APPENDIX

# Proofs

## A.1 *Quod Erat Demonstrandum*, or What Is a Proof?

Our aim in this Appendix is not to present an essay on the nature of mathematical proofs. Many of the sections in the text provide a variety of arguments that can fuel such an essay, but our aim here is simply to present examples of proofs at various levels of formality and to illustrate the main techniques, so as to give the reader some help in developing his or her own proofs.

A proof can be viewed simply as a convincing argument. In casual conversation, we may challenge someone to "prove" her assertion, be it that she memorized the *Iliad* in the original Greek or that she skied a double-diamond run. The proof presented could be her reciting *ex tempore* a sizable passage from the *Iliad* (assuming we have a copy handy and can read Greek) or a picture or video of her skiing the run. In political, economic, or social discussions, we may present a detailed argument in support of some assertion. For instance a friend may have claimed that a needle-exchange program reduces both morbidity and medical costs; when challenged, he would proceed to cite statistics, prior studies, and, on the basis of his data, construct an argument. More formally, courts of law have standards of proof that they apply in adjudicating cases, particularly in criminal law; lawyers speak of "proof beyond a reasonable doubt" (needed to convict someone of a crime) or "preponderance of evidence" (a lesser standard used in civil cases).

None of these qualifies as a mathematical proof. A mathematical proof is intended to establish the truth of a precise, formal statement and is

typically couched in the same precise, formal language. In 1657, the English mathematician John Dee wrote:

> Probability and sensible proof, may well serve in things naturall and is commendable: In Mathematicall reasonings, a probably Argument, is nothing regarded: nor yet the testimony of sens, any whit credited: But onely a perfect demonstration, of truths certain, necessary, and invincible: universally and necessarily concluded is allowed as sufficient for an Argument exactly and purely Mathematicall.

One of life's great pleasures for a theoretician is writing the well-earned "q.e.d." that marks the end of a proof; it stands for the Latin *quod erat demonstrandum*, meaning literally "what was to be proved."

Our typical vision of a proof is one or more pages of formulae and text replete with appearances of "therefore," "hence," etc. Yet, when two mathematicians talk about their work, one may present a proof to the other as a brief sketch of the key ideas involved and both would agree that the sketch was a proof. In Section 7.1, we present a dozen proofs of NP-completeness for various classes of complexity in about twenty-five pages: all of these proofs and many more were given by Richard Karp in 1972 in about three pages. In Section 9.3, we discuss average-case complexity, for the most part eschewing proofs because of their complexity; yet the groundwork for the entire theory, including the basic proof of completeness, was described by Leonid Levin in 1984 in a one-page paper! (Admittedly this paper set something of a record for conciseness.) At the other extreme, several recent proofs in mathematics have taken well over a hundred pages, with at least one requiring nearly five hundred. Faced with one of these extremely long proofs, the challenge to the reader is to keep in mind all of the relevant pieces; faced with a one-page foundation for an entire area, the challenge is to fill in the steps in the (necessarily sketchy) derivations. Conversely, the challenges to the writers of these proofs were to present the very long proof in as organized and progressive a manner as possible and to present the one-page foundation without omitting any of the key ideas.

The main goal of a proof is communication: the proof is written for other people to read. In consequence, the communication must be tailored to the audience. A researcher talking to another in the same area may be able to describe a very complex result in a few minutes; when talking to a colleague in another area, he may end up lecturing for a few hours. In consequence, proofs are not completely formal: a certain amount of "handwaving" (typified by the prefatory words "it is obvious that. . .") is characteristic, because the steps in the proof are tailored to the reader.

Most mathematicians believe that every proof can be made completely formal; that is, it can be written down as a succession of elementary derivation steps from a system of axioms according to a system of rules of logical inference. Such proofs stand at one extreme of the scale: their steps are tiny. Of course, writing down any but the most trivial proofs in this completely formal style would result in extremely long and completely unintelligible proofs; on the other hand, any such proof could be verified automatically by a simple program. At the other extreme is the conversation between two researchers in the same area, where key ideas are barely sketched—the steps are huge. Thus a proof is not so much a passive object as a process: the "prover" advances arguments and the "checker" verifies them. The prover and the checker need to be working at the same level (to be comfortable with the same size of step) in order for the process to work. An interesting facet of this process is that the prover and the checker are often the same person: a proof, or an attempt at one, is often the theoretician's most reliable tool and best friend in building new theories and proposing new assertions. The attempt at proof either establishes the correctness of the assertion or points out the flaws by "stalling" at some point in the attempt. By the same token, a proof is also the designer's best friend: an attempt at proving the correctness of a design will surely uncover any remaining flaw.

In consequence, proofs cannot really be absolute; even after a proof is written, its usefulness depends on the audience. Worse yet, there is no absolute standard: just because our proof convinced us (or several people) does not make the proof correct. (Indeed, there have been several examples of proofs advanced in the last century that turned out to be flawed; perhaps the most celebrated example is the four-color theorem, which states that every planar graph can be colored with four colors. The theorem was known, as a conjecture, for several centuries and received several purported proofs in the 19th and 20th centuries, until the currently accepted proof—which fills in omissions of previous proofs, in part through an enormous, computer-driven, case analysis.) Of course, if every proof were written in completely formal style, then it could be verified mechanically. But no one would ever have the patience to write a proof in that style—this entire textbook would barely be large enough to contain one of its proofs if written in that style.

