Learning objectives:
- ☐ prove an implication directly
- ☐ divide a proof into *cases*

Last time, we talked about deduction, where we looked at two strategies for deducing a conclusion from a set of premises: (1) using a truth table and (2) using rules of inference to reason through the premises. Today, we'll use our reasoning skills to start proving propositions, lemmas and theorems. The structure of the proofs we will see today is very similar to what we saw with deduction. Ultimately, we want you to write rock-solid proofs, unlike the one below:

Example 1:
What's wrong with this proof?

$$1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \left(\sqrt{-1}\right)^2 = -1$$

Solution:
The problem is that $\sqrt{xy} \neq \sqrt{x}\sqrt{y}$ unless both x and y are non-negative, which is not true.

1 Structure

The structure of a proof is very similar to what we have seen so far. However, you generally will not write out all your steps in tabular form like we did with deduction. Instead, you will write complete sentences, interspersed with equations, to describe the steps in your proof.

Here are some guidelines for writing proofs (adapted from *Mathematics for Computer Science*[1]):

- **State your plan:** Specify which proof method you are using. Use the personal pronoun *We* to start off this description. For example, *We use the contrapositive* or *We argue by contradiction*.
- **Introduce your variables:** Remember to define all variables you use in your proof. Start these sentences off with something like *Let x be an integer* or *There exists some y such that ...*.
- **State your assumptions:** Your assumptions might be incorrect, but your proof might logically follow. You'll still get a lot of credit for your proof (in this class). Start these sentences off with *Suppose ...* or *Assume ...*.

What if I have equations?

You'll often have equations that will complement the textual description of your proof. Make sure that the equals sign is left-aligned when simplifying your expressions. Don't write

$$A = B = C = D$$

unless you are embedding the equations within your sentences. If you are separating your text and equations, then you should instead write

$$\begin{aligned} A &= B \\ &= C \\ &= D. \end{aligned}$$

For example,

$$\begin{aligned} x^3 + 2x^2 + x &= x(x^2 + 2x + 1) \\ &= x(x+1)^2 \end{aligned}$$

- **A proof is an essay, not a calculation:** I know, this is a math class. But proofs involve complete sentences.
- **Revise and simplify:** Ask yourself if you are conveying all the information in as little space (and words) as possible.
- **Finish:** Don't forget to write a concluding sentence (*Therefore*, *As a result*, *Thus*) that re-iterates what you are trying to prove (and also don't forget the little box).

2 Proving an "if"

Here, we are looking to prove statements like *if* p *then* q. Recall the truth table for the implication $p \implies q$, reproduced on the right.

You don't need to worry about the cases in which p is false, but q is true, because we want to prove that p being true leads to q being true. There are a few methods that are useful for proving an implication: $p \implies q$.

Truth table for if ($\implies$)

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

2.1 Method # 1: massage

There's nothing special here, but all the other methods depend on it, so we might as well give it a name. The idea is to start with your statement p and massage your equations until you prove what you're looking for. This will involve bringing in other information, such as your premises, or other mathematical identities. Here are the steps:

1. Write: Assume p or Suppose p, then state p.
2. Explain, manipulate and play around (following the guidelines).
3. Therefore, q.

There is a lot of art in Step 2, where you need to manipulate the information you have, whether they be premises or other mathematical identities. It's a good idea to use scrap paper (separate from your proof).

Example 2:
If $a|b$ and $b|c$ then $a|c$ (for integers a, b, c). Note: The vertical bar you see here refers to *divides*. So $a|b$ reads: *a divides b*, which means that $b/a \in \mathbb{Z}$.
Proof. Let $a, b, c \in \mathbb{Z}$. Assume $a|b$ and $b|c$. This means $\exists m, n \in \mathbb{Z}$ such that $b = am$ and $c = bn$. Then $c = bn = (am)n = a(mn) = a(k)$ for some $k \in \mathbb{Z}$. Therefore, $c = ak$ for k an integer, and $a|c$. □

Example 3:
If n is an odd integer, then $n^2 + 3n + 5$ is odd.
Proof. Let n be an odd integer, $n = 2k + 1$, $k \in \mathbb{Z}$. Then

$$\begin{aligned} n^2 + 3n + 5 &= (2k+1)^2 + 3(2k+1) + 5 \\ &= 4k^2 + 4k + 1 + 6k + 3 + 5 \\ &= 4k^2 + 10k + 9 \\ &= 2(2k^2 + 5k + 4) + 1 \\ &= 2m + 1 \end{aligned}$$

for some $m \in \mathbb{Z}$. Therefore $n^2 + 3n + 5$ is odd. □

The last example is a bit tricky at first, but remember that we were trying to show $n^2 + 3n + 5$ is odd. This means that we want to massage it into something that looks like $2m + 1$ for some integer m.

How do I represent even or odd numbers?

