Learning objectives:

□ prove an implication using the contrapositive

□ prove by assuming a contradiction

□ prove an if-and-only-if

One of my favorite stories about proofs involves John F. Nash, who is popularly known for his contributions to game theory. However, there is one particular proof that I find beautiful, which is known as the *isometric embedding theorem*. Very loosely speaking, it relates whether *any* description of a surface can exist in 3d without intersecting itself. Many people tried to prove you could "embed" such a surface ever since the theorem was first postulated in 1873. They came up with special cases and restrictions but no one was able to fully prove the existence of such an embedding. Then John Nash comes along, a young professor at MIT. He learns about this theorem but isn't sure if it's worth his time to prove it. So he decides to go around MIT, telling everyone that he proved the theorem (which he hadn't) but the jaw-dropping reactions he got from his colleagues was enough to motivate him to actually prove the theorem, which he completed in 1956.

John F. Nash

If you're interested, there's a really nice movie starring Russell Crowe called *A Beautiful Mind*. Or you can read the biography by Sylvia Nasr [1].

1 Method # 3: contrapositive

Remember rule # 3 when we studied deduction? Specifically, $p \implies q$ is logically equivalent to $\neg q \implies \neg p$. So if we prove that $\neg q \implies \neg p$, then we are done. Here are the steps:

1. Write: *We prove the contrapositive.*
2. State the contrapositive: $\neg q \implies \neg p$.
3. Start with $\neg q$.
4. Proceed as in Method #1.

Example 1:

If a^2 is not divisible by 4, then a is odd.

Proof. We use the contrapositive. Let $a \in \mathbb{Z}$. Suppose a is even. Then $\exists\, k \in \mathbb{Z}$: $a = 2k$. This means $a^2 = 4k^2$. Since a is an integer, $4|a^2$. □

Example 2:

If x is irrational, then $\sqrt{x}$ is also irrational.

Proof. We use the contrapositive. Let $\sqrt{x}$ be a rational number. This means $\sqrt{x} = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ by the definition of a rational number. Then $x = \frac{m^2}{n^2} = \frac{a}{b}$ for $a, b \in \mathbb{Z}$. Therefore, x is also rational. □

2 Method # 4: proof by contradiction

So far, we've seen a variety of methods for proving implications: $p \implies q$. But say you just want to prove that a proposition p is true. You might be able to reason that p is true directly (as in the last lecture), but we'll now look at another useful method: *proof by contradiction*. The main idea is to suppose the proposition p is false, and then come up with a contradiction. Thus, p must be true. Here are the steps:

- Write *We use a proof by contradiction.*
- Write *Suppose the proposition p is false.*
- Deduce something known to be false (the contradiction).
- Write *This is a contradiction. Therefore, p must be true.*

Let's practice:

Example 3:
Prove that $\sqrt{2}$ is irrational.

Solution:
Proof. We use a proof by contradiction. Let p be the proposition that $\sqrt{2}$ is irrational. Suppose this claim is false, which means $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ for some $a, b \in \mathbb{Z}$. Without loss of generality, assume that the fraction a/b is simplified in lowest terms. Then $a^2 = 2b^2$ which means a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. This means $a^2 = 4k^2 = 2b^2$, so $b^2 = 2k^2$, meaning b is also even. We said a/b was simplified in lowest terms, but if a and b are both even, then this is a contradiction, because we can simplify it further. Thus, $\sqrt{2}$ is irrational. □

Another example?

Suppose there are n holes in the sand (where a clam might be) and greater than n sandpipers. Prove that at least two pipers will go for the same clam. *This is actually known as the pigeonhole principle.*

Example 4:
Prove $\neg\exists x, y \in \mathbb{Z}$ such that $x^2 = 4y + 2$.

