m+1-k} && (10.8)\\
&= \sum_{k=0}^{m+1}\binom{m+1}{k}x^k y^{m+1-k}. && (10.9)
\end{aligned}
$$

Here (5) follows from (4) by noting that

$$\sum_{k=0}^{m} f(k) = \sum_{k=1}^{m+1} f(k-1)$$

and (8) follows from (7) by Pascal's rule. The other steps are simple algebraic manipulation. This completes the proof by induction. □

The binomial theorem can be used to immediately derive an identity we have seen before: By substituting $x = y = 1$ into the theorem we get

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n.$$

Here is another interesting calculation: Putting $x = -1$ and $y = 1$ yields

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

This implies

$$\sum_{k \text{ odd}} \binom{n}{k} = \sum_{k \text{ even}} \binom{n}{k} = 2^{n-1}.$$

This means that the number of odd-size subsets of an n-element set A is the same as the number of even-size subsets, and equals 2^{n-1}. This can be proved by a combinatorial argument as follows: Fix an element $a \in A$ and note that the number of subsets of $A \setminus \{a\}$ is 2^{n-1}. There is a bijective map between subsets of $A \setminus \{a\}$ and odd-size subsets of A, as follows: Map an odd-sized subset of $A \setminus \{a\}$ to itself, and map an even-sized subset $B \subseteq A \setminus \{a\}$ to $B \cup \{a\}$. Observe that this is a bijection and conclude that the number of odd-sized subsets of A is 2^{n-1}. Even-size subsets can be treated similarly, or by noting that their number is 2^n minus the number of odd-size ones.

Chapter 11

The Inclusion-Exclusion Principle

11.1 Statement and proof of the principle

We have seen the sum principle that states that for n pairwise disjoint sets $A_1, A_2, \ldots, A_n$,

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| .$$

What happens when the sets are not pairwise disjoint? We can still say something. Namely, the sum $\sum_{i=1}^{n} |A_i|$ counts every element of $\bigcup_{i=1}^{n} A_i$ at least once, and thus even with no information about the sets we can still assert that

$$\left|\bigcup_{i=1}^{n} A_i\right| \leq \sum_{i=1}^{n} |A_i| .$$

However, with more information we can do better. For a concrete example, consider a group of people, 10 of whom speak English, 8 speak French, and 6 speak both languages. How many people are in the group? We can sum the number of English- and French-speakers, getting $10 + 8 = 18$. Clearly, the bilinguals were counted twice, so we need to subtract their number, getting the final answer $18 - 6 = 12$. This argument can be carried out essentially verbatim in a completely general setting, yielding the following formula:

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

What if there are three sets? Suppose in addition to the above English and French speakers, we have 14 German-language enthusiasts, among which 8 also speak English, 5 speak French, and 2 speak all three languages. How many people are there now? We can reason as follows: The sum $10 + 8 + 14 = 32$ counts the people speaking two languages twice, so we should subtract their number, getting $32 - 6 - 8 - 5 = 13$. But now the trilinguals have not been counted: They were counted three times in the first sum, and then subtracted three times as part of the bilinguals. So the final answer is obtained by adding their number: $13 + 2 = 15$. In general,

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

In the case of arbitrarily many sets we obtain the inclusion-exclusion principle:

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{k=1}^{n}(-1)^{k-1} \sum_{1\le i_1<i_2<\cdots<i_k\le n} |A_{i_1} \cap A_{i_2} \cap \ldots A_{i_k}|\,.$$

Proof. Each element in $\bigcup_{i=1}^{n} A_i$ is counted exactly once on the left side of the formula. Consider such an element a and let the number of sets A_i that contain a be j. Then a is counted

$$\binom{j}{1} - \binom{j}{2} + \ldots + (-1)^{j-1}\binom{j}{j}$$

times on the right side. But recall from our exploration of binomial coefficients that

$$\sum_{i=0}^{j}(-1)^i\binom{j}{i} = \sum_{i=0}^{j}(-1)^{i-1}\binom{j}{i} = -1 + \sum_{i=1}^{j}(-1)^{i-1}\binom{j}{i} = 0,$$

which implies

$$\binom{j}{1} - \binom{j}{2} + \ldots + (-1)^{j-1}\binom{j}{j} = 1,$$

meaning that a is counted exactly once on the right side as well. This establishes the inclusion-exclusion principle. □

11.2 Derangements

Given a set $A = \{a_1, a_2 \ldots, a_n\}$, we know that the number of bijections from A to itself is $n!$. How many such bijections are there that map no element $a \in A$ to itself? That is, how many bijections are there of the form $f : A \to A$, such that $f(a) \neq a$ for all $a \in A$. These are called *derangements*, or bijections with no *fixed points*.

We can reason as follows: Let S_i be the set of bijections that map the i-th element of A to itself. We are the looking for the quantity

$$n! - \left|\bigcup_{i=1}^{n} S_i\right|.$$

By the inclusion-exclusion principle, this is

$$n! - \sum_{k=1}^{n}(-1)^{k-1} \sum_{1\le i_1<i_2<\cdots<i_k\le n} |S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_k}|\,.$$

Consider an intersection $S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_k}$. Its elements are the permutations that map $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$ to themselves. The number of such permutations is $(n-k)!$, hence $|S_{i_1} \cap S_{i_2} \cap \ldots \cap S_{i_k}| = (n-k)!$. This allows expressing the number of derangements

as

$$\begin{aligned} n! - \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} (n-k)! &= n! - \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} (n-k)! \\ &= \sum_{k=0}^{n} (-1)^{k} \binom{n}{k} (n-k)! \\ &= \sum_{k=0}^{n} (-1)^{k} \frac{n!}{k!} \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \end{aligned}$$

Now, $\sum_{k=0}^{n} \frac{(-1)^k}{k!}$ is the beginning of the Maclaurin series of e^{-1}. (No, you are not required to know this for the exam.) This means that as n gets larger, the number of derangements rapidly approaches $n!/e$. In particular, if we just pick a random permutation of a large set, the chance that it will have no fixed points is about $1/e$. Quite remarkable, isn't it!?

Chapter 12

The Pigeonhole Principle

12.1 Statements of the principle

In we put more than n pigeons into n pigeonholes, at least one pigeonhole will house two or more pigeons. This trivial observation is the basis of ingenious combinatorial arguments, and is the subject of this chapter. Let's begin with the various guises of the pigeonhole principle that are encountered in combinatorics.

Basic form. If m objects are put in n boxes and $n < m$, then at least one box contains at least two objects. The one-line proof is by contradiction: If every box contains at most one object, there are at most $n \cdot 1 = n$ objects. A more rigorous formulation of the principle is as follows: Given two sets A and B, with $|A| = m > n = |B|$, for any function $f : A \to B$ there exists $b \in B$ such that

$$\big|\{x \in A : f(x) = b\}\big| > 1.$$

General form. If m objects are put in n boxes, then at least one box contains at least $\lceil m/n \rceil$ objects. The proof is again by contradiction: If every box contains at most $\lceil m/n \rceil - 1 < m/n$ objects, there are less than $n(m/n) = m$ objects. The more rigorous formulation is: Given two sets A and B, for any function $f : A \to B$ there exists $b \in B$ such that

$$\big|\{x \in A : f(x) = b\}\big| \geq \left\lceil \frac{m}{n} \right\rceil.$$

Dijkstra's form. For a nonempty finite collection of integers (not necessarily distinct), the maximum value is at least the average value. It is a good exercise to verify that this is equivalent to the general form above.

12.2 Simple applications

Let's begin with some easy applications of the pigeonhole principle.

First application. There are two San Franciscans with the exact same number of hairs on their heads. Indeed, according to P&G Hair Facts, the average person's head has about 100,000 hairs, while "some people have as many as 150,000." So it seems safe to bet that every San Franciscan has at most 700,000 hairs on his or her head. On the other hand, the year 2000 US Census counted 776,733 San Francisco residents. The pigeonhole principle implies that at least two of them have the exact same number of hairs.

