Chapter 4

Proofs

4.1 What is a proof?

A proof is an argument that convinces someone who is logical, careful and precise. The form and detail of a proof can depend on the audience (for example, whether our audience has as much general math knowledge, and whether we're writing in English or our symbolic form), but the fundamentals are the same whether we're talking mathematics, computer science, physical sciences, philosophy, or writing an essay in literature class. A proof communicates what (and how) someone understands, to save others time and effort. If you don't understand why something is true, don't expect to be able to prove it!
How do you go about writing a proof? Generally, there are two steps or phases to creating a proof:

1. Understanding why something is true.

   This step typically requires some creativity and multiple attempts until an approach works. You should ask yourself why you are convinced something is true, and try to express your thoughts precisely and logically. This step is the most important (and requires the most effort), and can be done in the shower or as you lie awake in bed (the two most productive thinking spots).

   Sometimes we call this finding a proof.

2. Writing up your understanding.

   Be careful and precise. Every statement you write should be true in the context it's written. It is often helpful to use our formal symbolic form, to ensure you're careful and precise. Often you will detect errors in your understanding, and it's common to then go back to step 1 to refine your understanding.

   This is when we are writing up a proof.

Sometimes these steps can be combined, and often these steps feedback on each other. As we try to write up our understanding, we discover a flaw, return to step 1 and refine our understanding, and try writing again.

Students are often surprised that most of the work coming up with a proof is understanding why something is true. If you go back to our definition of what is a proof, this should be obvious: to convince someone, we first need to convince ourselves and order our thoughts precisely and logically. You will see that once we gain a good understanding, proofs nearly write themselves.

Taxonomy of results

A lemma is a small result needed to prove something we really care about. A theorem is the main result that we care about (at the moment). A corollary is an easy (or said to be easy) consequence of another result. A conjecture is something suspected to be true, but not yet proven.[1] An axiom is something we assert to be true, without justification — usually because it is "self-evident."[2]

4.2 DIRECT PROOF OF UNIVERSALLY-QUANTIFIED IMPLICATION

We want to make convincing arguments that a statement is true. We're allowed (forced, actually) to use previously proven statements and axioms. For example, if D is the set of real numbers, then we have plenty of rules about arithmetic and inequalities in our toolbox. From these statements, we want to extend what we know, eventually to include the statement we're trying to prove. Let's examine how we might go about doing this.
Consider an implication we would like to prove that is of the form:

C1: $\forall x \in D, p(x) \Rightarrow q(x)$

Many already-known-to-be-true statements are universally quantified implications, having an identical structure to C1. We'd like to find among them a chain:

C2.0: $\forall x \in D, p(x) \Rightarrow r_1(x)$

C2.1: $\forall x \in D, r_1(x) \Rightarrow r_2(x)$

$\vdots$

C2.N: $\forall x \in D, r_n(x) \Rightarrow q(x)$

This, in n steps, proves C1, using the transitivity of implication.

A more flexible way to summarize that the chain C2.0,...,C2.N proves C1 is to cite the intermediate implications that justify each intermediate step. Here you write the proof that $\forall x \in D, p(x) \Rightarrow q(x)$ as:

Assume $x \in D$. # x is a generic element of D
  Assume $p(x)$. # x has property p, the antecedent
    Then $r_1(x)$. # by C2.0
    Then $r_2(x)$. # by C2.1
      $\vdots$
    Then $q(x)$. # by C2.N
  Then $p(x) \Rightarrow q(x)$. # assuming antecedent leads to consequent
Then $\forall x \in D, p(x) \Rightarrow q(x)$. # we only assumed x is a generic D

This form emphasizes what each existing result adds to our understanding. And when it's obvious which result was used, we can just avoid mentioning it (but be careful, one person's obvious is another's mystery).

Although this form seems to talk about just one particular x, by not assuming anything more than $x \in D$ and $p(x)$, it applies to every $x \in D$ with $p(x)$.

The indentation shows the scope of our assumptions. When we assume that $x \in D$, we are in the "world" where x is a generic element of D. Where we assume $p(x)$, we are in the "world" where $p(x)$ is assumed true, and we can use that to derive consequences.

4.3 HUNTING THE ELUSIVE DIRECT PROOF

In general, the difficulty with direct proof is there are lots of known results to consider. The fact that a result is true may not help your particular line of argument (there are many, many, many true but irrelevant facts). In practice, to find a chain from $p(x)$ to $q(x)$, you gather two lists of results about x:

1. results that $p(x)$ implies, and
2. results that imply $q(x)$

Your fervent hope is that some result appears on both lists, since then you'll have a chain.

$p(x)$
$r_1(x)$
$r_2(x)$
$\vdots$
$s_2(x)$
$s_1(x)$
$q(x)$

Anything that one of the r_i implies can be added to the first list. Anything that implies one of the s_i can be added to the second list.

What does this look like in pictures? In Venn diagrams we can think of the r_i as sets that contain p and may, or may not, be contained in q (the ones that aren't contained in q are dead ends). On the other hand, the s_i are contained in q and may, or may not, contain p (the ones that don't are dead ends). We hope to find a patch of containment from p to q. Another way to visualize this is by having the r_i represented as a tree. In one tree we have root p, with children being the r_i that p implies, and their children being results they imply. In a second tree we have root q, with children being the results that imply q, and their children being results that imply them. If the two trees have a common node, we have a chain.

Are you done when you find a chain? No, you write it up, tidying as you go. Remove the results that don't contribute to the final chain, and cite the results that take you to each intermediate link in the chain.

What do $\wedge$ and $\vee$ do?

