Chapter 3

Proofs

Many mathematical proofs use a small range of standard outlines: direct proof, examples/counter-examples, and proof by contrapositive. These notes explain these basic proof methods, as well as how to use definitions of new concepts in proofs. More advanced methods (e.g. proof by induction, proof by contradiction) will be covered later.

3.1 Proving a universal statement

Now, let's consider how to prove a claim like

> For every rational number q, $2q$ is rational.

First, we need to define what we mean by "rational".

> A real number r is *rational* if there are integers m and n, $n \neq 0$, such that $r = \frac{m}{n}$.

In this definition, notice that the fraction $\frac{m}{n}$ does not need to satisfy conditions like being proper or in lowest terms So, for example, zero is rational because it can be written as $\frac{0}{1}$. However, it's critical that the two numbers

in the fraction be integers, since even irrational numbers can be written as fractions with non-integers on the top and/or bottom. E.g. $\pi = \frac{\pi}{1}$.

The simplest technique for proving a claim of the form $\forall x \in A, P(x)$ is to pick some representative value for x.[1]. Think about sticking your hand into the set A with your eyes closed and pulling out some random element. You use the fact that x is an element of A to show that $P(x)$ is true. Here's what it looks like for our example:

> Proof: Let q be any rational number. From the definition of "rational," we know that $q = \frac{m}{n}$ where m and n are integers and n is not zero. So $2q = 2\frac{m}{n} = \frac{2m}{n}$. Since m is an integer, so is $2m$. So $2q$ is also the ratio of two integers and, therefore, $2q$ is rational.

At the start of the proof, notice that we expanded the word "rational" into what its definition said. At the end of the proof, we went the other way: noticed that something had the form required by the definition and then asserted that it must be a rational.

WARNING!! Abuse of notation. Notice that the above definition of "rational" used the word "if". If you take this literally, it would mean that the definition could be applied only in one direction. This isn't what's meant. Definitions are always intended to work in both directions. Technically, I should have written "if and only if" (frequently shortened to "iff"). This little misuse of "if" in definitions is very, very common.

Notice also that we spelled out the definition of "rational" but we just freely used facts from high school algebra as if they were obvious. In general, when writing proofs, you and your reader come to some agreement about what parts of math will be considered familiar and obvious, and which require explicit discussion. In practical terms, this means that, when writing solutions to homework problems, you should try to mimic the level of detail in examples presented in lecture and in model solutions to previous homeworks.

[1]The formal name for this is "universal instantiation."

3.2 Another example of direct proof involving odd and even

Here's another claim that can be proved by direct proof.

Claim 1 *For any integer k, if k is odd then k^2 is odd.*

This has a slightly different form from the previous claim: $\forall x \in \mathbb{Z}$, if $P(x)$, then $Q(x)$

Before doing the actual proof, we first need to be precise about what we mean by "odd". And, while we are on the topic, what we mean by "even."

Definition 1 *An integer n is even if there is an integer m such that $n = 2m$.*

Definition 2 *An integer n is odd if there is an integer m such that $n = 2m + 1$.*

Such definitions are sometimes written using the jargon "has the form," as in "An integer n is even if it has the form $2m$, where m is an integer."

We'll assume that it's obvious (from our high school algebra) that every integer is even or odd, and that no integer is both even and odd. You probably also feel confident that you know which numbers are odd or even. An exception might be zero: notice that the above definition makes it definitely even. This is the standard convention in math and computer science.

Using these definitions, we can prove our claim as follows:

> Proof of Claim 1: Let k be any integer and suppose that k is odd. We need to show that k^2 is odd.
>
> Since k is odd, there is an integer j such that $k = 2j + 1$. Then we have
>
> $$k^2 = (2j + 1)^2 = 4j^2 + 4j + 1 = 2(2j^2 + 2j) + 1$$
>
> Since j is an integer, $2j^2 + 2j$ is also an integer. Let's call it p. Then $k^2 = 2p + 1$. So, by the definition of odd, k^2 is odd.