Second application. At a cocktail party with six or more people, there are three mutual acquaintances or three mutual strangers. Indeed, pick an arbitrary person a. By the pigeonhole principle, among the other five or more people, either there are three of a's acquaintances, or three people who are strangers to a. Let's say there are three that are a's acquaintances, the other case is analogous. If those three are mutual strangers we are done. Otherwise there are two among them, call them b and c, who know each other. Then a, b and c are mutual acquaintances and we are done.

Third application. Consider an infinite two-dimensional plane, every point of which is colored either red or blue; then there are two points one yard apart that are the same color. Indeed, take an arbitrary equilateral triangle with a side length of one yard. By the pigeonhole principle, two of its vertices have the same color.

Fourth application. Consider the numbers $1, 2, \ldots, 2n$, and take any $n+1$ of them; then there are two numbers in this sample that are coprime. Indeed, consider the pairs $\{1,2\}, \{3,4\}, \ldots, \{2n-1, 2n\}$. By the pigeonhole principle, both numbers from one of these pairs are in the sample. These numbers differ by 1 and are thus coprime. (This follows from the same argument as in Euclid's proof of the infinity of primes.)

12.3 Advanced applications

The following lemma comes from a classical 1935 paper by Paul Erdös and George Szekeres titled "A combinatorial problem in geometry":

Lemma 12.3.1. *In any ordered sequence of n^2+1 distinct real numbers $a_1, a_2, \ldots, a_{n^2+1}$, there is either a monotone increasing subsequence of length $n+1$ or a monotone decreasing subsequence of length $n+1$. Namely, there is a set of indices $1 \le i_1 < i_2 < \cdots < i_{n+1} \le n^2+1$, such that either $a_{i_1} > a_{i_2} > \cdots > a_{i_{n+1}}$ or $a_{i_1} < a_{i_2} < \cdots < a_{i_{n+1}}$.*

Proof. For $1 \le i \le n^2+1$, let η_i be the length of the longest monotone increasing subsequence that starts at a_i. If some $\eta_i > n$, we are done. Otherwise, by the pigeonhole principle, there exists $1 \le j \le n$, and some set $i_1 < i_2 < \cdots < i_m$ of size $m \ge \lceil (n^2+1)/n \rceil = n+1$, such that $\eta_{i_1} = \eta_{i_2} = \cdots = \eta_{i_m} = j$. Now, consider two numbers a_{i_k} and $a_{i_{k+1}}$. If $a_{i_k} < a_{i_{k+1}}$, we get an increasing subsequence starting at a_{i_k} of length $j+1$, which is a contradiction. Hence $a_{i_k} > a_{i_{k+1}}$ in particular, and

$a_{i_1} > a_{i_2} > \cdots > a_{i_m}$ in general, giving us a decreasing subsequence of length at least $n+1$. □

Here is another pigeonhole gem, the last one for today:

Proposition 12.3.2. *Given a sequence of n not necessarily distinct integers $a_1, a_2, \ldots, a_n$, there is a nonempty consecutive subsequence $a_i, a_{i+1}, \ldots, a_j$ whose sum $\sum_{m=i}^{j} a_m$ is a multiple of n. (The subsequence might consist of a single element.)*

Proof. Consider the collection

$$\left(\sum_{i=1}^{0} a_i, \sum_{i=1}^{1} a_i, \sum_{i=1}^{2} a_i, \ldots, \sum_{i=1}^{n} a_i \right).$$

This collection has size $n+1$ and its first element is the empty sum $\sum_{i=1}^{0} a_i = 0$. There are only n possible remainders modulo n, thus by the pigeonhole principle, there are two numbers in the above collection of size $n+1$ that leave the same remainder. Let these be $\sum_{i=1}^{l} a_i$ and $\sum_{i=1}^{k} a_i$, with $l < k$. By a lemma we once proved, it follows that

$$n \Big| \left(\sum_{i=1}^{k} a_i - \sum_{i=1}^{l} a_i \right),$$

which implies

$$n \Big| \sum_{i=l+1}^{k} a_i.$$

□

Chapter 13

Asymptotic Notation

13.1 Definitions

Analysis of algorithms is concerned with estimating how many steps various algorithms make while solving problems of various sizes. In particular, given an algorithm, we want to make statements like "For input of size n, the algorithm will terminate in at most $f(n)$ steps." If we try to accurately estimate the number of steps, a cumbersome bound like

$$f(n) = \frac{1}{11}n^3 + 12n^2 + 15\frac{1}{2}n + \log_3 n + 17$$

might arise. Such precision only complicates matters and does not add to our understanding of the algorithm's efficiency. The following notational convention allows to simplify bounds by concentrating on their "main terms."

Definition 13.1.1. *For two functions $f, g : \mathbb{N}^+ \to \mathbb{R}$,*

- *$f(n) = O(g(n))$ if and only if there exists a positive constant $c \in \mathbb{R}$ and a constant $n_0 \in \mathbb{N}$, such that $|f(n)| \leq c|g(n)|$ for all $n \geq n_0$.*
- *$f(n) = \Omega(g(n))$ if and only if $g(n) = O(f(n))$.*
- *$f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.*

Asymptotic notation does wonders to the above ugly bound: We can now say that $f(n) = \Theta(n^3)$, which makes it easier to see how the number of steps performed by the algorithm grows as n gets larger and larger. Notice how the asymptotic notation swallowed all the constants and lower-order terms! To prove that $f(n) = \Theta(n^3)$ we need to show that there exist positive constants $c_1, c_2 \in \mathbb{R}$ and a constant $n_0 \in \mathbb{N}$, such that $c_1 n^3 \leq f(n) \leq c_2 n^3$ for all $n \geq n_0$. (We dropped the absolute values that come from Definition 13.1.1 since $f(n)$ and n^3 are nonnegative for $n \in \mathbb{N}^+$.) We can take $n_0 = 1$, $c_1 = \frac{1}{11}$, and $c_2 = 45.6$. For the lower bound, clearly $f(n) \geq \frac{1}{11}n^3$ when $n \in \mathbb{N}^+$. For the upper bound, note that in this range $n^3 \geq n^2 \geq n \geq \log_3 n$, and $n^3 \geq 1$. All these inequalities can be proved by elementary algebraic manipulation. Thus we get

$$f(n) \leq \frac{1}{11}n^3 + 12n^3 + 15\frac{1}{2}n^3 + n^3 + 17n^3 \leq 45.6n^3.$$

We can also perfectly well say that $f(n) = O(n^4)$ or that $f(n) = O(n^{25})$; these bounds are considerably less informative but correct. On the other hand, the bound $f(n) = O(n^2)$ (or even $f(n) = O(n^{2.99})$) is *not* correct. Indeed, we have seen that $f(n) \geq \frac{1}{11}n^3$. On the other hand, for any positive constant $c \in \mathbb{R}$, $\frac{1}{11}n^3 \geq cn^2$ for all $n \geq 11c$. Thus there is no positive constant $c \in \mathbb{R}$ and a constant $n_0 \in \mathbb{N}$ so that $f(n) \leq cn^2$ for all $n \geq n_0$.

Asymptotic notation is asymmetric, so we never write a statement like $O(g(n)) = f(n)$; the O, Ω, and Θ are always present on the right side of the equality sign. (However, we can write $n^2 + O(n) = \Theta(n^2)$, for example.) The right way to think of statements like $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$ is as inequalities; always remember what the notation means according to Definition 13.1.1.

