Proofs: Logic in Action
Poll

Did you attend the tutorials?

A: None of them
B: On Monday only
C: On Tuesday only
D: On Monday and Tuesday
Consider the following propositions:

1. \( (\exists x \text{ Flies}(x) ) \rightarrow (\forall x \text{ Flies}(x) ) \)
2. \( \forall x,y \text{ Flies}(x) \leftrightarrow \text{ Flies}(y) \)
3. \( \exists x \forall y \text{ Flies}(x) \leftrightarrow \text{ Flies}(y) \)
4. \( \exists x \forall y \text{ Flies}(x) \rightarrow \text{ Flies}(y) \)

Which one(s) say “Either everyone flies or no one flies”?

A: None of them
B: 1 only
C: 1 and 2 only
D: 1, 2 and 3 only
E: 1, 2, 3 and 4
Using Logic

Logic is used to deduce results in any (mathematically defined) system

Typically a human endeavour (but can be automated if the system is relatively simple)

Proof is a means to convince others (and oneself) that a deduced result is correct

Verifying a proof is meant to be easy (automatable)

Coming up with a proof is typically a lot harder (not easy to fully automate, but sometimes computers can help)
What are we proving?

- We are proving propositions
  - Often called Theorems, Lemmas, Claims, ...
- Propositions may employ various predicates already specified as Definitions
  - e.g. All positive even numbers are larger than 1
    \[ \forall x \in \mathbb{Z} \ ( \text{Positive}(x) \land \text{Even}(x) ) \rightarrow \text{Greater}(x,1) \]
- These predicates are specific to the system (here arithmetic). The system will have its own “axioms” too (e.g., \( \forall x \ x+0=x \))
  - For us, numbers (reals, integers, rationals) and other systems like sets, graphs, functions, ...
- Goal: Use logical operations to establish the truth of a given proposition, starting from the axioms (or already proven propositions) in a system
Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like $+$, $-$, $\times$, $/$, exponentiation...)

We will not attempt to formally define this system!

**Definition:** An integer $x$ is said to be odd if there is an integer $y$ s.t. $x=2y+1$

$\text{Odd}(x) = \exists y \in \mathbb{Z} \ (x = 2y+1)$

**Proposition:** If $x$ is an odd integer, so is $x^2$

$\forall x \in \mathbb{Z} \ \text{Odd}(x) \rightarrow \text{Odd}(x^2)$
Example

Def: \( \text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y+1) \)

Proposition: \( \forall x \in \mathbb{Z} \text{ Odd}(x) \rightarrow \text{Odd}(x^2) \)

Proof: (should be written in more readable English)

Let \( x \) be an arbitrary element of \( \mathbb{Z} \). Variable \( x \) introduced.

Suppose \( \text{Odd}(x) \). Then, we need to show \( \text{Odd}(x^2) \).

By def., \( \exists y \in \mathbb{Z} \ x = 2y + 1 \). So let \( x = 2a + 1 \) where \( a \in \mathbb{Z} \). Variable \( a \).

Then, \( x^2 = (2a + 1)^2 = 4a^2 + 4a + 1 \)

= \( 2(2a^2 + 2a) + 1 \) From arithmetic.

\( \exists w \in \mathbb{Z} \ (2a^2 + 2a) = w \) From arithmetic.

So let \( 2a^2 + 2a = b \), where \( b \in \mathbb{Z} \). Variable \( b \).

Hence, \( x^2 = 2b + 1 \)

Then, by definition, \( \text{Odd}(x^2) \).

Hence for every \( x \), \( \text{Odd}(x) \rightarrow \text{Odd}(x^2) \). QED.
Anatomy of a Proof

☐ Clearly state the proposition \( p \) to prove (esp’ly, if rephrased)

☐ Derive propositions \( p_0, ..., p_n \) where for each \( i \), either \( p_i \) is an axiom or an already proven proposition in the system, or

\[
(p_0 \land p_1 \land ... \land p_{i-1}) \rightarrow p_i
\]

☐ Usually one or two propositions so far imply the next

☐ An explanation should make it easy to verify the implication (e.g., “By \( p_j \) and \( p_{i-1} \), we obtain \( p_i \”)

☐ \( p_n \) should be the proposition to be proven.