As in the previous proof, we used our key definition twice in the proof: once at the start to expand a technical term ("odd") into its meaning, then again at the end to summarize our findings into the appropriate technical terms.

At the start of the proof, notice that we chose a random (or "arbitrary" in math jargon) integer k, like last time. However, we also "supposed" that the hypothesis of the if/then statement was true. It's helpful to collect up all your given information right at the start of the proof, so you know what you have to work with.

The comment about what we need to show is not necessary to the proof. It's sometimes included because it's helpful to the reader. You may also want to include it because it's helpful *to you* to remind you of where you need to get to at the end of the proof.

Similarly, introducing the variable p isn't really necessary with a claim this simple. However, using new variables to create an exact match to a definition may help you keep yourself organized.

3.3 Direct proof outline

In both of these proofs, we started from the known information (anything in the variable declarations and the hypothesis of the if/then statement) and moved gradually towards the information that needed to be proved (the conclusion of the if/then statement). This is the standard "logical" order for a direct proof. It's the easiest order for a reader to understand.

When working out your proof, you may sometimes need to reason backwards from your desired conclusion on your scratch paper. However, when you write out the final version, reorder everything so it's in logical order.

You will sometimes see proofs that are written partly in backwards order. This is harder to do well and requires a lot more words of explanation to help the reader follow what the proof is trying to do. When you are first starting out, especially if you don't like writing a lot of comments, it's better to stick to a straightforward logical order.

3.4 Proving existential statements

Here's an existential claim:

Claim 2 *There is an integer k such that $k^2 = 0$.*

An existential claim such as the following asserts the existence of an object with some set of properties. So it's enough to exhibit some specific concrete object, of our choosing, with the required properties. So our proof can be very simple:

Proof: Zero is such an integer. So the statement is true.

We could spell out a bit more detail, but it's really not necessary. Proofs of existential claims are often very short, though there are exceptions.

Notice one difference from our previous proofs. When we pick a value to instantiate a universally quantified variable, we have no control over exactly what the value is. We have to base our reasoning just on what set it belongs to. But when we are proving an existential claim, we get to pick our own favorite choice of concrete value, in this case zero.

Don't prove an existential claim using a general argument about why there must exist numbers with these properties.[2] This is not only overkill, but very hard to do correctly and harder on the reader. Use a specific, concrete example.

3.5 Disproving a universal statement

Here's a universal claim that is false:

Claim 3 *Every rational number q has a multiplicative inverse.*

[2]In higher mathematics, you occuasionally must make an abstract argument about existence because it's not feasible to produce a concrete example. We will see one example towards the end of this course. But this is very rare.

Definition 3 *If q and r are real numbers, r is a multiplicative inverse for q if $qr = 1$.*

In general, a statement of the form "for all x in A, $P(x)$" is false exactly when there is some value y in A for which $P(y)$ is false.[3] So, to disprove a universal claim, we need to prove an existential statement. So it's enough to exhibit one concrete value (a "counter-example") for which the claim fails. In this case, our disproof is very simple:

> Disproof of Claim 3: This claim isn't true, because we know from high school algebra that zero has no inverse.

Don't try to construct a general argument when a single specific counterexample would be sufficient.

3.6 Disproving an existential statement

There's a general pattern here: the negation of $\forall x, P(x)$ is $\exists x, \neg P(x)$. So the negation of a universal claim is an existential claim. Similarly the negation of $\exists x, P(x)$ is $\forall x, \neg P(x)$. So the negation of an existential claim is a universal one.

Suppose we want to disprove an existential claim like:

Claim 4 *There is an integer k such that $k^2 + 2k + 1 < 0$.*

We need to make a general argument that, no matter what value of k we pick, the equation won't hold. So we need to prove the claim

Claim 5 *For every integer k, it's not the case that $k^2 + 2k + 1 < 0$.*

Or, said another way,

[3]Notice that "for which" is occasionally used as a variant of "such that." In this case, it makes the English sound very slightly better.