Fortunately mathematicians and other scientists have been writing and reading proofs for a long time and have evolved a certain style of communication. Most proofs are written in plain text with the help of formulae but are organized in a fairly rigid manner. The use of language is also somewhat codified—as in the frequent use of verbs such as "let" or

"follow" and adverbs or conjunctions such as "therefore" or "hence." The aim is to keep the flow of a natural language but to structure the argument and reduce the ambiguity inherent in a natural language so as to make it possible to believe that the argument could be couched in a completely formal manner if one so desired (and had the leisure and patience to do it).

## A.2 Proof Elements

The beginning for any proof is an *assertion*—the statement to be proved. The assertion is often in the form of an implication (if $A$ then $B$), in which case we call the antecedent of the implication ($A$), the *hypothesis*, and its consequent ($B$), the *conclusion*. Of course, the assertion does not stand alone but is inspired by a rich context, so that, in addition to the stated hypothesis, all of the relevant knowledge in the field can be drawn upon.

The proof then proceeds to establish the conclusion by drawing on the hypothesis and on known results. Progress is made by using *rules of inference*. For the most part, only two rules need to be remembered, both rules with which we are familiar:

- The rule of *modus ponens*: Given that $A$ is true and given that the implication $A \Rightarrow B$ is true, conclude that $B$ is true:

$$A \wedge (A \Rightarrow B) \vdash B$$

- The rule of *(hypothetical) syllogism*: Given that the two implications $A \Rightarrow B$ and $B \Rightarrow C$ are true, conclude that the implication $A \Rightarrow C$ is also true:

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \vdash (A \Rightarrow C)$$

For the second rule, we would simply note that implication is a transitive relation. Most other rules of inference are directly derived from these two and from basic Boolean algebra (such as de Morgan's law). For instance, the rule of *modus tollens* can be written

$$\overline{A} \wedge (B \Rightarrow A) \vdash \overline{B}$$

but is easily recognizable as *modus ponens* by replacing $(B \Rightarrow A)$ by its equivalent contrapositive $(\overline{A} \Rightarrow \overline{B})$; as another example, the rule of *disjunctive syllogism* can be written as

$$\overline{A} \wedge (A \vee B) \vdash B$$

but is recognizable as another use of *modus ponens* by remembering that $(X \Rightarrow Y)$ is equivalent to $(\overline{X} \vee Y)$ and so replacing $(A \vee B)$ by the equivalent $\overline{A} \Rightarrow B$.

A completely formal proof starts from the *axioms* of the theory. Axioms were perhaps best described by Thomas Jefferson in another context: "We hold these truths to be self-evident. . ." Axioms are independent of each other (one cannot be proved from the others) and together supply a sufficient basis for the theory. (A good axiomatization of a theory is an extremely difficult endeavor.) A formal proof then proceeds by applying rules of inference to the axioms until the conclusion is obtained. This is not to say that every proof is just a linear chain of inferences: most proofs build several lines of derivation that get suitably joined along the way. Of course, since implication is transitive, there is no need to go back to the axioms for every new proof: it suffices to start from previously proved results.

A mathematical proof is thus a collection of valid inferences, from known results and from the hypothesis of the theorem, that together lead to the conclusion. For convenience, we can distinguish among several proof structures: constructive proofs build up to the conclusion from the hypothesis; contradiction proofs use the law of excluded middle (a logic statement must be either true or false—there is no third choice[1]) to affirm the conclusion without deriving it from the hypothesis; induction proofs use the induction principle at the heart of counting to move from the particular to the general; and diagonalization proofs combine induction and contradiction into a very powerful tool. In the following section we take up each style in turn.

## A.3 Proof Techniques

### A.3.1 Construction: Linear Thinking

In its simplest form, a proof is simply a mathematical derivation, where each statement follows from the previous one by application of some elementary algebraic or logical rule. In many cases, the argument is constructive in the sense that it builds a structure, the existence of which establishes the truth of the assertion. A straight-line argument from hypothesis to conclusion typically falls in this category.

[1] Indeed, the scholarly name for this law is *tertium non datur*, Latin for "there is no third."

An example of a simple mathematical derivation is a proof that, if $n$ is an odd integer, then so is $n^2$. Because $n$ is an odd integer, we can write $n = 2k + 1$ for some integer $k$—we are using the hypothesis. We can then express $n^2$ as $(2k + 1)^2$. Expanding and regrouping (using known facts about arithmetic, such as associativity, distributivity, and commutativity of addition and multiplication), we get

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

where we have set $m = 2k^2 + 2k$, an integer. Thus $n^2$ is itself of the form $2m + 1$ for some integer $m$ and hence is odd, the desired conclusion. We have constructed $n^2$ from an odd number $n$ in such a way as to show conclusively that $n^2$ is itself odd.