☐ Notation: This sequence is often written as \( p_0 \Rightarrow p_1 \Rightarrow ... \Rightarrow p_n \)

☐ May use “sub-routines” (lemmas). [e.g., \( p_0 \Rightarrow ... \Rightarrow p_k \). Now, by Lemma 1, \( p_i \land p_k \rightarrow p_{k+1} \). So we have \( p_{k+1} \). Now, \( ... \Rightarrow p_n \).]
Templates

To prove $p \rightarrow q$:

May set $p_0$ as $p$ (even though we don’t know if $p$ is True), and proceed to prove $q$

Proof starts with “Suppose $p$.”

Why is this a proof of $p \rightarrow q$?

If $p$ is False, we are done with the proof

If $p$ is True, the above proof holds

In either case $p \rightarrow q$ holds
Often it is helpful to first rewrite the proposition into an equivalent proposition and prove that. Should clearly state this if you are doing this.

An important example: contrapositive

\[ p \rightarrow q \equiv \neg q \rightarrow \neg p \]

Both equivalent to \( \neg p \lor q \)

An example:

If function \( f \) is “hard” then crypto scheme \( S \) is “secure”
\[ \equiv \text{If crypto scheme } S \text{ is not “secure,” then function } f \text{ is not “hard”} \]

To prove the former, we can instead show how to transform any attack on \( S \) into an efficient algorithm for \( f \)
More Examples

Positive integers

Proposition: \( \forall x, y \in \mathbb{Z}^+ \ x \cdot y > 25 \rightarrow (x \geq 6) \lor (y \geq 6) \)

Enough to prove that: \( \forall x, y \in \mathbb{Z}^+ \ (x < 6) \land (y < 6) \rightarrow x \cdot y \leq 25 \)

Proposition: “p only if q.” i.e., if not q, then not p: \( \neg q \rightarrow \neg p \)

Same as \( p \rightarrow q \)

“p if and only if q”: That is, \( (q \rightarrow p) \land (\neg q \rightarrow \neg p) \)

Equivalent to \( (q \rightarrow p) \land (p \rightarrow q) \), or \( p \leftrightarrow q \).

Also, \( (p \rightarrow q) \land (\neg p \rightarrow \neg q) \).
Proof by contradiction as an instance of proving equivalent propositions:

\[ p \equiv \neg p \to \text{False}. \text{ To prove } p, \text{ enough to show that } \neg p \to \text{False}. \]

Now, to prove \( \neg p \to \text{False} \), as we saw, we will start by assuming \( \neg p \)

Can start the proof directly by saying “Suppose for the sake of contradiction, \( \neg p \)” (instead of saying we shall prove \( \neg p \to \text{False} \))

\( p_n \) is simply “False.”

E.g., we may have \( \neg p \to \ldots \to q \ldots \to \neg q \to \text{False} \)

“But that is a contradiction! Hence \( p \) holds.”
Claim: There's a village barber who shaves exactly those in the village who don't shave themselves

Proposition: The claim is false

Proposition, formally: \[ \neg (\exists B \forall x \; \neg \text{shave}(x,x) \iff \text{shave}(B,x)) \]

Suppose for the sake of contradiction,
\[ \exists B \forall x \; \neg \text{shave}(x,x) \iff \text{shave}(B,x) \]

\[ (\exists B \forall x \; \neg \text{shave}(x,x) \iff \text{shave}(B,x) ) \]
\[ \Rightarrow (\exists B \; \neg \text{shave}(B,B) \iff \text{shave}(B,B) ) \]
\[ \Rightarrow \exists B \; \text{False} \]
\[ \Rightarrow \text{False, which is a contradiction!} \]
Example

For every pair of distinct primes $p,q$, $\log_p(q)$ is irrational

(Will use basic facts about log and primes from arithmetic.)