You will often encounter problems that involve even and/or odd numbers. Here is a trick to represent them. If n is an even integer, we can write it as

$$n = 2k, \quad k \in \mathbb{Z}.$$

Similarly, if n is an odd number, we can write it as

$$n = 2k + 1, \quad k \in \mathbb{Z}.$$

2.2 Method # 2: split into cases

Sometimes, it's easier to split the domain of your variables into separate cases, and prove each case separately. It's important to be explicit about which case you are proving. For example, if you are proving something involving $\forall x \in \mathbb{Z}$, you might split into: **Case 1:** $x < 0$ or **Case 2:** $x > 0$ or **Case 3:** $x = 0$. Make sure you consider all cases!

Example 4:
If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$ is a multiple of 4.

Solution:
Proof. Suppose $n \in \mathbb{N}$. We consider the cases when n is even or odd.

Case 1: Let n be a positive even integer. Then $n = 2k$ for $k \in \mathbb{N}$. This means $1 + (-1)^{2k}(2(2k) - 1) = 4k$ which is a multiple of 4.

Case 2: Let n be a positive odd integer. Then $n = 2k + 1$ for $k \in \mathbb{N}$. This means $1 + (-1)^{2k+1}(2(2k + 1) - 1) = -4k$ which is a multiple of 4.

□

Example 5:

If $n \in \mathbb{Z}$ then $n^2 + 3n + 4$ is even.

Solution:

We are told that n is any integer, so the trick here is to split into cases by considering the case when n is even and then when n is odd.

Proof. We consider two cases.

Case 1: Let n be an even integer. Then $n = 2k$ for some $k \in \mathbb{Z}$. This means

$$\begin{aligned} n^2 + 3n + 4 &= (2k)^2 + 3(2k) + 4 \\ &= 4k^2 + 6k + 4 \\ &= 2(2k^2 + 3k + 2) \\ &= 2m \end{aligned}$$

for some $m \in \mathbb{Z}$. Therefore, $n^2 + 3n + 4$ is even when n is even.

Case 2: Let n be an odd integer. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. This means

$$\begin{aligned} n^2 + 3n + 4 &= (2k+1)^2 + 3(2k+1) + 4 \\ &= 4k^2 + 4k + 1 + 6k + 3 + 4 \\ &= 4k^2 + 10k + 8 \\ &= 2(2k^2 + 5k + 4) \\ &= 2m \end{aligned}$$

for some $m \in \mathbb{Z}$. Therefore, $n^2 + 3n + 4$ is even when n is odd.

□

Do I have to use the same proof method for each case?

Good question! You are free to mix and match whichever method is easiest to prove a particular case. This could be the ones we've seen so far (direct) or the ones we will see soon (contrapositive, contradiction, induction).

Example 6:

For any integer n, $n^3 - n$ is even.

Solution:

Proof. We consider two cases.

Case 1: Let n be an even integer. Then $n = 2k$ for some $k \in \mathbb{Z}$. This means

$$\begin{aligned} n^3 - n &= (2k)^3 - 2k \\ &= 8k^3 - 2k \\ &= 2(4k^3 - 2k) \\ &= 2m \end{aligned}$$

for some $m \in \mathbb{Z}$. Therefore, $n^3 - 3n$ is even when n is even.

Case 2: Let n be an odd integer. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. This means

$$\begin{aligned} n^3 - n &= (2k+1)^3 - (2k+1) \\ &= 8k^3 + 12k^2 + 6k + 1 - 2k - 1 \\ &= 8k^3 + 12k^2 + 4k \\ &= 2(4k^3 + 6k^2 + 2k) \\ &= 2m \end{aligned}$$

for some $m \in \mathbb{Z}$. Therefore, $n^3 - n$ is even when n is odd.

□

Example 7:
Suppose a, b, c are positive integers and abc is even. Show that $a+b+c \geq 4$.

Solution:
Before proving $a+b+c \geq 4$, we need a lemma.

Lemma 1. *For positive integers a, b, c. If abc is even, then one of a, b or c is even.*

Proof. Suppose abc is even. Then $abc = 2k$ for some $k \in \mathbb{N}$. Decompose $k = k_1k_2k_3$. Then $abc = (2k_1)k_2k_3 = k_1(2k_2)k_3 = k_1k_2(2k_3)$. Therefore, either a, b or c is even. □

Now we can prove the actual proposition.

Proof. Let a, b, c be positive integers. Since abc is even, at least one of a, b, c is even by Lemma 1. Without loss of generality, assume a is even. Then $a \geq 2$ and $a+b+c \geq 2+1+1 = 4$. □

Convince yourself that splitting into the three cases: **Case 1:** a is even, **Case 2:** b is even and **Case 3:** c is even, uses the same logic sequence in the proof.

I feel like I'm doing the same thing for all my cases.

If you feel like you're repeating the same logic, you may use the term *Without loss of generality* or (WLOG) and only prove one of the cases. Be very careful here! When using the term WLOG, make sure the logic truly is the same for all cases!

References

[1] E. Lehman, F. T. Leighton, and A. Meyer. *Mathematics for Computer Science*. 2018 (cit. on p. 1).