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 knows as much about 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 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 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 usually helpful to use our formal symbolic form, to ensure you're careful and precise. Often you will detect errors in your undertanding, and it's common to then go back to step 1 to refine our 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.

4.2 Setting up direct proof of implication

We want to make convincing arguments that a statement is true. We're allowed (forced, actually) to use previously proven statements and axioms (things that are defined to be true, or assumed to be true, for the domain). For example, if D is the set of real numbers, then we have plenty of rules about arithmetic and inequalities. 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 like 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 prove C1 is to cite the intermediate implications that justify each intermediate step. Here you write the proof that $p(x) \Rightarrow q(x)$ as:

LET $x \in D$ be such that $p(x)$

THEN $r_1(x)$ (by C2.0)

SO $r_2(x)$ (by C2.1)

$\vdots$

SO $q(x)$ (by C2.N)

THUS $p(x) \Rightarrow q(x)$.

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 $p(x)$.

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.

$p(x)$

$r_1(x)$

$r_2(x)$

$\vdots$

$s_2(x)$

$s_1(x)$

$q(x)$

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 but may not be contained in q (the ones that don't are dead ends). On the other hand, the s_i are contained in q but 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

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

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

Suppose you are asked to prove that every odd natural number has a square that is odd. You can start by writing the outline of the proof you would like to have:

Let $n \in \mathbb{N}$, and assume n is odd.
$\vdots$
So n^2 is odd.
Thus $\forall n \in \mathbb{N}$, n odd $\Rightarrow n^2$ 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 why not carry out the almost-automatic squaring of $2j + 1$? So now, on our first list, we have that, for some natural number j, $n^2 = 4j^2 + 2j + 1$. Using some algebra (distributivity of multiplication over addition), this means that for some natural number j, $n^2 = 2(2j^2 + j) + 1$. If we let k from our second list be $2j^2 + j$, 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:[1]

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?[2]

We can set this up similarly, assuming the negation of our consequent (i.e that n is even), and trying to chain to the negation of our antecedent (i.e. that n^2 is even).

4.5 More proof structure

We continue to develop a structured format for presenting proofs in this course. The intention is to provide you with an example of proof structure that can guide your future work either (a) writing proofs of your own, or (b) evaluating proofs written by others. If you don't see this formalization as simply a more careful, precise and detailed version of what we've been doing all along, then you probably need to work more on your understanding of logical statements.

We'll be using certain explicit proof forms. The structure presented here isn't meant to restrict you to a particular way of writing and presenting proofs, but rather to provide a framework to decide whether a given proof has all its working parts intact. Proofs you read elsewhere might not be laid out so clearly and completely (much to the annoyance of some readers). But once you have learned our forms you can start detecting them hidden in less formal proofs. (This is similar to why we use symbolic statements: they underlie the myriad English phrasings used more commonly elsewhere.)

negation (contrapositive)

Earlier we described the search for a chain of implications of the form $p(x) \Rightarrow r_1(x) \Rightarrow r_2(x) \Rightarrow \cdots$, in order to eventually prove $\forall x \in D, p(x) \Rightarrow q(x)$. To help form promising links in this chain, consider whether implications such as $\forall x \in D, t(x) \Rightarrow \neg r_k(x)$. You recognize this as the contrapositive of $\forall x \in D, r_k(x) \Rightarrow \neg t(x)$, so if you have $r_k(x)$ on your list, you can now add $\neg t(x)$.

Symmetrically, we were looking (from the other end) for a chain of the form $s_n(x) \Rightarrow \cdots \Rightarrow s_1(x) \Rightarrow q(x)$. It helps to consider implications of the form $\forall x \in D, \neg s_k(x) \Rightarrow t(x)$, since this is the contrapositive of $\forall x \in D, \neg t(x) \Rightarrow s_k(x)$, adding another link to the chain.

bi-implication

Even when searching for an implication, adding bi-implication links is useful. Consider

$$\forall x \in D, r_k(x) \Leftrightarrow r_{k+1}(x)$$

This is the conjunction of two implications, so that if $r_k(x) \Rightarrow q(x)$ then $r_{k+1}(x) \Rightarrow q(x)$, which means that r_{k+1} is a "dead end" if and only if r_k is. This helps trim down the search tree by leading to fewer dead ends.

