Writing Proofs

Goal: prove a statement to be true (or false).

Proof should have/be

- A beginning (maybe list of assumptions, proof strategy, what you're trying to show)
- clear logical arguments / deductions
- grammatically correct English (or mathematical shorthand / symbols)
- Precision!! — no room for doubt.
- A conclusion (might be just a sentence).
- Readable without necessarily knowing the statement you're trying to prove.

Proof should not have/be:

- Long-winded — you don't need to state every detail (especially ones already given in class). This takes practice and feedback. Use your judgment.
- A "proof by example". e.g. you can't show that the sum of two odd numbers is even by saying "$3+5=8$, which is even." (You can, however, disprove by example!)
- variables you haven't defined. e.g. you could write "Let A and B be finite sets..." or "Let $x \in \mathbb{R}$..."

- start w/ what you are trying to prove!
- Incorrect logic (more generally) (e.g. negating a statement incorrectly, proving the converse, etc)

Some types of proofs

Direct Proof

Want to show: $P \Rightarrow Q$

Shape of proof:

Assume P.

$P \Rightarrow P_1$

$P_1 \Rightarrow P_2$

$P_2 \Rightarrow P_3$

$P_3 \Rightarrow Q$.

Thus, Q. $\square$

Example: Show that if $A \subseteq B$, then $A \cap B = A$.

Pf: Assume $A \subseteq B$.

Let $x \in A \cap B$. $A \cap B \subseteq A$, so $x \in A$.

Now let $y \in A$. Then $y \in B$, so $y \in A \cap B$.

Thus,

$A \cap B = A$. $\square$

Note: The shape of this argument was actually

Assume P. $(P \Rightarrow P_1)$ and $(P \Rightarrow P_2)$. $P_1 \wedge P_2 \Rightarrow Q$.

Thus, Q.

Proof of the contrapositive

The contrapositive of "$P \Rightarrow Q$" is "$(\neg Q) \Rightarrow (\neg P)$"

Truth table:

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

so $(P \Rightarrow Q) \iff (\neg Q \Rightarrow \neg P)$

Ex: The contrapositive of "If $A \subseteq B$ then $A \cup B = B$."

is "If $A \cup B \neq B$, then $A \not\subseteq B$."

or "If $A \cup B \neq B$, then $\exists\, x \in A$ s.t. $x \notin B$."

Proving the contrapositive is equivalent to proving the original statement.

Shape of Proof: Want to show $P \Rightarrow Q$.

Assume $\neg Q$. $\neg Q \Rightarrow Q_1 \Rightarrow Q_2 \Rightarrow Q_3 \Rightarrow \neg P$.

Thus $\neg P$. Therefore $P \Rightarrow Q$. $\square$

Proof by Contradiction

Idea: Assume the statement you are trying to prove is false, or equivalently, that the negation of the statement

is true. Conclude something that you know to be false (or reach an internal contradiction!)

Shape of proof: Want to prove P. Assume $\neg P$.

$\neg P \Rightarrow A_1 \Rightarrow A_2 \Rightarrow Q$.

However, we know that Q is false. Thus $\neg P$ is false, so P is true. $\square$

Notice: We are using the fact that

$$[(\neg P \Rightarrow Q) \wedge (\neg Q)] \Rightarrow P$$

Example: Show that there are infinitely many prime numbers.

Pf: Assume there are only finitely many primes $p_1, \dots, p_n$.

Consider the integer $p = p_1 p_2 \cdots p_n + 1$.

$p > p_i \quad \forall \; i \in \{1, \dots, n\}$, so $p \neq p_i$ for any i.

Thus, p is not prime itself, so it must be divisible by some p_j.

$p_1 p_2 \cdots p_n$ is divisible by p_j, but 1 is not. Thus p can't be divisible by p_j, which gives us a contradiction. $\square$

Notice that the structure of the argument here is:

Assume $\neg P$. $\neg P \Rightarrow A$ and $\neg P \Rightarrow \neg A$. Thus $(A \wedge \neg A)$, which we know to be false.

Proof by Induction

We will come back to this later.

Essentially, if you want to prove P_i for all $i \in \mathbb{N}$, you can prove P_1 and $P_i \Rightarrow P_{i+1}$ for all i.

What kinds of statements do we try to prove?

Examples:

- $x = y$

  How to prove this depends on what x and y are.

  * If x and y have values in $\mathbb{R}$, might show $x \leq y$ and $y \leq x$.
  * If x and y are sets, might show $x \subseteq y$ and $y \subseteq x$.
  * Might show $x = x_1 = x_2 = \ldots = y$.

- $P \Rightarrow Q$

- $P \Leftrightarrow Q$

  Some Proof strategies:

  * $P \Rightarrow Q$ and $Q \Rightarrow P$
  * $P \Rightarrow Q$ and $\neg P \Rightarrow \neg Q$
  * $P \Leftrightarrow P_1 \Leftrightarrow \ldots \Leftrightarrow P_r \Leftrightarrow Q$

- $\forall x, P(x)$.

  Typical strategy: Pick an arbitrary x (not specific!) and show that x has the desired property.

Example: Show that any rational number can be expressed as $\frac{m}{n}$ where m and n are not both even.

Pf: Let x be a rational number.

Then $x = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ and $q \neq 0$.

We can factor p and q as $p = 2^a \cdot b$ and $q = 2^c \cdot d$ where b and d are the product of odd primes.
(Exercise: finish the proof.)

- $\exists\, x$ s.t. $P(x)$.

  Can be shown by example! e.g. to prove "$\exists\, x \in \mathbb{Z}$ s.t. $x < 0$" you can just say "$-1 \in \mathbb{Z}$ and $-1 < 0$." □

- $\forall\, x, \exists\, y$ s.t. $P(x, y)$.

  Example: Show that $\forall\, x \in \mathbb{Q}$ s.t. $x > 0$, $\exists\, y \in \mathbb{R}$ s.t. $0 < y < x$.

  Pf: (combination of previous strategies)
  Let $x \in \mathbb{Q}$ s.t. $x > 0$. Then $\frac{x}{2} < x$ and

  $\frac{x}{2} > \frac{0}{2} = 0$ and $\frac{x}{2} \in \mathbb{Q}$. Thus, $0 < \frac{x}{2} < x$ for all x. □ [Depending on context, more details may be required.]

- Suppose A, B, and C. Then D.

Proof might look something like:

$$A \Rightarrow D_1 \Rightarrow D_2 \,,\; (B \wedge C) \Rightarrow D_3$$

$$(D_2 \wedge D_3) \Rightarrow D_4 \Rightarrow D.$$

(Generally, you'll need to use all assumptions, so if you don't use one, you may have made a mistake.

Getting started on a proof

If you don't know where to start, on scratch paper:

- write out assumptions and definitions
- write out desired conclusion
- work from both ends: What can you conclude from assumptions? What do you need to be true in order to reach the conclusion?
- Sketch outline of proof before writing final version.