Proof by proving the contrapositive

The contrapositive of a conditional statement

What is a contrapositive?

A contrapositive is a statement that's formed from a conditional statement ("If A, then B") and doing the following:

- Swap the hypothesis and conclusion; then
- Negate both the (new) hypothesis and the (new) conclusion.

In notation, the contrapositive of $A \to B$ is $\neg B \to \neg A$.

(The order in which those steps are done is irrelevant.) For example, if the original statement is "If n is an even number, then n^2 is even," then the contrapositive is "If n^2 is not even, then n is not even". The hypothesis and conclusion have been switched and negated. A better way to say it is to note that "not even" means "odd":

> If n^2 is an odd number, then n is odd.

Here are a couple more examples:

Original statement	Contrapositive
If if is not raining, then I am riding my bike.	If I am not riding my bike, then it is raining.
If p is a prime number, then $2^p - 1$ is prime.	If $2^p - 1$ is not a prime number, then p is not prime.

What's so special about contrapositives?

What's special and useful about the contrapositive is that **the contrapositive of a conditional statement is logically equivalent to the original statement**. That is, it has the exact same truth values in all the same conditions.

You can see this in a truth table:

A	B	$\neg B$	$\neg A$	$\neg B \to \neg A$
True	True	False	False	True
True	False	True	False	False
False	True	False	True	True
False	False	True	True	True

The final column has the same truth values in the same rows as the truth table for $A \to B$.

Proofs using the contrapositive

So the contrapositive is just another way of phrasing the original if-then statement. That makes it very useful at times for proofs because **if proving the original conditional statement gets difficult or messy, we can try proving the contrapositive instead**. Since the two statements are logically equivalent, proving one suffices to prove the other.

Example: A proof about squares

Think about proving this statement:

> Conjecture: If n^2 is even, then n is even.

Since this is a conditional statement, we might attempt a proof using a direct proof. This is where you assume the hypothesis is true, and then try to prove the conclusion is true. A table outline for this proof would look like this after the initial setup and then a forward and a backward step. Here we are using the definition of "even" number which says that a number a is even if there exists an integer b such that $a = 2b$. (For example 34 is even because $34 = 2(17)$.)

Statement	Reason
Assume that n^2 is even.	Assuming the hypothesis
There exists an integer k such that $n^2 = 2k$	Definition of "even"
More steps will go here	
There exists an integer m such that $n = 2m$	*Don't know why yet*
Therefore, n is even.	Definition of "even"

So far so good, but that middle row seems very tricky. If I know that n^2 is a multiple of 2, how am I supposed to show that n is a multiple of 2? The only readily apparent way to go from n^2 to n, is to take a square root! But if I start with $n^2 = 2k$ in line 2 and take the square root of both sides, I get $n = \sqrt{2k}$. I've got the n I wanted on the left, but it's not clear at all that expression on the right is an even integer --- or even an integer in the first place.

A direct proof of the original statement, in other words, has hit a dead end. **This is where you would want to consider doing a direct proof of the contrapositive instead**. The contrapositive would say:

> If n is odd, then n^2 is odd.

This already seems much easier. If I know something about n, then finding information about n^2 only involves squaring something --- not something bizarre like a square root.

In fact we did a proof very similar to this in the "Conditional statements and direct proof" tutorial, where we showed that if n is odd, then n^3 is odd. Review that proof; then stop reading this and set up an outline table for the "If n is odd, then n^2 is odd" statement. The only difference is we are squaring, not cubing!

Here's what that ouline might look like:

Statement	Reason
Assume n is odd	Assuming the hypothesis
There exists an integer k such that $n = 2k + 1$.	Definition of "odd"
Therefore $n^2 = (2k+1)^2$	Square both sides
So $n^2 = 4k^2 + 4k + 1$	Algebra
So $n^3 = 2(2k^2 + 2k) + 1$	Factoring out a 2
The number $2k^2 + 2k$ is an integer	Adding and multiplying integers gives another integer
There exists an integer m such that $n^2 = 2m + 1$.	Set m equal to the integer from the previous line
n^3 is odd	Definition of "odd"

The finished proof is so similar to the earlier one that we won't do it here.

