Education is not the learning of facts but the training of the mind to think. – **Albert Einstein**

For tech support, press the exact value of pi.
– **automated sadistic phone system**

DAD: Can you say the alphabet backwards?
SON: Sure, Z,Y,X,.... Can you say π backwards?
DAD: Urghh ...??!!**&$#??...

Chapter 2

Discrete Objects

1: Sets; sequences; graphs.
2: Building an intuition for proofs.

To say anything about discrete mathematics, at the very least we must introduce the cast of discrete objects.

2.1 Sets

Sets are everywhere. A set is a collection of items. Instead of an axiomatic set theory[1], we rely on your intuition about sets, and focus on set-operations. Here are two sets.

$$M = \{m, a, l, i, k\}; \qquad V = \{a, e, i, o, u\}.$$

We use short descriptive names for sets and list the elements inside curly brackets. Order does not matter and repeated elements can be removed: $\{a, a, r, d, v, a, r, k\}$ and $\{k, r, a, v, d\}$ are the same set of letters. The "belongs to" symbol $\in$ indicates set-membership: $m \in M$ means the letter m is in the set M. The universal set $\mathcal{U}$ contains <u>all</u> items. The elements in $\mathcal{U}$ depend on the context. The empty set $\varnothing$ (also written $\{\}$) contains <u>no</u> items. For our two sets M and V, the natural universal set is the lower-case alphabet,

$$\mathcal{U} = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}.$$

It is tedious to list all elements of a large set. We prefer to use compact descriptions of sets. We may write:

$$\mathcal{U} = \{a, b, c, \ldots, x, y, z\}, \qquad \text{or} \qquad \mathcal{U} = \{\text{lower case letters}\}.$$

Compact descriptions are essential for complex large sets which are hard to list out. Two such important sets are the natural numbers $\mathbb{N}$ the numbers we use to count (the counting numbers); and, the integers $\mathbb{Z}$.

$$\begin{aligned} \text{natural numbers } \mathbb{N} &= \{1, 2, 3, 4, 5, \ldots\} \\ \text{integers } \mathbb{Z} &= \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \ldots\}. \end{aligned}$$

We start counting from 1.[2] As you guessed, "..." ("dot, dot, dot") means going on forever. Another important set is the real numbers $\mathbb{R}$, which is not so easy to describe, let alone list out. We can build complex sets by specifying the properties of a generic element in the set. Let us work through an example.

$$E = \{2, 4, 6, 8, 10, \ldots\}.$$

How do we continue this list for E? You might guess E is the set of even numbers. But, what if I wrote

$$E' = \{2, 4, 6, 8, 10, 13, \ldots\}.$$

[1] The standard foundation of set theory is based on the Zermelo-Fraenkel axioms with Choice, **ZFC**.

[2] Many texts define $\mathbb{N}$ to include 0. We will use $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ if we need to refer to the counting numbers together with zero. In enumerative combinatorics, the set of positive integers, which we are calling $\mathbb{N}$, is often called $\mathbb{P}$. We reserve $\mathbb{P}$ to denote probability, to distinguish it from the many other uses we will have for P (predicate, polynomial, etc). P is a polular letter.

How do you interpret the nebulous "..." in E'? We used "..." to define $\mathbb{N}$ because $\mathbb{N}$ is familiar to us, so there is not much at risk. But, from now on, we must try to avoid "...". So, how do we define the positive even numbers E? We use a variable in the definition:

$$\begin{aligned} E &= \{\text{Natural numbers } n \text{ that are twice some other natural number } k.\}. \\ E &= \{n \mid n = 2k, \text{ where } k \in \mathbb{N}\}. \end{aligned} \tag{2.1}$$

To the left of the "|" is the variable n which represents a generic member of the set E. To the right of the "|" are properties that n must satisfy to be in E. Every n that satisfies these properties is in E and any n that does not satisfy these properties is not in E. So, E contains all the natural numbers which are multiples of 2.

Pop Quiz 2.1

Use a variable to define the set of positive odd numbers $O = \{1, 3, 5, 7, \ldots\}$.

Another important set is the rational numbers $\mathbb{Q}$, the ratios of integers. Here is one way to define $\mathbb{Q}$,

$$\text{rational numbers } \mathbb{Q} = \{r \mid r = a/b \text{ , where } a \in \mathbb{Z},\ b \in \mathbb{N}\}.$$

To define rational numbers, we used the variable r as a generic representative of a rational number in $\mathbb{Q}$. The property r must satisfy is that it must be the ratio of an integer and a natural number.

The Subset Relation. The subset relation indicates that one set contains another.