Claim 6 *For every integer k, $k^2 + 2k + 1 \geq 0$.*

The proof of this is fairly easy:

> Proof: Let k be an integer. Then $(k+1)^2 \geq 0$ because the square of any real number is non-negative. But $(k+1)^2 = k^2+2k+1$. So, by combining these two equations, we find that $k^2 + 2k + 1 \geq 0$.

3.7 Recap of proof methods

So, our general pattern for selecting the proof type is:

	prove	disprove
universal	general argument	specific counter-example
existential	specific example	general argument

Both types of proof start off by picking an element x from the domain of the quantification. However, for the general arguments, x is a random element whose identity you don't know. For the proofs requiring specific examples, you can pick x to be your favorite specific concrete value.

3.8 Direct proof: example with two variables

Let's do another example of direct proof. First, let's define

Definition 4 *An integer n is a perfect square if $n = k^2$ for some integer k.*

And now consider the claim:

Claim 7 *For any integers m and n, if m and n are perfect squares, then so is mn.*

> Proof: Let m and n be integers and suppose that m and n are perfect squares.

> By the definition of "perfect square", we know that $m = k^2$ and $n = j^2$, for some integers k and j. So then mn is k^2j^2, which is equal to $(kj)^2$. Since k and j are integers, so is kj. Since mn is the square of the integer kj, mn is a perfect square, which is what we needed to show.

Notice that we used a different variable name in the two uses of the definition of perfect square: k the first time and j the second time. It's important to use a fresh variable name each time you expand a definition like this. Otherwise, you could end up forcing two variables (m and n in this case) to be equal when that isn't (or might not be) true.

Notice that the phrase "which is what we needed to show" helps tell the reader that we're done with the proof. It's polite to indicate the end in one way or another. In typed notes, it may be clear from the indentation. Sometimes, especially in handwritten proofs, we put a box or triangle of dots or Q.E.D. at the end. Q.E.D. is short for Latin "Quod erat demonstrandum," which is just a translation of "what we needed to show."

3.9 Another example with two variables

Here's another example of a claim involving two variables:

Claim 8 *For all integers j and k, if j and k are odd, then jk is odd.*

A direct proof would look like:

> Proof: Let j and k be integers and suppose they are both odd. Because j is odd, there is an integer p such that $j = 2p + 1$. Similarly, there is an integer q such that $k = 2q + 1$.
>
> So then $jk = (2p+1)(2q+1) = 4pq+2p+2q+1 = 2(2pq+p+q)+1$. Since p and q are both integers, so is $2pq + p + q$. Let's call it m. Then $jk = 2m + 1$ and therefore jk is odd, which is what we needed to show.

3.10 Proof by cases

When constructing a proof, sometimes you'll find that part of your given information has the form "p or q." Perhaps your claim was stated using "or," or perhaps you had an equation like $|x| > 6$ which translates into an or ($x > 6$ or $x < -6$) when you try to manipulate it. When the given information allows two or more separate possibilities, it is often best to use a technique called "proof by cases."

In proof by cases, you do part of the proof two or more times, once for each of the possibilities in the "or." For example, suppose that our claim is:

Claim 9 *For all integers j and k, if j is even or k is even, then jk is even.*

We can prove this as follows:

> Proof: Let j and k be integers and suppose that j is even or k is even. There are two cases:
>
> Case 1: j is even. Then $j = 2m$, where m is an integer. So the $jk = (2m)k = 2(mk)$. Since m and k are integers, so is mk. So jk must be even.
>
> Case 2: k is even. Then $k = 2n$, where n is an integer. So the $jk = j(2n) = 2(nj)$. Since n and j are integers, so is nj. So jk must be even.
>
> So jk is even in both cases, which is what we needed to show.

It is ok to have more than two cases. It's also ok if the cases overlap, e.g. one case might assume that $x \leq 0$ and another case might assume that $x \geq 0$. However, you must be sure that all your cases, taken together, cover all the possibilities.

In this example, each case involved expanding the definition of "even." We expanded the definition twice but, unlike our earlier examples, only one expansion is active at a given time. So we could have re-used the variable m when we expanded "even" in Case 2. I chose to use a fresh variable name (n) because this is a safer strategy if you aren't absolutely sure when re-use is ok.