Even in strict algebraic derivations, the line may not be unique or straight. A common occurrence in proofs is a *case analysis*: we break the universe of possibilities down into a few subsets and examine each in turn. As a simple example, consider proving that, if the integer $n$ is not divisible by 3, then $n^2$ must be of the form $3k + 1$ for some integer $k$. If $n$ is not divisible by 3, then it must be of the form $3m + 1$ or $3m + 2$ for some integer $m$. We consider the two cases separately. If $n$ is of the form $3m + 1$, then we can write $n^2$ as $(3m + 1)^2$; expanding and regrouping, we get

$$n^2 = (3m + 1)^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1 = 3l + 1$$

where we have set $l = 3m^2 + 2m$, an integer. Thus $n^2$ is of the desired form in this case. If, on the other hand, $n$ is the form $3m + 2$, then we get

$$\begin{aligned} n^2 = (3m + 2)^2 &= 9m^2 + 12m + 4 = 9m^2 + 12m + 3 + 1 \\ &= 3(3m^2 + 4m + 1) + 1 = 3l' + 1 \end{aligned}$$

where we have set $l' = 3m^2 + 4m + 1$, an integer. Thus $n^2$ is of the desired form in this second case; overall, then, $n^2$ is always of the desired form and we have completed our proof.

In this text, many of our proofs have to do with sets. In particular, we often need to prove that two sets, call them $S$ and $T$, with apparently quite different definitions, are in fact equal. In order to prove $S = T$, we need to show that every element of $S$ belongs to $T$ (i.e., we need to prove $S \subseteq T$) and, symmetrically, that every element of $T$ belongs to $S$ (i.e., we need to prove $T \subseteq S$). Thus a proof of set equality always has two parts. The same is true of any proof of equivalence (typically denoted by the English phrase "if and only if"): one part proves the implication in one direction ($A$ if $B$,

or, in logic notation, $B \Rightarrow A$) and the other part proves the implication in the other direction ($A$ only if $B$ or $A \Rightarrow B$). When we have to prove the equivalence of several statements, we prove a circular chain of implications instead of proving each equivalence in turn: $A \Rightarrow B \Rightarrow \cdots \Rightarrow Z \Rightarrow A$. By transitivity, every statement implies every other statement and thus all are equivalent.

We give just one small example. We prove that the following three characterizations of a finite tree are equivalent:

1. It is an acyclic and connected graph.
2. It has one more vertex than edges and is acyclic.
3. It has a unique simple path between any two vertices.

We construct three proofs. First we show that the first characterization implies the second. Both require the graph to be acyclic; assume then that the graph is also connected. In order for a graph of $n$ vertices to be connected, it has to have at least $n - 1$ edges because every vertex must have at least one edge connecting it to the rest of the graph. But the graph cannot have more than $n - 1$ edges: adding even one more edge to the connected graph, say from vertex $a$ to vertex $b$, creates a cycle, since there is already a path from $a$ to $b$.

Next we show that the second characterization implies the third. Since our graph is acyclic, it will have at most one path between any two vertices. (If there were two distinct simple paths between the same two vertices, they would form a cycle from the first vertex where they diverge to the first vertex where they reconverge.) We note that an acyclic graph with any edges at all must have a vertex of degree 1—if all degrees were higher, the graph would have at least one cycle. (Vertices of degree 0 clearly do not affect this statement.) To prove that the graph is connected, we use induction, which we discuss in detail in a later section. If the graph has two vertices and one edge, it is clearly connected. Assume then that all acyclic graphs of $n$ vertices and $n - 1$ edges, for some $n \geq 1$, are connected and consider an acyclic graph of $n + 1$ vertices and $n$ edges. This graph has a vertex of degree 1; if we remove it and its associated edge, the result is an acyclic graph of $n$ vertices and $n - 1$ edges, which is connected by the inductive hypothesis. But then the entire graph is connected, since the vertex we removed is connected to the rest of the graph by an edge.

Finally, we show that the third characterization implies the first. If there is a simple path between any two vertices, the graph is connected; if, in addition, the simple path is always unique, the graph must be acyclic (in any cycle, there are always two paths between two vertices, going around the cycle in both directions).

### A.3.2 Contradiction: *Reductio ad Absurdum*

As we have stated before, many theorems take the form of implications, i.e., assertions of the form "given $A$, prove $B$." The simplest way to prove such an assertion is a straight-line proof that establishes the validity of the implication $A \Rightarrow B$, since then *modus ponens* ensures that, given $A$, $B$ must also be true. An implication is equivalent to its contrapositive, that is, $A \Rightarrow B$ is equivalent to $\overline{B} \Rightarrow \overline{A}$. Now suppose that, in addition to our hypothesis $A$, we also assume that the conclusion is false, that is, we assume $\overline{B}$. Then, if we can establish the contrapositive, we can use *modus ponens* with it and $\overline{B}$ to obtain $\overline{A}$, which, together with our hypothesis $A$, yields a contradiction. This is the principle behind a proof by contradiction: it proceeds "backwards," from the negated conclusion back to a negated hypothesis and thus a contradiction. This contradiction shows that the conclusion cannot be false; by the law of excluded middle, the conclusion must then be true.

Let us prove that a chessboard of even dimensions (the standard chessboard is an $8 \times 8$ grid, but $2n \times 2n$ grids can also be considered) that is missing its leftmost top square and its rightmost bottom square (the end squares on the main diagonal) cannot be tiled with dominoes. Assume we could do it and think of each domino as painted black and white, with one white square and one black square. The situation is depicted in Figure A.1. In any tiling, we can always place the dominoes so that their black and white squares coincide with the black and white squares of the chessboard—any two adjacent squares on the board have opposite colors. Observe that all squares on a diagonal bear the same color, so that our chessboard will have unequal numbers of black and white squares—one of the numbers will exceed the other by two. However, any tiling by dominoes will have strictly equal numbers of black and white squares, a contradiction.