13.2 Examples and properties

The following asymptotic inequalities can all be easily proved and are very useful. Do the proofs as an exercise. You might find induction or tools from elementary calculus helpful for some of these. You'll also need simple properties of logarithms, like the identity

$$\log_a n = \frac{\log_b n}{\log_b a}.$$

- For two constants $u, v \in \mathbb{R}$, if $u < v$ then $n^u = O(n^v)$. ("A bigger power swallows a smaller one.")
- If $f(n)$ is a degree-d polynomial in n then $f(n) = O(n^d)$. If the coefficient of n^d in $f(n)$ is nonzero then $f(n) = \Theta(n^d)$.
- For any real constants $b > 1$ and p, $n^p = O(b^n)$. ("An exponential swallows a power.")
- For any real constants $q > 0$ and p, $(\ln n)^p = O(n^q)$. ("A power swallows a logarithm.")
- For any real constants $a, b > 1$, $\log_a n = \Theta(\log_b n)$. This implies that we can write bounds like $O(\log n)$, $O(n \log n)$, etc., without specifying the base of the logarithm. ("Asymptotic notation swallows bases of logarithms.")

We conclude this lecture by demonstrating how new asymptotic inequalities can be derived from existing ones. These are often used in the analysis of algorithms, although they are so much a part of the folklore that they are rarely referred to explicitly.

Proposition 13.2.1. *The following hold:*

(a) If $f(n) = O(g(n))$ and $p \in \mathbb{N}$ is a constant then $p \cdot f(n) = O(g(n))$.

(b) If $f(n) = O(h(n))$ and $g(n) = O(w(n))$ then $f(n)+g(n) = O(\max(|h(n)|, |w(n)|))$.

(c) If $f(n) = O(h(n))$ and $g(n) = O(w(n))$ then $f(n) \cdot g(n) = O(h(n) \cdot w(n))$.

Proof. We prove each claim individually.

(a) If $f(n) = O(g(n))$ then there exists a positive constant $c \in \mathbb{R}$ and a constant $n_0 \in \mathbb{N}$, such that $|f(n)| \leq c|g(n)|$ for all $n \geq n_0$. Thus for $p \in \mathbb{N}$, $|p \cdot f(n)| = p|f(n)| \leq (pc)|g(n)|$ for all $n \geq n_0$, and by Definition 13.1.1, $p \cdot f(n) = O(g(n))$.

(b) If $f(n) = O(h(n))$ and $g(n) = O(w(n))$ then there exist two positive constants $c_1, c_2 \in \mathbb{R}$ and constants $n_1, n_2 \in \mathbb{N}$, such that $|f(n)| \leq c_1|h(n)|$ for all $n \geq n_1$ and $|g(n)| \leq c_2|w(n)|$ for all $n \geq n_2$. Then

$$|f(n)+g(n)| \leq |f(n)|+|g(n)| \leq c_1|h(n)|+c_2|w(n)| = (c_1+c_2)\max(|h(n)|, |w(n)|)$$

for all $n \geq \max(n_1, n_2)$, and by Definition 13.1.1, $f(n)+g(n) = O(\max(|h(n)|, |w(n)|))$.

(c) If $f(n) = O(h(n))$ and $g(n) = O(w(n))$ then there exist two positive constants $c_1, c_2 \in \mathbb{R}$ and constants $n_1, n_2 \in \mathbb{N}$, such that $|f(n)| \leq c_1|h(n)|$ for all $n \geq n_1$ and $|g(n)| \leq c_2|w(n)|$ for all $n \geq n_2$. Then

$$|f(n) \cdot g(n)| = |f(n)| \cdot |g(n)| \leq (c_1|h(n)|) \cdot (c_2|w(n)|) = (c_1c_2)|h(n) \cdot w(n)|$$

for all $n \geq \max(n_1, n_2)$, and by Definition 13.1.1, $f(n) \cdot g(n) = O(h(n) \cdot w(n))$.

□

Chapter 14

Graphs

14.1 Introduction

A *graph* G is an ordered pair (V, E), where V is a set and E is a set of two-element subsets of V. That is,

$$E \subseteq \big\{\{x, y\} : x, y \in V, x \neq y\big\}.$$

Elements of V are the *vertices* (sometimes called *nodes*) of the graph and elements of E are the *edges*. If $e = \{x, y\} \in E$ we say that x and y are *adjacent* in the graph G, that y is a *neighbor* of x in G and vice versa, and that the edge e is *incident* to x and y.

What are graphs good for? Graphs are perhaps the most pervasive abstraction in computer science. It is hard to appreciate their tremendous usefulness at first, because the concept itself is so elementary. This appreciation comes through uncovering the deep and fascinating theory of graphs and its applications.

Graphs are used to model and study transportation networks, such as the network of highways, the London Underground, the worldwide airline network, or the European railway network; the 'connectivity' properties of such networks are of great interest. Graphs can also be used to model the World Wide Web, with edges corresponding to hyperlinks; Google uses sophisticated ideas from graph theory to assign a PageRank to every vertex of this graph as a function of the graph's global properties. In this course we will introduce the basic concepts and results in graph theory, which will allow you to study and understand more advanced techniques and applications in the future.

14.2 Common graphs

A number of families of graphs are so common that they have special names that are worth remembering:

Cliques. A graph on n vertices where every pair of vertices is connected is called a *clique* (or n-clique) and is denoted by K_n. Formally, $K_n = (V, E)$, where $V = \{1, 2, \ldots, n\}$ and $E = \{\{i, j\} : 1 \leq i < j \leq n\}$. The number of edges in K_n is $\binom{n}{2}$.

Paths. A *path* on n vertices, denoted by P_n, is the graph $P_n = (V, E)$, where $V = \{1, 2, \ldots, n\}$ and $E = \{\{i, i+1\} : 1 \leq i \leq n-1\}$. The number of edges in P_n is $n-1$. The vertices 1 and n are called the *endpoints* of P_n.

Cycles. A *cycle* on $n \geq 3$ vertices is the graph $C_n = (V, E)$, where $V = \{1, 2, \ldots, n\}$ and $E = \{\{i, i+1\} : 1 \leq i \leq n-1\} \cup \{\{1, n\}\}$. The number of edges in C_n is n.

14.3 Some important concepts

Graph isomorphism. If the above definition of a cycle is followed to the letter, a graph is a cycle only if its vertices are natural numbers. So, for example, the graph $G = (V, E)$ with $V = \{A, B, C\}$ and $E = \{\{A, B\}, \{B, C\}, \{C, A\}\}$ would not be a cycle. This seems wrong, because G "looks like" a cycle, and for all practical purposes it is exactly like C_3. The concept of *graph isomorphism* provides a way to formally say that C_3 and G are "the same."

Definition 14.3.1. *Two graphs $G = (V, E)$ and $G' = (V', E')$ are said to be* isomorphic *if there exists a bijection $f : V \to V'$ such that*

$$\{x, y\} \in E \text{ if and only if } \{f(x), f(y)\} \in E'.$$

In this case we write $G \equiv G'$ and the function f is called an isomorphism *of G and G'.*

We generally regard isomorphic graphs to be essentially the same, and sometimes do not even draw the distinction. Hence graphs that are isomorphic to cliques, cycles and paths are themselves said to be cliques, cycles and paths, respectively.

Size. The number of edges of a graph is called it *size*. The size of an n-vertex graph is at most $\binom{n}{2}$, achieved by the n-clique.

Degree. The *degree* (or *valency*) of a vertex v in a graph $G = (V, E)$, denoted by $d_G(v)$, is the number of neighbors of v in G. More formally, this degree is

$$d_G(v) = \big|\{u \in V : \{v, u\} \in E\}\big|.$$

A graph in which every vertex has degree k is called *k-regular* and a graph is said to be *regular* if it is k-regular for some k.

The following is sometimes called the Handshake lemma. It can be interpreted as saying that the number of people at a cocktail party who shake hands with an odd number of others is even.

Proposition 14.3.2. *The number of odd-degree vertices in a graph is even.*

Proof. For a graph $G = (V, E)$, consider the sum of the degrees of its vertices:

$$s = \sum_{v \in V} d_G(v).$$

Observe that this sum counts every edge e twice, once for each of the vertices incident to e. Thus $s = 2|E|$, and, in particular, s is even. Subtracting from s the degrees of even-degree vertices of G, we see that the resulting quantity is the sum of the degrees of odd-degree vertices and is still even. This implies the proposition. □

Subgraphs and Connectivity.

