IIT KGP
Dept. of Computer Science & Engineering

CS 30053
Foundations of Computing

Debdeep Mukhopadhyay

LOGICAL INFERENCE
&
PROOFs

Defn

- A *theorem* is a mathematical assertion which can be shown to be true. A *proof* is an argument which establishes the truth of a theorem.

Nature & Importance of Proofs

- In mathematics, a *proof* is:
  - a *correct* (well-reasoned, logically valid) and *complete* (clear, detailed) argument that rigorously & undeniably establishes the truth of a mathematical statement.
- Why must the argument be correct & complete?
  - *Correctness* prevents us from fooling ourselves.
  - *Completeness* allows anyone to verify the result.

Overview

- Methods of mathematical argument (*i.e.*, proof methods) can be formalized in terms of *rules of logical inference*.
- Mathematical *proofs* can themselves be represented formally as discrete structures.
- We will review both <u>correct</u> & <u>fallacious</u> inference rules, & several proof methods.

Applications of Proofs

- An exercise in clear communication of logical arguments in any area of study.
- The fundamental activity of mathematics is the discovery and elucidation, through proofs, of interesting new theorems.
- Theorem-proving has applications in program verification, computer security, automated reasoning systems, *etc.*
- Proving a theorem allows us to rely upon on its correctness even in the most critical scenarios.

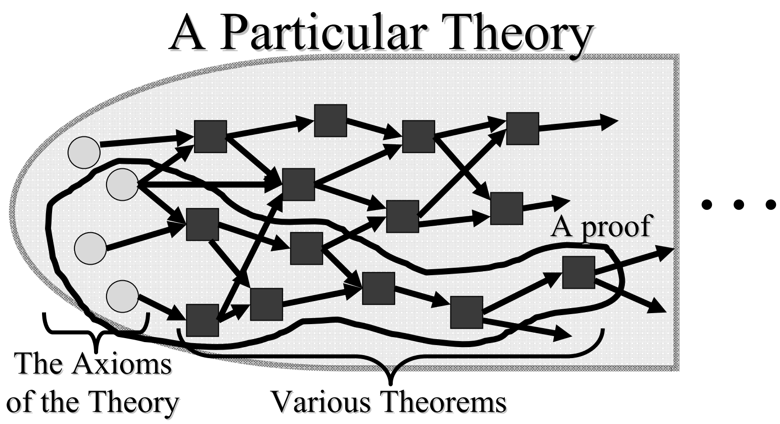
Proof Terminology

- *Theorem*
  - A statement that has been proven to be true.
- *Axioms*, *postulates*, *hypotheses*, *premises*
  - Assumptions (often unproven) defining the structures about which we are reasoning.
- *Rules of inference*
  - Patterns of logically valid deductions from hypotheses to conclusions.

More Proof Terminology

- *Lemma* - A minor theorem used as a stepping-stone to proving a major theorem.
- *Corollary* - A minor theorem proved as an easy consequence of a major theorem.
- *Conjecture* - A statement whose truth value has not been proven. (A conjecture may be widely believed to be true, regardless.)
- *Theory* – The set of all theorems that can be proven from a given set of axioms.

Graphical Visualization



Inference Rules - General Form

- An *Inference Rule* is
  - A pattern establishing that if we know that a set of *antecedent* statements of certain forms are all true, then we can validly deduce that a certain related *consequent* statement is true.
- *antecedent 1*
  antecedent 2 …
  ∴ *consequent*   "∴" means "therefore"

Inference Rules & Implications

- Each valid logical inference rule corresponds to an implication that is a tautology.
- $\begin{array}{l} \textit{antecedent 1} \\ \underline{\textit{antecedent 2} \ \ldots} \\ \therefore \textit{ consequent} \end{array}$ Inference rule
- Corresponding tautology:

  $((\textit{ante. 1}) \wedge (\textit{ante. 2}) \wedge \ldots) \rightarrow \textit{consequent}$

Some Inference Rules

- $\begin{array}{c} p \\ \hline \therefore\ p \vee q \end{array}$ Rule of Addition
- $\begin{array}{l} p \wedge q \\ \hline \therefore\ p \end{array}$ Rule of Simplification
- $\begin{array}{c} p \\ q \\ \hline \therefore\ p \wedge q \end{array}$ Rule of Conjunction

Modus Ponens & Tollens

- p
$\underline{p \to q}$
$\therefore q$
- $\neg q$
$\underline{p \to q}$
$\therefore \neg p$

Rule of *modus ponens* (a.k.a. *law of detachment*)

"the mode of affirming"

Rule of *modus tollens*

"the mode of denying"

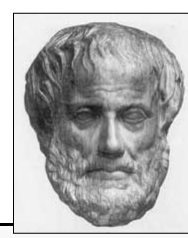
Syllogism Inference Rules

- $p \to q$
$\underline{q \to r}$
$\therefore p \to r$

  Rule of hypothetical syllogism

- $p \lor q$
$\underline{\neg p}$
$\therefore q$

  Rule of disjunctive syllogism



Aristotle
(ca. 384-322 B.C.)

