Proofs

Def A proof is a finite list of statements, each of which is logically implied by the previous statement, used to establish the truth of some proposition. By one of a short list of rules of logic.

Good: High level of certainty that the statement is correct

Bad: Can only prove tautologies

How do you confirm your beliefs are correct?

Math Proof

Science Experiment
**Def. A proof** is a finite list of statements, each of which is logically implied by the previous statement, which is used to establish the truth of some proposition.

→ Not really! Proofs are written for humans.

→ A formal proof written using the Lean proof assistant

\[ \forall a, b \in \mathbb{Z}, |a+b| \leq |a|+|b| \]

My advice: Imagine your proof is being read by a skeptical friend who questions every statement you make.

For now: Err on the side of being too formal.
2. How to prove things

How you should prove a proposition depends on the logical structure of the proposition.

<table>
<thead>
<tr>
<th>Structure</th>
<th>How to prove it</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P \land Q$</td>
<td>Prove $P$ and prove $Q$</td>
</tr>
<tr>
<td>$P \Rightarrow Q$</td>
<td>Assume $P$ is true and prove $Q$</td>
</tr>
<tr>
<td>$P \iff Q$</td>
<td>Prove $P \Rightarrow Q$ and $Q \Rightarrow P$</td>
</tr>
<tr>
<td>$\exists x \in S, P(x)$</td>
<td>Provide some $a \in S$ and prove $P(a)$</td>
</tr>
<tr>
<td>$\forall x \in S, P(x)$</td>
<td>Let $a$ be an arbitrary element of $S$ and prove $P(a)$</td>
</tr>
</tbody>
</table>

Can also replace the proposition to be proved with a logically equivalent proposition that has a different structure.

Example: Replace $P \Rightarrow Q$ with $\neg Q \Rightarrow \neg P$
A direct proof follows the structure of the original proposition.

**Example**

**Theorem** For every natural number, there is a natural number greater than it. \[ \forall n \in \mathbb{N}, \exists m \in \mathbb{N} \ (n < m) \]

**Proof** Let \( n \) be a natural number. Observe that \( n+1 \) is a natural number which is greater than \( n \). To be totally rigorous, should show that \( n+1 > n \). Not necessary in this class.

**Reminder**

\[ \forall x \in S, P(x) \] Let \( a \) be an arbitrary element of \( S \) and prove \( P(a) \)

\[ \exists x \in S, P(x) \] Provide some \( a \in S \) and prove \( P(a) \)
Def: Given $n, m \in \mathbb{Z}$, we say $n$ divides $m$, written $n \mid m$, if there is some $k \in \mathbb{Z}$ such that $m = nk$.

Example: $2 \mid 26$ because $26 = 2 \cdot 13$. $3 \nmid 26$.

Then: For all $a, b, n \in \mathbb{Z}$, if $n \mid a$ and $n \mid b$ then $n \mid (a-b)$.

\[
\forall a \in \mathbb{Z} \forall b \in \mathbb{Z} \forall n \in \mathbb{Z} \left( (n \mid a \land n \mid b) \Rightarrow n \mid (a-b) \right)
\]

Proof: Let $a, b,$ and $n$ be integers and assume $n \mid a$ and $n \mid b$. So by definition, there are $k, l \in \mathbb{Z}$ such that $a = nk$ and $b = nl$. Therefore

\[
a - b = nk - nl = n(k - l).
\]

So by definition, $n \mid (a-b)$.

Reminder: $P \Rightarrow Q$. Assume $P$ is true and prove $Q$.

One lesson: Definitions give you things (e.g., $k$ and $l$).
4 Proof by contraposition

A proof by contraposition proves an implication $P \Rightarrow Q$ by proving its contrapositive, $\neg Q \Rightarrow \neg P$.

Fact: $n \in \mathbb{Z}$ is even iff $\exists k \in \mathbb{Z} (n = 2k)$ and odd iff $\exists k \in \mathbb{Z} (n = 2k + 1)$.

Example

For every $n \in \mathbb{Z}$, if $n^2$ is even then so is $n$.

