Math 321: more about proofs

Kameryn J Williams

University of Hawaiʻi at Mānoa

Fall 2020

Last time

- Last time we talked about proof strategies involving if-then statements.
- Now let's talk about proof strategies involving negations ($\neg$).

How to prove a negative?

- One sometimes hears the commonsensical claim that “You can’t prove a negative”.

How to prove a negative?

- One sometimes hears the commonsensical claim that "You can't prove a negative".
- At least if one confines that to mathematics, that statement is wrong.
- One of the main methods at our disposal is known as proof by contradiction or *reductio ad absurdum*.

Reductio ad absurdum

- To prove $\neg P$: Assume P as a premise and derive a contradiction—a statement that can never be true.
- Often the contradiction is of the form $Q \wedge \neg Q$.

Reductio ad absurdum

- To prove $\neg P$: Assume P as a premise and derive a contradiction—a statement that can never be true.
- Often the contradiction is of the form $Q \wedge \neg Q$.

We can also represent this in terms of what our knowns and goals are:

knowns	goals
$\vdots$	$\neg P$

gets trasformed into

knowns	goals
P	$Q \wedge \neg Q$
$\vdots$	

Reductio ad absurdum

- To prove $\neg P$: Assume P as a premise and derive a contradiction—a statement that can never be true.
- Often the contradiction is of the form $Q \wedge \neg Q$.

We can also represent this in terms of what our knowns and goals are:

knowns	goals
$\vdots$	$\neg P$

gets trasformed into

knowns	goals
P	$Q \wedge \neg Q$
$\vdots$	

A tricky part: what Q do we want to use? This is often not obvious. My suggestion: just start working, and see what pops up. You can stumble upon a contradiction without knowing in advance what specifically you are looking for.

A famous example

Theorem

$\sqrt{2}$ *is irrational.*

A famous example

Theorem

$\sqrt{2}$ is irrational.

- Saying $\sqrt{2}$ is irrational is exactly saying that $\sqrt{2}$ is not rational, i.e. that $\sqrt{2}$ cannot be written in the form p/q for integers p and q.
- So to prove this by contradiction, we want to assume that $\sqrt{2} = p/q$ for some integers p and q, and then derive a contradiction. How might we do this?

A famous example

Theorem

$\sqrt{2}$ is irrational.

- Saying $\sqrt{2}$ is irrational is exactly saying that $\sqrt{2}$ is not rational, i.e. that $\sqrt{2}$ cannot be written in the form p/q for integers p and q.
- So to prove this by contradiction, we want to assume that $\sqrt{2} = p/q$ for some integers p and q, and then derive a contradiction. How might we do this?
- We only have a limited amount of information, so let's just try to use it.

$$\sqrt{2} = \frac{p}{q} \quad \Rightarrow \quad 2 = \frac{p^2}{q^2} \quad \Rightarrow \quad p^2 = 2q^2.$$

A famous example

Theorem

$\sqrt{2}$ is irrational.

- Saying $\sqrt{2}$ is irrational is exactly saying that $\sqrt{2}$ is not rational, i.e. that $\sqrt{2}$ cannot be written in the form p/q for integers p and q.
- So to prove this by contradiction, we want to assume that $\sqrt{2} = p/q$ for some integers p and q, and then derive a contradiction. How might we do this?
- We only have a limited amount of information, so let's just try to use it.

$$\sqrt{2} = \frac{p}{q} \quad \Rightarrow \quad 2 = \frac{p^2}{q^2} \quad \Rightarrow \quad p^2 = 2q^2.$$

- So we have seen that p^2 must be even, and so p must also be even, because $a \in \mathbb{Z}$ is even iff $a = 2k$ for some integer k.

A famous example

Theorem

$\sqrt{2}$ *is irrational.*

- We assumed toward a contradiction that $\sqrt{2} = p/q$, and have figured out that p is even.

A famous example

Theorem

$\sqrt{2}$ *is irrational.*

- We assumed toward a contradiction that $\sqrt{2} = p/q$, and have figured out that p is even.
- But then we can also conclude that q^2 and q must be even: If $p = 2k$ then

$$2q^2 = p^2 = 4k^2 \quad \Rightarrow \quad q^2 = 2k^2.$$

A famous example

Theorem

$\sqrt{2}$ is irrational.

- We assumed toward a contradiction that $\sqrt{2} = p/q$, and have figured out that p is even.
- But then we can also conclude that q^2 and q must be even: If $p = 2k$ then
$$2q^2 = p^2 = 4k^2 \quad \Rightarrow \quad q^2 = 2k^2.$$
- Why is this a problem? It means that p and q must have a common factor, but we can always write a fraction in reduced form so the denominator and numerator don't have a common factor. This is our desired contradiction.

Let's write this up now

Theorem

$\sqrt{2}$ is irrational.

Proof.

Suppose toward a contradiction that $\sqrt{2}$ is rational.* Then we have that $\sqrt{2} = p/q$ for some integers p and q with no common factors. Doing some algebra then yields that $p^2 = 2q^2$ and so p^2 is even. Then p is also even. This means that $p = 2k$ for some integer k and so substituting $p = 2k$ into the earlier equation gives $q^2 = 2k^2$. Thus, q^2 and hence also q are even. But then 2 is a common factor of p and q, contradicting that they have no common factor. □

* Phrases like "Suppose toward a contradiction that P" signify to the reader that we are going to prove $\neg P$ by contradiction.

Proving positive statements by contradiction

- You can also prove positive statements by contradiction.
- P is equivalent to $\neg\neg P$, and you can prove $\neg\neg P$ by contradiction.
- Namely, you assume $\neg P$ and derive a contradiction.

$\neg$'s and $\rightarrow$'s together

- Combining facts about $\neg$ and $\rightarrow$ gives us another method to prove if-then statements.
- $P \rightarrow Q$ is equivalent to its contrapositive $\neg Q \rightarrow \neg P$.
- To prove the contrapositive, we assume $\neg Q$ and try to derive $\neg P$.
- This is called, naturally enough, proof by contrapositive.

$\neg$'s and $\rightarrow$'s together

- Combining facts about $\neg$ and $\rightarrow$ gives us another method to prove if-then statements.
- $P \rightarrow Q$ is equivalent to its contrapositive $\neg Q \rightarrow \neg P$.
- To prove the contrapositive, we assume $\neg Q$ and try to derive $\neg P$.
- This is called, naturally enough, proof by contrapositive.
- This also gives us another way to use if-then statements as knowns.
- If we know both $P \rightarrow Q$ and $\neg Q$ then we can conclude $\neg P$.
- This method is known as *modus tollens*.