Chapter 4

Proofs

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. 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.

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 $p(x)$.

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 ∧ and ∨ 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 $r_2(x) \Rightarrow q(x)$.

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).

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.

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 $i = \underline{\quad}$. 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 $i = \underline{\quad}$. 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 $i \in \mathbb{N}$, $\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i$.

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) $0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, 6, ...$

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]

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
$n^2 - 1 = 2k$ 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.

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)
        ⋮ (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 $D$, $\forall x \in D, q(x)$.
```

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 $x \in D$, $\exists x \in D, p(x)$.
```

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

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.