Suppose for the sake of contradiction that there exists a pair of distinct primes $(p,q)$, s.t. $\log_p(q)$ is rational.

$\Rightarrow \log_p(q) = \frac{a}{b}$ for positive integers $a,b$.

(Note, since $q>1$, $\log_p(q) > 0$.)

$\Rightarrow p^{\frac{a}{b}} = q \Rightarrow p^a = q^b$.

But $p$, $q$ are distinct primes. Thus $p^a$ and $q^b$ are two distinct prime factorisations of the same integer!

Contradicts the Fundamental Theorem of Arithmetic!

Will prove later
To prove $\exists x\ P(x)$

- Demonstrate a particular value of $x$ s.t. $P(x)$ holds

  e.g. to prove $\exists x\ P(x) \rightarrow Q(x)$

    - find an $x$ s.t. $P(x) \rightarrow Q(x)$ holds
      
      if you can find an $x$ s.t. $P(x)$ is false, done!

      or, you can find an $x$ s.t. $Q(x)$ is true, done!

    (May not be easy to show either, but still may be able to find an $x$ and argue $\neg P(x) \lor Q(x)$

    (May not be able to find one, but still show one exists!)
To prove \(\neg(\forall x \ P(x))\), the most natural/correct approach is to:

A. prove that \(\neg P(x)\) holds for all \(x\)

B. prove that \(P(x)\) holds for all \(x\)

C. demonstrate an \(x\) s.t. \(P(x)\) is false

D. demonstrate an \(x\) s.t. \(P(x)\) is true

E. prove that \(P(x)\) or \(\neg P(x)\) holds for all \(x\)
To prove $\forall x \ P(x) \rightarrow Q(x)$

Let $x$ be an arbitrary element (in the domain of the predicates $P$ and $Q$)

Now prove $P(x) \rightarrow Q(x)$

Assume $P(x)$ holds, i.e., set $p_0$ to be $P(x)$

Prove $Q(x)$ using a sequence, $p_0 \implies p_1 \implies \ldots \implies p_n$, where $p_n$ is $Q(x)$

Since $x$ is arbitrary, this proof applies to every $x$. Hence $\forall x \ P(x) \rightarrow Q(x)$

Caution: You are not proving $(\forall x \ P(x)) \rightarrow (\forall x \ Q(x))$. So to prove $Q(x)$, may only assume $P(x)$, and not $P(x')$ for $x' \neq x$. 
Some Valid Approaches

∀x P(x)

Let x be an arbitrary element
Show Q(x) → P(x)
Show Q(x) holds
Then P(x)  Because, (Q(x) ∧ (Q(x) → P(x))) ≡ P(x) ∧ (…)

∃x ¬Q(x)

Show ∃x Q(x) → P(x)
Show ∀x ¬P(x)

Or, Show ∀x ¬Q(x) (Much more than needed, but OK)

May or may not be possible/true for a given problem.

At this point, we have reduced the problem of proving P(x) to the problem of proving Q(x)

If we demonstrate an element x s.t. Q(x)→P(x) holds, now enough to show that for that x, P(x) holds
Some Valid Approaches

\[ \exists x \ P(x) \land Q(x) \equiv \forall x \ \neg P(x) \lor \neg Q(x) \]

- Show \( \forall x \neg Q(x) \)
- Or, show \( \forall x \neg P(x) \)
- Or, more generally, show \( \forall x \ P(x) \rightarrow \neg Q(x) \)

\[ \exists x \ P(x) \]

- Show \( P(0) \)
- \( \neg \forall x \ P(x) \equiv \exists x \neg P(x) \)
- Show \( \neg P(0) \)

May or may not be possible/true for a given problem.
Today

Proofs: A style guide

Proofs should be easy to verify. All the cleverness goes into finding/writing the proof, not reading/verifying it!

Multiple approaches:

Today: Direct deduction; Rewriting the proposition, e.g., as contrapositive; Proof by contradiction; Proof by giving a (counter)example, when applicable.

Next:

Proof by case analysis

Mathematical induction