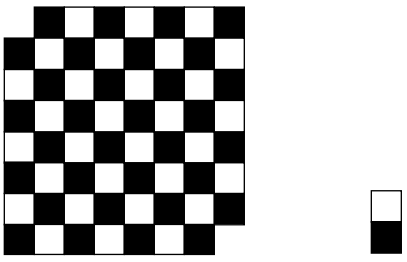


**Figure A.1** An $8 \times 8$ chessboard with missing opposite corners and a domino tile.

Proofs by contradiction are often much easier than direct, straight-line proofs because the negated conclusion is added to the hypotheses and thus gives us one more tool in our quest. Moreover, that tool is generally directly applicable, since it is, by its very nature, intimately connected to the problem. As an example, let us look at a famous proof by contradiction known since ancient times: we prove that the square root of 2 is not a rational number. Let us then assume that it is a rational number; we can write $\sqrt{2} = a/b$, where $a$ and $b$ have no common factor (the fraction is irreducible). Having formulated the negated conclusion, we can now use it to good effect. We square both sides to obtain $2b^2 = a^2$, from which we conclude that $a^2$ must be even; then $a$ must also be even, because it cannot be odd (we have just shown that the square of an odd number is itself odd). Therefore we write $a = 2k$ for some $k$. Substituting in our first relation, we obtain $2b^2 = 4k^2$, or $b^2 = 2k^2$, so that $b^2$, and thus also $b$, must be even. But then both $a$ and $b$ are even and the fraction $a/b$ is not irreducible, which contradicts our hypothesis. We conclude that $\sqrt{2}$ is not a rational number. However, the proof has shown us only what $\sqrt{2}$ is not—it has not constructed a clearly irrational representation of the number, such as a decimal expansion with no repeating period.

Another equally ancient and equally famous result asserts that there is an infinity of primes. Assume that there exists only a finite number of primes; denote by $n$ this number and denote these $n$ primes by $p_1, \ldots, p_n$. Now consider the new number $m = 1 + (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$. By construction, $m$ is not divisible by any of the $p_i$s. Thus either $m$ itself is prime, or it has a prime factor other than the $p_i$s. In either case, there exists a prime number other than the $p_i$s, contradicting our hypothesis. Hence there is an infinity of prime numbers. Again, we have not shown how to construct a new prime beyond the collection of $n$ primes already assumed—we have learned only that such a prime exists. (In this case, however, we have strong clues: the new number $m$ is itself a new prime, or it has a new prime as one of its factors; thus turning the existential argument into a constructive one might not prove too hard.)

### A.3.3 Induction: the Domino Principle

In logic, induction means the passage from the particular to the general. Induction enables us to prove the validity of a general result applicable to a countably infinite universe of examples. In practice, induction is based on the natural numbers. In order to show that a statement applies to all $n \in \mathbb{N}$, we prove that it applies to the first natural number—what is called the *basis* of the induction—then verify that, if it applies to any natural number, it

must also apply to the next—what is called the *inductive step*. The induction principle then says that the statement must apply to all natural numbers. The induction principle can be thought of as the *domino principle*: if you set up a chain of dominoes, each upright on its edge, in such a way that the fall of domino $i$ unavoidably causes the fall of domino $i+1$, then it suffices to make the *first* domino fall to cause the fall of *all* dominoes. The first domino is the basis; the inductive step is the placement of the dominoes that ensures that, if a domino falls, it causes the fall of its successor in the chain. The step is only a potential: nothing happens until domino $i$ falls. In terms of logic, the induction step is simply a generic implication: "if $P(i)$ then $P(i+1)$"; since the implication holds for every $i$, we get a chain of implications,

$$\cdots \Rightarrow P(i-1) \Rightarrow P(i) \Rightarrow P(i+1) \Rightarrow \cdots$$

equivalent to our chain of dominoes. As in the case of our chain of dominoes, nothing happens to the chain of implications until some true statement, $P(0)$, is "fed" to the chain of implications. As soon as we know that $P(0)$ is true, we can use successive applications of *modus ponens* to propagate through the chain of implications:

$$\begin{aligned} P(0) \wedge (P(0) \Rightarrow P(1)) &\vdash P(1) \\ P(1) \wedge (P(1) \Rightarrow P(2)) &\vdash P(2) \\ P(2) \wedge (P(2) \Rightarrow P(3)) &\vdash P(3) \\ &\cdots \end{aligned}$$

In our domino analogy, $P(i)$ stands for "domino $i$ falls."

Induction is used to prove statements that are claimed to be true for an infinite, yet countable set; every time a statement uses " ... " or "and so on," you can be sure that induction is what is needed to prove it. Any object defined recursively will need induction proofs to establish its properties. We illustrate each application with one example.

Let us prove the equality

$$1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = n(4n^2-1)/3$$

The dots in the statement indicate the probable need for induction. Let us then use it for a proof. The base case is $n = 1$; in this case, the left-hand side has the single element $1^2$ and indeed equals the right-hand side. Let us then assume that the relationship holds for all values of $n$ up to some $k$ and examine what happens with $n = k+1$. The new left-hand side is the

old left-hand side plus $(2(k+1)-1)^2 = (2k+1)^2$; the old left-hand side obeys the conditions of the inductive hypothesis and so we can write it as $k(4k^2-1)/3$. Hence the new left-hand side is

$$\begin{aligned} k(4k^2-1)/3 + (2k+1)^2 &= (4k^3 - k + 12k^2 + 12k + 3)/3 \\ &= ((k+1)(4k^2+8k+3))/3 \\ &= ((k+1)(4(k+1)^2-1))/3 \end{aligned}$$

which proves the step.