> **Lesson:** When trying to prove a conditional statement, if direct proof gets hard or messy, try proving the contrapositive to see if it's any easier.

Example: Proving negated statements

Contrapositives are often useful when proving a statement about something *not* happening, or *not* existing. Here is an example.

But first, a bit of terminology: A number (not necessarily an integer) is *rational* if it can be written as a fraction of two integers. And a number is *irrational* if it cannot be written as a fraction of two integers. For example, $3/4$ is a rational number (because it's a fraction of two integers) and so is $0.11111\ldots$ (because this number is $1/9$). But some numbers that can't be written as fractions of integers include π, $\sqrt{2}$, and e (from calculus). The proof that these numbers are irrational is beyond the scope of the class... for now.

Now consider this conjecture:

> If x^2 is an irrational number, then x is also irrational.

This is a basic if-then statement, so maybe we'd like to try a direct proof. We would start by assuming that x^2 is irrational --- that is, x^2 cannot be written as a fraction of two integers. And we would like to prove that x is irrational.

But right away this is difficult and weird:

- A *forward step* in the proof would be to take the fact that x^2 cannot be written as a fraction of integers and then elaborate on it using some previous knowledge or a calculation. But how would you do that? It's not clear at all.
- Same for a *backward step*.

At this point -- when a direct proof becomes difficult and weird -- it's a good idea to look at the contrapositive. The contrapositive would say:

> If x is not irrational, then x^2 is not irrational.

Since "rational" is the opposite of "irrational", this says:

> If x is a rational number, then x^2 is a rational number.

What about a direct proof of *this* statement? We would assume that x is rational, and want to prove that x^2 is rational. **This is a lot easier** than the direct proof of the original statement because saying that a number *is* rational, gives us a way to rewrite it. It gives, rather than withholds information.

Specifically, if we assume that x is rational, we get some definite knowledge, namely that $x = a/b$ for some pair of integers a and b. Then we can do stuff with that fraction.

Here's what a table outline might look like:

Statement	Reason
Assume that x is a rational number	Assumption of hypothesis (of contrapositive)
x can be written as a fraction of two integers	Definition of "rational"
There exist integers a, b such that $x = a/b$	Putting names on the integers in step 2
Therefore $x^2 = a^2/b^2$	Square both sides
Both a^2 and b^2 are integers	Multiplying an integer to itself gives another integer
Therefore x^2 is rational	Definition of "rational"

In completed form, the proof is short and sweet:

> **Proposition**: If x^2 is an irrational number, then x is also irrational.
> **Proof**: We will prove the contrapositive instead. So assume that x is a rational number. Therefore there are integers a, b such that $x = a/b$. Squaring both sides gives $x^2 = a^2/b^2$. Since a, b are integers, so are a^2 and b^2 because multiplying two integers together gives another integer. Therefore x^2 is a fraction of two integers, meaning that x^2 is rational.

Some notes on this example:

- In the completed proof, notice that the very first item in the proof is to tell the reader what proof method you are employing. This is never a bad idea!
- We've been using some reasoning along the lines of "If you add/subtract/multiply two integers, you get another integer" in our proofs. See line 5 above. The fact that $a + b$, $a - b$, and ab are integers whenever a and b themselves are integers, is called the **closure property** of addition, subtraction, and multiplication of integers. Closure is considered to be a fundamental property of arithmetic that we accept without proof. We refer to such statements -- ones that we accept "on faith" without proof -- as **axioms**. Mathematics is grounded in axioms. For example, geometry is built on five particular axioms such as the notion that there exists only one line that goes between any two distinct points. Axioms are "facts" that we can, and often do use as justifications in proofs of theorems and propositions.