Now your two lists have the form

$\forall x \in D, p(x) \Rightarrow (r_1(x) \wedge r_2(x) \wedge \cdots \wedge r_m(x))$
$\forall x \in D, (s_k(x) \vee \cdots \vee s_1(x)) \Rightarrow q(x)$

Since $p(x)$ implies any "and" of the r_i, you can just collect them in your head until you find a known result, say $r_1(x) \wedge r_2(x) \Rightarrow r_k(x)$, and then add $r_k(x)$ to the list. On the other hand, if you have a result on the first list of the form $r_1(x) \wedge r_2(x)$, you can add them separately to the list. On the second list, use the same approach but substitute $\vee$ for $\wedge$. Any result on the first list can be spuriously "or'ed" with anything: $r_1(x) \Rightarrow (r_1(x) \vee l(x))$ is always true. On the second list, we can spuriously "and" anything, since $(s_1(x) \wedge l(x)) \Rightarrow s_1(x)$.

If we have a disjunction $r_1(x) \vee r_2(x)$ on the first list, we can use it if we have a result that $(r_1(x) \vee r_2(x)) \Rightarrow q(x)$, or the pair of results $r_1(x) \Rightarrow q(x)$, and $r_2(x) \Rightarrow q(x)$.

4.4 An odd example of direct proof

Suppose you are asked to prove that every odd natural number has a square that is odd. Typically we don't see all the links in the chain from "n is odd" to "n^2 is odd" instantly, so we engage in thoughtful wishing (like wishful thinking, only with a much better reputation). We start by writing the outline of the proof we would like to have, to clarify what information we've got, what we lack, and hope to fill in the gaps:

Assume $n \in \mathbb{N}$.
  Assume n is odd.
    $\vdots$
    Then n^2 is odd.
  Then n is odd $\Rightarrow n^2$ is odd.
Then $\forall n \in \mathbb{N}, n$ is odd $\Rightarrow n^2$ is odd.

Start scratching away at both ends of the $\vdots$ (the bit that represents the chain of results we need to fill in). What does it mean for n^2 to be odd? Well, if there is a natural number k such that $n^2 = 2k + 1$, then n^2 is odd (by definition of odd numbers). Add that to the end of the list. Similarly, if n is odd, then there is a natural number j such that $n = 2j + 1$ (by definition of odd numbers). It seem unpromising to take the square root of $2k+1$, so instead carry out the almost-automatic squaring of $2j + 1$. Now, on our first list, we have that, for some natural number j, $n^2 = 4j^2+4j+1$. Using some algebra (distributivity of multiplication over addition), this means that for some natural number j, $n^2 = 2(2j^2 + 2j) + 1$. If we let k from our second list be $2j^2 + 2j$, then we certainly satisfy the restriction that k be a natural number (they are closed under multiplication and addition), and we have linked the first list to the second. Here's an example of how to format your finished chain:

Assume $n \in \mathbb{N}$. # n is a generic natural number
  Assume n is odd. # n a typical odd natural number
    Then, $\exists j' \in \mathbb{N}$, $n = 2j' + 1$. # by definition of n odd
    Let $j \in \mathbb{N}$ be such that $n = 2j + 1$. # name it j
    Then $n^2 = 4j^2 + 4j + 1 = 2(2j^2 + 2j) + 1$. # definition of n^2 and some algebra
    Then $\exists k \in \mathbb{N}, n^2 = 2k + 1$. # $2j^2 + 2j \in \mathbb{N}$, since $\mathbb{N}$ closed under $+, \times$
    Then n^2 is odd. # by definition of n^2 odd
  Then n is odd $\Rightarrow n^2$ is odd. # when I assumed n odd, I derived n^2 odd
Then $\forall n \in \mathbb{N}$, n odd $\Rightarrow$ n^2 odd. # since n was a generic natural number

How about the converse, $\forall n \in \mathbb{N}$, if n^2 is odd, then n is odd. If we try creating a chain, it seems a bit as though the natural direction is wrong: somehow we'd like to go from q back to p. What equivalent of an implication allows us to do this?[3] You set up the proof of the contrapositive of the converse (whew!) very similarly to the proof above, mostly changing "odd" to "even." Try it out.

4.5 Another example of direct proof

Let $\mathbb{R}$ be the set of real numbers. Prove:

$\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x + 2) < 3$

Structure the proof as before:

Assume $x \in \mathbb{R}$. # x is a typical real number
  Assume $x > 0$. # antecedent
    $\vdots$ # prove $1/(x + 2) < 3$
    Then $1/(x + 2) < 3$. # get here somehow
  Then $x > 0 \Rightarrow 1/(x + 2) < 3$. # assume antecedent, derived consequent
Then $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x + 2) < 3$. # only assume x was a typical element of $\mathbb{R}$

Of course, you need to unwrap the sub-proof that $1/(x + 2) < 3$:

Assume $x \in \mathbb{R}$. # x is a typical element of $\mathbb{R}$
  Assume $x > 0$. # antecedent
    Then $x + 2 > 2$. # $x > 0$, add 2 to both sides
    Then $1/(x + 2) < 1/2$. # reciprocals reverse inequality, and are defined for numbers > 2
    Then $1/(x + 2) < 3$. # since $1/(x + 2) < 1/2$ and $1/2 < 3$
  Then $x > 0 \Rightarrow 1/(x + 2) < 3$. # assumed antecedent, derived consequent
Then $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x + 2) < 3$. # x was assumed to be a typical element of $\mathbb{R}$

Is the converse true (what is the converse)?[4]

4.6 Direct proof of universally-quantified predicate

When no implication is stated, then we don't assume (suppose) anything about x other than membership in the domain. For example, $\forall x \in D, p(x)$ has this proof structure:

Assume $x \in D$.
  $\vdots$ # prove $p(x)$
Then $p(x)$.
Then $\forall x \in D, p(x)$. # x was assumed to be a typical element of D

