Contrapositives

It is about time we discuss another proving technique. Most problems you encounter will not be as straightforward as the ones we saw in the last few discussions.

If there isn't a direct line of sight from start to finish, it is expected that a direct proof wouldn't work. So we look at *indirect proofs*. Any technique that is not a direct proof is naturally indirect, meaning there could be an absolute plethora of them.

So we'll do the next best thing - look at a broad classification of them. And the first one I want to shed light on is *Proof by Contrapositive*.

A little exposition

Those of you who remember your mathematical reasoning know what a contrapositive is. Let me give a refresher regardless.

Consider the statement $p \implies q$. Semantically, this means whenever p is `True`, it *triggers* q to be `True` as well.

In formal logic, it is assumed that given a statement p, *precisely* one of p and $\neg p$ holds. i.e., it cannot be the case that neither holds, and it cannot be the case that both hold. (This may seem like unnecessary pedantic detail and almost a triviality, but trust me, that is not the case).

In the language of Boolean Algebra, we express this as $(p \vee \neg p)$. Since $\neg p$ always has a truth value opposing that of p, *at most* of these can be true. If we further assume that any statement of this form is always true, then *at least* one of them has to be true. Thus precisely one of them is true.

Implication in Boolean Form

Consider a statement $p \implies q$. The implication has a nice property that it is a congruence relation. Meaning, given $p \implies q$, I can conclude, for all statements r, $p \vee r \implies q \vee r$.

Think about this implication. If $p \vee r$ is true, atleast one of p and r must be so. If it is p, then q is true. If it is r, then, well, r is true. Thus $q \vee r$ is true.

Since r can be any statement, choose $r \equiv \neg p$. Thus, given an implication $p \implies q$, it follows that $p \vee r \implies q \vee r$. But $r \equiv \neg p$ so $p \vee \neg p \implies q \vee \neg p$. But $p \vee \neg p$ is always true, thus whenever $p \implies q$ is true, $\neg p \vee q$ is true.

Now suppose $\neg p \vee q$ is true. i.e., atleast one of $\neg p$ and q must be true. If p is true, then $\neg p$ can't be so and thus q must be so. Hence, given $\neg p \vee q$ we may conclude $p \implies q$.

Thus the statements $p \implies q$ and $\neg p \vee q$ imply each other and are thus **logically equivalent**.

What is a Contrapositive?

Think about what we just concluded. The first statement says if p happens, q must happen. The other says if $\neg p$ *doesn't* happen, q must happen. In formal logic, p happening and $\neg p$ not happening are **the** same thing. Thus these statements must be equivalent.

What this allows me to do is make a clever substitution. Start with $(\neg p \vee q) \iff (p \implies q)$

In formal logic, p and $\neg\neg p$ are equivalent statements. So we make this substitution for both p and q in the LHS.

$$(\neg(\neg\neg p) \vee \neg\neg q) \iff (p \implies q)$$

Rewrite the LHS

$$(\neg(\neg q) \vee \neg p) \iff (p \implies q)$$

Now note that if we let $\neg q = p'$ and $\neg p = q'$, the LHS looks like $\neg p' \vee q'$ which is equivalent to $p' \implies q'$. Thus,

$$(p' \implies q') \iff (p \implies q)$$

Substituting back the values of p' and q' we obtain a new logical equivalence,

$$(\neg q \implies \neg p) \iff (p \implies q)$$

The implication on the LHS is called the **contrapositive** of the implication on the RHS, and vice versa. As I have just demonstrated, these two implications are **logically equivalent**. Thus if one wants to prove an implication, it suffices to prove its contrapositive. This is an often handy proving technique that I'll explore in the next discussion.

Not much to say for the closing remarks. I do want to acknowledge that I have played with a **lot** of fire here. Anyone familiar with even intro level logic or model theory would execute me for the absolutely horrendous abuse of notation.

Not to worry, all the things I have stated and all the "proofs" I have written are still mathematically sound. Just that to discuss statements, we need to use a higher kind of statements.

For example, here I've shown an implication holds iff another implication holds. But to prove that they both imply each other, *I've used the same kind of implication that I wanted to prove in the first place.*

The fix to this is to realise that a "higher kind" of implication exists, give it a name and notation, and then work with it. But although it exists, it works **identical** to the usual one. So what I've done above is not incorrect, just a horrible abuse of notation which is a slanderous betrayal akin to no less than some mathematical warcrime.

But again, too much precision and I risk an infodump. More reading for you, more writing for me. This is a win-win right here.