4.6 Proving statements about sequences

Consider the statement:

Claim 1: $\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i$

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 like how computers count) and a_i is the element of the sequence indexed by i. Looking at the pattern of (A1), we can write the closed form for a_i.[3]

We should of course try to understand Claim 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 Claim 1 is true could take. This may even help us understand Claim 1.

We have been justifying existentials with an example. So, our proof should start off something like:

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

$\vdots$

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 that i is in $\mathbb{N}$, between the two sentences of our outline.

Next, we need to prove something for all j in $\mathbb{N}$. (Actually, we see "$\forall j \in \mathbb{N}, a_j \leq i \Rightarrow$", so we can restrict ourselves to certain j's in $\mathbb{N}$. But for the moment let's not be so smart).

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.

By the way, here's a tip for finding a proof of a universal: first try proving it for a specific concrete example (e.g. your favourite number). You usually get some feel for the general case from it. What's really exciting is that sometimes you find that you never used the specific value! Then you simply erase the specific value everywhere in your proof and replace it with the general variable!

Back to our proof outline:

Let $i =$ __. Then $i \in \mathbb{N}$.
    Let $j \in \mathbb{N}$.
        $\vdots$

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

- $\exists x \in D$: We pick x, but have to follow the rules and pick from D.
- $\forall x \in D$: Someone else 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.

Notice also the indentation, similar to what we do in code. We are following the structure of Claim 1: we are proving that all j's work for this i.

Continuing, the next level of Claim 1 is an implication. We've already seen how to deal with proving an implication: it lets us restrict our attention to only certain j's (in this case, only the ones with $a_j \leq i$). In our proof, this lets us assume $a_j \leq i$.

We need only now to check that $j < i$ (this is something left to prove).

Let $i =$ __. Then $i \in \mathbb{N}$.
    Let $j \in \mathbb{N}$.
        Suppose $a_j \leq i$.
            $\vdots$
        Thus $j < i$.

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 things: that value of i, $j \in \mathbb{N}$, and $a_j \leq i$.

After a little thought, we decide that setting $i = 2$ is a good idea, since then $a_j \leq i$ is only true for $j = 0$ and $j = 1$, and these are smaller than 2. Now let's fill in the rest of our proof, for (A1):

Let $i = 2$. Then $i \in \mathbb{N}$.
    Let $j \in \mathbb{N}$.
        Suppose $a_j \leq i$.
            Then $a_j \leq 2$.
            Looking at the sequence, this means $j = 0$ or $j = 1$.
            So $j < 2$.
            Thus $j < i$.
        Thus $a_j \leq i \Rightarrow j < i$ (since assuming $a_j \leq i$ leads to the conclusion $j < i$).
    Since j is an arbitrary element of $\mathbb{N}$, $\forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i$.
Since $i \in \mathbb{N}$, $\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i$.

4.7 Disproving statements

Consider now the statement:

Claim 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 2′: $\forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$

Following the same strategy as we used before, we get as far as:

Let $i \in \mathbb{N}$.
  Let $j =$ __. Then $j \in \mathbb{N}$.
    ⋮
    Hence $j > i \wedge a_j \neq a_i$.
  Since $j \in \mathbb{N}$, $\exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$.
Since i is an arbitrary element of $\mathbb{N}$, $\forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$.

So we don't pick i. But we get to pick j. And we are allowed to make j depend on i.

Using our game analogy: we get to pick j after someone else picks i. Unfortunately, while writing up the proof we can't wait for someone to pick j. 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 Claim 1, we weren't allowed to use j. If we write a Java 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, you will lose a lot of marks (and it will probably be wrong).

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?[4]

Let $i \in \mathbb{N}$.
  Let $j =$ __. Then $j \in \mathbb{N}$.
    ⋮
    So $j > i$.
    ⋮
    So $a_j \neq a_i$.
    Hence $j > i \wedge a_j \neq a_i$.
  Since $j \in \mathbb{N}$, $\exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$.
Since i is an arbitrary element of $\mathbb{N}$, $\forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i$.

To finish this off, we need to choose a value for j. If we choose wisely, the rest of the proof falls into place.[5] What elementary property of arithmetic will we require?[6]

4.8 An odd example revisited

Earlier we considered the implication "$\forall n \in \mathbb{N}$, n odd $\Rightarrow n^2$ odd," and its converse. We developed a direct proof of the implication, and found that the same template could not be applied to prove the converse (even though the converse is true). This asymmetry shows that the search through the implication trees from p to q does not necessarily follow the same path as from q to p, even when both paths exist and $p \Leftrightarrow q$.