	Said out loud	What it means
$A \subseteq B$	A is a subset of B	Everything in A is in B.
$A \subset B$	A is a proper subset of B	Everything in A is in B and something in B is not in A.
$A = B$	A equals B	Everything in A is in B and everything in B is in A, $A \subseteq B$ *and* $B \subseteq A$.

The empty set $\varnothing$ is a subset of any set: $\varnothing \subseteq A$ for any set A. This is vacuously the case because the empty set has nothing in it. Therefore every item in the empty set, there happen to be none, is in the set A.

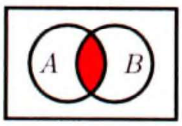
Exercise 2.2

True or False, and why: "All pigs that fly are green with purple spots." (Relate to $\varnothing \subseteq A$ for any A.)
[Hint: Define two sets: PF $=$ *{pigs that fly};* GP $=$ *{things that are green with purple spots}.]*

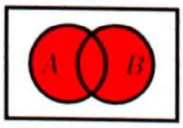
Set Operations. The intersection, union and complement can be used to to get new sets from old sets. The union of two sets combines the elements in both, and the intersection takes the common elements. The complement takes all elements outside a set and only makes sense within the context of some universal set.

	Said out loud	Set produced	Formal definition
$A \cap B$	A intersection B	Elements common to A and B.	$\{x \mid x \in A \text{ and } x \in B\}$
$A \cup B$	A union B	Combine elements in A with B.	$\{x \mid x \in A \text{ or } x \in B\}$
$\overline{A}$	A complement	Elements not in A.	$\{x \mid x \notin A\}$ ($x \notin A$ means x is not in A).

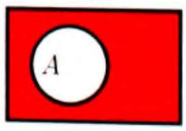
$A \cap B$



$A \cup B$



$\overline{A}$



Pop Quiz 2.3

$M = \{m, a, l, i, k\}$ and $V = \{a, e, i, o, u\}$. What are $M \cap V$, $M \cup V$ and $\overline{M}$? (State your universal set.)

Power Set. A set can be both a subset and a member of another set. Consider the two sets:

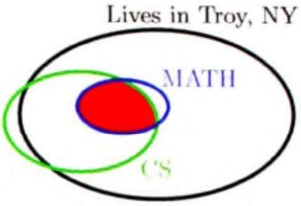
$$A = \{a, b\}; \qquad B = \{\{a, b\}, a, b, c\}.$$

A is a subset of B because every item in A is in B. But, A is also a member of B because B actually contains the *set* $\{a, b\}$ as an element. The power set of A, written $\mathcal{P}(A)$, is a set consisting of all the subsets of A,

$$\mathcal{P}(A) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}.$$

The power set contains sets that are subsets of the underlying set. Since $\varnothing$ is a subset of any set, $\varnothing \in \mathcal{P}(A)$. The number of elements in a finite set is its size, denoted by $|\cdot|$. So, $|A| = 2$, $|B| = 4$ and $|\mathcal{P}(A)| = 4$.

Venn Diagram. A Venn diagram pictorially shows the relationship between sets. A set is a region whose area corresponds to the size of the set. On the right are sets of students at a school in Troy, NY. The MATH students are fewer than the CS students (from the sizes of the regions). All the MATH students live in Troy (the MATH region is inside the Troy region). Most CS students live in Troy. The red region is CS $\cap$ MATH, the CS-MATH dual majors. Most MATH-majors are also CS-majors, but many CS-majors are not MATH-majors. Use Venn diagrams to convince yourself of the following relationships for combining set operations.



1. *Associative:* $(A \cap B) \cap C = A \cap (B \cap C)$;
   $(A \cup B) \cup C = A \cup (B \cup C)$.
2. *Commutative:* $A \cap B = B \cap A$;
   $A \cup B = B \cup A$.
3. *Complements:* $\overline{(\overline{A})} = A$;
   $\overline{A \cap B} = \overline{A} \cup \overline{B}$;
   $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
4. *Distributive:* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Figure 2.1: Combining set operations.

2.2 Sequences

Like a set, a sequence is a list of objects. Unlike a set, the order is important and repetition matters. Here are 3 different sequences: *malik*; *kilam*; *maalik*. Sometimes we refer to a sequence as a string. Computers deal only in ones and zeros – binary sequences. This is in part due to practical limitations of their hardware implementation: it is only possible to reliably differentiate between high voltage (a "1") and low voltage (a "0"). The 8-bit ASCII code allows us to convert alpha-numeric to binary. Here is an example.

m	a	l	i	k
01101101	01100001	01101100	01101001	01101011

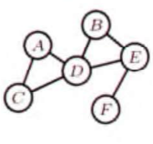
The alpha-numeric sequence *malik* corresponds (via the ASCII code) to the binary sequence

$$0110110101100001011011000110100101101011.$$

Any sequence can be converted to binary in this way. For more details on ASCII, we suggest the Internet.

