3. Proofs By Contradiction

Lots of if-then statements can be proven using either a Direct Proof or a Contrapositive Proof, but there are also plenty of exceptions to this pattern. Here is perhaps one example.

Example 3.1. *Consider the following proposition:*

Proposition. If $x^2 = 2$ then $x \notin \mathbb{Q}$

*Proving this directly would require us to make a negative statement, namely that the real number x is **not** rational. Our desired conclusion would sound something like this*

$$\text{Desired Conclusion} : \forall\, a, b \in \mathbb{Z},\ x \neq \frac{a}{b}$$

*and this is a difficult fact to establish directly. Would we have to check every possible fraction a/b? (Talk about a long proof.) The contrapositive isn't much better, though; we'd first assume $x \in \mathbb{Q}$ (okay, this part is better), but then we'd also need to confirm that $x^2 \neq 2$ and this gets us back to needing to check **all** possible fractions.*

The square-root-of-2 example above suggests that a third proof-strategy is useful, and this example is a ***classic***. Before addressing it in more detail, let's outline our new proof method:

Proof by Contradiction Outline

Proposition. $P \Rightarrow Q$

Proof. (By Contradiction)

(First Step) Suppose the entire proposition is false
In other words, assume $\neg\,(P \Rightarrow Q) = P \,\wedge\, \neg Q$

(Intermediate Steps) Use facts and definitions about both P and $\neg Q$
to find a contradiction – *any* contradiction.

$\vdots$

(Last Step) End the proof once a contradiction is established. $\Rightarrow\Leftarrow$

The idea behind this strategy is simple and works almost like an aggressive challenge. Imagine that you and your best math-friend are chatting when you tell them "I think $P \Rightarrow Q$ is true," and they reply with "Hmmm, I'm not so certain. Can you explain why?" And instead of directly proving it, you basically say "I ***dare you*** to think its false. If you do that, ***then all of math falls apart***. So you'd better accept this as true!"

There is a big drawback to using a Proof by Contradiction, though: *you never quite know which contradiction you're looking for!* As our outline suggests, you just need any contradiction to show up, any statement that you know cannot possibly be true. For instance, you might end up concluding "$0 = 1$" and this is a contradiction because its negation is (obviously) true.

The good news is that these proofs often give you *way* more to work with in your first steps – the part where you assume stuff. For an if-then, $P \Rightarrow Q$, for example, you get to assume not only P but you *also* get to assume $\neg Q$. The idea is then to squeeze everything you can from these two assumptions, P and $\neg Q$, and combine it with things you already know until you end up with something wrong.

As you will see in the next example, Proofs by Contradiction usually end once the "something wrong" part shows up, and we don't use the regular proof square "□" here. Once the contradiction is established we identify it with the symbol "$\Rightarrow\Leftarrow$" and end the proof.

Example 3.2. *Consider the following proposition:*

Proposition. If $x^2 = 2$ then $x \notin \mathbb{Q}$

Proof. (By Contradiction) *Suppose $x^2 = 2$ and that $x \in \mathbb{Q}$. This means $x = a/b$ for integers $a, b \in \mathbb{Z}$ with $b \neq 0$. We can assume that the fraction a/b is fully reduced, and we can rewrite $x^2 = 2$ as $2b^2 = a^2$. This equation tells us that a^2 is even, and from this it follows that a is even. As a result $a = 2m$ for some $m \in \mathbb{Z}$. Plugging this into our equation yields $2b^2 = 4m^2$ from which it follows that $b^2 = 2m^2$. Therefore b^2 is even, and so b is even, too. Since a and b are both even, the fraction a/b is not fully reduced, and this is a contradiction.* $\Rightarrow\Leftarrow$

You'll likely want or need to re-read the Proof By Contradiction above, very carefully and step-by-step. Its main idea, though, is easy to summarize: "If there were a rational number $x = a/b$ that satisfied $x^2 = 2$, then a/b could never be reduced (its numerator and denominator would always be divisible by 2)."

The astute reader will have noticed that one of the steps used in our proof depended on the following proposition being true:

Proposition. If z^2 is an even integer, then z is even.

Proving this result is an excellent exercise for an up-and-coming mathematician or computer scientist (hint: try a contrapositive proof).