The famous Fibonacci numbers are defined recursively with a recursive step, $F(n+1) = F(n) + F(n-1)$, and with two base cases, $F(0) = 0$ and $F(1) = 1$. We want to prove the equality

$$F^2(n+2) - F^2(n+1) = F(n)F(n+3)$$

We can easily verify that the equality holds for both $n = 0$ (both sides equal 0) and $n = 1$ (both sides equal 3). We needed two bases because the recursive definition uses not just the past step, but the past two steps. Now assume that the relationship holds for all $n$ up to some $k$ and let us examine the situation for $n = k+1$. We can write

$$\begin{aligned} F^2(k+3) - F^2(k+2) & \\ &= (F(k+2) + F(k+1))^2 - F^2(k+2) \\ &= F^2(k+2) + F^2(k+1) + 2F(k+2)F(k+1) - F^2(k+2) \\ &= F^2(k+1) + 2F(k+2)F(k+1) \\ &= F(k+1)(F(k+1) + 2F(k+2)) \\ &= F(k+1)(F(k+1) + F(k+2) + F(k+2)) \\ &= F(k+1)(F(k+3) + F(k+2)) \\ &= F(k+1)F(k+4) \end{aligned}$$

which proves the step.

Do not make the mistake of thinking that, just because a statement is true for a large number of values of $n$, it must be true for all $n$.[2] A famous example (attributed to Leonhard Euler) illustrating this fallacy is

[2]Since engineers and natural scientists deal with measurements, they are accustomed to errors and are generally satisfied to see that most measurements fall close to the predicted values. Hence the following joke about "engineering induction." An engineer asserted that all odd numbers larger than 1 are prime. His reasoning went as follows: "3 is prime, 5 is prime, 7 is prime . . . Let's see, 9 is not prime, but 11 is prime and 13 is prime; so 9 must be a measurement error and all odd numbers are indeed prime."

the polynomial $n^2 + n + 41$: if you evaluate it for $n = 0, \ldots, 39$, you will find that every value thus generated is a prime number! From observing the first 40 values, it would be very tempting to assert that $n^2 + n + 41$ is always a prime; however, evaluating this polynomial for $n = 40$ yields $1681 = 41^2$ (and it is obvious that evaluating it for $n = 41$ yields a multiple of 41). Much worse yet is the simple polynomial $991n^2 + 1$. Write a simple program to evaluate it for a range of nonzero natural numbers and verify that it never produces a perfect square. Indeed, within the range of integers that your machine can handle, it cannot produce a perfect square; however, if you use an unbounded-precision arithmetic package and spend years of computer time on the project, you may discover that, for $n = 12{,}055{,}735{,}790{,}331{,}359{,}447{,}442{,}538{,}767$, the result *is* a perfect square! In other words, you could have checked on the order of $10^{28}$ values before finding a counterexample!

While these examples stress the importance of proving the correctness of the induction step, the basis is equally important. The basis is the start of the induction; if it is false, then we should be able to "prove" absurd statements. A simple example is the following "proof" that every natural number is equal to its successor. We shall omit the basis and look only at the step. Assume then that the statement holds for all natural numbers up to some value $k$; in particular, we have $k = k + 1$. Then adding 1 to each side of the equation yields $k + 1 = k + 2$ and thus proves the step. Hence, if our assertion is valid for $k$, it is also valid for $k + 1$. Have we proved that every natural number is equal to its successor (and thus that all natural numbers are equal)? No, because, in order for the assertion to be valid for $k + 1$, it must first be valid for $k$; in order to be valid for $k$, it must first be valid for $k - 1$; and so forth, down to what should be the basis. But we have no basis—we have not identified some fixed value $k_0$ for which we can prove the assertion $k_0 = k_0 + 1$. Our dominoes are not falling because, even though we have set them up so that a fall would propagate, the first domino stands firm.

Finally, we have to be careful how we make the step. Consider the following flawed argument. We claim to show that, in any group of two or more people where at least two people are blond, everyone must be blond. Our basis is for $n = 2$: by hypothesis, any group we consider has at least two blond people in it. Since our group has exactly two people, they are both blond and we are done. Now assume that the statement holds for all groups of up to $n$ ($n \geqslant 2$) people and consider a group of $n + 1$ people. This group contains at least two blond people, call them John and Mary. Remove from the group some person other than John and Mary, say Tim. The remaining group has $n$ people in it, including two blond ones (John

and Mary), and so it obeys the inductive hypothesis; hence everyone in that group is blond. The only question concerns Tim; but bring him back and now remove from the group someone else (still not John or Mary), say Jane. (We have just shown that Jane must be blond.) Again, by inductive hypothesis, the remaining group is composed entirely of blond people, so that Tim is blond and thus every one of the $n + 1$ people in the group is blond, completing our "proof" of the inductive step. So what went wrong? We can look at the flaw in one of two ways. One obvious flaw is that the argument fails for $n + 1 = 3$, since we will not find both a Tim and a Jane and thus will be unable to show that the third person in the group is blond. The underlying reason is more subtle, but fairly clear in the "proof" structure: we have used *two different* successor functions in moving from a set of size $n$ to a set of size $n + 1$.