However, it seems aesthetically disturbing that when $p \Leftrightarrow q$ we don't find a doubly-linked list of implications connecting them. One of your classmates came up with an approach that allows this symmetry (I've modified it slightly)

CLAIM: $\forall n \in \mathbb{N}$, n odd $\Leftrightarrow$ n^2 odd.

PROOF:

Let $n \in \mathbb{N}$.
Then
n^2 is odd
is equivalent to
$\exists k \in \mathbb{N}$ such that $n^2 = 2k + 1$ (definition of odd natural numbers);
is equivalent to
$n^2 - 1 = 2k$ for some integer k;
is equivalent to
$n^2 - 1$ is even (definition of even integer);
is equivalent to
$(n-1)(n+1)$ is even (complete the square);
is equivalent to
$(n-1)$ is even or $(n+1)$ is even ($\Rightarrow$ if prime number 2 divides a product, it divides some factor) ($\Leftarrow$ definition of even);
is equivalent to
$(n-1)$ is even or $(n+1)-2 = (n-1)$ is even (integer i is even if and only if $i-2$ is even);
is equivalent to
$(n-1)$ is even (idempotent law);
is equivalent to
$n - 1 = 2j$ for some integer j (definition of even);
is equivalent to
$n = 2j + 1$ for some integer j;
is equivalent to
n is odd.
Thus n^2 is odd $\Leftrightarrow$ n is odd.
Since n is an arbitrary natural number, $\forall n \in \mathbb{N}$, n^2 odd $\Leftrightarrow$ n odd.

4.9 Direct proof structure of the universal

Our general form of a direct proof of the implication $\forall x \in D,\ p(x) \Rightarrow q(x)$ is:

Let $x \in D$. (introduce variable x with scope indicated by indentation).
Suppose $p(x)$. (indentation indicates where $p(x)$ is assumed true)
$\vdots$ (fill in the proof of $q(x)$)
$q(x)$
Hence $p(x) \Rightarrow q(x)$.
Since x is an arbitrary element of D, $\forall x \in D, p(x) \Rightarrow q(x)$.

Here's a concrete example. 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 above:

Let $x \in \mathbb{R}$.
Suppose $x > 0$.

$\vdots$ (prove $1/(x+2) < 3$)
Therefore $1/(x+2) < 3$.
Hence $x > 0 \Rightarrow 1/(x+2) < 3$.
Since x is an arbitrary element of $\mathbb{R}$, $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x+2) < 3$.

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

Let $x \in \mathbb{R}$.
Suppose $x > 0$.
so $x + 2 > 2$ (since $x > 0$)
so $1/(x+2) < 1/2$ (since $x + 2 > 2$ and $2 > 0$)
so $1/(x+2) < 3$ (since $1/(x+2) < 1/2$ and $1/2 < 3$)
Therefore $1/(x+2) < 3$.
Hence $x > 0 \Rightarrow 1/(x+2) < 3$.
Since x is an arbitrary element of $\mathbb{R}$, $\forall x \in \mathbb{R}, x > 0 \Rightarrow 1/(x+2) < 3$.

Is the converse true (what is the converse)?[7]

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:

Let $x \in D$.
$\vdots$ (prove $q(x)$)
Hence $q(x)$.
Since x is an arbitrary element of D, $\forall x \in D, q(x)$.

4.10 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 $x = -1$.
Then $x \in \mathbb{R}$.
Also, $x^3 + 2x^2 + 3x + 4 = (-1)^3 + 2(-1)^2 + 3(-1) + 4 = -1 + 2 - 3 + 4 = 2$.
Since $x \in \mathbb{R}$, $\exists x \in \mathbb{R},\ x^3 + 2x^2 + 3x + 4 = 2$.

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

Let $x =$ [pick a specific value, unlike the universal]
Then $x \in D$. [this may be obvious from choice of x]
$\vdots$ (prove $p(x)$)
Hence $p(x)$.
Since $x \in D$, $\exists x \in D, p(x)$.

4.11 Multiple quantifiers

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

Let $x \in D$.
Let $y_x =$ (select something that helps prove $p(x, y)$)
$\vdots$
Then $y_x \in D$.
$\vdots$
Also $p(x, y_x)$.