2.3 Graphs

Sets and sequences represent collections of objects. They don't capture relationships between objects. Relationships are important. Graphs are the discrete-mathematical object for modeling and visualizing relationships. Recall our social network of six friends Alice, Bob, Charles, David, Edward and Fiona. We denote the set of people by V,



$$V = \{A, B, C, D, E, F\}.$$

A friendship can exist between a pair of people. In the friendship network above, each circle is a person, and two people are friends if they are linked. If there is no link between two people, for example A and B above, it means A and B are not friends. Does that mean they are enemies? That is open to interpretation and depends on the context. If we are modeling foreign relations between countries, then two countries are either friends or they are enemies. This is the interpretation we will take – if you are not friends, you are enemies.

To get a mathematical as opposed to visual representation of this social network, we identify each friend-link by a pair of people. For example the friend-link between A and D could be represented as (A, D). All the friend-links can be collected into a set, let us call it E. For our social network this set E would be

$$E = \{(A, C), (A, D), (C, D), (B, D), (B, E), (D, E), (E, F)\}.$$

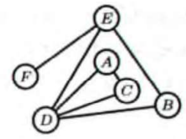
Given the set of people V and the set of friendships E, you should feel comfortable that you could draw a picture of the friendship network as we did above.

Exercise 2.4

Compare the friendship network shown on the right with the one above in the text.

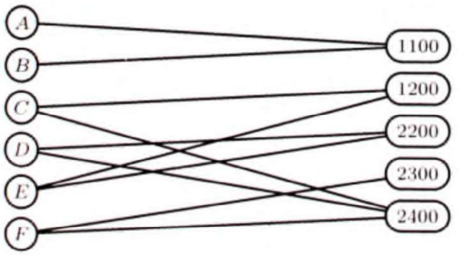
(a) Are the two friendship networks visually similar?

(b) Can this network be the same set of friends? Explain.

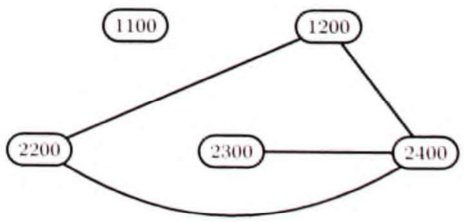


The take away from Exercise 2.4 is that different people may draw the same social network differently. The picture in Exercise 2.4 is very different from the one at the begining of this section, but they are both pictures of the same social network. What matters is who the people are, the set V, and who is friends with whom, the set E of friendships. The sets V and E together are a graph. The picture with circles and links is a visual representation of the graph. In high-school, a graph was a picture of a function $f(x)$ against x. That is not so in this book. When we say graph, visualize circles for objects with links between them identifying relationships. We refer to the picture of a function $f(x)$ against x as a plot or line-plot of the function.

Graphs model a variety of settings, not just social networks: road networks where objects are points of interest and links are roads; airport networks where objects are cities and two cities are linked if there is a non-stop flight from one to the other; etc. Graphs also model different kinds of relationships. Two examples, which occur often in computer science are affiliation graphs and conflict graphs. Affiliation graphs model the membership relationship between objects and groups to which those objects are affiliated. Conflict graphs model contention or competition between objects, for example different animals competing with each other in a food web. We illustrate affiliation and conflict graphs in the next two figures.



Affiliation graphs. Our friends are taking courses. The friends are on the left and the course numbers on the right. A link between a person and a course means the person is taking the course.



Conflict graphs. A student enrolled in two courses creates a conflict for those courses. The exams of the two courses must be at different times. A link between two courses means they conflict.

Affiliation graphs and conflict graphs are often related. The conflict graph on the right is derived from the affiliation graph on the left by linking two courses if some student is in both courses.

Pop Quiz 2.5

Which discrete object would you use to model the grid in the 2-contact EBOLA model. Explain.

2.4 Easing into Proofs

Let us ease you into proofs informally, before developing the formal infrastructure.

When is a Number a Square?

Suppose n is an integer, written $n \in \mathbb{Z}$. We would like to understand when n^2 is even. Let us tinker with the squares of the first few numbers.

n	0	± 1	± 2	± 3	± 4	± 5	± 6	± 7	± 8	± 9	± 10	± 11	...
n^2	$\boxed{\mathbf{0}}$	1	$\boxed{\mathbf{4}}$	9	$\boxed{\mathbf{16}}$	25	$\boxed{\mathbf{36}}$	49	$\boxed{\mathbf{64}}$	81	$\boxed{\mathbf{100}}$	121	...