Definition 14.3.3. *Given a graph $G = (V, E)$,*

- *A graph $G' = (V', E')$ is said to be a* subgraph *of G if and only if $V' \subseteq V$ and $E' \subseteq E$.*
- *A graph $G' = (V', E')$ is said to be an* induced subgraph *of G if and only if $V' \subseteq V$ and $E' = \{\{u, v\} \in E : u, v \in V'\}$.*

Given a graph G, a path, cycle, or clique in G is a subgraph of G that is a path, cycle, or clique, respectively. Two vertices v and u of G are said to be *connected* if and only if there is a path in G with endpoints u and v. A graph G as a whole is said to be connected if and only if every pair of vertices in G is connected.

A subgraph G' of G is called a *connected component* of G if it is connected and no other graph G'', such that $G' \subset G'' \subseteq G$, is connected. Clearly, a graph is connected if and only if it has a single connected component.

Finally, there is a related notion to a path that is also useful: Given a graph $G = (V, E)$, a *walk* W in G is a sequence $W = (v_1, e_1, v_2, e_2, \ldots, v_{n-1}, e_{n-1}, v_n)$ of vertices and edges in G that are not necessarily distinct, such that $\{v_1, v_2, \ldots, v_n\} \subseteq V$, $\{e_1, e_2, \ldots, e_{n-1}\} \subseteq E$, and $e_i = \{v_i, v_{i+1}\}$ for all $1 \leq i \leq n-1$. A walk differs from a path in that vertices and edges can be repeated. The set of edges $\{e_1, e_2, \ldots, e_{n-1}\}$ covered by W is denoted by $E(W)$. Similarly, the set of vertices covered by W is $V(W) = \{v_1, v_2, \ldots, v_n\}$.

14.4 Kinds of graphs

What we have been calling graph is actually only one of many kinds of graphs, namely an undirected, unweighted, simple graph. Let's see how each of these qualities can differ and what other kinds of graphs there are.

A *directed* (simple, unweighted) graph G is an ordered pair (V, E), where V is a set and E is a set of ordered pairs from V. That is,

$$E \subseteq \big\{(x, y) : x, y \in V, x \neq y\big\}.$$

Directed graphs are suitable for modeling one-way streets, non-reflexive relations, hyperlinks in the World Wide Web, and so on. The notion of degree as defined above

is no longer applicable to a directed graph. Instead, we speak of the *indegree* and the *outdegree* of a vertex v in G, defined as $|\{u \in V : (u, v) \in E\}|$ and $|\{u \in V : (v, u) \in E\}|$, respectively.

A graph that is not simple can have *multi-edges* and *self-loops*. Multi-edges are multiple edges between the same pair of vertices. (Their presence means that the collection of edges is no longer a set, but a so-called *multiset*.) A self-loop is an edge to and from a single vertex v.

Finally, a graph can also be *weighted*, in the sense that numerical weights are associated with edges. Such weights are extremely useful for modeling distances in transportation networks, congestion in computer networks, etc. We will not dwell on weighted graphs in this course. In fact, unless specified otherwise, the word "graph" will continue to refer to undirected, unweighted, simple graphs.

Chapter 15

More Graphs—Eulerian, Bipartite, and Colored

15.1 Eulerian graphs

Ever seen those puzzles that ask you to trace some shape without lifting the pencil off the paper? For graph theory initiates such questions present no difficulty, separating this select elite from the rest of the human race who are doomed to spend their Sunday afternoons hunched over, putting page after page out of commission, searching in vain for the ever-elusive drawing.

Given a graph $G = (V, E)$, define a *tour* of G as a walk $T = (v_1, e_1, v_2, e_2, \ldots, v_n, e_n, v_{n+1})$ in G, such that T does not trace any edge more than once. (That is, $e_i \neq e_j$ for all $1 \leq i < j \leq n$.) The tour is said to be *Eulerian* if, in addition, $v_{n+1} = v_1$, $V(T) = V$, and $E(T) = E$. Thus an Eulerian tour traverses all the edges of G, "walking along" each exactly once, eventually coming back to where it started. (Particular vertices may and generally will be visited more than once.) A graph is said to be Eulerian if and only if it has an Eulerian tour.

Eulerian graphs were discussed by the great Leonhard Euler, the most prolific mathematician of all time. Euler's analysis of these graphs, presented in 1736, marks the birth of graph theory.

Theorem 15.1.1. *A graph is Eulerian if and only if it is connected and each of its vertices has even degree.*

Proof. We first prove that if G is Eulerian its vertices all have even degree. Indeed, trace an Eulerian tour of G starting and ending at a vertex v. Every time the tour enters an intermediate vertex it also leaves it along a different edge. In the very first step the tour leaves v and in the last step it enters v. Thus we can label the edges incident to any vertex as "entering" and "leaving", such that there is a bijection between these two sets. This shows that the degree of every vertex is even.

To prove that a graph $G = (V, E)$ with all vertex degrees being even is Eulerian, consider the longest tour $T = (v_1, e_1, v_2, e_2, \ldots, v_n, e_n, v_{n+1})$ in G. (The length of a tour is measured by its number of edges.) We prove below that T is Eulerian. Namely, we prove that:

(a) $v_1 = v_{n+1}$

(b) $n = |E|$

Proof of (a). Assume for the sake of contradiction that $v_1 \neq v_{n+1}$. Then the number of edges of T incident to v_1 is odd. (After T first leaves v_1, it enters and leaves it an even number of times.) Since the degree of v_1 in G is even, there is an edge e of G that is incident to v_1 but not part of T. We can extend T by this edge, obtaining a contradiction.

Proof of (b). We can assume that $v_1 = v_{n+1}$. Suppose $V(T) \neq V$. Consider a vertex $v \in V \setminus V(T)$ and a vertex $u \in V(T)$. Since G is connected, there is a path P between v and u in G. Consider the first time a vertex of T is encountered along P; this vertex is v_i for some $1 \leq i \leq n$. Let $e' = \{v', v_i\}$ be the edge along which P arrives at v_i and note that $v' \notin V(T)$. This implies that we can augment T by v' and e', and obtain a longer tour T', namely

$$T' = (v', e', v_i, e_i, \ldots, v_n, e_n, v_1, e_1, \ldots, v_{i-1}, e_{i-1}, v_i).$$

We have reached a contradiction and can therefore assume that $V(T) = V$. That is, T visits all the vertices of G. Assume for the sake of contradiction that $E(T) \neq E$, so there exists an edge $e' = \{v_i, v_j\}$ of G, for some $1 \leq i < j \leq n$, that is not part of T. Then we can augment T by the edge e', and obtain a longer tour T', namely

$$T' = (v_i, e', v_j, e_j, v_{j+1}, e_{j+1}, \ldots, v_n, e_n, v_1, e_1, \ldots, v_i, e_i, \ldots, v_{j-1}, e_{j-1}, v_j).$$

T' is longer than T by one edge, which is a contradiction that proves the theorem.

□

Proof technique: Considering an extremal configuration. In the above proof the crucial idea was to consider the longest tour in the graph. This is an instance of a common proof technique: If we need to prove that some configuration with particular properties exists (like an Eulerian tour), consider the *extremal* (longest, shortest, etc.) configuration of a related type (usually one that has some but not all of the required properties), and prove that this extremal configuration has to satisfy *all* of the required properties. Some steps in the proof usually proceed by contradiction: If the extremal configuration wasn't of the required type we could find a "more extremal" one, which is a contradiction.

15.2 Graph coloring

Consider a wireless company that needs to allocate a transmitter wavelength to each of its users. Two users who are sufficiently close need to be assigned different wavelengths to prevent interference. How many different wavelengths do we need? Of

course, we can just assign a new wavelength to every user, but that would be wasteful if some users are far apart. So what's the least number of wavelengths we can get away with?