4.7 Indirect proof of universally-quantified implication

Recall that $p \Rightarrow q$ is equivalent to its contrapositive, $\neg q \Rightarrow \neg p$. This means that proving one proves the other. This is called an "indirect proof." The outline format of an indirect proof of $\forall x \in D, p(x) \Rightarrow q(x)$ is

Assume $x \in D$. # x is a typical element of D
  Assume $\neg q(x)$. # negation of the CONSEQUENT!
    $\vdots$
    Then $\neg p(x)$. # negation of the ANTECEDENT!
  Then $\neg q(x) \Rightarrow \neg p(x)$. # assuming $\neg q(x)$ leads to $\neg p(x)$
  Then $p(x) \Rightarrow q(x)$. # implication is equivalent to contrapositive
Then $\forall x \in D, p(x) \Rightarrow q(x)$. # assume x was a typical element of D

This is a useful approach, for example, in proving that $\forall n \in \mathbb{N}, n^2$ is odd $\Rightarrow n$ is odd.

4.8 Proof by contradiction

Sometimes you want to prove a conclusion, Q, without any suitable hypothesis, P to imply it. One approach is to say "if everything we already know is true is assumed, then Q follows." How do you choose which particular portion of "everything we already know is true" to focus on? Let logic help focus your argument.

Symbolically you can represent "everything we already know is true" as a huge conjunction of statements, $P = P_1 \wedge P_2 \wedge \cdots \wedge P_m$. So now we aim to prove $P \Rightarrow Q$ using the CONTRAPOSITIVE: $\neg Q \Rightarrow \neg P$. Start by assuming that Q is FALSE, and then show that something you already know to be true must be false — a contradiction! Since $P = P_1 \wedge P_2 \wedge \cdots \wedge P_m$ is a huge conjunction of statements, its negation is a huge disjunction $\neg P = \neg P_1 \vee \neg P_2 \vee \cdots \vee \neg P_m$, so you don't need to know in advance which of them is contradicted. You just follow your (educated) nose. Here's the general format:

Assume $\neg Q$. # in order to derive a contradiction
  $\vdots$ # some steps leading to a contradiction, say $\neg P_j$
  Then $\neg P$. # contradiction, since P is known to be true
Then Q. # since assuming $\neg Q$ leads to contradiction

Euclid used this technique over 2,000 years ago to prove that there are infinitely many prime numbers. Before looking at Euclid's proof, you might experiment with proving this fact directly.
Let's start by naming some of the sets/predicates we'll need for this proof:

- $P = \{p \in \mathbb{N} : p \text{ has exactly two factors}\}$
- SP: $\forall n \in \mathbb{N}, |P| > n$

In spite of appearances, SP is not a good candidate for mathematical induction (which we'll see later in this course). However, let's try $\neg$SP:

Assume $\neg$SP: $\exists n \in \mathbb{N}, |P| \leqslant n$. # to derive a contradiction
  Then there is a finite list, $p_1, \ldots, p_k$ of elements of P. # at most n elements in the list
  Then I can take the product $p' = p_1 \times \cdots \times p_k$. # finite products are well-defined
  Then p' is the product of some natural numbers 2 and greater. # 0, 1 aren't primes, 2, 3 are
  Then $p' > 1$. # p' is at least 6
  Then $p' + 1 > 2$. # add 1 to both sides
  Then $\exists p \in P, p$ divides $p' + 1$. # by math prerequisites sheet, since $p' + 1 > 2$
  Let $p_0 \in P$ be such that p_0 divides $p' + 1$. # instantiate existential
  Then p_0 is one of $p_1, \ldots, p_k$. # by assumption, the only primes
  Then p_0 divides $p' + 1 - p' = 1$. # a divisor of each term divides difference
  Then $1 \in P$. Contradiction! # 1 is not prime
Then SP. # "assume $\neg$SP" leads to a contradiction

4.9 Direct proof structure of the existential

Consider the example $\exists x \in \mathbb{R}, x^3 + 2x^2 + 3x + 4 = 2$. Since this is the existential, we need only find a single example to show that the statement is true. We structure the proof as follows:

Let $x = -1$. # choose a particular element that will work
Then $x \in \mathbb{R}$. # verify that the element is in the domain
Then $x^3 + 2x^2 + 3x + 4 = (-1)^3 + 2(-1)^2 + 3(-1) + 4 = -1 + 2 - 3 + 4 = 2$. # substitute -1 for x
Then $\exists x \in \mathbb{R}$, $x^3 + 2x^2 + 3x + 4 = 2$. # we gave an example

The general form for a direct proof of $\exists x \in D, p(x)$ is:

Let $x = \ldots$ # choose a particular element of the domain
Then $x \in D$. # this may be obvious, otherwise prove it
  $\vdots$ # prove $p(x)$
Then $p(x)$. # you've shown that x satisfies p
$\exists x \in D, p(x)$. # introduce existential

4.10 Multiple quantifiers, implications, and conjunctions

Consider $\forall x \in D, \exists y \in D, p(x, y)$. The corresponding proof structure is:

Assume $x \in D$. # typical element of D
  Let $y_x = \ldots$ # choose an element that works
    $\vdots$
  Then $y_x \in D$. # verify that $y \in D$
    $\vdots$
  Then $p(x, y_x)$. # y satisfies $p(x, y)$
  Then $\exists y, p(x, y)$. # introduce existential
Then $\forall x \in D, \exists y \in D, p(x, y)$. # introduce universal

Here's a concrete example. Suppose we have a mystery function f, mystery constants a and l, and the following statement (I have added parentheses to indicate the conventional parsing):

$$\forall e \in \mathbb{R},\, e > 0 \Rightarrow (\exists d \in \mathbb{R}, d > 0 \wedge (\forall x \in \mathbb{R},\, 0 < |x - a| < d \Rightarrow |f(x) - l| < e))$$

If we want to prove this TRUE, structure the proof as follows...[5]

If we want to prove the statement FALSE, we first negate it, and then use one of our proof formats (I use the equivalences $\neg(p \Rightarrow q) \Leftrightarrow (p \wedge \neg q)$ and $\neg(p \wedge q) \Leftrightarrow (p \Rightarrow \neg q)$):

$$\exists e \in \mathbb{R},\, e > 0 \wedge \forall d \in \mathbb{R},\, d > 0 \Rightarrow \exists x \in \mathbb{R},\, 0 < |x - a| < d \wedge |f(x) - l| \geqslant e$$

Of course, this negation involved several applications of rules we already know, and now its proof may be written step-by-step. Notice that, in the middle of our proof, we had a "$\wedge$" to prove.