Induction works with natural numbers, but in fact can be used with any structures that can be linearly ordered, effectively placing them into one-to-one correspondence with the natural numbers. Let us look at two simple examples, one in geometry and the other in programming.

Assume you want to tile a kitchen with a square floor of size $2^n \times 2^n$, leaving one unit-sized untiled square in the corner for the plumbing. For decorative reasons (or because they were on sale), you want to use only L-shaped tiles, each tile covering exactly three unit squares. Figure A.2 illustrates the problem. Can it be done? Clearly, it can be done for a hamster-sized kitchen of size $2 \times 2$, since that will take exactly one tile. Thus we have proved the basis for $n = 1$. Let us then assume that all kitchens of size up to $2^n \times 2^n$ with one unit-size corner square missing can be so tiled and consider a kitchen of size $2^{n+1} \times 2^{n+1}$. We can mentally divide the kitchen into four equal parts, each a square of size $2^n \times 2^n$. Figure A.3(a) illustrates the result. One of these parts has the plumbing hole for the full kitchen

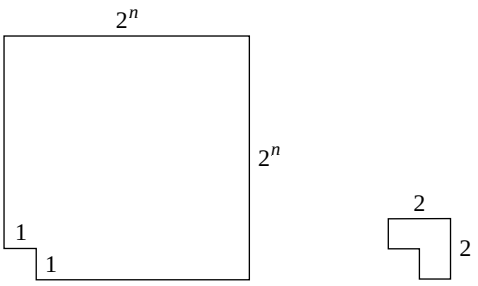
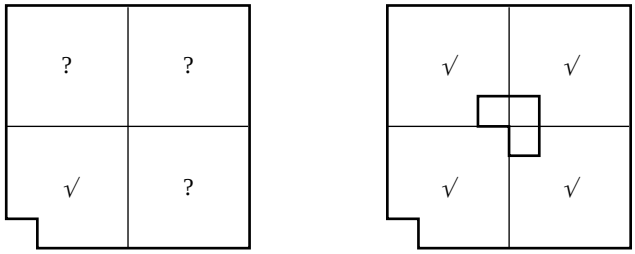



**Figure A.2** The kitchen floor plan and an L-shaped tile.




*(a) the subdivision of the kitchen* *(b) placing the key tile*

**Figure A.3** The recursive solution for tiling the kitchen.

and so obeys the inductive hypothesis; hence we can tile it. The other three, however, have no plumbing hole and must be completely tiled. How do we find a way to apply the inductive hypothesis? This is typically the crux of any proof by induction and often requires some ingenuity. Here, we place one L-shaped tile just outside the corner of the part with the plumbing hole, so that this tile has one unit-sized square in each of the other three parts, in fact at a corner of each of the other three parts, as illustrated in Figure A.3(b). Now what is left to tile in each part meets the inductive hypothesis and thus can be tiled. We have thus proved that the full original kitchen (minus its plumbing hole) can be tiled, completing the induction step. Figure A.4 shows the tilings for the smallest three kitchens. Of course, the natural numbers figure prominently in this proof—the basis was for $n = 1$ and the step moved from $n$ to $n + 1$.

As another example, consider the programming language Lisp. Lisp is based on atoms and on the list constructor `cons` and two matching destructors `car` and `cdr`. A list is either an atom or an object built with the

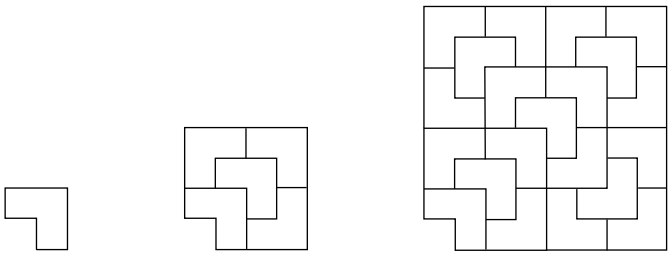


**Figure A.4** Recursive tilings for the smallest three kitchens.

constructor from other lists. Assume the existence of a Boolean function `listp` that tests whether its argument is a list or an atom (returning true for a list) and define the new constructor `append` as follows.

```
(defn append (x y)
  (if (listp x)
    (cons (car x) (append (cdr x) y))
     y))
```

Let us prove that the function `append` is associative; that is, let us prove the correctness of the assertion

```
(equal (append (append a b) c)
       (append a (append b c)))
```

We proceed by induction on `a`. In the base case, `a` is an atom, so that `(listp a)` fails. The first term, `(append (append a b) c)`, becomes `(append b c)`; and the second term, `(append a (append b c))`, becomes `(append b c)`; hence the two are equal. Assume then that the equality holds for all lists involving at most $n$ uses of the constructor and let us examine the list `a` defined by `(cons a' a")`, where both `a'` and `a"` meet the conditions of the inductive hypothesis. The first term, `(append (append a b) c)`, can be rewritten as

```
append (append (cons a' a") b) c
```

Applying the definition of `append`, we can rewrite this expression as

```
append (cons a' (append a" b)) c
```

A second application yields

```
cons a' (append (append a" b) c)
```

Now we can use the inductive hypothesis on the sequence of two `append` operations to yield

```
cons a' (append a" (append b c))
```

The second term, `(append a (append b c))`, can be rewritten as

```
append (cons a' a") (append b c)
```

Applying the definition of `append` yields

```
cons a' (append a" (append b c))
```

which is exactly what we derived from the first term. Hence the first and second terms are equal and we have proved the inductive step. Here again, the natural numbers make a fairly obvious appearance, counting the number of applications of the constructor of the abstract data type.