If $n \in \mathbb{Z}$ ("$n^2$ is even" $\Rightarrow$ "$n$ is even")

Direct proof? $n^2$ even $\Rightarrow \exists k (n^2 = 2k) \Rightarrow n = \sqrt{2k} \Rightarrow ??$

Proof

Let $n$ be an integer. We will show that if $n$ is odd then $n^2$ is odd. Assume $n$ is odd. So there is some $k \in \mathbb{Z}$ such that $n = 2k + 1$. Thus

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

So $n^2$ is odd.
Proof by contraposition is especially useful if you are trying to prove something of the form $(\forall x \, P(x)) \Rightarrow (\forall y \, Q(y))$.

$\forall x \, P(x) \Rightarrow \forall y \, Q(y) \equiv \neg (\forall y \, Q(y)) \Rightarrow \neg (\forall x \, P(x))$

$\equiv (\exists y \, \neg Q(y)) \Rightarrow (\exists x \, \neg P(x))$

**Definition**: A real number $r$ is **rational** if there are $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $r = \frac{p}{q}$. Otherwise, $r$ is **irrational**.

Thus, for every real number $a$, if $a$ is irrational then so is $3a$.

For every real number $a$, if $a$ is irrational then so is $3a$.

Proof: Let $a$ be a real number. We will show that if $3a$ is rational, then so is $a$. Assume $3a$ is rational. So there are $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $3a = \frac{p}{q}$.

Dividing by 3 gives us $a = \frac{p}{3q}$.

So $a$ is rational.
(5) Proof by contradiction

A proof by contradiction proves a proposition $P$ by assuming $\neg P$ and proving both $R$ and $\neg R$ for some proposition $R$.

Comment: Why does this work?

$$\neg P \Rightarrow (R \land \neg R) \equiv \neg P \Rightarrow F \\
\equiv P$$

<table>
<thead>
<tr>
<th>$P$</th>
<th>$\neg P$</th>
<th>$F$</th>
<th>$\neg P \Rightarrow F$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
</tbody>
</table>

Useful for proving non-existence statements

= statements of the form $\forall x \neg P(x) \equiv \neg \exists x P(x)$
**Def** A natural number is prime if it is greater than 1 and has no divisors other than 1 and itself.

**Example** 2, 3, 5, 7, 11, ... prime, 15 = 3 · 5 not prime

**Fact** Every natural number greater than 1 has a prime divisor → tomorrow we will see how to prove this.

**Thm** (Euclid?) There are infinitely many prime numbers.

**Proof** Suppose for contradiction that there are only finitely many primes, $p_1, p_2, ..., p_n$. Define

$q = p_1 · p_2 · ... · p_n$.

Note that $q + 1 > 1$, so by the fact, $q + 1$ has a prime divisor, $p$. This $p$ must be equal to $p_i$ for some $i ≤ n$, so we have

$p | q$ and $p | (q + 1) \implies p | (q + 1 - q)$

$\implies p | 1$

But the only number that divides 1 is 1 itself, so $p$ is not prime.
Fact: If $a \in \mathbb{Q}$ then there are $p, q \in \mathbb{Z}$ such that $q \neq 0$, $a = \frac{p}{q}$ and $p$ and $q$ share no common factors.

Thus $\sqrt{2}$ is irrational.

**Example:** Suppose for contradiction $\sqrt{2}$ is rational. So by the fact, there are $p, q \in \mathbb{Z}$ such that $q \neq 0$, $p$ and $q$ share no common factors and $\sqrt{2} = \frac{p}{q}$.

Hence,

$$2 = (\sqrt{2})^2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$$

$$\Rightarrow 2q^2 = p^2.$$ 

Therefore $p^2$ is even, so by a thm from before, $p$ is even. So by def., there is $k \in \mathbb{Z}$ such that $p = 2k$.

Hence

$$2q^2 = p^2 = (2k)^2 = 4k^2 = 2(2k^2)$$

Dividing both sides by 2 gives $q^2 = 2k^2$. By the same reasoning as before, $q$ is even. This contradicts the fact that $p$ and $q$ share no common factors.
Proof by Cases

A proof by cases proves a proposition \( P \) by splitting into several cases, at least one of which must be true.

