Guide to Indirect Proofs

In Handout #07, we gave some general guidance on how to write mathematical proofs. Over the course of the quarter, we'll introduce several new proof techniques. To help you write proofs using these new techniques, we'll periodically release handouts, like this one, that focus on the specific details of those new techniques.

This handout explores issues specific to the two types of indirect proofs we've explored so far (proofs by contradiction and contrapositive).

Proof by Contrapositive

Many important mathematical statements have the following form:

If P is true, then Q is true.

These statements are called implications. You can prove them in many ways, one of which is the *proof by contrapositive*. In a proof by contrapositive, instead of proving the original implication, you'll prove a different implication. Specifically, instead of proving the statement

If P is true, then Q is true (1)

you'll prove the statement

If Q is false, then P is false. (2)

Statement (2) is called the *contrapositive* of statement (1), hence "proof by contrapositive."

When writing a proof by contrapositive, we recommend structuring the proof as follows:

1. Start off by announcing that you're going to prove the contrapositive of the statement you wish to prove. For example, you could say something like "We will prove the contrapositive of this statement, namely, that ..." or "By contrapositive; we will instead prove that …"

   Don't skip this step! It's important for several reasons. First, it communicates to the reader what they should expect in the proof: you're not going to prove the original statement, and instead that you're going to prove the contrapositive. Second, it forces you to write out the contrapositive of the statement that you're trying to prove, reducing the likelihood that you accidentally take the contrapositive incorrectly.

2. Using any proof technique you'd like, prove the contrapositive of the statement. Often, you'll prove the contrapositive of the statement using a direct proof. Overall, this means that if you want to prove the statement "If P is true, then Q is true," you'll start off by assuming that Q is false and will prove that P is false.

Proof by contrapositive is useful for proving implications, but can also be used to prove certain other results that don't necessarily look like implications. For example, consider the statement

All wizards can perform magic

This statement doesn't look like an implication, but it can actually be thought of as one. Specifically, it's equivalent to the statement

For any choice of x, if x is a wizard, then x can perform magic.

Now, it's clearer that there's an implication here, so if we chose to do so, we could prove it using a proof by contrapositive. That proof might start out like this:

> ***Proof***: We will prove that if x is a wizard, then x can perform magic. To do so, we will instead prove the contrapositive of this statement, namely that if x cannot perform magic, then x is not a wizard. …

Similarly, consider this statement:

No Death Eater is trustworthy.

This again doesn't immediately appear to be an implication, but it can be rewritten as one. Namely, it's equivalent to the statement

For any choice of x, if x is a Death Eater, then x is not trustworthy.

From here, it's clearer what the implication is. We'll leave it as an exercise to determine what the contrapositive of this statement actually is and whether this statement is true. ☺

Proof by Contradiction

One of the most common and most powerful forms of indirect proof is the *proof by contradiction*. In a proof by contradiction, to prove that some statement X is true, you instead assume that X is false, then proceed to derive an impossible statement (a contradiction). This means that X cannot be false, and therefore X has to be true. We recommend writing proofs by contradiction along these lines:

1. Start off by saying that you're going to write a proof by contradiction. For example, you could write "Assume for the sake of contradiction that ..." or "By contradiction; assume that …." Then, explicitly write out the negation of the statement you're trying to prove.

   As with a proof by contrapositive, it's important to actually write out the negation of what you want to prove. This communicates to the reader what assumptions you're making and forces you to put into writing what you believe the negation of the statement is. It therefore makes the proof easier to read and reduces the chances that you accidentally take the negation of the statement incorrectly.

2. Starting with your assumption from part (1), proceed to conclude something impossible, such as that $1 = 0$, that a number is both even and odd, that a number is both rational and irrational, that something belongs to the empty set, that $|S| = |\wp(S)|$, etc.

3. State that you've reached a contradiction and, if it's not obvious, explain why it's a logical contradiction. This explains to the reader why your assumption couldn't possibly be right.

4. Conclude the proof. I commonly say something to the effect of "Therefore, our assumption must have been wrong, so […]." You can put whatever you'd like here as long as it explains why the contradiction you arrived at actually shows that the original assumption was incorrect.

One of the trickiest parts of writing a proof by contradiction is properly assuming the opposite of what you want to prove. When we talk about first-order logic later in a few weeks, you'll see several techniques for negating statements and you'll get a better feel for how to do this in general. For now, though, we recommend that you use the following set of rules and your own intuition.

Here are some very common types of statements and their negations.

If you want to prove this by contradiction...	*...assume this.*
All P's are Q's.	Some P is not a Q.
No P's are Q's.	Some P is a Q.
Some P's are Q's.	All P's are not Q's.
Some P is not a Q.	All P's are Q's.
If P is true, then Q is true.	P is true, but Q is not true.
P is true and Q is true.	P is false, or Q is false, or both are false.
P is true or Q is true, or both are true.	P is false and Q is false.

Two Sample Problems

Here are two sample problems with proofs by contradiction and contrapositive to think about. We've included sample proofs of these results on the next page, and we'd suggest taking a few minutes to work over these problems on your own before looking at our solutions.

Recall from lecture that a real number r is called *rational* if it can be written as a ratio p / q where both p and q are integers and q is nonzero. Every rational number can be written as a ratio where p and q have no common divisors other than ±1.

- *Theorem 1:* If r is a rational number and s is irrational, then $r + s$ is irrational.
- *Theorem 2:* For any real number r, if r^2 is irrational, then r is irrational.

Solutions to Sample Problems

Theorem 1: If r is a rational number and s is irrational, then $r + s$ is irrational.

Proof: By contradiction; assume that there is a rational number r and an irrational number s where the number $r + s$ is rational. Because $r + s$ is rational, we can write it as p / q for some integers p and q where $q \neq 0$. Similarly, since r is rational, we can express it as a / b for some integers a and b where $b \neq 0$.

Notice that $s = (r + s) - r$. Plugging in p / q and a / b from above into this expression and simplifying gives us the following:

$$\begin{aligned} s &= (r + s) - r \\ &= p / q - a / b \\ &= (pb - qa) / qb \end{aligned}$$

From this, we see that we can write s as the ratio of two integers, $pb - qa$ and qb. Moreover, the integer qb is nonzero because neither q nor b is zero. This means that s must be rational. However, this contradicts our earlier assumption that s is irrational.

We have reached a contradiction, so our assumption must have been wrong. Therefore, if r is rational and s is irrational, then $r + s$ is irrational. ■

Theorem 2: For any real number r, if r^2 is irrational, then r is irrational.

Proof: By contrapositive; we'll prove that if r is rational, then r^2 is rational.

Suppose that r is a rational number. That means that we can write $r = p / q$ where p and q are integers and $q \neq 0$. Squaring both sides, we see that $r^2 = p^2 / q^2$. We also note that since q is nonzero, q^2 is also nonzero. Therefore, we can write r^2 as the ratio of two integers (namely, p^2 and q^2) where the denominator (q^2) is nonzero. Consequently, r^2 is rational. ■