Induction is not limited to one process of construction: with several distinct construction mechanisms, we can still apply induction by verifying that each construction mechanism obeys the requirement. In such a case, we still have a basis but now have several steps—one for each constructor. This approach is critical in proving that abstract data types and other programming objects obey desired properties, since they often have more than one constructor.

Induction is very powerful in that it enables us to reduce the proof of some complex statement to two much smaller endeavors: the basis, which is often quite trivial, and the step, which benefits immensely from the inductive hypothesis. Thus rather than having to plot a course from the hypothesis all the way to the distant conclusion, we have to plot a course only from step $n$ to step $n+1$, a much easier problem. Of course, both the basis and the step need proofs; there is no reason why these proofs have to be straight-line proofs, as we have used so far. Either one may use case analysis, contradiction, or even a nested induction. We give just one simple example, where the induction step is proved by contradiction using a case analysis.

We want to prove that, in any subset of $n+1$ numbers chosen from the set $\{1, 2, \ldots, 2n\}$, there must exist a pair of numbers such that one member of the pair divides the other. The basis, for $n = 1$ is clearly true, since the set is $\{1, 2\}$ and we must select both of its elements. Assume then that the statement holds for all $n$ up to some $k$ and consider the case $n = k+1$. We shall use contradiction: thus we assume that we can find some subset $S$ of $k+2$ elements chosen from the set $\{1, 2, \ldots, 2k+2\}$ such that no element of $S$ divides any other element of $S$. We shall prove that we can use this set $S$ to construct a new set $S'$ of $k+1$ elements chosen from $\{1, 2, \ldots, 2k\}$ such that no element of $S'$ divides any other element of $S'$, which contradicts the induction hypothesis and establishes our conclusion, thereby proving the induction step. We distinguish three cases: (i) $S$ contains neither $2k+1$ nor $2k+2$; (ii) $S$ contains one of these elements but not the other; and (iii) $S$ contains both $2k+1$ and $2k+2$. In the first case, we remove an arbitrary element of $S$ to form $S'$, which thus has $k+1$ elements, none larger than $2k$, and none dividing any other. In the second case, we remove the one element of $S$ that exceeds $2k$ to form $S'$, which again will have the desired properties. The third case is the interesting one: we must remove both $2k+1$ and $2k+2$ from $S$ but must then add some other element (not in $S$) not exceeding $2k$ to obtain an $S'$ of the correct size. Since $S$ contains $2k+2$, it cannot contain $k+1$ (otherwise one element, $k+1$, would divide another, $2k+2$); we thus add $k+1$ to replace the two elements $2k+1$ and $2k+2$ to form $S'$. It remains to show that no element of $S'$ divides any other; the only candidate pairs are those involving $k+1$, since all others were pairs

in $S$. The element $k+1$ cannot divide any other, since all others are too small (none exceeds $2k$). We claim that no element of $S'$ (other than $k+1$ itself) divides $k+1$: any such element is also an element of $S$ and, dividing $k+1$, would also divide $2k+2$ and would form with $2k+2$ a forbidden pair in $S$. Thus $S'$ has, in all three cases, the desired properties.

### A.3.4 Diagonalization: Putting It all Together

Diagonalization was devised by Georg Cantor in his proof that a nonempty set cannot be placed into a one-to-one correspondence with its power set. In its most common form, diagonalization is a contradiction proof based on induction: the inductive part of the proof constructs an element, the existence of which is the desired contradiction. There is no mystery to diagonalization: instead, it is simply a matter of putting together the inductive piece and the contradiction piece. Several simple examples are given in Sections 2.8 and 2.9. We content ourselves here with giving a proof of Cantor's result. Any diagonalization proof uses the implied correspondence in order to set up an enumeration. In our case, we assume that a set $S$ can be placed into one-to-one correspondence with its power set $2^S$ according to some bijection $f$. Thus given a set element $x$, we have uniquely associated with it a subset of the set, $f(x)$. Now either the subset $f(x)$ contains $x$ or it does not; we construct a new subset of $S$ using this information for each $x$. Specifically, our new subset, call it $A$, will contain $x$ if and only if $f(x)$ does not contain $x$; given a bijection $f$, our new subset $A$ is well defined. But we claim that there cannot exist a $y$ in $S$ such that $f(y)$ equals $A$. If such a $y$ existed, then we would have $f(y) = A$ and yet, by construction, $y$ would belong to $A$ if and only if $y$ did not belong to $f(y)$, a contradiction. Thus the bijection $f$ cannot exist. More precisely, any mapping from $S$ to $2^S$ cannot be surjective: there must be subsets of $S$, such as $A$, that cannot be associated with any element of $S$—in other words, there are "more" subsets of $S$ than elements of $S$.

## A.4 How to Write a Proof

Whereas developing a proof for a new theorem is a difficult and unpredictable endeavor, (re)proving a known result is often a matter of routine. The reason is that the result itself gives us guidance in how to prove it: whether to use induction, contradiction, both, or neither is often apparent from the nature of the statement to be proved. Moreover, proving a theorem is a very goal-oriented activity, with a very definite and explicit goal;

effectively, it is a path-finding problem: among all the derivations we can create from the hypotheses, which ones will lead us to the desired conclusion? This property stands in contrast to most design activities, where the target design remains ill-defined until very near the end of the process.