Since $y_x \in D$, $\exists y, p(x, y)$.
Since x is an arbitrary element of D, $\forall x \in D, \exists y \in D, p(x, y)$.

Here's a concrete example. Suppose we have a mystery function f 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:[8]

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 $\neg(p \wedge q) \Leftrightarrow (p \Rightarrow \neg q)$):

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

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.

Proving $\wedge$

The $\wedge$ subproof has the following form:

So, $d_e > 0$.
Let $x \in \mathbb{R}$.
$\vdots$
Since x is an arbitrary real number, $\forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow |f(x) - l| < e$.
So $d_e > 0 \wedge \forall x \in \mathbb{R}, 0 < |x - a| < d \Rightarrow |f(x) - l| < e$...

We rolled the conclusion into the statement beginning "Therefore, $\exists d$..." The general form to prove $A \wedge B$ is:

$\vdots$

Then A.

$\vdots$

Then B.

Thus $A \wedge B$.

Don't let variables introduced while proving A "bleed" over into the proof of B (remember the scope rules!). If we had to open a new indentation level to prove A, once we close that level we can't use anything mentioned inside there again (and, particularly, we can't use it to help prove B).

Proving $\Leftrightarrow$

This also tells us how to prove a bi-implication, since bi-implication is just a conjunction of implications. To prove $A \Leftrightarrow B$, start from its definition:

$\vdots$
Then $(A \Rightarrow B) \wedge (B \Rightarrow A)$.
Thus $A \Leftrightarrow B$.

4.12 Non-boolean function example

Earlier we discussed how non-boolean functions cannot take the place of predicates (which are analogous to boolean functions) in a proof. How should they be used? Define $\lfloor x \rfloor : \mathbb{R} \to \mathbb{R}$ by:

> $\lfloor x \rfloor$ is the largest integer $\leq x$.

Now we can form the statement:

Claim 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 $\forall \lfloor x \rfloor \in \mathbb{R}$ or $\forall x \in \mathbb{R},\ \lfloor x \rfloor \vee \lfloor x + 1 \rfloor$. The structure of Claim 3 is a direct proof of a universally-quantified predicate:[9]

> Since x is an arbitrary element of $\mathbb{R}$, $\forall x \in \mathbb{R},\ \lfloor x \rfloor < x + 1$.

Of course, we need to fill in the "meat" of the proof.[10]

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

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

We didn't need the entire 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:

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

4.13 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

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[11]

> Now we have to fill in the $\vdots$ part.[12]

4.14 Proof by cases

To prove $A \Rightarrow B$, it can help to treat some A's differently than others. For example, to prove that for all integers $x^2 + x$ is even, 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.[13]

A simple two-case $\vee$ can be expressed in "if... else/otherwise..." style

> If x is even, then $x(x + 1)$ is even.
>
> Otherwise, x is odd, so $x + 1$ is even, and thus $x(x + 1)$ is even.

This is a special case of an "OR" clause being the antecedent of an implication. If you want to prove $(A_1 \vee A_2 \vee \cdots A_n) \Rightarrow B$, (this could happen if, along the way to proving $A \Rightarrow B$ you use the fact that $A \Rightarrow (A_1 \vee \cdots A_n)$. Now you need to prove $A_1 \Rightarrow B$, $A_2 \Rightarrow B, \cdots, A_n \Rightarrow B$. 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 $A_i = D_i \wedge A$. 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, $D = D_1 \cup \neg D_1$, so you can rewrite A as $(A \wedge D_1) \vee (A \wedge \neg D_1)$.

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

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).

Let $n \in \mathbb{Z}$.