Note. Most other textbooks reword the above example so that there is no conditional statement (at least not an explicit one). If you look at other texts or online videos, you'll likely find it written as

$$\boxed{\textbf{Proposition.}\quad \sqrt{2} \notin \mathbb{Q}}.$$

Accordingly, their Proof by Contradiction will start off by saying "Assume $\sqrt{2} \in \mathbb{Q}$." In fact, Proofs by Contradiction can work for all types of Propositions (not just ones that are written as conditionals $P \Rightarrow Q$):

Proof by Contradiction Outline (general)

Proposition. S

Proof. (By Contradiction)
(First Step) Suppose the entire proposition is false
In other words, assume $\neg S$
(Intermediate Steps) Use facts and definitions about $\neg S$
to find a contradiction – *any* contradiction.
$\vdots$
(Last Step) End the proof once a contradiction is established. $\Rightarrow\Leftarrow$

"Book of Proof" features excellent writing on and examples about this topic. See the following pages and examples:

- Chapter 6, pages 137-142 (6.1 and 6.2) and pages 143-144 (6.4) contain excellent summaries and examples.
- Exercises 1 and 3 (page 144) are good ones to try (solutions are included at the end of the book)

Closing Thoughts and Summary

Our discussions on Direct, Contrapositive and Contradiction Proofs have focused on if-then statements, but, of course, there are a variety of *other* statements one might want to prove, too.

Proving an if-and-only-if statement, one of the form $P \iff Q$, is probably at the top of this "other" to-do list. Thankfully

$$P \iff Q = (P \Rightarrow Q) \wedge (Q \Rightarrow P),$$

and so this task reduces to proving *two* if-then statements. In other words: to prove $P \iff Q$ one first proves $P \Rightarrow Q$ (using any of our three methods), and then *next* proves $Q \Rightarrow P$ (again, using any of our three methods).

We already saw that proving a subset fact like $A \subseteq B$ is the same as proving an if-then statement, but here we should point out that proving a fact about **set equality** – i.e. that $A = B$ – is similar to proving an if-and-only-if:

$$\boxed{A = B \text{ means } A \subseteq B \ \wedge \ B \subseteq A}$$

To prove two sets are equal, then, we will need to handle a statement of the form $P \iff Q$. That is

$$\boxed{\text{To prove } A = B : \text{prove } x \in A \iff x \in B.}$$

Sometimes propositions are existential claims, but these are handled in a fairly straightforward way: write down an object that satisfies the claim – that's right, just one. Even if there are lots that will work, one will always do. Here is a short example of this.

Example 3.3. *Consider the proposition:*

Proposition. $\exists\, S \in \mathcal{P}(\mathbb{N}),\ |S| = 4$

Remember to carefully read (and explore) a proposition before attempting any type of proof. In this case, our proposition is merely claiming that "there exist subsets of naturals that contian four elements." Once we understand this ***existential*** *proposition, a proof is quite natural to write.*

Proof. Consider the set $S = \{2, 0, 206, 12\}$. This is a set of natural numbers and so $S \subseteq \mathbb{N}$. Moreover, S contains four elements, and so $|S| = 4$. □

Proving Propositions that make existential claims *can be* and often *is* this straightforward – and notice our proof does not deserve to be called "direct" or "contrapositive" since the proposition was not phrased as an if-then.

Existential claims can sometimes be proved in less-direct ways; sometimes an explicit object cannot be produced, but its existence can nonetheless be proven. The Intermediate Value Theorem from Calculus, for example, can be used to prove the existence of certain function values, and this is done *without ever writing down the actual inputs that "cause" them*!

An attempt at summarizing our proof strategies is presented in the tables below.

Proposition	Direct	Contrapositive	Contradiction
$P \Rightarrow Q$	Assume P and then Conclude Q	Assume $\neg Q$ and then Conclude $\neg P$	Assume $P \wedge \neg Q$ and then Conclude $\Rightarrow\Leftarrow$
$A \subseteq B$	Assume $a \in A$ and then Conclude $x \in B$	Assume $a \notin B$ and then Conclude $x \notin A$	Assume $\exists\, a \in A - B$ and then Conclude $\Rightarrow\Leftarrow$

Proposition	Step 1	Step 2
$P \iff Q$	Prove $P \Rightarrow Q$	Prove $Q \Rightarrow P$
$A = B$	Prove $A \subseteq B$	Prove $B \subseteq A$
$\exists\, x \in U,\ P(x)$	Find x that works	Show x works