We observe a few things. The squares are growing much faster than the numbers themselves. But what we care about is "When is the square even?" The even squares have been highlighted for you. At this point, it is not hard to make a guess – a conjecture.

Conjecture 2.1. Every even square came from an even number and every even number has an even square.

If we prove our conjecture, it becomes a theorem – a mathematical truth – and you can take it to the bank. Let us prove the conjecture. When n is even it means n is a multiple of 2, or $n = 2k$ for an integer k. Then,

$$n^2 = 4k^2 = 2 \cdot (2k^2).$$

Thus, n^2 is also a multiple of 2 because $2k^2$ is an integer, hence n^2 is even. Are we done? Not quite. What we have shown is that the squares of even numbers are even. That does not mean that every even square came from an even number. Since integers are either even or odd, consider an odd integer $n = 2k + 1$ for an integer k. Taking the square, we get

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

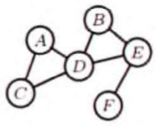
This time, n^2 is odd since it is 1 larger than a multiple of 2. So an odd integer cannot give rise to an even square, therefore an even square must have come from an even integer. Are we done? Have we shown that every even square came from an even number and every even number has an even square? Is our proof general? Yes, because we made no assumptions about n in our argument. So, our argument applies to any even n and any even n^2 which means we proved the conjecture. The conjecture is now a theorem.

Theorem 2.2. Every even square is the square of an even number and every even number has an even square.

You should be convinced of the theorem, and that is the purpose of a proof. We will slowly build a language for mathematical proofs and an infrastructure of proof patterns to standardize the notion of a proof and make things more concise. However, the purpose of a proof will always remain the same.

A proof must **convince** someone that a claim is true.

Every 6-person party has a 3-person friend clique or a 3-person war.



We model friendship networks using graphs. Our six friends $V = \{A, B, C, D, E, F\}$ are having a party. We reproduced their friendship network from page 17 here. Observe that $\{A, C, D\}$ are all mutual friends, and so form a 3-person friend clique. Also observe that $\{A, B, F\}$ are all mutual enemies as there are no friendships between them, so they could have a 3-person war if left unchaperoned. Our little social network has both a 3-person friend clique and a 3-person war. Is this always the case? Let's tinker with some easy examples.

If everyone was mutual friends, there can't be a 3-person war. Similarly, if everyone were enemies, there can't be a 3-person friend clique. So, in general, we cannot expect both a 3-person friend clique and a 3-person war. Is there any network with neither a 3-person friend clique nor a 3-person war? You can think of a 3-person friend clique as some kind of structure. Similarly, a 3-person war is also a kind of structure. We are asking whether there is a 6-person friendship network that has no structure.

Let's try to build a 6-person friendship network with no structure. To do so, we consider the network from the perspective of one of the friends, it might as well be Alice. If Alice has more friends than enemies, then she has at least 3 friends because there are 5 other people. The only other possibility is that she has more enemies than friends, in which case she has at least 3 enemies, again because there are 5 other people. We illustrate the two possible situations for Alice in the figure below. In (a) we show three of her friends (she has at least 3 friends) and in (b) we show three of her enemies (she has at least 3 enemies).

(a) More friends than enemies. (b) More enemies than friends.

In (a), if any pair of A's friends are also friends as indicated by the dashed line then 3 people form a friend clique. If all A's friends are mutual enemies, we have a 3-person war. So in case (a), there is either a 3-person friend clique or a 3 person war. The argument in (b) is similar. If any pair of A's enemies are also enemies, then together with A we have a 3-person war. If all A's enemies in (b) are mutual friends there is a 3-person friend clique. Since (a) and (b) are the only possibilities, in all cases it is not possible to construct such a friend network with neither a 3-person friend clique nor a 3-person war.

Theorem 2.3. Every 6-person friend network has either a 3-person friend clique or a 3-person war or both.

Every 6-person friendship network must have some structure. Isn't that interesting!

2.4.1 An Axiom: The Well-Ordering Principle

Can we prove everything? No. Some things, which we must take for granted, are the starting point for proving other things. In mathematics, we have three main types of claims:

1. **Axioms:** A self-evident statement that is asserted as true without proof.
2. **Conjectures:** A claim that is believed true but is not true until proven so.
3. **Theorems:** A proven truth. You can take it to the bank.