3.11 Rephrasing claims

Sometimes you'll be asked to prove a claim that's not in a good form for a direct proof. For example:

Claim 10 *There is no integer k such that k is odd and k^2 is even.*

It's not clear how to start a proof for a claim like this. What is our given information and what do we need to show?

In such cases, it is often useful to rephrase your claim using logical equivalences. For example, the above claim is equivalent to

Claim 11 *For every integer k, it is not the case that k is odd and k^2 is even.*

By DeMorgan's laws, this is equivalent to

Claim 12 *For every integer k, k is not odd or k^2 is not even.*

Since we're assuming we all know that even and odd are opposites, this is the same as

Claim 13 *For every integer k, k is not odd or k^2 is odd.*

And we can restate this as an implication using the fact that $\neg p \vee q$ is equivalent to $p \rightarrow q$:

Claim 14 *For every integer k, if k is odd then k^2 is odd.*

Our claim is now in a convenient form: a universal if/then statement whose hypothesis contains positive (not negated) facts. And, in fact, we proved this claim earlier in these notes.

3.12 Proof by contrapositive

A particularly common sort of rephrasing is to replace a claim by its contrapositive. If the original claim was $\forall x, P(x) \to Q(x)$ then its contrapositive is $\forall x, \neg Q(x) \to \neg P(x)$. Remember that any if/then statement is logically equivalent to its contrapositive.

Remember that constructing the hypothesis requires swapping the hypothesis with the conclusion AND negating both of them. If you do only half of this transformation, you get a statement that isn't equivalent to the original. For example, the converse $\forall x, Q(x) \to P(x)$ is not equivalent to the original claim.

For example, suppose that we want to prove

Claim 15 *For any integers a and b, if $a + b \geq 15$, then $a \geq 8$ or $b \geq 8$.*

This is hard to prove in its original form, because we're trying to use information about a derived quantity to prove something about more basic quantities. If we rephrase as the contrapositive, we get

Claim 16 *For any integers a and b, if it's not the case that $a \geq 8$ or $b \geq 8$, then it's not the case that $a + b \geq 15$.*

And this is equivalent to:

Claim 17 *For any integers a and b, if $a < 8$ and $b < 8$, then $a + b < 15$.*

Notice that when we negated the conclusion of the original statement, we needed to change the "or" into an "and" (DeMorgan's Law).

When you do this kind of rephrasing, your proof should start by explaining to the reader how you rephrased the claim. It's technically enough to say that you're proving the contrapositive. But, for a beginning proof writer, it's better to actually write out the contrapositive of the claim. This gives you a chance to make sure you have constructed the contrapositive correctly. And, while you are writing the rest of the proof, it helps remind you of exactly what is given and what you need to show.

So a proof our our original claim might look like:

Proof: We'll prove the contrapositive of this statement. That is, for any integers a and b, if $a < 8$ and $b < 8$, then $a + b < 15$.

So, suppose that a and b are integers such that $a < 8$ and $b < 8$. Since they are integers (not e.g. real numbers), this implies that $a \leq 7$ and $b \leq 7$. Adding these two equations together, we find that $a + b \leq 14$. But this implies that $a + b < 15$. □

There is no hard-and-fast rule about when to switch to the contrapositive of a claim. If you are stuck trying to write a direct proof, write out the contrapositive of the claim and see whether that version seems easier to prove.

3.13 Another example of proof by contrapositive

Here's another example where it works well to convert to the contrapositive:

Claim 18 *For any integer k, if $3k + 1$ is even, then k is odd.*

If we rephrase as the contrapositive, we get:

Claim 19 *For any integer k, if k is even, $3k + 1$ is odd.*

So our complete proof would look like:

Proof: We will prove the contrapositive of this claim, i.e. that for any integer k, if k is even, $3k + 1$ is odd.

So, suppose that k is an integer and k is even. Then, $k = 2m$ for some integer m. Then $3k + 1 = 3(2m) + 1 = 2(3m) + 1$. Since m is an integer, so is $3m$. So $3k + 1$ must be odd, which is what we needed to show.