4.11 EXAMPLE OF PROVING A STATEMENT ABOUT A SEQUENCE

Consider the statement:

CLAIM 4.1: $\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leqslant i \Rightarrow j < i$

and the sequence:

(A1) $0, 1, 4, 9, 16, 25, \ldots$

We'll use the convention that sequences are indexed by natural numbers (recall that $\mathbb{N} = \{0, 1, 2, \ldots\}$, starting at zero just as computers count) and a_i is the element of the sequence indexed by i, so $a_0 = 0$, $a_1 = 1$, $a_2 = 4$. Looking at the pattern of (A1), we can write a "closed form" formula for a_i.[6]

We should of course try to understand 4.1, by putting it in natural English, picturing tables and diagrams, thinking of code that could check it, trying it on various examples, *etc.* To understand whether it is true or false for (A1) we should use this understanding, including tracing it. But let's focus on the form that a proof that 4.1 is true could take. This may even help us understand 4.1.
We have been justifying existentials with an example. So, our proof should start off something like:

Let $i =$ ____. Then $i \in \mathbb{N}$.
⋮

We leave ourselves a blank to fill in: a specific value of i. We also need to make sure the i is in $\mathbb{N}$. Often it will be obvious and we will simply note it. If not, we'll actually need to put in a proof.

Next, we need to prove something for all j in $\mathbb{N}$. As a syntactic convenience, we prove something for all j's in $\mathbb{N}$ by proving it for some *unknown* j in $\mathbb{N}$. If we're careful to not assume anything about which j we have, our proof will handle all j's.

Let $i =$ __. Then $i \in \mathbb{N}$. # choose a helpful one
Assume $j \in \mathbb{N}$. # j is a typical element of $\mathbb{N}$
⋮

Notice this time we *assume* j is in $\mathbb{N}$. You can imagine $\exists$ and $\forall$ as part of a game:

- $\exists x \in D$: We get to pick x, but have to follow the rules and pick from D.
- $\forall x \in D$: Our opponent will pick x, but we can assume they will follow the rules and pick from D. We can't make any assumptions here about which one from D they will pick.

Going back to our proof structure, we have:

Let $i =$ __. Then $i \in \mathbb{N}$.
Assume $j \in \mathbb{N}$. # typical element of $\mathbb{N}$
  Assume $a_j \leqslant i$.
    ⋮
  Then $j < i$.

We leave ourselves room (the $\vdots$) for a proof of $j < i$. Once we fill in a value of i, the proof of $j < i$ may use three facts: the value we chose for i, $j \in \mathbb{N}$, and $a_j \leqslant i$.

After a little thought, we decide that setting $i = 2$ is a good idea, since then $a_j \leqslant i$ is only true for $j = 0$ and $j = 1$, and these are smaller than 2. A bit of experimentation shows that the contrapositive, $\neg(j < i) \Rightarrow \neg(a_j \leqslant a_i)$ is a bit easier to work with.

Let $i = 2$. Then $i \in \mathbb{N}$. # $2 \in \mathbb{N}$
Assume $j \in \mathbb{N}$. # typical element of $\mathbb{N}$
  Assume $\neg(j < i)$. # antecedent for contrapositive
    Then $j \geqslant 2$. # negation of $j < i$ when $i = 2$
    Then $a_j = j^2 \geqslant 2^2 = 4$. # since $a_j = j^2$, and $j \geqslant 2$
    Then $a_j > 2$. # since $4 > 2$
  Then $\neg(j < i) \Rightarrow \neg(a_j \leqslant 2)$. # assuming antecedent leads to consequent
  Then $a_j \leqslant 2 \Rightarrow j < i$. # implication equivalent to contrapositive
Then $\forall j \in \mathbb{N}, a_j \leqslant i \Rightarrow j < i$. # introduce universal
Then $\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leqslant i \Rightarrow j < i$. # introduce existential

4.12 EXAMPLE OF DISPROVING A STATEMENT ABOUT A SEQUENCE

Consider now the statement:

CLAIM 4.2: $\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, j > i \Rightarrow a_j = a_i$

and the sequence:

(A2) $0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, 6, \ldots$

Let's disprove it. Is disproof a whole new topic? Thankfully no. We simply prove the negation:

CLAIM 4.2′: $\forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$

As usual, we sketch in the outline of the proof first:

Assume $i \in \mathbb{N}$.
  Let $j =$ ____. Then $j \in \mathbb{N}$.
    $\vdots$
  Then $j > i \wedge a_j \neq a_i$.
  Then $\exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$. # introduction of existential
Then $\forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$. # introduction of universal

Our opponent picks i, but we get to pick j. And we are allowed to make j depend on i. Unfortunately, while writing up the proof we can't wait for someone to actually pick i. So how does it help us? We get to describe a general strategy for how we would pick a particular j if we knew which particular i. In other words, j can be described as function of i.

