Proofs by Contradiction

Having now completed what comprises about half a course in mathematical logic (lol, not), it is time we get back to what we originally set out to do and discuss another proofwriting technique. I'm picking up the pace a bit here because we've already discussed a lot of nuance I would otherwise point out.

Another Old Friend

I'm sure you are all familiar with the proof that the square root of 2 is irrational. Let's have a look.

Theorem 1. The square root of 2 is irrational.

Proof. *Suppose otherwise* *(Note the language)*
and that there are integers $p, q > 0$ such that

$$\frac{p^2}{q^2} = 2$$

Suppose $\gcd(p, q) = 1$.

Cross-multiplying, we have

$$p^2 = 2q^2$$

This implies p^2 is even, and thus p is even. So

$$p = 2p'$$

Substituting back we get

$$\begin{aligned}(2p')^2 &= 2q^2\\ 4p'^2 &= 2q^2\\ 2p'^2 &= q^2\end{aligned}$$

This implies q^2 is even, and thus q is even.

Thus, p and q are both even, thus $\frac{p}{q}$ fails to be in lowest terms. Contradiction. □

What I want you to observe is the overall structure of the proof as I have presented it.

1. Assume $r = \sqrt{2}$ is rational.
2. Assume r has simplest form $\frac{p}{q}$.
3. Show that the simplest form is, in fact, not simplest (this is direct).
4. ???
5. Profit.

In a proof by contradiction, it is always essential to point out *what exactly is being contradicted.* Here, in the last line, I have stated that $\frac{p}{q}$ being in lowest terms is being contradicted. But it is not clear why that should mean $\sqrt{2}$ being rational is contradicted.

Let's add to our list of assumptions (and facts) the following.

> **Theorem 2.** For every rational number $r = \frac{p}{q}$, there exist unique integers p', q' such that $\gcd(p', q') = 1$ and $r = \frac{p'}{q'}$.

In other words, every rational number has a unique representation in lowest terms. This is a fact that we take for granted, but it is essential to the proof.

Now let's look at our list of facts again.

1. If $r = \sqrt{2}$ is rational, then there exist integers $p, q > 0$ such that $p^2 = 2q^2$.
2. If $p^2 = 2q^2$, then $p'^2 = 2q'^2$ for some integers p', q' with $\gcd(p', q') = 1$. (This is the simplest form of r that we just discussed.)
3. If $p'^2 = 2q'^2$, then p' and q' are both even and thus have $\gcd \neq 1$.

We have established that 3. is true.

Statement 2. is an implication whose consequent is the negation of 3. Since 3 is true, the antecedent of 2 must be false. Thus, $p^2 = 2q^2$ is false.

$p^2 = 2q^2$ is the consequent of 1. Thus, the antecedent of 1 must be false.

The antecedent of 1 is that $\sqrt{2}$ is rational. Thus, $\sqrt{2}$ is irrational.

So between our original contradiction (existence of simplest form) and what we want to show ($\sqrt{2}$ being rational), we need a chain of implications. Contradicting *anything* within this chain of implications is enough to contradict the required statement.

Let me rephrase. Here, we do not need to show that $\sqrt{2}$ is irrational directly. I observe that every rational number has a simplest form. Thus if I show that $\sqrt{2}$ fails to have a simplest form, it couldn't be rational.

To some extent, all proofs by contradiction abuse the contrapositive. If we are able to show the contradiction in its entirety (i.e. if we could've contradicted $\sqrt{2} \in \mathbb{Q}$ directly), it would've just been a proof by contrapositive. Here, we contradict a necessary condition. This is essentially the distinction between a proof by contrapositive and a proof by contradiction.

Cantor's Paradise

As another example, I will now present a proof of Cantor's Theorem.

> **Theorem 3.** (Cantor) Given a nonempty set A and its power set $\mathcal{P}(A)$, there is no bijection $f : A \to \mathcal{P}(A)$

Proof. *Suppose otherwise* and that f is a bijection between A and $\mathcal{P}(A)$.

For a given $a \in A$, a can either fall into $f(a)$, or not fall into $f(a)$.

Let B be the set of all a such that $a \notin f(a)$. In other words,

$$B = \{a \in A \mid a \notin f(a)\}$$

Now, B is a subset of A, and thus $B \in \mathcal{P}(A)$. Since f is a bijection, there exists some $b \in A$ such that $f(b) = B$.

Suppose $b \in B$. Then by definition of B, $b \notin f(b)$. But $f(b) = B$, so $b \notin B$.

Similarly suppose $b \notin B$. Then by definition of B, $b \in f(b)$. But $f(b) = B$, so $b \in B$.

Therefore we get

$$b \in B \iff b \notin B$$

We have thus obtained a contradiction. But what exactly is it we're contradicting? One possible answer is the existence of B, but B is a perfectly well defined set. *(The curious may look up Axiom of Specification)*

Thus the only candidate is the existence of b. If b exists, we get a contradiction. Thus b cannot exist. But b was by definition the pre-image of B.

We have thus constructed a set for which there is no pre-image under f and thus we contradict surjectivity of f. By extension, f fails to be bijective as well. □

This proof is a bit more complicated, but the structure is similar. We assume the existence of a bijection f and then construct a set B that cannot be in the image of f. This contradicts the assumption that f is surjective, and thus we conclude that no such bijection can exist.

Again, I did not have to prove f fails to be a bijection directly, that would've been a full fledged proof by contrapositive. Instead, I contradict a necessary condition – f is surjective – and it takes care of the rest.

You should observe I had to be clever (what I earlier called step 4) and *construct* a set with no pre-image. You have to do this often. You have to be clever and just with the limited info you have about a system, *construct* objects (sequences, sets, etc) with desired properties. Obviously, constructions are often required in existence proofs. Here, the existence of a set without a pre-image.

Conclusion

You should have noticed I'm picking up the pace with these examples, as after all this discussion on logic, you should notice some nuance on your own. If you get stuck, read through the previous sections again and try to reconstruct the presented proofs on your own, that should be helpful.

In the next, I will discuss another proof technique, and revisit an assumption we made in PW-06.