Axioms are taken to be true on faith. Therefore, axioms should be believable. We take high-school math for granted, for example the rules of algebra, geometry, etc., and some basic calculus. We also assume a very powerful fact that might seem obvious to you. Consider any set of positive integers. Such a set is a subset of the natural numbers, for example

$$\{2, 5, 4, 11, 7, 296, 81\}; \qquad \text{or,} \qquad \{6, 19, 24, 18, \ldots\}.$$

The first set is finite. In the second set, the "$\ldots$" indicates that the set goes on forever, but we don't know how, except that every number is positive. The first set has a minimum element equal to 2. Does the second set have a minimum element? You might feel that somehow the answer is yes, but unfortunately it cannot be proved. We have to assume this fact of the natural numbers, i.e. the natural numbers are well-ordered.

Axiom 2.4 (Well-ordering principle). Any non-empty subset of $\mathbb{N}$ has a minimum element.

This seems obvious. The next exercise might convince you that the axiom is non-trivial.

Exercise 2.6
(a) Construct a subset of the integers $\mathbb{Z}$ that has no minimum element.
(b) Construct a positive subset of the rationals $\mathbb{Q}$ that has no minimum element.

The well-ordering principle looks benign but it's very powerful. The game in mathematics is to string together previously established facts, i.e. axioms or theorems, to prove new interesting facts. The starting point is axioms. Let us use the well-ordering principle to prove something that looks completely unrelated.

$\sqrt{2}$ is not a rational number.[3]

$\sqrt{2}$ is not a discrete object. Our interest lies not in $\sqrt{2}$ *per-se* but in using the well-ordering principle to prove something apparently unrelated. If you believe the well-ordering principle, then you must accept that $\sqrt{2}$ is irrational. The method of proof is a little strange, and we will say much more about it later. If a number is rational, there are many ways to represent it as a ratio. For example, $\frac{2}{3} = \frac{4}{6}$. So let us try to write $\sqrt{2}$ as a ratio. If it can be done, there are many ways to do it. We collect all these ways into a hypothetical set:[4]

$$\boxed{\sqrt{2}} = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \frac{a_3}{b_3}, \frac{a_4}{b_4}, \cdots \right\},$$

where $\{a_1, a_2, \ldots\}$ are all integers and $\{b_1, b_2, \ldots\}$ are all natural numbers. The set $\boxed{\sqrt{2}}$, given that it is non-empty, implicitly defines two other sets: the numerators $\{a_1, a_2, \ldots\}$ and the denominators $\{b_1, b_2, \ldots\}$. The denominators form a set containing only natural numbers, so by the well-ordering principle, there is a minimum element. Call this minimum element b_* and the corresponding numerator a_*. So,

$$\sqrt{2} = \frac{a_*}{b_*}.$$

For b_* to be the minimum possible, it must be that a_* and b_* have no factors in common, for otherwise you could divide out that factor and get a smaller b_*.[5] Squaring both sides gives $2 = a_*^2/b_*^2$, or

$$a_*^2 = 2b_*^2.$$

Observe that a_*^2 is even since it is a multiple of 2. Recall that we proved the only way for a_*^2 to be even is for a_* to be even, that is $a_* = 2k$ (Theorem 2.2). Alas, $(2k)^2 = 2b_*^2$, or

$$b_*^2 = 2k^2.$$

Ha! b_*^2 is also even, which means b_* is even. Both a_* and b_* are even, so 2 is a common factor. Something smells fishy. What is going on? If the set $\boxed{\sqrt{2}}$ is non-empty, by the well-ordering principle there must be a minimum denominator b_*, and a_* and b_* have no common factor. But, we showed that a_* and b_* have the common factor 2. We have an impossible situation if $\boxed{\sqrt{2}}$ is non-empty. Therefore, $\boxed{\sqrt{2}}$ must be empty, in which case $\sqrt{2}$ is not a ratio and hence not rational.[6] Are you convinced?

Theorem 2.5. $\sqrt{2} \notin \mathbb{Q}$. That is, the square-root of two is not a rational number.

The method of proof is subtle, and goes by the name *reductio ad absurdum*, reduction to the absurd. In modern mathematics it is called a proof by contradiction. As Hardy comments, contradiction is far finer a gambit than a mere pawn or queen sacrifice in chess. With contradiction you give away the game and hope to steal it back later. The endpoint in the proof was something that smelled fishy. Another way to arrive at something smelling fishy is to make a mistake in the proof, and therein lies the danger in this type of gambit.

To prove $\sqrt{2}$ is not rational, we strung together several known facts. Here is a summary of those facts.

- The well-ordering principle (an axiom). Axioms are fundamental, plausible facts, and we do not prove them. Axioms are simply believed to be true. Axioms are the starting points in mathematics.
- Highschool knowledge that you either have or must accept as true without proof (e.g. algebra, basic properties of numbers, addition, multiplication, etc.). For example, we will not prove that $(x+1)^2 = x^2 + 2x + 1$. Use judgement in deciding whether some basic knowledge can be assumed. When in doubt, err on the cautious side and state your assumptions.
- Theorem 2.2 on the evenness of a square. We proved this using basic highschool math.