In programming terms, i is in scope when we pick j: it has been declared and can be seen from where we declare j. Notice that j is not in scope when we declare i: so when we picked i for 4.1, we weren't allowed to use j. If we write a program that uses a variable before it's declared and initialized, the program doesn't even compile. This is a major error. If you write a proof that does this, it will almost certainly be wrong — and you will most likely lose a lot of marks!

Now we are left with proving $j > i \wedge a_j \neq a_i$ (notice we wrote this at the bottom... we must have been thinking ahead). What form does the proof of a conjunction take?[7]

Assume $i \in \mathbb{N}$.
  Let $j =$ ____. Then $j \in \mathbb{N}$.
    ⋮
  Then $j > i$.
    ⋮
  Then $a_j \neq a_i$.
  Then $j > i \wedge a_j \neq a_i$.
  Then $\exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$.
Then $\forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$.

To finish this off, we need to choose a value for j. If we choose wisely, the rest of the proof falls into place.[8] What elementary property of arithmetic will we require?[9]

4.13 Non-boolean function example

Non-boolean functions cannot take the place of predicates (since predicates are expected to return a true or false value) in a proof. How should non-boolean functions be used? Define $\lfloor x \rfloor : \mathbb{R} \to \mathbb{R}$ by:

$\lfloor x \rfloor$ ("floor of x") is the largest integer $\leqslant x$.

Now we can form the statement:

Claim 4.3: $\forall x \in \mathbb{R}, \lfloor x \rfloor < x + 1$

It makes sense to apply $\lfloor x \rfloor$ to elements of our domain, or variables that we have introduced, and to evaluate it in predicates such as "$<$" but $\lfloor x \rfloor$ itself is not a variable, nor a sentence, nor a predicate. We can't (sensibly) say things such as $\forall \lfloor x \rfloor \in \mathbb{R}$ or $\forall x \in \mathbb{R}, \lfloor x \rfloor \vee \lfloor x + 1 \rfloor$. The structure of 4.3 is a direct proof of a universally-quantified predicate:[10]

Assume $x \in \mathbb{R}$. # x is a typical element of $\mathbb{R}$
  Let $y = \lfloor x \rfloor$. # introduce a variable
  Then y is the largest integer $\leqslant x$, so $y \leqslant x$. # definition of floor
  Since $x < x + 1$, $y < x + 1$. # transitivity of $<$
  So $\lfloor x \rfloor < x + 1$. # since $y = \lfloor x \rfloor$
Then $\forall x \in \mathbb{R}, \lfloor x \rfloor < x + 1$. # since x was a typical element of $\mathbb{R}$

In some cases you need to break down a statement such as "y is the largest integer $\leqslant x$":

$$y \in \mathbb{Z} \wedge y \leqslant x \wedge (\forall z \in \mathbb{Z}, z \leqslant x \Rightarrow z \leqslant y)$$

We didn't need all three parts of the definition for our proof above, and in practice we don't always have to return to definitions when dealing with functions. For example, we may have an existing result, such as:

$$\forall x \in \mathbb{R}, \lfloor x \rfloor > x - 1$$

How would you prove this result, using the three-part version of the definition of $\lfloor x \rfloor$?

4.14 Substituting known results

Every proof would become unmanageably long if we had to include "inline" all the results that it depended on. We inevitably refer to standard results that are either universally known (among math wonks) or can easily be looked up. Sometimes we need to prove a small technical result in order to prove something larger. You may view the smaller result as a helper method (usually returning boolean results) that you use to build a larger method (your bigger proof). To make things modular, you should be able to "call" or refer to the smaller result. An example occurs if we want to re-cycle something proved earlier:

THEOREM 1: $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x+2) < 3$.

We want to use this in proving $\forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2+2) < 3$. The template to fill in is

Assume $y \in \mathbb{R}$.
  Assume $y \neq 0$.
    $\vdots$
    Then $1/(y^2+2) < 3$.
  Then $y \neq 0 \Rightarrow 1/(y^2+2) < 3$.
Then $\forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2+2) < 3$.

Now we have to fill in the $\vdots$ part:

Assume $y \in \mathbb{R}$. # y is a typical element of $\mathbb{R}$
  Assume $y \neq 0$. # y positive
    Then $y^2 \in \mathbb{R}$ and $y^2 \geqslant 0$. # $\mathbb{R}$ closed under $\times$, squares of non-zero reals
    Then $y^2 > 0$, since $y^2 \neq 0$ and $y^2 \geqslant 0$. # only real number whose square is 0 is 0
    Then $1/(y^2+2) < 3$. # by Theorem 1
  Then $y \neq 0 \Rightarrow 1/(y^2+2) < 3$. # introduction of $\Rightarrow$
Then $\forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2+2) < 3$. # introduction of universal

4.15 PROOF BY CASES

To prove $A \Rightarrow B$, it can help to treat some A's differently than others. For example, to prove that $x^2 + x$ is even for all integers x, you might proceed by noting that $x^2 + x$ is equivalent to $x(x+1)$. At this point our reasoning has to branch: at least one of the factors x or $x+1$ is even (for integer x), but we can't assume that a particular factor is even for every integer x. So we use proof by cases.[11]

This is a special case of an "or" clause being the antecedent of an implication, *i.e.*, if you want to prove $(A_1 \vee A_2 \vee \cdots \vee A_n) \Rightarrow B$. This could happen if, along the way to proving $A \Rightarrow B$ you use the fact that $A \Rightarrow (A_1 \vee \cdots \vee A_n)$. Now you need to prove $A_1 \Rightarrow B$, $A_2 \Rightarrow B, \ldots, A_n \Rightarrow B$. Notice that in setting this up it is not necessary that the A_i be disjoint (mutually exclusive), just that they cover A (think of A being a subset of the union of the A_i). One way to generate the cases is to break up the domain $D = D_1 \cup \cdots \cup D_n$, so A_i is the predicate that corresponds to the set $D_i \cap A$. Now you have an equivalence, $A \Leftrightarrow A_1 \vee \cdots \vee A_n$. A very common case occurs when the domain partitions into two parts, $D = D_1 \cup \overline{D_1}$, so you can rewrite A as $(A \wedge D_1) \vee (A \wedge \neg D_1)$ — we're abusing the notation slightly here by treating D_1 both as a set and as a predicate, as we've done before.