By (*), $\forall n \in \mathbb{Z}, (\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$.
So $(\exists k \in \mathbb{Z}, n = 2k + 1) \vee (\exists k \in \mathbb{Z}, n = 2k)$ (since $n \in \mathbb{Z}$).
Case 1: $\exists k \in \mathbb{Z}, n = 2k + 1$
Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0 + 1$.
Then $n^2 + n = n(n + 1) = (2k_0 + 1)(2k_0 + 2) = 2[(2k_0 + 1)(k_0 + 1)]$
Let $k = (2k_0 + 1)(k_0 + 1)$. Then $k \in \mathbb{Z}$.
And $n^2 + n = 2k$, from above.
Thus $\exists k \in \mathbb{Z}, n^2 + n = 2k$.
Case 2: $\exists k \in \mathbb{Z}, n = 2k)$.
Let $k_0 \in \mathbb{Z}$ be such that $n = 2k_0$.
Then $n^2 + n = n(n + 1) = 2k_0(2k_0 + 1) = 2[k_0(2k_0 + 1)]$
Let $k = k_0(2k_0 + 1)$. Then $k \in \mathbb{Z}$.
And $n^2 + n = 2k$, from above.
Thus $\exists k \in \mathbb{Z}, n^2 + n = 2k$.
So $\exists k \in \mathbb{Z}, n^2 + n = 2k$, since we concluded it in each case, and one of these cases must occur.
Since n is an arbitrary element of $\mathbb{Z}$, $\forall n \in \mathbb{Z}, \exists k \in \mathbb{Z}, n^2 + n = 2k$.

LINKING PROOF TO PROGRAMMING

Let's relate this to programming. We can think of a predicate "even(n)" as being a Java method that returns a Boolean value:

```
/* Return whether n is even. */
static boolean isEven(int n)
```

We can also imagine an example generator for even numbers:

```
/* Requires: n even.
   Return k such that n = 2k. */
static int evenWitness(int n)
```

We'll leave it as an exercise to define `isOdd` and `oddWitness`.

Now we can imagine (S1) as saying we can implement the following method, and the proof as the implementation and internal comments.

```
/* Return k such that n^2 + n = k */
static int S1(int n) {
  if (odd(n)) {
    int k0 = oddWitness(n);
    // n = 2k0 + 1
    // so n^2 + n = ... = 2[(2k0 + 1)(k0 + 1)
    int k = (2 * k0 + 1) * (k0 + 1);
    return k;
  } else { // even(n)
    int k0 = evenWitness(n);
    // ...
    int k = k0 * (2 * k0 + 1);
    return k;
  }
}
```

In some (very strong) sense, programming and proving are really the same thing. Improving your skills in one area will improve your skills in the other. Sometimes it's easier to think in terms of programming, and sometimes it's easier to think in terms of deriving proofs.

Consider the following CSC 108-like example: prove that whomever goes first in a game of tic-tac-toe should not lose, assuming correct play. If you can write a program that never loses, you should be able to write a mathematical proof of this fact.

4.15 Proving $\vee$ using cases

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

Claim 5: $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k + 1)$.

This will involve proving a disjunction. This can be done by cases. If we know $P \vee Q$, we can prove $R \vee S$ as follows:

$P \vee Q$
Case 1: Assume P
$\vdots$
Then R
Case 2: Assume Q
$\vdots$
Then S
Thus $R \vee S$[14]

If we have 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, make up a name for P, and 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.

Let $n \in \mathbb{N}$.
By (*), $\exists k \in \mathbb{N}, n = 3k \vee n = 3k + 1 \vee n = 3k + 2$.
So let $k_0 \in \mathbb{N}$ be such that $n = 3k_0 \vee n = 3k + 0 + 1 \vee n = 3k_0 + 2$.
Case 1: $n = 3k_0$.
Let $k = 3{k_0}^2$. Then $k \in \mathbb{N}$.
And $n^2 = (3k_0)^2 = 3(3{k_0}^2) = 3k$.
Thus $\exists k \in \mathbb{N}, n^2 = 3k$.
Case 2: $n = 3k_0 + 1$.
Let $k = 3{k_0}^2 + 2k_0$. Then $k \in \mathbb{N}$.
And $n^2 = (3k_0 + 1)^2 = 9{k_0}^2 + 6k_0 + 1 = 3(3{k_0}^2 + 2k_0) + 1 = 3k + 1$.
Thus $\exists k \in \mathbb{N}, n^2 = 3k + 1$.
Case 3: $n = 3k_0 + 2$.
Exercise.
Thus, by cases, $(\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k + 1)$.
Since n is an arbitrary element in $\mathbb{N}$, $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n^2 = 3k) \vee (\exists k \in \mathbb{N}, n^2 = 3k + 1)$.

4.16 Indirect proof

Since $p \Rightarrow q$ is equivalent to its contrapositive, $\neg q \Rightarrow \neg p$, proving the latter proves the former. This is called an "indirect proof." The outline format of an indirect proof of $\forall x \in D, p(x) \Rightarrow q(x)$ is[15].

