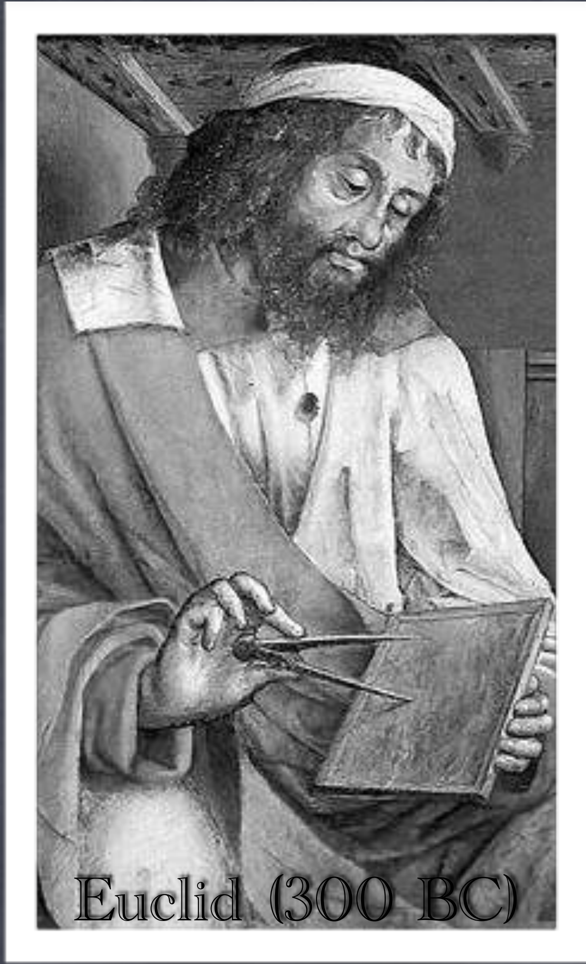

Proofs: Logic in Action

Poll

- Did you attend the tutorials?

  A: None of them
  B: On Monday only
  C: On Tuesday only
  D: On Monday and Tuesday

Review Question

- 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
  - <u>Verifying</u> 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
  - $\forall x \in \mathbb{Z}$ (Positive(x) $\wedge$ Even(x)) $\rightarrow$ 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

Example

- Our system here is that of integers (comes with the set of integers $\mathbb{Z}$ and operations like +, -, *, /, 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. $x=2y+1$
  - $\text{Odd}(x) \equiv \exists y \in \mathbb{Z} \ (x = 2y+1)$

"if" used by convention; actually means "iff"

- 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: Odd(x) $\equiv \exists y \in \mathbb{Z}\ (x = 2y+1)$
- Proposition: $\forall x \in \mathbb{Z}$ Odd(x) $\rightarrow$ Odd(x^2)
- Proof: (should be written in more readable English)
  - Let x be an arbitrary element of $\mathbb{Z}$. Variable x introduced.
  - Suppose Odd(x). Then, we need to show 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, Odd(x^2).
  - Hence for every x, Odd(x) $\rightarrow$ Odd(x^2). QED.

Anatomy of a Proof

- Clearly state the proposition p to prove (esp'ly, if rephrased)
- Derive propositions $p_0, \ldots, p_n$ where for each i, either p_i is an axiom or an already proven proposition in the system, or $(p_0 \wedge p_1 \wedge \ldots \wedge p_{i-1}) \rightarrow p_i$
  - 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 $p_0 \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_n$
- May use "sub-routines" (lemmas). [e.g., $p_0 \Rightarrow \ldots \Rightarrow p_k$. Now, by Lemma 1, $p_i \wedge p_k \rightarrow p_{k+1}$. So we have p_{k+1}. Now, $\ldots \Rightarrow p_n$.]

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

Templates

- 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 $\neg p \vee q$
  - An example:
    - If function f is "hard" then crypto scheme S is "secure" $\equiv$ If crypto scheme S is not "secure," then function f 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: $\forall x,y \in \mathbb{Z}^+ \;\; x \cdot y > 25 \rightarrow (x \geq 6) \vee (y \geq 6)$
  - Enough to prove that: $\forall x,y \in \mathbb{Z}^+ \;\; (x<6) \wedge (y<6) \rightarrow x \cdot y \leq 25$
- 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, $(q \rightarrow p) \wedge (\neg q \rightarrow \neg p)$
  - Equivalent to $(q \rightarrow p) \wedge (p \rightarrow q)$, or $p \longleftrightarrow q$.

    Also, $(p \rightarrow q) \wedge (\neg p \rightarrow \neg q)$.

Templates

- **Proof by contradiction** as an instance of proving equivalent propositions:
  - $p \equiv \neg p \rightarrow False$. To prove p, enough to show that $\neg p \rightarrow False$.
  - Now, to prove $\neg p \rightarrow False$, 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 $\neg p \rightarrow False$)
    - p_n is simply "False."
      - E.g., we may have $\neg p \Rightarrow \ldots \Rightarrow q \ldots \Rightarrow \neg q \Rightarrow False$
        - "But that is a contradiction! Hence p holds."

Example

- 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: $\neg(\exists B \forall x \;\; \neg shave(x,x) \longleftrightarrow shave(B,x))$
  - Suppose for the sake of contradiction,
    $\exists B \; \forall x \;\; \neg shave(x,x) \longleftrightarrow shave(B,x)$
  - $(\exists B \; \forall x \;\; \neg shave(x,x) \longleftrightarrow shave(B,x) \;)$

$$\Rightarrow (\exists B \; \neg shave(B,B) \longleftrightarrow shave(B,B) \;)$$

$$\Rightarrow \exists B \text{ False}$$

$$\Rightarrow \text{False, which is a contradiction!}$$

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.
- $\Rightarrow \log_p(q) = a/b$ for positive integers a,b.

  (Note, since $q>1$, $\log_p(q) > 0$.)
- $\Rightarrow p^{a/b} = q \Rightarrow p^a = q^b$.
- 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

Template

- 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 $\neg P(x) \vee Q(x)$)
  - (May not be able to find one, but still show one exists!)

Question

- 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

$\exists x\ \neg P(x)$

Templates

- To prove $\forall x\ \underline{P(x) \rightarrow Q(x)}$
  - 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, $p_0 \Rightarrow p_1 \Rightarrow \ldots \Rightarrow p_n$, 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 $x' \neq x$.

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

Some Valid Approaches

- $\forall x\ P(x)$
  - Let x be an arbitrary element
    Show $Q(x) \rightarrow P(x)$
    Show $Q(x)$ holds
    Then $P(x)$ Because, $(Q(x) \land (Q(x) \rightarrow P(x))) \equiv P(x) \land (\ldots)$

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

- $\exists x\ \neg Q(x)$
  - Show $\exists x\ Q(x) \rightarrow P(x)$
    Show $\forall x\ \neg P(x)$
  - Or, Show $\forall x\ \neg Q(x)$ (Much more than needed, but OK)

If we demonstrate an element x s.t. $Q(x) \rightarrow P(x)$ holds, now enough to show that for that x, $P(x)$ holds

Some Valid Approaches

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

- $\nexists x\ P(x) \wedge Q(x) \equiv \forall x\ \neg P(x) \vee \neg Q(x)$

  Rewrite

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

  Rewrite

  - Show $\neg P(0)$

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