Proof by contrapositive, contradiction

Margaret M. Fleck

8 September 2010

This lecture covers proof by contradiction and proof by contrapositive (section 1.6 of Rosen).

1 Announcements

The second quiz will be a week from today (September 15th). It's based on material through the end of this week. Study materials are posted on the 173 Exams web page. If you need extra time or other special arrangements for the quiz, please contact Margaret ASAP.

2 Direct proof: example with two variables

Last class, we saw examples of direct proof. Let's do another example. First, let's define

Definition 1 *An integer n is a perfect square if $n = k^2$ for some integer k.*

And now consider the claim:

Claim 1 *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 Another example with two variables

Here's another example of direct proof that I didn't do in class. Suppose that we want to prove the following

Claim 2 *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.

4 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 3 *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 4 *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 5 *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 6 *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 7 *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 last class.

5 Proof by contrapositive

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

Remember that contructing 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 $\forall x, Q(x) \rightarrow P(x)$ is not equivalent to the original claim.

For example, suppose that we want to prove

Claim 8 *For any integer k, if $3k + 1$ is even, then k is odd.*

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

Claim 9 *For any integer k, if k is not odd, then $3k + 1$ is not even.*

which is equivalent to:

Claim 10 *For any integer k, if k is even, $3k + 1$ is odd.*

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 the proof of our original claim might 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.

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.

6 Another example

Here's another claim where proof by contrapositive is helpful.

Claim 11 *For any integers a and b, $a + b \geq 15$ implies that $a \geq 8$ or $b \geq 8$.*

A proof by contrapositive would look like:

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

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

7 Proof by contradiction

Another way to prove a claim P is to show that its negation $\neg P$ leads to a contradiction. If $\neg P$ leads to a contradiction, then $\neg P$ can't be true, and therefore P must be true. A contradiction can be any statement that is well-known to be false or a set of statements that are obviously inconsistent with one another, e.g. n is odd and n is even, or $x < 2$ and $x > 7$.

Proof by contradiction is typically used to prove claims that a certain type of object cannot exist. The negation of the claim then says that an object of this sort **does** exist. For example:

Claim 12 *There is no largest even integer.*

> Proof: Suppose not. That is, suppose that there were a largest even integer. Let's call it k.
>
> Since k is even, it has the form $2n$, where n is an integer. Consider $k+2$. $k+2 = (2n)+2 = 2(n+1)$. So $k+2$ is even. But $k+2$ is larger than k. This contradicts our assumption that k was the largest even integer. So our original claim must have been true. $\square$.

The proof starts by informing the reader that you're about to use proof by contradiction. The phrase "suppose not" is one traditional way of doing this. Next, you should spell out exactly what the negation of the claim is. Then use mathematical reasoning (e.g. algebra) to work forwards until you deduce some type of contradiction.

8 $\sqrt{2}$ is irrational

One of the best known examples of proof by contradiction is the proof that $\sqrt{2}$ is irrational. This proof, and consequently knowledge of the existence of irrational numbers, apparently dates back to the Greek philosopher Hippasus in the 5th century BC.

We defined a rational number to be a real number that can be written as a fraction $\frac{a}{b}$, where a and b are integers and b is not zero. If a number can be written as such a fraction, it can be written as a fraction in lowest terms, i.e. where a and b have no common factors. If a and b have common factors, it's easy to remove them.

Also, we proved last class that, for any integer k, if k is odd then k^2 is odd. So the contrapositive of this statement must also be true: (*) if k^2 is even then k is even.

Now, we can prove our claim:

Suppose not. That is, suppose that $\sqrt{2}$ were rational.

Then we can write $\sqrt{2}$ as a fraction $\frac{a}{b}$ where a and b are integers with no common factors.

Since $\sqrt{2} = \frac{a}{b}$, $2 = \frac{a^2}{b^2}$. So $2b^2 = a^2$.

By the definition of even, this means a^2 is even. But then a must be even, by (*) above. So $a = 2n$ for some integer n.

If $a = 2n$ and $2b^2 = a^2$, then $2b^2 = 4n^2$. So $b^2 = 2n^2$. This means that b^2 is even, so b must be even.

We now have a contradiction. a and b were chosen not to have any common factors. But they are both even, i.e. they are both divisible by 2.

Because assuming that $\sqrt{2}$ was rational led to a contradiction, it must be the case that $\sqrt{2}$ is irrational. $\square$