The final proof used these facts to convince you that $\sqrt{2}$ is not rational.

---

[3] Hipassus of the Pythagorean school discovered this around 500BC. The discovery was a crime, going against the Pythagorean school which held that all numbers are ratios of integers. Hipassus was sentenced to death by drowning for this crime, or his other crime which was to show how to inscribe a dodecahedron in a sphere. Mathematics is a dangerous profession.

[4] Listing the ratios implies the elements of the set can be listed out. Don't worry, we don't need this, even though it's true.

[5] In high-school, we knew this as reducing a fraction to its simplest form, or lowest terms.

[6] We take for granted a property of logic called the law of the excluded middle which says a statement is either true or false, there's no in-between. So $\boxed{\sqrt{2}}$ is either non-empty or it's empty. If it can't be non-empty, it must therefore be empty.

We did not set up any formal infrastructure for proofs. Our goal was to introduce basic proofs in the context of some elementary problems. In doing so, we have demonstrated three basic proof methods in action. Here are the proof methods we have seen.

- Direct and contrapositive proof. We used this to prove that even squares come from even numbers.
- Exhaustive proof using case by case analysis. We used this to prove our little facts about friendship cliques and wars in a 6-person social network.
- Proof by contradiction. We used this to show that $\sqrt{2}$ is irrational.

Without detailing the formal mechanics for how these proofs work, we hoped to give you an intuition for what it takes to convince somebody that a claim is true. Just as in a court of law you are innocent until proven guilty, in mathematics a claim is treated as false until proven true. Anytime you see the word proof, get prepared to be convinced, but also be skeptical.

We want to convince you of many things. So, you will see many proofs in this book. We also want you to convince others of many things, so you must become an expert in proofs. There are three main phases to making and proving a claim: identify the claim, prove it, and finally check that your proof is correct.

Three Steps for Making and Proving a Claim

Step 1: Precisely state the right thing to prove. Often, creativity and imagination are needed to identify the right claim. A trade off is usually achieved: the claim should be non-trivial otherwise it won't be useful, but the claim should also be within the realm of "the provable" given the tools you have. Most importantly, the claim should be true and how do you know that before proving it? The knack to come up with the right things to prove is a gift. Some people, like Paul Erdős, had an inordinate amount of this gift.

Step 2: Prove the claim. In any proof, some "genius" but often simple idea may be needed to make the proof go through. Again, creativity and imagination play a role. Sometimes standard proof techniques can be used. You can become proficient in these standard techniques through training and practice.

Step 3: Check the proof for correctness. No creativity is needed to look a proof in the eye and determine if it is correct, to determine if you are convinced. Never let anyone claim bogus things and convince you with invalid proofs. Make it a second nature to seek and validate proofs. Be skeptical. This advice will never let you down.

At a minimum, you should be able to precisely state what you want to prove. That is our next order of business. We will then set up an infrastructure of proof templates for proving different types of precisely stated claims. Needless to say, we cannot cover all possible proof strategies.[7] As you work through this book, and in general with all things mathematical, keep an eye out for nifty tricks and tactics for proving things. File them away, for someday they may come in handy.

A trick that is used twice becomes a method. — G. Polya

[7] It would be nice if we could list all proof strategies and write a program to prove any given theorem by exhaustively trying every strategy — an automated theorem prover. Then, we wouldn't have to worry about proving things. Ironically, it is a deep theorem of mathematics that there does not exist a general automated theorem prover. It appears that creativity will always have a place in mathematics.

2.5 Problems

Problem 2.1. What is the difference between a Theorem, a Conjecture and an Axiom?

Problem 2.2. List the elements in the following sets (E is the set of even numbers).

(a) $A = \{n \mid -4 \le n \le 15;\ n \in E\}$.
(b) $B = \{x \mid x^2 = 9;\ x \in \mathbb{Z}\}$.
(c) $C = \{x \mid x^2 = 6;\ x \in \mathbb{Z}\}$.
(d) $D = \{x \mid x = x^2 - 1;\ x \in \mathbb{R}\}$.

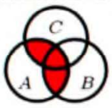
Problem 2.3. Give formal definitions of these sets using a variable.

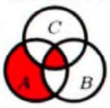
(a) $A = \{0, 1, 4, 9, 16, 25, 36, \ldots\}$.
(b) $B = \{0, 4, 16, 36, 64, 100, \ldots\}$.
(c) $C = \{1, 2, 4, 7, 11, 16, 22, \ldots\}$.
(d) $D = \{\ldots, 1/8, 1/4, 1/2, 1, 2, 4, 8, \ldots\}$.