As an exercise, consider: $\forall x \in \mathbb{Z}$, if x^2 is odd, then x is odd.

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 managable size (can you imagine always having to prove $2 + 2 = 4$ from primative 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?[16]

Existential elimination

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. It exists, so if we look for it, we're sure to find it (actually finding it might be hard, so that's a job for the engineers—we have a proof to finish!). We can convert an existential statement about some object into a statement about a specific object as follows:

$\exists x \in D$, B
Consider $a \in D$ such that $B_{x \leftarrow a}$.
$\vdots$

In the $\vdots$, we can use a and B (with each reference to x replaced by a) and even $\exists x \in D, B$ however we please. We do not have to open a new scope, but there are some important rules we need to follow:

- a must be a brand new object/variable name that cannot have been used before! Just because we know such an object exists does *not* mean it's the same as anything we've mentioned before (you would need to prove that).
- All references to x (that are bound to this existential) must be replaced by references to a (that's what $B_{x \leftarrow a}$ means: replace x with a inside B).

Here's an example. Suppose we need to prove that the square of an even natural number is even. We know a natural number n is even if $\exists k \in \mathbb{N}, n = 2k$. We expand this fact to complete our proof:

Assume n is even.
  So $\exists k \in \mathbb{N}, n = 2k$ by definition.
  Consider $k \in \mathbb{N}$ such that $n = 2k$.
  Then $n^2 = 2k \cdot n$ (multiply both sides by n).
  Let $k' = kn$.
    Then $k' \in \mathbb{N}$ (closure of natural numbers).
    So $n^2 = 2k'$.
  Since $k' \in \mathbb{N}$, $\exists k \in \mathbb{N}, n^2 = 2k$.
  Thus n^2 is even.
Thus n is even implies n^2 is even.

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

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 disjunction over all the elements of $D = \{d_1, d_2, d_3, \dots\}$:

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

From this expansion (even if we can't write it[17]) 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 Proof by contradiction

Recall that every statement you write in a proof must be true in their context (the set of assumptions you've made to get to the present scope). And remember that only one of a statement and its negation should be true in the same context. Sometimes, however, we discover that both a statement and its negation are true at the same time! Error! Error?

What's happened? Do we have a flaw in our proof? Probably not. All this means is that we've wandered into a non-existent world. When we have a statement that's both true and false at the same time, we've discovered a CONTRADICTION. This indicates that the assumptions we've made are inconsistent, and thus could not have occurred. This is a good thing, because we've proven that this case cannot have occurred, so we don't need to deal with it.

When we detect that both A and $\neg A$ are true at the same time, we're allowed to derive "contradiction," and we're allowed to conclude that the last assumption we've made is incorrect. In other words, we're allowed to introduce a negation of a formula.

Consider the following statement about sequences of natural numbers:

$$\forall i \in \mathbb{N}, (i > 0 \wedge a_i < a_{i-1}) \Rightarrow a_i \text{ is even}$$

and the sequence:

$$\text{(A3) } a_n = \begin{cases} n+1 & \text{if } n \text{ even} \\ n-1 & \text{if } n \text{ odd} \end{cases}$$

Our proof proceeds as follows:

Let $i \in \mathbb{N}$.
  Assume $i > 0 \wedge a_i < a_{i-1}$.
    So $i > 0$ (by $\wedge$E).
    Since $i - 1 \geq 0$, $i - 1 \in \mathbb{N}$ (by math, $\mathbb{N}$ definition).
    So $a_i < a_{i-1}$ (by $\wedge$E).
    $\vdots$
    Thus a_i is even.
  Thus $(i > 0 \wedge a_i < a_{i-1}) \Rightarrow a_i$ is even (by $\Rightarrow$I).
Since i is an arbitrary element of $\mathbb{N}$, $\forall i \in \mathbb{N}, (i > 0 \wedge a_i < a_{i-1}) \Rightarrow a_i$ is even (by $\forall$I).

We get stuck at this point (trying to fill in the $\vdots$), so we observe that i is either odd or even and try to proceed by cases:

i is odd $\vee$ i is even (by law of excluded middle).
Case 1: [Assume] i is odd.
  Then $a_i = i - 1$ (by (A3)).
  Thus a_i is even.
Case 2: [Assume] i is even.
  Then $a_i = i + 1$ (by (A3)).
  Then $a_{i-1} = (i - 1) - 1 = i - 2$ (by (A3)).
  So $\neg(a_i < a_{i-1})$.
  Thus contradiction.