We can model the users as vertices in a graph and connect two vertices by an edge if the corresponding users are sufficiently close. A *coloring* of this graph $G = (V, E)$ is an assignment of colors to vertices, such that no two adjacent vertices get the same color. The above question can now be restated as asking for the minimum number of colors that are needed for a coloring of G.

Let us be a bit more precise in defining colorings: A *k-coloring* of G is said to be a function $c : V \to \{1, 2, \ldots, k\}$, such that if $\{v, u\} \in E$ then $c(v) \neq c(u)$. The smallest $k \in \mathbb{N}$ for which a k-coloring of G exists is called the *chromatic number* of G. If a k-coloring of G exists, the graph is said to be k-colorable. There are many deep results concerning colorings and the chromatic number. At this point we only give the simplest one:

Proposition 15.2.1. *If the degree of every vertex in a graph G is at most k, then the chromatic number of G is at most $k + 1$.*

Proof. By induction on the number of vertices in G. (The degree bound k is fixed throughout the proof.) If G has a single vertex, then the maximal degree is 0 and the graph is 1-colorable. Since $1 \leq k+1$, the proposition holds. Suppose every graph with at most n vertices and all vertex degrees at most k is $(k+1)$-colorable. Consider a particular graph $G = (V, E)$ with $n + 1$ vertices, and all degrees at most k. Let G' be the graph obtained from G by deleting a particular vertex v and all the edges incident to v. That is, G' is the incident subgraph of G on the vertices $V \setminus \{v\}$. G' has n vertices, all of degree at most k, and is thus $(k + 1)$-colorable. Let c' be such a coloring of G'. We extend it to a coloring c of G as follows. For every vertex $u \in G$ such that $u \neq v$ we define $c(u) = c'(u)$. The vertex v has at most k neighbors in G and there is at least one color i among $\{1, 2, \ldots, k + 1\}$ that has not been assigned to any of them. We define $c(u) = i$. This is a $(k + 1)$-coloring, and the proposition follows. □

15.3 Bipartite graphs and matchings

A bipartite graph is a graph that can be partitioned into two parts, such that edges of the graph only go between the parts, but not inside them. Formally, a graph $G = (V, E)$ is said to be bipartite if and only if there exist $U \subseteq V$, such that

$$E \subseteq \{\{u, u'\} : u \in U \text{ and } u' \in V \setminus U\}.$$

The sets U and $V \setminus U$ are called the *classes* of G. A *complete bipartite graph* $K_{m,n}$ is a graph in which all the edges between the two classes are present. Namely, $K_{m,n} = (V, E)$, where $V = \{1, 2, \ldots, m+n\}$ and $E = \{\{i, j\} : 1 \leq i \leq m, m+1 \leq j \leq m+n\}$. The number of edges in K_n is mn. From the definition of coloring, it follows that a graph is bipartite if and only if it is 2-colorable. (Check!) Here is another useful characterization of bipartite graphs:

Proposition 15.3.1. *A graph is bipartite if and only if it contains no cycle of odd length.*

Proof. For one direction of the claim, let G be a bipartite graph and let $C = (v_1, v_2, \ldots, v_n, v_1)$ be a cycle in G. Suppose without loss of generality that $v_1 \in U$, where U is as in the definition of bipartiteness. Then by simple induction that we omit, $v_i \in U$ for every odd $1 \leq i \leq n$. Since $\{v_n, v_1\} \in E$, $v_n \in V \setminus U$ and thus n is even. It follows that the number of edges in C is even.

Before proving the other direction, we need a simple lemma.

Lemma 15.3.2. *Given a graph $G = (V, E)$, let $P = (v_1, v_2, \ldots, v_n)$ be a shortest path between two vertices v_1 and v_n in G. Then for all $1 \leq i < j \leq n$, $P_i = (v_i, v_{i+1}, \ldots, v_j)$ is a shortest path between v_i and v_j.*

Proof. Proof by contradiction. Let $Q_i = (v_i, u_1, u_2, \ldots, u_l, v_j)$ be a shortest path between v_i and v_j. Assume for the sake of contradiction that Q_i is shorter than P_i. Consider the walk

$$Q = (v_1, v_2, \ldots, v_i, u_1, u_2, \ldots, u_l, v_j, v_{j+1}, \ldots, v_n).$$

Since Q_i is shorter than P_i, Q is shorter than P. Now consider the graph $G' = (V(Q), E(Q))$. This graph is connected, and thus there is a shortest path P' between v_1 and v_n in G'. The number of edges in this shortest path cannot exceed the total number of edges in G', and thus P' is shorter than P. Since P' is also a path between v_1 and v_n in G, we have reached a contradiction. □

We now turn to the other direction of the proposition. Assume that $G = (V, E)$ has no odd cycle. If G has more than one connected component we look at every component separately. Clearly, if every component is bipartite, G as a whole is bipartite. Thus assume that G is connected. Pick an arbitrary vertex $v \in V$ and define a set $U \subseteq V$ as

$$U = \{x \in V : \text{ the shortest paths from } v \text{ to } x \text{ have even length}\}.$$

Clearly, $V \setminus U$ is the set

$$V \setminus U = \{x \in V : \text{ the shortest paths from } v \text{ to } x \text{ have odd length}\}.$$

We prove that no two vertices in U are adjacent; the proof for $V \setminus U$ is similar. Consider for the sake of contradiction an edge $e = \{u, u'\} \in E$, such that $u, u' \in U$. Denote a shortest path from v to u by P_1 and a shortest path from v to u' by P_2. Given two vertices s and t on a path P, let $P^{s,t}$ be the part of P that connects s and t. Consider a vertex w that lies on both P_1 and P_2. The above lemma implies that $P_1^{v,w}$ and $P_2^{v,w}$ are shortest paths between v and w and thus have the same length, which we denote by $l(w)$. Consider the vertex w^* shared by P_1 and P_2 that maximizes $l(w)$ among all such w. The paths $P_1^{w^*,u}$ and $P_2^{w^*,u'}$ share no vertex in common other than w^*. Furthermore, the length of $P_1^{w^*,u}$ is the length of P_1 minus $l(w^*)$ and the length of $P_2^{w^*,u'}$ is the length of P_2 minus $l(w^*)$. Since the lengths of P_1 and P_2 are

both even, the lengths of $P_1^{w^*,u}$ and $P_2^{w^*,u'}$ have the same parity (that is, they are either both even or both odd). Now consider the cycle C composed of $P_1^{w^*,u}$, the edge $\{u, u'\}$, and $P_2^{w^*,u'}$. Since $P_1^{w^*,u}$ and $P_2^{w^*,u'}$ share no vertex in common other than w^*, C really is a cycle in G. Moreover, since the lengths of $P_1^{w^*,u}$ and $P_2^{w^*,u'}$ have the same parity, the number of edges in C is odd! We have reached a contradiction that completes the proof. □

Bipartite graphs are particularly useful to model symmetric relations from one set to another. For example, given a collection of boys and girls, we could model the relation "wants to go to the prom with" by a bipartite graph. Given such preferences, an interesting question is whether we can pair the boys up with the girls, so that they all end up going to the prom with someone they actually want to go with. It turns out that this question has a very precise answer. To state the theorem we need to define the notion of matching:

Definition 15.3.3. *Given a bipartite graph $G = (V, E)$, a* matching *B in G is a set of disjoint edges. Namely, $B \subseteq E$ and $e_1 \cap e_2 = \emptyset$ for any $e_1, e_2 \in B$. A matching is said to be* perfect *if $\bigcup_{e \in B} e = V$.*

Consider now a set B of boys, a set G of girls, and a symmetric relation P from B to G. Define a graph $W = (B \cup G,\ \{\{b, g\} : (b, g) \in P\})$. The above question simply asks to characterize when there exists a perfect matching in W. The below result, known as Hall's theorem, provides such a characterization. To state the theorem, we use another piece of notation: Given a subset S of the vertices of W, we let $\Gamma(S)$ be the set of vertices of W adjacent to at least one of the vertices of S.