Of course, knowing where to go helps only if we can see a path to it; if the goal is too distant, path finding becomes difficult. A common problem that we all experience in attempting to derive a proof is getting lost on the wrong path, spending hours in fruitless derivations that do not seem to take us any closer to our goal. Such wanderings are the reason for the existence of lemmata—signposts in the wilderness. A lemma is intended as an intermediate result on the way to our main goal. (The word comes from the Greek and so has a Greek inflection for its plural; the Greek word $\lambda\varepsilon\mu\mu\alpha$ denotes what gets peeled, such as the skin of a fruit—we can see how successive lemmata peel away layers of mathematics to allow us to reach the core truth.) When faced with an apparently unreachable goal, we can formulate some intermediate, simpler, and much closer goals and call them lemmata. Not only will we gain the satisfaction of completing at least some proofs, but we will also have some advance positions from which to mount our assault on the final goal. (If these statements are reminiscent of explorations, military campaigns, or mountaineering expeditions, it is because these activities indeed resemble the derivation of proofs.) Naturally, some lemmata end up being more important than the original goal, often because the goal was very specialized, whereas the lemma provided a broadly applicable tool.

Once we (believe that we) have a proof, we need to write it down. The first thing we should do is to write it for ourselves, to verify that we indeed have a proof. This write-up should thus be fairly formal, most likely more formal than the write-up we shall use later to communicate to colleagues; it might also be uneven in its formality, simply because there will be some points where we need to clarify our own thoughts and others where we are 100% confident. In the final write-up, however, we should avoid uneven steps in the derivation—once the complete proof is clear to us, we should be able to write it down as a smooth flow. We should, of course, avoid giant steps; in particular, we would do well to minimize the use of "it is obvious that."[3] Yet we do not want to bore the reader with

[3] A professor of mathematics was beginning his lecture on the proof of a somewhat tricky theorem. He wrote a statement on the board and said to the class, "It is obvious that this follows from the hypothesis." He then fell silent and stepped back looking somewhat puzzled. For the next forty minutes, he stood looking at the board, occasionally scratching his head, completely absorbed in his thoughts and ignoring the students, who fidgeted in their chairs and kept making aborted attempts to leave. Finally, just a few minutes before the end of the period, the professor smiled, lifted his head, looked at the class, said, "Yes, it is obvious," and moved on with the proof.

unnecessary, pedantic details, at least not after the first few steps. If the proof is somewhat convoluted, we should not leave it to the reader to untangle the threads of logic but should prepare a description of the main ideas and their relationships before plunging into the technical part. In particular, it is always a good idea to tell the reader if the proof will proceed by construction, by induction, by contradiction, by diagonalization, or by some combination. If the proof still looks tangled in spite of these efforts, we should consider breaking off small portions of it into supporting lemmata; typically, the more technical (and less enlightening) parts of a derivation are bundled in this manner into "technical" lemmata, so as to let the main ideas of the proof stand out. A proof is something that we probably took a long time to construct; thus it is also something that we should take the time to write as clearly and elegantly as possible.

We should note, however, that the result is what really matters: any correct proof at all, no matter how clunky, is welcome when breaking new ground. Many years often have to pass before the result can be proved by elegant and concise means. Perhaps the greatest mathematician, and certainly the greatest discrete mathematician, of the twentieth century, the Hungarian Paul Erdős (1913–1996), used to refer, only half-jokingly, to "The Book," where all great mathematical results—existing and yet to be discovered—are written with their best proofs. His own work is an eloquent testimony to the beauty of simple proofs for deep results: many of his proofs are likely to be found in The Book. As we grope for new results, our first proof rarely attains the clarity and elegance needed for inclusion into that lofty volume. However, history has shown that simple proofs often yield entirely new insights into the result itself and thus lead to new discoveries.

## A.5 Practice

In this section we provide just a few examples of simple proofs to put into practice the precepts listed earlier. We keep the examples to a minimum, since the reader will find that most of the two hundred exercises in the main part of the text also ask for proofs.

**Exercise A.1** *(construction)* Verify the correctness of the formula

$$(1-x)^{-2} = 1 + 2x + 3x^2 + \ldots$$

**Exercise A.2** *(construction)* Prove that, for every natural number $n$, there exists a natural number $m$ with at least $n$ distinct divisors.

**Exercise A.3** *(construction and case analysis)* Verify the correctness of the formula $\min(x, y) + \max(x, y) = x + y$ for any two real numbers $x$ and $y$.

**Exercise A.4** *(contradiction)* Prove that, if $n$ is prime and not equal to 2, then $n$ is odd.

**Exercise A.5** *(contradiction)* Prove that $\sqrt{n}$ is irrational for any natural number $n$ that is not a perfect square.

**Exercise A.6** *(induction)* Prove that, if $n$ is larger than 1, then $n^2$ is larger than $n$.

**Exercise A.7** *(induction)* Verify the correctness of the formula

$$\sum_{i=1}^{n} i = \tfrac{1}{2}n(n+1)$$

**Exercise A.8** *(induction)* Prove that $2^{2n} - 1$ is divisible by 3 for any natural number $n$.

**Exercise A.9** *(induction)* Verify that the $n$th Fibonacci number can be described in closed form by

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

(This exercise requires some patience with algebraic manipulations.)