We discovered a contradiction in case 2, so we know that case 2 could not have occurred. We rewrite this argument into a proof by contradiction (instead of a proof by cases):

Assume $\neg$(i is odd). Then i is even.
  Then $a_i = i + 1$ (by (A3)).
  Then $a_{i-1} = (i - 1) - 1 = i - 2$ (by (A3)).
  So $\neg(a_i < a_{i-1})$.
  Thus contradiction.

Then $\neg(\neg(i \text{ is odd}))$ (by $\neg$I).
So i is odd (by $\neg$E).
Then $a_i = i - 1$ (by (A3)).
Thus a_i is even.

Interestingly, you can prove any statement at all from a contradiction.[18] So everything is true and everything is false in dreamworlds.

4.19 Summary of inference rules

There are several basic and derived rules we're allowed to use in our proofs. Many of them are summarized here. 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

$\Rightarrow$I implication introduction
(direct proof for implication)

$$\frac{\begin{array}{l}\text{Assume } A\\ \quad\vdots\\ \quad B\end{array}}{A \Rightarrow B}$$

$\wedge$I conjunction introduction

$$\frac{\begin{array}{l}A\\ B\end{array}}{A \wedge B}$$

$\vee$I disjunction introduction

$$\frac{A}{\begin{array}{l}A \vee B\\ B \vee A\end{array}}$$

$\Leftrightarrow$I equivalence/bi-implication introduction

$$\frac{\begin{array}{l}\vdots\\ A \Rightarrow B\\ \vdots\\ B \Rightarrow A\end{array}}{\begin{array}{l}(A \Rightarrow B) \wedge (B \Rightarrow A)\\ A \Leftrightarrow B\end{array}}$$

$\neg$I negation introduction

$$\frac{\begin{array}{l}\text{Assume } A\\ \quad\vdots\\ \quad \text{contradiction}\end{array}}{\neg A}$$

$\forall$I universal introduction

$$\frac{\begin{array}{l}\text{Let } a \in D \text{ be arbitrary.}\\ \quad\vdots\\ \quad P(a)\end{array}}{\forall x \in D, P(x)}$$

$\exists$I existential introduction

$$\frac{\begin{array}{l}P(a)\\ a \in D\end{array}}{\exists x \in D, P(x)}$$

Other rules

ContraI contradiction introduction

$$\frac{\begin{array}{l}A\\ \neg A\end{array}}{\text{contradiction}}$$

Elimination rules

$\neg$E negation elimination

$$\frac{\neg\neg A}{A}$$

$\wedge$E conjunction elimination

$$\frac{A \wedge B}{\begin{array}{l}A\\ B\end{array}}$$

$\vee$E disjunction elimination

$$\frac{\begin{array}{l}A \vee B\\ \neg A\end{array}}{B}$$

$\Rightarrow$E implication elimination (Modus Ponens)

$$\frac{\begin{array}{l}A \Rightarrow B\\ A\end{array}}{B}$$

$\Leftrightarrow$E equivalence/bi-implication elimination

$$\frac{\begin{array}{l}A \Leftrightarrow B\\ A\end{array}}{B}$$

$\forall$E universal elimination

$$\frac{\begin{array}{l}\forall x \in D, P(x)\\ a \in D\end{array}}{P(a)}$$

$\exists$E existential elimination

$$\frac{\exists x \in D, P(x)}{\begin{array}{l}\text{Consider } a \in D \text{ such that } P(a)\\ \quad\vdots\end{array}}$$

Other rules

RE rewriting/repetition

$$\frac{A}{A}$$

excluded middle

$$\frac{}{A \vee \neg A}$$

MT reverse implication elimination
(Modus Tollens)

$$\frac{\begin{array}{l}A \Rightarrow B\\ \neg B\end{array}}{\neg A}$$

Chapter 4 Notes

[1]Let $n \in \mathbb{N}$ such that n is odd.
Then, for some $j \in \mathbb{N}$, $n = 2j + 1$ (definition of odd number).
So $n^2 = 4j^2 + 2j + 1$ (definition of squaring a number)
So $n^2 = 2(2j^2 + j) + 1$ (distributive law)
So there exists a natural number $k = 2j^2 + j$ such that $n^2 = 2k + 1$. ($\mathbb{N}$ is closed under addition and multiplication)
So n^2 is odd.
Thus $\forall n \in \mathbb{N}$, n odd $\Rightarrow n^2$ odd.