Here's the general form of proving something by cases:

$A \vee B$
Case 1: Assume A.
  $\vdots$
  Then C.
Case 2: Assume B.
  $\vdots$
  Then C.
Since $A \vee B$ and in both (all) cases we concluded C, then C.

Remember that we need one case for each disjunct, so if we knew $A_1 \vee \cdots \vee A_n$, we'd need n cases.

When you're reading (or writing) proofs, often the word "assume" is omitted when defining the case. Though it might say "Case $x < k$," remember that $x < k$ is an assumption, thus opens a new indentation (scope) level.

Law of the excluded middle

Often we want to proceed by cases, but don't have a disjunction handy to use. We can always introduce one using the Law of the Excluded Middle. This law of logic states that a formula is either TRUE or FALSE—there's nothing between (or "in the middle"). Thus, for any formula P, the following is sure to be true:

$$P \vee \neg P$$

In your proof, you can then split into two cases depending on whether P is true or false. Just be sure to negate P correctly!

Example proof using cases

Suppose we wanted to prove the following statement: if n is an integer then $n^2 + n$ is even.
Let's formalize what we mean by the term "integer n is even":

For $n \in \mathbb{Z}$, let even(n) mean $\exists k \in \mathbb{Z}, n = 2k$.

Let's formalize what we're proving:

Claim 4.4: $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

Noticing that $n^2 + n = n(n+1)$, we consider whether n is odd or even. We know that every integer is either odd or even, so let's state this formally:

(*) $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.

Now to the proof of our claim. In it we will know that an existential is true, and we will want to use that knowledge. We may ask the existential to "return" an example element, which we get to name and use (we name it k_0 so that it won't conflict with any other elements we're talking about).

Assume $n \in \mathbb{Z}$. # n is a typical natural number
  Then $(\exists k \in \mathbb{Z}, n = 2k+1) \vee (\exists k \in \mathbb{Z}, n = 2k)$. # by (*), $n \in \mathbb{Z}$
  Case 1: Assume $\exists k \in \mathbb{Z}, n = 2k+1$.
    Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$. # instantiate existential
    Then $n^2 + n = n(n+1) = (2k_0+1)(2k_0+2) = 2(2k_0+1)(k_0+1)$.
    Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # $k = (2k_0+1)(k_0+1) \in \mathbb{Z}$
  Case 2: Assume $\exists k \in \mathbb{Z}, n = 2k$.
    Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0$. # instantiate existential
    Then $n^2 + n = n(n+1) = 2k_0(2k_0+1) = 2[k_0(2k_0+1)]$.
    Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # $k = k_0(2k_0+1) \in \mathbb{Z}$
  Then $\exists k \in \mathbb{Z}, n^2 + n = 2k$. # true in all (both) possible cases
Then $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$. # introduction of universal

4.16 Proving $\vee$ using cases

Let's prove that the square of an integer is a triple or one more than a triple.

Claim 4.5: $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k+1)$.

If we know $P \vee Q$, we can prove a disjunction $R \vee S$ by cases, as follows:

$P \vee Q$
Case 1: Assume P.
  ⋮
  Then R.

Case 2: Assume Q.
$\vdots$
Then S.
Thus $R \vee S$.[12]

If we already have some $P \vee Q$ we can use, then those are the obvious cases to consider, though we still have to decide between the two ways of pairing them up with R and S. In general though, picking P and Q that work depends completely on context. When constructing proof structures, a standard strategy is to use $\neg P$ for Q: the Law of the Excluded Middle ensures this is true, and it is the simplest yet still general structure.

This of course generalizes to more than two cases: if we know $P_1 \vee P_2 \vee \cdots \vee P_n$, and we want to prove $Q_1 \vee \cdots \vee Q_m$, then we can do cases for each P_i, in each case proving a Q_j. We don't have to prove all the Q_j, and we can prove some of them in more than one case.
To prove our claim, we want to use part of the Remainder Theorem:

(*) $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n = 3k \vee n = 3k+1 \vee n = 3k+2)$

We now proceed with our proof of the claim by cases. One case is left for you to do as an exercise.

Assume $n \in \mathbb{N}$. # n is a typical element of $\mathbb{N}$
Then $\exists k \in \mathbb{N}, n = 3k \vee n = 3k+1 \vee n = 3k+2$. # by (*)
Let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \vee n = 3k_0 + 1 \vee n = 3k_0 + 2$.
Case 1: Assume $n = 3k_0$.
Then $3(3k_0^2) = 9k_0^2 = n^2$. # algebra
Then $\exists k \in \mathbb{N}, n^2 = 3k$. # $k = 3k_0^2 \in \mathbb{N}$
Case 2: Assume $n = 3k_0 + 1$.
Then $3(3k_0^2 + 2k_0) + 1 = 9k_0^2 + 6k + 1 = n^2$. # algebra
Then $\exists k \in \mathbb{N}, n^2 = 3k + 1$. # $k = 3k_0^2 + 2k_0 \in \mathbb{N}$
Case 3: Assume $n = 3k_0 + 2$.
(Exercise.)
Then $(\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k+1)$. # true in all possible cases
Then $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k+1)$. # introduction of universal

4.17 Building formulae and taking formulae apart

So far we've been concentrating on proving more and more complicated sentences. This makes sense, since the sentence we've proving determines the structure our proof will take. For each of the logical connectives and quantifiers, we've seen structures that allow us to conclude big statements from smaller ones. The inference rules that allow us to do this are collectively called INTRODUCTION RULES, since they allow us to introduce new sentences of a particular type.