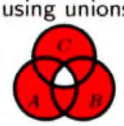
Problem 2.4. On the x–y plane, sketch the points in the sets:

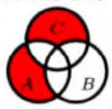
(a) $A = \{(x, y) \mid x \in [0, 1], y \in [0, 1]\}$.
(b) $B = \{(x, y) \mid x, y \in \mathbb{R}, x^2 + y^2 = 1\}$.
(c) $C = \{(x, y) \mid x, y \in \mathbb{R}, x^2 + y^2 \le 1\}$.
(d) $D = \{(x, y) \mid x \ge 1, y \in \mathbb{R}\}$.
(e) $E = \{(x, x^2) \mid x \in \mathbb{R}\}$.
(f) $F = \{(x, x + y) \mid x \in \mathbb{R}, y \in \mathbb{Z}\}$.

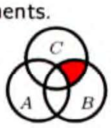
Problem 2.5. Express the shaded region using unions, intersections and complements.

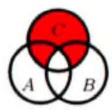
(a) 

(b) 

(c) 

(d) 

(e) 

(f) 

Problem 2.6. Give two sets A, B for which $A \not\subseteq B$ and $B \not\subseteq A$.

Problem 2.7. Complement depends on the universal set $\mathcal{U}$. Let $X = \{a, e\}$. What is $\overline{X}$ when:
(a) $\mathcal{U}$ = {lower case vowels}. (b) $\mathcal{U}$ = {lower case letters}

Problem 2.8. True or False: (a) $\mathbb{N} \subseteq \mathbb{Z}$ (b) $\mathbb{N} \subset \mathbb{Z}$ (c) $\mathbb{Z} \subseteq \mathbb{Q}$ (d) $\mathbb{Z} \subset \mathbb{Q}$

Problem 2.9. For each case, find $\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots$ and $\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots$.
(a) $A_i = \{n | n \in \mathbb{N}, n \ge i\}$. (b) $A_i = \{0, i\}$. (c) $A_i = \{x | x \in \mathbb{R}, 0 < x < i\}$.

Problem 2.10. Let $A_i = \{(x, y) \mid x \in [0, 1], y \in [1/(i + 1), 1/i]\}$. On the x–y plane, sketch:
(a) A_1 and A_2. (b) $A_1 \cup A_2$. (c) $A_1 \cup A_5$. (d) $A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$. (e) $A_1 \cup A_2 \cup \cdots = \bigcup_{i=1}^{\infty} A_i$.

Problem 2.11. Let $B = \{\{a, b\}, a, b, c\}$. List the power set $\mathcal{P}(B)$ (it has 16 elements)?

Problem 2.12. List all subsets of $\{a, b, c, d\}$ that contain c but not d.

Problem 2.13. (a) What are $|M \cap V|$ and $|\mathcal{P}(M \cap V)|$ for $M = \{m, a, l, i, k\}, V = \{a, e, i, o, u\}$? (b) What is $|\mathbb{N}|$?

Problem 2.14. $|A| = 7$ and $|B| = 4$. What are the possible values for $|A \cap B|$ and $|A \cup B|$?

Problem 2.15. What is the set $\mathbb{Z} \cap \overline{\mathbb{N}} \cap S$, where $S = \{z^2 \mid z \in \mathbb{Z}\}$ is the set perfect squares.

Problem 2.16 (Cartesian Product). Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$. The Cartesian product $A \times B$ is the set of pairs formed from elements of A and elements of B,

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

(a) List the elements in $A \times B$. What is $|A \times B|$? ($|X|$ is the number of elements in X.)
(b) List the elements in $B \times A$. What is $|B \times A|$?
(c) List the elements in $A \times A = A^2$. What is $|A \times A|$?
(d) List the elements in $B \times B = B^2$. What is $|B \times B|$?

Generalize the definition of $A \times B$ to a Cartesian product of three sets $A \times B \times C$.

Problem 2.17. Sketch the Cartesian products $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, $\mathbb{R} \times \mathbb{N}$, $\mathbb{N} \times \mathbb{R}$, $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$. (See Problem 2.16.)

Problem 2.18. List as a set all the 4-bit binary sequences. How many did you get? Now, list all the 4-bit binary sequences in which 00 does not occur. How many did you get?

Problem 2.19. How many binary sequences are of length 1,2,3,4,5? Guess the pattern.