I.e. have propositions \( R_1, R_2, \ldots, R_n \) know \( R_1 \lor R_2 \lor \ldots \lor R_n \) is true

Enough to show \((R_1 \Rightarrow P) \land (R_2 \Rightarrow P) \land \ldots \land (R_n \Rightarrow P)\)

Thm There are irrational numbers \( a \) and \( b \) such that \( a^b \) is rational.

\[ \exists a, b \in \mathbb{R} \quad (a \notin \mathbb{Q} \land b \notin \mathbb{Q} \land a^b \in \mathbb{Q}) \]

How to find \( a \) and \( b \)?

Example

Either \( \sqrt{2}^\sqrt{2} \) is rational or it is not.

Case 1: Assume \( \sqrt{2}^\sqrt{2} \) is rational. Then we are done because \( \sqrt{2} \) is irrational.

Case 2: Assume \( \sqrt{2}^\sqrt{2} \) is irrational. Then

\[ (\sqrt{2}^\sqrt{2})^\sqrt{2} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2. \]
Sometimes proof by cases is really cool, other times...

Fact: For every natural number $n$, there is a natural number $k$ such that one of the following holds:

- $n = 3k$
- $n = 3k + 1$
- $n = 3k + 2$

Theorem: For all $n \in \mathbb{N}$, $3 \mid (n^3 - n)$

Proof:

Let $n$ be a natural number and let $K$ be as in the fact above.

Case 1: $n = 3k$

$$n^3 - n = (3k)^3 - 3k = 27k^3 - 3k = 3(9k^3 - k)$$

Case 2: $n = 3k + 1$

$$n^3 - n = (3k+1)^3 - (3k+1) = 27k^3 + 27k^2 + 9k + 1 - 3k - 1 = 3(9k^3 + 9k^2 + 2k)$$

Case 3: $n = 3k + 2$

$$n^3 - n = (3k+2)^3 - (3k+2) = 27k^3 + 54k^2 + 36k + 8 - 3k - 2 = 27k^3 + 54k^2 + 33k + 6 = 3(9k^3 + 18k^2 + 11k + 2)$$

next week, we'll see another way to do this
<table>
<thead>
<tr>
<th><strong>Summary</strong></th>
</tr>
</thead>
</table>
| **Direct proof** | **Goal:** $P \implies Q$
| **Method:** Assume $P$
| **Conclude:** $Q$ |
| **Proof by contraposition** | **Goal:** $P \implies Q$
| **Method:** Prove $\neg Q \implies \neg P$ |
| **Proof by contradiction** | **Goal:** $P$
| **Method:** Assume $\neg P$
| Prove $R$
| Prove $\neg R$ |
| **Proof by cases** | **Goal:** $P$
| **Method:** Show $R_1, \ldots, R_n$ is true
| ;
| Show $R_1 \implies P$
| Show $R_n \implies P$ |
Other comments

Today I wrote full proofs.

Usually: proof sketches ← proofs you write on homework should be more complete than proofs in lecture/discussion.

Problem solving: think creatively, take leaps of faith, experiment, etc.

Proof writing: every step must be justified and follow logically from previous steps.

A common pattern:

1. Think about problem.
2. Come up with solution.
3. Try to write proof.
4. Realize solution is wrong.
Some tips

When you are trying to prove something, ask yourself:

- What do I have/know?
- Definitions give you things!
- Look for the existential quantifiers!

- What am I trying to build/prove/etc?
- What conclusion are you working towards?
- Look for the existential quantifiers!

- What proofs have I seen before which do something similar to what I am trying to do here?
- Are those ideas helpful here?
Challenge question

Can you find a propositional formula using only $P, Q,$ and $\land$ which is logically equivalent to $P \Rightarrow Q$? If not, can you prove it?

What about logically equivalent to $P \land Q$ using only $P, Q,$ and $\Rightarrow$?