But rarely do we prove things directly from predicates. We often have to use known theorems and results or separately proven lemmas to reduce the length of our proofs to a manageable size (can you imagine always having to prove $2 + 2 = 4$ from primitive sets each time you use this fact?). Good theorems are useful in a number of settings, and typically use a number of connectives and quantifiers. Knowing how to break complex sentences down is equally important as knowing how to build complex sentences up.

Just as there are inference rules allowing us to introduce new, complex sentences, there are inference rules allowing us to break sentences down in a formal, precise and valid way. These rules are collectively called ELIMINATION RULES, since they allow us to eliminate connectives and quantifiers we don't want anymore. Most rules should be fairly straight-forward and should make sense to you at this point; if not, you should review your manipulation rules.

Double negation elimination

We can't do much to remove one negation (unless we can move it further inside), but we know how to get rid of two negations. Indeed, this was a manipulation rule from the previous chapter, but we can also treat it as a reasoning rule: if we know $\neg\neg A$ is true, we know A is true.

Conjunction elimination

Nearly as easy as negation, how can we break up a conjunction? If we know $A \wedge B$, what can we conclude?[13]

Existential elimination (or instantiation)

We might know that $\exists x \in D, B$, where B likely mentions x somewhere inside. In other words, we know B is true for some element in D, but we don't know which one. How can we proceed? We'd probably like to say something about that element in D that B is true for, but how do we know which element it is?

We don't really need to know which element B is true for, only that it exists. We can proceed by using B with every reference to x replaced by a new variable x' (just notation to distinguish it from x).

Disjunction elimination

$A \vee B$ itself cannot be split, as we don't know which part of the disjunction is true. However, if we also know $\neg A$, we can conclude B must be true. Analogously, with $\neg B$ we can conclude A.

Another good way to deal with a disjunction is proof by cases, which we discussed above.

Implication elimination

Suppose we know $A \Rightarrow B$. If we are able to show A is true, then we could immediately conclude B. This is perhaps the most basic reasoning structure, and has a fancy latin name: *modus ponens* (meaning "mode that affirms"). This form is the basis to deductive argument (you can imagine Sherlock Holmes using modus ponens to reveal the criminal).

On the other hand, if we knew $\neg B$, we could still get something from $A \Rightarrow B$: we'd be able to conclude $\neg A$. This form of reasoning is using the contrapositive and is known as *modus tollens* (Latin for "mode that denies").

We can also appeal to the manipulation rules to rewrite $A \Rightarrow B$ as a disjunction, $\neg A \vee B$, and expand this formula as desired.

Bi-implication elimination

To take apart a sentence like $A \Leftrightarrow B$, we simply exploit its equivalence to $(A \Rightarrow B) \wedge (B \Rightarrow A)$ and expand it appropriately.

If we also know A, we can skip some work and directly conclude that B must be true (using the implication $A \Rightarrow B$ hidden in the bi-implication). Likewise, if we also knew $\neg A$, we could conclude $\neg B$. Each of these properties are easily proven using preceding rules.

Universal elimination (or instantiation)

Suppose you know that $\forall x \in D, B(x)$. How can we use this fact to help prove other things? This sentence says $B(x)$ is true for all members of domain D. So we could use this as meaning a huge conjunction over all the elements of $D = \{d_1, d_2, d_3, \ldots\}$:

$$B(d_1) \wedge B(d_2) \wedge B(d_3) \wedge \ldots$$

From this expansion (even if we can't write it[14]) it's clear that if $a \in D$, we can conclude that $B(a)$ is true. This is sometimes called universal instantiation, or universal specialization, since we're allowed to conclude a specialized statement from our general statement. Intuitively, what holds for everything must hold for any specific thing. Typically, a will have been mentioned already, and you'll want to express that a has some specific property (in this case, $B(a)$).

4.18 Summary of inference rules

There are several basic and derived rules we're allowed to use in our proofs. Many of them are summarized below. For each rule, if you know (have already shown) everything that is above the line, you are allowed to conclude anything that's below the line.

Introduction rules

[$\neg$I] negation introduction

Assume A
$\vdots$
contradiction

$\neg A$

[$\wedge$I] conjunction introduction

A
B

$A \wedge B$

[$\vee$I] disjunction introduction

A

$A \vee B$
$B \vee A$

$A \vee \neg A$

[$\Rightarrow$I] implication introduction

(direct)

Assume A
$\vdots$
B

$A \Rightarrow B$

(indirect)

Assume $\neg B$
$\vdots$
$\neg A$

$A \Rightarrow B$

[$\Leftrightarrow$I] equivalence/bi-implication introduction

$A \Rightarrow B$
$B \Rightarrow A$

$A \Leftrightarrow B$

[$\forall$I] universal introduction

Assume $a \in D$
$\vdots$
$P(a)$

$\forall x \in D, P(x)$

[$\exists$I] existential introduction

$P(a)$
$a \in D$

$\exists x \in D, P(x)$

Elimination rules

[$\neg$E] negation elimination

$\neg\neg A$

A

A
$\neg A$
---
contradiction

[$\wedge$E] conjunction elimination

$A \wedge B$

A
B

[$\vee$E] disjunction elimination

$A \vee B$
$\neg A$

B

$A \vee B$
$\neg B$

A

[$\Rightarrow$E] implication elimination

(Modus Ponens)

$A \Rightarrow B$
A

B

(Modus Tollens)

$A \Rightarrow B$
$\neg B$

$\neg A$

[$\Leftrightarrow$E] equivalence/bi-implication elimination

$A \Leftrightarrow B$

$A \Rightarrow B$
$B \Rightarrow A$

[$\forall$E] universal elimination

$\forall x \in D, P(x)$
$a \in D$

$P(a)$

[$\exists$E] existential elimination

$\exists x \in D, P(x)$

Let $a \in D$ such that $P(a)$
$\vdots$

It may surprise you to learn that by this point, we've covered all of the basic proof techniques you will need during your undergraduate career (and beyond). There is one basic proof technique that we have yet to

cover (mathematical induction) but it is more properly the main subject of the course CSC 236 H. (Though we will discuss it a little bit in the next chapter.)