Problem 2.20. A sequence $s_0, s_1, s_2, s_3, \ldots$ is described below. Give a "simple" formula for the nth term s_n in the sequence, for $n = 0, 1, 2, 3, \ldots$. Your answer should be of the form $s_n = f(n)$ for some function $f(n)$.

(a) $0, 1, 2, 3, 4, 5, 6 \ldots$
(b) $1, -1, 1, -1, 1, -1, \ldots$
(c) $0, 1, -2, 3, -4, 5, -6, \ldots$
(d) $2, 0, 2, 0, 2, 0, \ldots$
(e) $1, 2, 4, 8, 16, \ldots$
(f) $1, 3, 5, 7, 9, \ldots$
(g) $1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, \ldots$
(h) $0, 3, 8, 15, 24, 35, 48, 63, \ldots$
(i) $1, 2, 1/3, 4, 1/5, 6, 1/7, 8, 1/9, 10, 1/11, 12, \ldots$
(j) $1, 1/2, 4, 1/8, 16, 1/32, 64, 1/128, \ldots$

Problem 2.21. For each case in Problem 2.20, use a variable as in (2.1) to formally define the set of numbers.

Problem 2.22. Draw a picture of each graph representing friendships among our 6 friends $V = \{A, B, C, D, E, F\}$.

(a) $E = \{(A, B), (B, C), (C, D), (D, E), (E, F), (F, A)\}$.
(b) $E = \{(A, B), (A, C), (A, D), (A, E), (A, F)\}$.
(c) $E = \{(A, D), (B, D), (C, D), (A, E), (B, E), (C, E), (A, F), (B, F), (C, F)\}$.
(d) $E = \{(A, B), (B, C), (A, C), (D, E), (E, F), (D, F)\}$.

You should recognize familiar social structures in your pictures.

Problem 2.23. How do you get the conflict graph from the affiliation on page 18?

Problem 2.24. Model the relationship between radio-stations in Problem 1.7 using a graph.

(a) Would you use friendship networks, affiliation graphs or conflict graphs?
(b) Draw a picture of your graph for the 5 radio stations.
(c) Show that 3 radio frequencies $(1, 2, 3)$ suffice for no listener to hear garbled nonsense.

Problem 2.25 (Internet Exercise). Research these settings and explain how they can be represented by graphs:

(a) Infectious disease spread.
(b) Collaborations between academic authors.
(c) Niche overlap in ecology.
(d) Protein interactions in human metabolism.

Problem 2.26. True or false and why? Every square which is a multiple of 4 came from a multiple of 4 and every multiple of 4 has a square which is a multiple of 4.

Problem 2.27. Do you believe this method for amplifying money? Explain why or why not.

$$1¢ = \$0.01 = (\$0.1)^2 = (10¢)^2 = 100¢ = \$1.$$

Problem 2.28 (Quotient Remainder Theorem). Given are $n \in \mathbb{Z}$ and a divisor $d \in \mathbb{N}$.

Theorem. There are a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$, with $0 \le r < d$, such that $n = qd + r$.

Suppose $n = 27$ and $d = 5$; compute q and r. Can you think of a way to prove the theorem?

Problem 2.29. Mimic the method we used to prove $\sqrt{2}$ is irrational and prove $\sqrt{3}$ is irrational. Now use the same method to try and prove $\sqrt{9}$ is irrational. What goes wrong?

Problem 2.30 (Simple Continued Fractions).
For $n \ge 1$, a non-terminating continued fraction x is shown on the right.

$$x = \cfrac{1}{n + \cfrac{1}{n + \cfrac{1}{n + \cfrac{1}{n + \cfrac{1}{n + \cdots}}}}}$$

Can you think of a way to show that x is irrational, for any $n \in \mathbb{N}$? (Tinker with $n = 1$ first.)

Problem 2.31 (Ramsey). Prove a crude generalization of the 6-person party theorem. Specifically, in any n-person party, there is either a friend-clique or war with more than $(\log_2 n)/2$ people. Here is a "constructive" proof. Make three sets C (for clique), W (for war) and V. Sets C and W are initially empty and V has all the people. We run a process in steps and continue until no one is left in V. At each step, pick any person x from V and:

- Place x in C if x is friends with more than half of V. Discard from V all the enemies of x.
- Place x in W if x is enemies with at least half of V. Discard from V all the friends of x.

(a) Show that at every step in the process, everyone in C are mutual friends and everyone in W are mutual enemies.
(b) Show that at each step in the process, the size of V shrinks from $|V|$ to no less than $(|V| - 1)/2$.
(c) Show that the process continues for at least $\log_2 n$ steps, where in each step a person is added to either C or W.
(d) Show that either C or W has more than $(\log_2 n)/2$ people at the end. Are we done?