Theorem 15.3.4. *A bipartite graph $W = (V, E)$ with classes B and G has a perfect matching if and only if $|B| = |G|$ and $|\Gamma(S)| \geq |S|$ for all $S \subseteq B$.*

Proof. One direction is easy: Assume W has a perfect matching and consider a set $S \subseteq B$. Every element of S is matched to a distinct element of G and hence $|\Gamma(S)| \geq |S|$. In particular, $|G| \geq |B|$. By a symmetric argument we get that $|B| \geq |G|$ and thus $|B| = |G|$.

For the other direction, assume that $|B| = |G|$ and that $|\Gamma(S)| \geq |S|$ for all $S \subseteq B$. We prove that there exists a perfect matching in W by strong induction on $|B|$. For the base case, if $|B| = |G| = 1$, the matching consists of the single edge of W. Assuming that the claim holds for all graphs with $|B| \leq k$, consider a graph W as above with $|B| = k + 1$. We distinguish between two possibilities:

(a) If for every $S \subset B$, $|\Gamma(S)| > |S|$, we take an arbitrary $x \in B$ and match it with an adjacent $y \in G$. Then for every subset S' of $B \setminus \{x\}$, it still holds that the number of vertices of $G \setminus \{y\}$ adjacent to at least one of the vertices of S' is at least $|S'|$. We can thus match the vertices of $B \setminus \{x\}$ with the vertices of $G \setminus \{y\}$ by the induction hypothesis.

(b) If for some $S \subset B$, $|\Gamma(S)| = |S|$, we note that for every $S' \subseteq S$, the number of vertices in $\Gamma(S)$ adjacent to at least one of the vertices of S' is at least $|S'|$.

Thus we can match S with $\Gamma(S)$ by the induction hypothesis. Now we need to show that we can match $B \setminus S$ with $G \setminus \Gamma(S)$. Consider a set $S' \subseteq B \setminus S$ and the set T' of its neighbors in $G \setminus \Gamma(S)$. Note that the set of neighbors of $S \cup S'$ in G is $\Gamma(S) \cup T'$. Thus $|S \cup S'| \leq |\Gamma(S) \cup T'|$. Since $|S| = |\Gamma(S)|$, we get that $|S'| \leq |T'|$. Thus by the induction hypothesis we can also match $B \setminus S$ with $G \setminus \Gamma(S)$.

This shows that in both cases all the vertices of B can be matched with vertices of G as required, and concludes the proof. $\square$

Chapter 16

Trees

16.1 Basic properties of trees

Trees in mathematics are graphs of a certain kind. In a sense, trees are the simplest interesting graphs, in that they have a very simple structure, but possess a rich variety of nontrivial properties. Trees have innumerable applications throughout computer science.

Definition 16.1.1. *A* tree *is a connected graph with no cycles. A vertex of degree one in a tree is called a* leaf.

An extensive theory of trees has been developed, and we give the tip of the iceberg below: Four additional characterizations that each could have been used to define trees.

Theorem 16.1.2. *Given a graph $G = (V, E)$, the following conditions are equivalent:*

(a) G is a connected graph with no cycles. (Thus G is a tree by the above definition.)

(b) For every two vertices $u, v \in V$, there exists exactly one path from u to v.

(c) G is connected, and removing any edge from G disconnects it. (Thus G is a minimal connected graph.*)*

(d) G has no cycles, and adding any edge to G gives rise to a cycle. (Thus G is a maximal acyclic graph.*)*

(e) G is connected and $|E| = |V| - 1$.

Proof. We will prove for each of the conditions (b)–(e) in turn that it is equivalent to condition (a). This implies the equivalence of all the conditions. The proof proceeds by induction on the number of vertices $|V|$ in G, and we relate a tree with $n + 1$ vertices to a tree with n vertices in the inductive step by "tearing off" a leaf. We begin by proving two lemmas that will be useful in this process.

Lemma 16.1.3. *Each tree with at least 2 vertices contains at least 2 leaves.*

Proof. Given a tree $T = (V, E)$, consider a path P of maximum length in T. We claim that the two end-points of P are leaves of T. Indeed, assume for the sake of contradiction that an end-vertex u of P has degree greater than 1 in T. Thus there exists an edge $\{u, u'\} \in E$ that is not part of P. If u' belongs to P then T contains a cycle. Otherwise we can extend P by the edge $\{u, u'\}$ and P is not a longest path in T. This contradiction proves the lemma. □

Lemma 16.1.4. *Given a graph $G = (V, E)$ and a leaf $v \in V$ that is incident to an edge $e = \{v, v'\} \in E$, the graph G is a tree if and only if $G' = (V \setminus \{v\}, E \setminus \{e\})$ is a tree.*

Proof. Assume that G is a tree and consider two vertices $u, w \in V \setminus \{v\}$. u and w are connected by a path P in G. Every vertex of P other than u and w has degree at least 2, and thus v cannot be a vertex of P. Therefore P is a path in G', which proves that G' is connected. Since G does not contain a cycle, G' cannot contain a cycle and is thus a tree.

For the other direction, assume that G' is a tree. Since a cycle only contains vertices with degree at least 2, a cycle in G must also be a cycle in G'. Therefore there are no cycles in G. Also, any two vertices of G other than v can be connected by the same path as in G', and v can be connected to any vertex u in G by a path that consists of the edge e and a path in G' between v' and u. Thus G is a tree. □

We are now ready to employ induction to prove that condition (a) implies each of (b)–(e). For the induction basis, all five conditions hold for the graph with a single vertex. Consider a graph $G = (V, E)$ with $|V| = n \geq 2$ and assume that (a) holds for G. By Lemma 16.1.3, G has a leaf $v \in V$ that is incident to an edge $e = \{v, v'\} \in E$. By Lemma 16.1.4, condition (a) holds for G'. The inductive hypothesis states that condition (a) implies conditions (b)–(e) for the graph $G' = (V \setminus \{v\}, E \setminus \{e\})$. We now need to prove that conditions (b)–(e) also hold for G.

Condition (b) holds for G by a similar argument to the one employed in the proof of Lemma 16.1.4. Condition (c) holds for G since removing any edge other than e disconnects G by the induction hypothesis, and removing e disconnects the vertex v from the rest of the graph. Condition (d) holds since G cannot have cycles by an argument similar to the proof of Lemma 16.1.4; adding an edge that is not incident to v creates a cycle by the inductive hypothesis, and adding an edge $\{v, u\}$, for some $u \in V \setminus \{v\}$ creates a cycle that consists of the edge $\{v, u\}$, the path from u to v', and the edge e. Finally, condition (e) holds since G is obtained from G' by adding one vertex and one edge.

We now prove that each of (b)–(d) imply (a). Conditions (b) and (c) on G each imply connectedness of G. By contrapositive, assume that G contains a cycle. Then taking two distinct vertices u, w on the cycle, there are two paths from u to w along the cycle, which implies $(b) \Rightarrow (a)$. Furthermore, removing one edge of the cycle does not disconnect G, which implies $(c) \Rightarrow (a)$. Condition (d) implies that G does not contain a cycle. By contrapositive, assume that G is disconnected. Then there are two vertices u and w that have no path connecting them and we can add the edge $\{u, w\}$ to G without creating a cycle. This implies $(d) \Rightarrow (a)$.

To prove $(e) \Rightarrow (a)$ we use induction on the number of vertices of G. The induction basis is the graph with one vertex and the claim trivially holds. For the induction hypothesis, assume that the claim holds for all graphs with $|V| - 1$ vertices. For the inductive step, assume that condition (e) holds for G and hence $|E| = |V| - 1$. Therefore the sum of the degrees of the vertices of G is $2|V| - 2$, and thus there is some vertex $v \in V$ of degree 1. The graph $G' = (V \setminus \{v\}, E \setminus \{e\})$ is connected and satisfies $|E \setminus \{e\}| = |V \setminus \{v\}| - 1$. By the induction hypothesis, G' is a tree. Lemma 16.1.4 now implies that G is a tree, which completes the proof. □

16.2 Spanning trees

One of the reasons that trees are so pervasive is that every connected graph G contains a subgraph that is a tree on all of the vertices of G. Such a subgraph is called a *spanning tree* of G.