Given this, you may feel that the proofs we've worked on so far have been nowhere near as complicated as what you might find in your calculus textbook, for example. But if you take the time to examine the structure of any such proof, you will most likely find that all of the techniques it uses were covered in this chapter. The complexity of these proofs stem, not from using more complex techniques, but from their scale and their reliance on numerous other results and complex definitions.

This is no different from the contrast between small programs and large ones: both are written using the same programming language, which provides just a small set of "building blocks" — conditionals, loops, functions, *etc.* The complexity of larger programs stems mainly from their size and/or their reliance on numerous external libraries.

Bearing this in mind, you now have all of the tools required to understand and appreciate some of the deepest and most beautiful results in the theory of computation (see Chapter 6). But first, in the next chapter, we'll apply those tools to something more concrete: the analysis of algorithms.

Chapter 4 Notes

[1]Here's an example of a conjecture whose proof has evaded the best minds for over 70 years — maybe you'll prove it?
Define $f(n)$, for $n \in \mathbb{N}$ by:

$$f(n) = \begin{cases} n/2, & n \text{ even} \\ 3n+1, & n \text{ odd} \end{cases}$$

Let's define $f^2(n)$ as $f(f(n))$, and more generally, $f^{k+1}(n)$ as $f(f^k(n))$ for all $k \in \mathbb{N}$ (with the special case $f^0(n) = n$). Here's the

Conjecture: $\forall n \in \mathbb{N}, n \geqslant 1 \Rightarrow \exists k \in \mathbb{N}, f^k(n) = 1$.

Easy to state, but (so far) hard to prove or disprove.

[2]For example, "for any two points on the plane, there is exactly one line that passes through both points" is an axiom in Euclidian geometry.

[3]The contrapositive.

[4]$\forall x \in \mathbb{R}$, $1/(x+2) < 3 \Rightarrow x > 0$. False, for example let $x = -4$, then $1/(-4+2) = -1/2 < 3$ but $-4 \not> 0$. Indeed, every $x < -2$ is a counter-example.

[5]
Assume $e \in \mathbb{R}$. # typical element of $\mathbb{R}$
  Assume $e > 0$. # antecedent
    Let $d_e = \ldots$ # something helpful, probably depending on e
    Then $d_e \in \mathbb{R}$. # verify d_e is in the domain
    Then $d_e > 0$. # show d_e is positive
    Assume $x \in \mathbb{R}$. # typical element of $\mathbb{R}$
      Assume $0 < |x - a| < d_e$. # antecedent
        $\vdots$
      Then $|f(x) - l| < e$. # inner consequent
    Then $0 < |x - a| < d_e \Rightarrow (|f(x) - l| < e)$. # introduce implication

Then $\forall x \in \mathbb{R}$, $0 < |x - a| < d_e \Rightarrow (|f(x) - l| < e)$. # introduce universal
Then $\exists d \in \mathbb{R}, d > 0 \wedge (\forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow (|f(x) - l| < e))$. # introduce existential
Then, $e > 0 \Rightarrow (\exists d \in \mathbb{R}, d > 0 \wedge (\forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow (|f(x) - l| < e)))$.
Then $\forall e \in \mathbb{R}$, $e > 0 \Rightarrow (\exists d \in \mathbb{R}, d > 0 \wedge (\forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow (|f(x) - l| < e)))$.

[6] In other words, a formula that depends only on i. In this case, we see that $a_i = i^2$.

[7] We need to prove both pieces of a conjunction.

[8] Try $j = i + 2$.

[9] $\forall a \in \mathbb{N}, \forall b \in \mathbb{N}, b > 0 \Rightarrow a + b > a$.

[10] Assume $x \in \mathbb{R}$.
⋮
Then $\lfloor x \rfloor < x + 1$.
Then $\forall x \in \mathbb{R}$, $\lfloor x \rfloor < x + 1$.

[11] Assume $x \in \mathbb{Z}$. # x is a typical integer
Either x is even or x is odd.
Case 1: [Assume] x is even.
Then $x(x + 1)$ is even. # if x is a multiple of 2, so is $x(x + 1)$
Case 2: [Assume] x is odd.
Then $x + 1$ is even. # if x leaves remainder 1, $x + 1$ leaves remainder 0
Then $x(x + 1)$ is even. # if $x + 1$ is a multiple of 2, so is $x(x + 1)$
Then $x(x + 1)$ is even. # true in all (both) possible cases
Then $\forall x \in \mathbb{Z}, x(x + 1)$ is even. # introduce universal

[12] Instead of concluding R in one case and S in the other, we are actually concluding $R \vee S$ in both cases, and then we bring $R \vee S$ outside the cases because we concluded it in each case, and one of the cases must hold. (Remember that once we conclude that R is true, we can immediately conclude that $R \vee S$ is true.) So this is exactly the same structure we've seen before.

[13] We know that A is true and that B is true.

[14] All our sentences are finite in length, so if our domain D is infinite (like the natural numbers or real numbers), we can't actually write this expansion down. That's the reason why we need a universal quantifier in our logic system.