Solution:
Proof. We use a proof by contradiction. Assume there exists $x, y \in \mathbb{Z}$ such that $x^2 = 4y + 2$. Then $x^2 = 2(2y + 1) = (2m)^2$ $(m \in \mathbb{Z})$ is even, so x is even. Solving for y yields

$$\begin{aligned} y &= \frac{4m^2 - 2}{4} \\ &= m^2 - \frac{1}{2} \end{aligned}$$

Since $m \in \mathbb{Z}$, this means $y \notin \mathbb{Z}$, which is a contradiction. □

Example 5:
For every $x \in [\pi/2, \pi]$, $\sin x - \cos x \geq 1$.
Proof. We use a proof by contradiction. Suppose $\sin x - \cos x < 1$ for $x \in [\pi/2, \pi]$. Squaring both sides gives $\sin^2 x + \cos^2 x - 2\sin x \cos x < 1$, which leads to $-2\sin x \cos x < 0$. We know that $-1 \leq \cos x \leq 0$ and $0 \leq \sin x \leq 1$ for $x \in [\pi/2, \pi]$. However, if $\sin x$ is always positive and $\cos x$ is always negative in the domain considered, then $-2\cos x \sin x$ is always positive. This is a contradiction, so $\sin x - \cos x \geq 1$ for $x \in [\pi/2, \pi]$. □

3 Proving an "iff"

In order to prove statements involving if-and-only-if, recall that the biconditional $p \iff q$ is logically equivalent to $(p \implies q) \wedge (q \implies p)$. Therefore, we need to prove both implications. Here are the steps:

1. Write *We prove p implies q and vice-versa.*
2. Write *First, we show p implies q*, then pick any method to prove $p \implies q$.
3. Write *Next, we show q implies p*, then pick any method to prove $q \implies p$.

Here is a nice example that combines some of the techniques we have learned so far:

Example 6:
Suppose $a \in \mathbb{Z}$. Prove that $14|a$ if and only if $7|a$ and $2|a$.

Solution:
We prove $14|a$ implies $7|a$ and $2|a$ and vice-versa.

First we prove that if $14|a$, then $7|a$ and $2|a$. Suppose $14|a$. Then, $a = 14k$ for some $k \in \mathbb{Z}$. This means $a = 7(2k) = 7m$ for some $m \in \mathbb{Z}$. This also means $a = 2(7k) = 2n$ for some $n \in \mathbb{Z}$. Therefore, both 2 and 7 divide a.

Next we prove that if $2|a$ and $7|a$, then $14|a$. Suppose $2|a$ and $7|a$. Then (1) $a = 2k$ for some $k \in \mathbb{Z}$ and (2) $a = 7n$ for some integer $n \in \mathbb{Z}$. By (1), a is even, which means $7n$ is even. This means that n is even and can be written as $n = 2m$ for some $m \in \mathbb{Z}$. So $a = 7n = 7(2m) = 14m$, therefore, $14|a$.

4 Existence proofs

Just like John Nash, sometimes you need to prove that something exists, or doesn't exist. In general, there are two techniques you can use:

- Proof by Example: useful if you have statements like *Prove there exists ....*
- Proof by Counterexample: useful if you have statements like *Prove not all ....*

Ultimately, both of these reduce down to finding an example in which you want to prove the existence to support or refute a proposition. Be very careful, it is wrong to use an example to prove a "for all" proposition!

"not all" versus "there is"?

Remember how we negate quantifiers:

$$\neg\forall x, p(x) \equiv \exists x\colon \neg p(x)$$

Example 7:
Which could be proved using an example?

(a) $\forall x \in S,\ p(x)$

(b) $\forall x \in S,\ \neg p(x)$

(c) $\neg\exists x \in S\colon\ p(x)$

(d) $\neg\forall x \in S, p(x)$

Solution:
We can use an example to prove (d) only. De Morgan's rules on (d) lead to $\neg\forall x \in S,\ p(x) \equiv \exists x \in S\colon\ p(x)$. For all other options (a), (b) and (c), a single example is not enough.

References

[1] S. Nasar. *A Beautiful Mind: A Biography of John Forbes Nash, Jr.* 1998 (cit. on p. 1).