Definition 16.2.1. *Consider a graph $G = (V, E)$. A tree of the form (V, E'), where $E' \subseteq E$ is called a spanning tree of G.*

Proposition 16.2.2. *Every connected graph $G = (V, E)$ contains a spanning tree.*

Proof. Consider a tree subgraph $T = (V', E')$ of G with the largest number of vertices. Suppose for the sake of contradiction that $V' \neq V$, and thus there exists $v \in V \setminus V'$. Take an arbitrary vertex $u \in V'$ and consider a path P between v and u. Let u' be the first vertex along P that belongs to V', and let v' be the vertex that immediately precedes u' in P. Consider the graph $T' = (V' \cup \{v'\}, E' \cup \{v', u'\})$. Lemma 16.1.4 implies that T' is a tree in G with a greater number of vertices than T, which is a contradiction. □

Chapter 17

Planar Graphs

17.1 Drawing graphs in the plane

As we have seen in class, graphs are often visualized by drawing them in the plane—vertices are drawn as points, and edges as curved segments (called *arcs*) that connect the corresponding points. A graph together with a drawing of it in the plane is called a *topological graph*.

A graph is called *planar* if there exists a drawing of it in which the interior of any arc does not touch or intersect any other arc. That is, two distinct arcs are either disjoint or touch at endpoints that they share. A planar graph together with a planar drawing of it is called a *plane graph*.

It is easy to verify that paths, cycles and trees of any size are planar. Transportation networks often provide examples of planar graphs, and graph planarity became important in computer science due to a connection with VLSI circuit design. Planar drawings are often considered superior when visualizing graphs, as they have no edge crossings that can be mistaken for vertices. In fact, a whole subfield of computer science called *graph drawing* is devoted to the study of various kinds of drawings of graphs.

It might not be obvious at first that there are any nonplanar graphs at all. There are, but we'll have to do some work to prove this, and we'll need two preliminary steps just to approach this issue. The first is to define the *faces* of a plane graph and the second is to mention the (in)famous Jordan curve theorem.

Let us begin with faces. Define an equivalence relation on the plane as follows: Two points $a, b \in \mathbb{R}^2$ are equivalent if they can be connected by an arc that does not intersect the edges of a given plane graph G. Then the set of all points that belong to a particular equivalence class of this relation are said to be a *face* of G. Intuitively, if we draw G on a white sheet of paper with a black pencil, the faces are the white regions; alternatively, if we cut the paper along the edges of the drawing, the faces are the resulting pieces. Note that faces are defined for plane graphs, but not for planar graphs without a drawing: Different drawings of the same graph can produce different sets of faces!

The second piece of mathematical equipment we'll need to study planar graphs

is the Jordan curve theorem.[1] It is a classical example of a mathematical statement that is intuitively obvious, but exceedingly difficult to prove. (Related specimens that arguably fall into this category are Kepler's conjecture and the Kneser-Poulsen conjecture.)

Theorem 17.1.1 (Jordan curve theorem)**.** *Every closed non-self-intersecting curve γ in the plane separates the plane into exactly two regions, one bounded and one unbounded, such that γ is the boundary of both. Alternatively, a plane drawing of any cycle C_i, for $i \geq 3$, has exactly two faces.*

To see why the Jordan curve theorem is not so easy to prove recall that there are some crazy curves out there—just think about fractals like the *Koch snowflake*. How would you go about proving that such monsters have "interior" and "exterior"?

The following corollary follows from the Jordan curve theorem by routine arguments.

Corollary 17.1.2. *Consider a plane graph G and an edge e that is part of a cycle in G. Then e lies on the boundary of exactly two faces of G.*

17.2 Euler's formula

The fundamental tool in the study of planar graphs is Euler's formula, presented by Euler in 1752.[2]

Theorem 17.2.1 (Euler's formula)**.** *Let G be a connected plane graph with n vertices, e edges, and f faces. Then*

$$n - e + f = 2.$$

Note that the theorem need not hold if the graph is not connected—Just think of a collection of isolated vertices. On the other hand, the formula remains true even for (non-simple) graphs with multiple edges and self-loops.

Proof. The proof proceeds by induction on the number of edges. If there are none, the graph consists of a single vertex, the drawing has one face, and the formula holds as $1 - 0 + 1 = 2$. Assume that the formula holds for all plane graphs having k edges. Consider a plane graph $G = (V, E)$ with n vertices, f faces, and $k + 1$ edges. We distinguish between two cases:

G is a tree. In this case $n = k + 2$, due to a tree characterization we have seen previously, and $f = 1$ since any planar drawing of a tree has exactly one face. Then the formula holds as $(k + 2) - (k + 1) + 1 = 2$.

[1] Jordan gets all the press even though his proof of the theorem was wrong, and it took almost 20 years until Veblen found a correct one in 1905.

[2] Caution: Due to Euler's prodigious output, there are multiple "Euler's formulae", "Euler's theorems", etc.

G **has a cycle** C**.** Take an edge e that lies on C and consider a plane graph $G' = (V, E \setminus \{e\})$, whose vertices and edges are drawn as in G. By Corollary 17.1.2, the edge e is adjacent to two faces of G, and these faces "merge" into one in G'. Thus G' has n vertices, $f - 1$ faces, and k edges. By the induction hypothesis, $n - k + (f - 1) = 2$, hence $n - (k + 1) + f = 2$.

This completes the proof by induction. □

Euler's formula implies that the number of faces of a plane graph does not depend on the drawing, so even though the faces themselves are only defined for a particular drawing, their number is fixed *a priori* for any planar graph! The formula has a number of other consequences that are frequently used in theoretical computer science. These consequences say that planar graphs have few edges, and always have at least one low-degree vertex. As they make abundantly clear, not only are not all graphs planar, but *most* graphs aren't. (Do you understand the sense in which the theorem below implies this?)

Theorem 17.2.2. *For any simple planar graph G with n vertices and e edges:*

(a) If $n \geq 3$ then $e \leq 3n - 6$. If $e = 3n - 6$ then every face of G is a 3-cycle (a "triangle") and G is called a triangulation*.*

(b) There is a vertex of G that has degree at most 5.

Proof. The proofs of the two parts are similar in their clever use of Euler's formula:

(a) If G is not connected, we can add edges to connect G while maintaining its planarity. Assume therefore that G is connected. Let f be the number of faces of G. For such a face t, let $\alpha(t)$ be the number of edges adjacent to t and consider the sum $\sum_t \alpha(t)$ that ranges over all faces t of G. As each edge is adjacent to at most two faces, a particular edge is counted at most twice in the above sum. Hence

$$\sum_t \alpha(t) \leq 2e.$$

On the other hand, each face has at least three edges on its boundary, so

$$\sum_t \alpha(t) \geq 3f.$$

We get $3f \leq 2e$, and, using Euler's formula, $3(2 - n + e) \leq 2e$ and

$$e \leq 3n - 6.$$

Finally, if $e = 3n - 6$ then $3f = 2e$ and it must be that every face has exactly three edges on its boundary.

(b) If the graph is disconnected we consider one particular connected component of it, so assume that G is connected. If G has two vertices or less the result is immediate, so assume that $n \geq 3$. Recall that $d_G(x)$ denotes the degree of

a vertex x in G. The sum $\sum_x d_G(x)$, ranging over the vertices x of G, counts every edge twice, so

$$\sum_x d_G(x) = 2e.$$

As we have seen, $e \leq 3n - 6$, so

$$\sum_x d_G(x) \leq 6n - 12.$$

If the degree of every vertex is at least 6, we get

$$6n \leq 6n - 12,$$

which is a contradiction. Therefore, there must be a vertex with degree at most 5.

