Examples of direct proof and disproof

Margaret M. Fleck

1 February 2010

This lecture does more examples of direct proof and disproof of quantified statements, based on section 1.6 of Rosen (which you still don't have to read yet).

1 Announcements

Quiz coming up a week from Wednesday (10th).

2 Recap

Last class, we saw how to prove a universal ("for all") claim and how to prove an existential ("there exists") claim. Proving the existential claim was easy: we just showed our reader a specific example with the required properties. For example:

Claim: There is an integer x such that $x^2 = 1$.

Proof: Consider 1. 1 is an integer and its square is 1.

We also proved a universal claim:

Claim 1 *For every rational number q, $2q$ is rational.*

This proof was more involved, because we needed to pick a representative rational number q and to give a general argument that would work no matter what specific value we picked for q.

This is a general difference between proving universal and existential claims. Universal claims can't be proved by showing that the claim holds for one specific value. This is a very serious flaw that will lose you a lot of points.

Less obviously, it's also wrong to prove an existential claim by writing a general argument about why the claim works for a whole bunch of values. Giving single concrete example is much simpler and also more convincing. It is quite rare for the proof of an existential claim to involve an abstract argument about why an object with certain properties must exist (even though we can't quite describe what it looks like).

3 Another example of direct proof involving odd and even

Last class, we proved our universal claim using a so-called "direct proof," in which the proof proceeded in a more-or-less straight line from the given facts to the desired conclusion, applying some definitions of key concepts along the way. Here's another claim that can be proved in this straightforward manner.

Claim 2 *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 **??**: 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 proof last class, 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.

Notice also that 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.

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.

4 Disproving a universal statement

Now, how about this claim?

Claim 3 *For every rational number q, there is a rational number r such that $qr = 1$.*

Or, in math jargon, every rational number has a (multiplicative) inverse. This isn't true, is it? Zero doesn't have an inverse.

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.[1] So, to disprove a universal claim, we are proving 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 **??**: This statement isn't true, because we know from high school algebra that zero has no inverse.

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

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

5 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 a 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,

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 $(k+1) = k^2 + 2k + 1$. So, by combining these two equations, we find that $k^2 + 2k + 1 \geq 0$.

6 An example with two variables

Suppose that we want to prove the following

Claim 7 *For all integers j and k, if j and k are odd, then jk is odd.*

The proof might 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.

Notice that we used a different variable name in the two uses of the definition of odd: p the first time and q 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 (e.g. j and k) 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."

7 Vacuous truth

Consider the following claim:

Claim 8 *For all natural numbers n, if $14 + n < 10$, then n wood elves will attack Siebel Center tomorrow.*

I claim this is true, a fact which most students find counter-intuitive. In fact, it wouldn't be true if n was declared to be an integer.

Notice that this statement has the form $\forall n, P(n) \to Q(n)$, where $P(n)$ is the predicate $14+n < 10$. Because n is declared to be a natural number, n is never negative, so $n + 14$ will always be at least 14. So $P(n)$ is always false. Therefore, our conventions about the truth values for conditional statements imply that $P(n) \to Q(n)$ is true. This argument works for any choice of n. So $\forall n, P(n) \to Q(n)$ is true.

Because even mathematicians find such statements a bit wierd, they typically say that such a claim is *vacuously* true, to emphasize to the reader that it is only true because of this strange convention about the meaning of conditionals. Vacuously true statements typically occur when you are trying to apply a definition or theorem to a special case involving an abnormally small or simple object, such as the empty set or zero or a graph with no arrows at all. As we encounter such examples during the term, I will normally point out how vacuous truth applies to them, because it's typically not obvious.