[2]The contrapositive.

[3]We see that $a_i = i^2$.

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

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

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

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

[8]Let $e \in \mathbb{R}$.
Assume $e > 0$.
Let $d_e =$ (something helpful, probably depending on e)
Then $d_e \in \mathbb{R}$.
Also $d_e > 0$.
Let $x \in \mathbb{R}$.
Assume $0 < |x - a| < d_e$.
$\vdots$
So $|f(x) - l| < e$.
Hence $0 < |x - a| < d_e \Rightarrow (|f(x) - l| < e)$.
Since x is an arbitrary element of $\mathbb{R}$, $\forall x \in \mathbb{R},\ 0 < |x - a| < d_e \Rightarrow (|f(x) - l| < e)$.
Thus $\exists d \in \mathbb{R}, d > 0 \wedge (\forall x \in \mathbb{R},\ 0 < |x - a| < d \Rightarrow (|f(x) - l| < e))$.
Then, $e > 0 \Rightarrow (\exists d \in \mathbb{R}, d > 0 \wedge (\forall x \in \mathbb{R},\ 0 < |x - a| < d \Rightarrow (|f(x) - l| < e)))$.

Since e is an arbitrary element of $\mathbb{R}$,

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

[9] Let $x \in \mathbb{R}$.
$\vdots$
Then $\lfloor x \rfloor < x + 1$.
Since x is an arbitrary element of $\mathbb{R}$, $\forall x \in \mathbb{R}$, $\lfloor x \rfloor < x + 1$.

[10] Let $x \in \mathbb{R}$.
Let $y = \lfloor x \rfloor$
Then y is the largest integer $\leq x$ (definition of floor)
So $y \leq x$ and $x < x + 1$ (adding 1 to both sides of an inequality)
So $y < x + 1$
So $\lfloor x \rfloor < x + 1$
Since x was an arbitrary element of $\mathbb{R}$, $\forall x \in \mathbb{R}$, $\lfloor x \rfloor < x + 1$.

[11] Let $y \in \mathbb{R}$.

Assume $y \neq 0$.

$\vdots$

Hence $1/(y^2+2) < 3$.

Thus $y \neq 0 \Rightarrow 1/(y^2+2) < 3$.

Since y is an arbitrary element of $\mathbb{R}$, $\forall y \in \mathbb{R},\ y \neq 0 \Rightarrow 1/(y^2+2) < 3$.

[12] Let $y \in \mathbb{R}$.

Assume $y \neq 0$.

Then $y^2 \in \mathbb{R}$ and $y^2 \geq 0$ (true for all elements of $\mathbb{R}$).

So $y^2 > 0$, since $y^2 \neq 0$ and $y^2 \geq 0$ (only real number whose square is 0 is 0).

So, by THEOREM 1, $1/(y^2+2) < 3$.

Hence $y \neq 0 \Rightarrow 1/(y^2+2) < 3$.

Since y is an arbitrary element of $\mathbb{R}$, $\forall y \in \mathbb{R}, y \neq 0 \Rightarrow 1/(y^2+2) < 3$.

[13] Let $x \in \mathbb{Z}$.

Either x is even or x is odd (by law of excluded middle).

We know that (at least) one of these disjuncts must hold, so we break into two cases.

Case 1: [Assume] x is even.

Then $x(x+1)$ is even.

Case 2: [Assume] x is odd.

Then $x+1$ is even.

So $x(x+1)$ is even.

Since x is either even or odd, $x(x+1)$ is even in all cases.

Since x is an arbitrary element of $\mathbb{Z}$, $\forall x \in \mathbb{Z}, x(x+1)$ is even.

[14]Instead of concluding R in once 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.

[15] Let $x \in D$.

Suppose $\neg q(x)$.

$\vdots$

Then $\neg p(x)$.

Then $p(x) \Rightarrow q(x)$.

Since x is an arbitrary element of D, $\forall x \in D, p(x) \Rightarrow q(x)$.

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

[17]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.

[18]Once we have a contradiction, to prove $\neg P$, we assume P, derive contradiction via rewriting, and thus conclude $\neg P$. The method to prove P is similar.