□

An intuitive way to think about Theorem 17.2.2(a) is that once a graph has too many edges, there is no more room for them in the plane and they start intersecting. This gives a way to prove that a particular graph is not planar. Take K_5, for example. It has 5 vertices and 10 edges, and $10 > 3 \cdot 5 - 6$. Thus K_5 is not planar! In fact, no K_n is planar for $n \geq 5$, since they all contain K_5 as a subgraph. On the other hand, K_n is planar for $n \leq 4$, as can be demonstrated by their simple planar drawings. This illustrates a point that might be obvious by now: proving a graph to be planar is often easier than proving the opposite. (Just draw it!™)

How about complete bipartite graphs? It is easy to verify that $K_{i,j}$ is planar when $i \leq 2$ or $j \leq 2$. The smallest remaining suspect is $K_{3,3}$. Playing around with drawings doesn't help: There seems to be no way to draw $K_{3,3}$ without intersections. Let's try the trick that worked for K_5: The number of vertices of $K_{3,3}$ is 6, its number of edges is 9, and $9 \leq 3 \cdot 6 - 6$. No luck. We need a stronger tool, and here it is:

Proposition 17.2.3. *For any simple planar graph G with n vertices and e edges, if G does not contain a cycle of length 3 then $e \leq 2n - 4$.*

Proof. We can assume that G is connected as in Theorem 17.2.2. Let f be the number of faces of G and let $\alpha(t)$ be the number of edges adjacent to a face t. These edges make up a cycle in G, and thus their number is at least 4, implying $\alpha(t) \geq 4$. Consider the sum $\sum_t \alpha(t)$, over all faces t of G. Each edge is adjacent to at most two faces, thus

$$4f \leq \sum_t \alpha(t) \leq 2e.$$

Using Euler's formula, we get $4(2 - n + e) \leq 2e$ and $e \leq 2n - 4$. □

With this result we're finally in business: $K_{3,3}$ does not contain an odd cycle since it is bipartite, thus every cycle in the graph has length at least 4. Since $9 > 2 \cdot 6 - 4$, $K_{3,3}$ is not planar. Let's summarize what we've learned.

Theorem 17.2.4. *K_n is planar if and only if $n \leq 4$ and $K_{i,j}$ is planar if and only if $i \leq 2$ or $j \leq 2$.*

At this point we have laid the groundwork for one of the most striking results concerning planar graphs, known as Kuratowski's theorem. To state it we need the following definition:

Definition 17.2.5. *Given a graph $G = (V, E)$, an* edge subdivision *operation on an edge $\{u, v\}$ of G results in the graph $(V \cup \{x\}, (E \setminus \{\{u, v\}\}) \cup \{\{u, x\}, \{x, v\}\})$, where $x \notin V$ is a new vertex. A graph G' is said to be a* subdivision *of G if it can be obtained from G by successive applications of edge subdivision.*

Kuratowski's theorem says that not only are K_5 and $K_{3,3}$ non-planar, but every non-planar graph contains either a subdivision of K_5 or a subdivision of $K_{3,3}$. That is, the graphs K_5 and $K_{3,3}$ characterize the whole family of non-planar graphs!

Theorem 17.2.6 (Kuratowski's theorem)**.** *A graph is planar if and only if it does not contain a subdivision of K_5 or a subdivision of $K_{3,3}$ as a subgraph.*

17.3 Coloring planar graphs

You might have heard of the four-color problem. It was posed in the mid-19th century and occupied some of the best discrete mathematicians since that time. The original formulation is in terms of political maps. In such maps, neighboring countries are drawn with different colors. The question is how many colors are needed. It is easy to construct simple examples of maps that need at least four colors. The four color problem asks whether four colors always suffice, for any political map. (We require that every country is *connected*, unlike, say, the US.)

This problem is equivalent to whether every planar graph can be colored with four colors. (To see this, construct a graph whose vertices correspond to countries and whose edges connect neighbors through border segments.) It took over a century until Appel and Haken found a proof that four colors always suffice, and even that was possible only by using computers to conduct extensive case enumeration and analysis. To this date no proof of the four color theorem is known that does not rely on computers. On the other hand, in 1890 Heawood discovered a beautiful proof that *five* colors always suffice. To prepare for his proof, let us warm up by showing that every planar graph can be colored with 6 colors. The proof is surprisingly simple.

Theorem 17.3.1. *The chromatic number of a planar graph G is at most six.*

Proof. By induction on the number n of vertices of G. If $n \leq 6$ the claim is trivial. Assume every planar graph with at most k vertices can be colored with 6 colors or less, and consider a graph $G = (V, E)$ with $k + 1$ vertices. By Theorem 17.2.2(b), there is a vertex v of G with degree at most 5. Let G' be the induced subgraph of G on the vertices $V \setminus \{v\}$. By the induction hypothesis, G' can be colored with five colors or less. Color the vertices $V \setminus \{v\}$ of G with the colors that they are assigned

in the coloring of G'. Assign to v the color that is not used by its neighbors. Since the degree of v is at most five, such a color exists. This specifies a valid coloring of G. □

We are now ready for Heawood's five color theorem.

Theorem 17.3.2. *The chromatic number of a planar graph $G = (V, E)$ is at most five.*

Proof. The proof proceeds by induction on the number n of vertices of G. The base case is trivial. Assume every planar graph with at most k vertices can be colored with 5 colors or less, and consider a graph $G = (V, E)$ with $k+1$ vertices. Let v be a vertex of G with degree at most 5. If $d_G(v) < 5$ we can produce a 5-coloring of G as in the proof of Theorem 17.3.1. Assume $d_G(v) = 5$ and let $c : (V \setminus \{v\}) \to \{1, 2, 3, 4, 5\}$ be a 5-coloring of the induced subgraph G' of G on the vertices $V \setminus \{v\}$. This coloring exists by the induction hypothesis.

We consider a particular drawing of G in the plane and henceforth regard G as a plane graph. Let v_1, v_2, v_3, v_4, v_5 be the neighbors of v in the order they appear around v in G. (That is, according to one of the circular orders in which the corresponding edges emanate from v in G.) Without loss of generality, assume that $c(v_i) = i$ for $1 \leq i \leq 5$. (Note that if some color is unused by v_1, v_2, v_3, v_4, v_5, we can simply assign that color to v.) We distinguish between two cases: Either there does not exist a path between v_1 and v_3 in G that uses only vertices of colors 1 and 3, or there does.

There is no such path. In this case consider the subgraph G'' of G that is the union of all paths that begin at v_1 and use only vertices with colors 1 and 3. Note that neither v_3 nor its neighbors belong to G''. We produce a 5-coloring of G as follows: All the vertices of G'' of color 1 are assigned the color 3, all the vertices of G'' of color 3 are assigned the color 1, the vertex v is assigned the color 1, and all other vertices of G keep the color assigned by c. No monochromatic edges are created by this assignment and the coloring is valid.

There is such a path. Consider a path P from v_1 to v_3 that uses only vertices with colors 1 and 3. Together with the edges $\{v, v_1\}$ and $\{v, v_3\}$ this forms a cycle. The vertices v_2 and v_4 lie on different sides of this cycle. (Here we use the Jordan curve theorem.) Therefore there is no path between v_2 and v_4 that uses only vertices with colors 2 and 4, and we can apply the reasoning of the previous case.

□

17.4 Concluding remarks

There are many more amazing results associated with planar graphs. Two of the most striking are Fáry's theorem and Koebe's theorem. Fáry's theorem states that every planar graph can be drawn in the plane without edge crossings, such that all the arcs

are *straight line segments*. Koebe's theorem says that every planar graph is in fact isomorphic to an "incidence graph" of a collection of nonoverlapping discs in the plane. (The vertices of this graph correspond to the discs, and two vertices are adjacent if and only if the corresponding disks are tangent.) Fáry's theorem is an immediate consequence of Koebe's theorem, although they were discovered independently. Both are remarkable.