Formal Proofs

- A formal proof of a conclusion *C*, given premises $p_1, p_2, \ldots, p_n$ consists of a sequence of *steps*, each of which applies some inference rule to premises or previously-proven statements (*antecedents*) to yield a new true statement (the *consequent*).
- A proof demonstrates that *if* the premises are true, *then* the conclusion is true.

Formal Proof Example

- Suppose we have the following premises:
  "It is not sunny and it is cold."
  "We will swim only if it is sunny."
  "If we do not swim, then we will canoe."
  "If we canoe, then we will be home early."
- Given these premises, prove the theorem **"We will be home early"** using inference rules.

Proof Example *cont.*

- Let us adopt the following abbreviations:
  - *sunny* = **"It is sunny"**; *cold* = **"It is cold"**; *swim* = **"We will swim"**; *canoe* = **"We will canoe"**; *early* = **"We will be home early"**.
- Then, the premises can be written as:
  (1) $\neg sunny \wedge cold$ (2) $swim \rightarrow sunny$
  (3) $\neg swim \rightarrow canoe$ (4) $canoe \rightarrow early$

Proof Example *cont*.

Step	Proved by
1. $\neg sunny \wedge cold$	Premise #1.
2. $\neg sunny$	Simplification of 1.
3. $swim \rightarrow sunny$	Premise #2.
4. $\neg swim$	Modus tollens on 2,3.
5. $\neg swim \rightarrow canoe$	Premise #3.
6. $canoe$	Modus ponens on 4,5.
7. $canoe \rightarrow early$	Premise #4.
8. $early$	Modus ponens on 6,7.

Inference Rules for Quantifiers

- $\dfrac{\forall x\, P(x)}{\therefore P(o)}$ **Universal instantiation** (substitute *any* specific object *o*)
- $\dfrac{P(g)}{\therefore \forall x\, P(x)}$ (for *g* a *general* element of u.d.) **Universal generalization**
- $\dfrac{\exists x\, P(x)}{\therefore P(c)}$ **Existential instantiation** (substitute a *new constant c*)
- $\dfrac{P(o)}{\therefore \exists x\, P(x)}$ (substitute any extant object *o*) **Existential generalization**

Common Fallacies

- A *fallacy* is an inference rule or other proof method that is not logically valid.
  - A fallacy may yield a false conclusion!
- Fallacy of *affirming the conclusion*:
  - "$p \rightarrow q$ is true, and q is true, so p must be true." (No, because $\mathbf{F} \rightarrow \mathbf{T}$ is true.)
  - If he stole, he will be nervous when he is interrogated. He was nervous when interrogated, so he stole.

Fallacy

- Fallacy of *denying the hypothesis*:
  - "$p \rightarrow q$ is true, and p is false, so q must be false." (No, again because **F**$\rightarrow$**T** is true.)
  - If his hands are full of blood, he has murdered. But he is sitting on his sofa, well dressed (without any sign of blood), so he did not murder.
  - He may have washed his hands !!!

Slightly complicated example

- Statement:
  - $\forall x[P(x) \vee Q(x)] \rightarrow \forall x P(x) \vee \forall x Q(x)$
  - Quick Check: P(x): x is even, Q(x): x is odd
- <u>Fallacious Proof:</u>

$\forall x\ [P(x) \vee Q(x)] \leftrightarrow \neg\exists \mathbf{x} \neg\ [\mathbf{P(x)} \vee Q(x)]$

$\leftrightarrow \neg\boxed{\exists \mathbf{x}[\neg \mathbf{P(x)} \wedge \neg \mathbf{Q(x)}]}$

$\rightarrow \neg\ \boxed{[\exists \mathbf{x}\ \neg \mathbf{P(x)} \wedge \exists \mathbf{x}\ \neg \mathbf{Q(x)}]}$

Remember we Proved in the last class

$\leftrightarrow [\neg\ \exists \mathbf{x}\ \neg \mathbf{P(x)} \vee \neg\ \exists \mathbf{x}\ \neg \mathbf{Q(x)}]$

$\leftrightarrow \forall x P(x) \vee \forall x Q(x)$

Fallacy of denying the antecedent

Circular Reasoning

- The fallacy of (explicitly or implicitly) assuming the very statement you are trying to prove in the course of its proof. Example:
- Prove that an integer n is even, if n^2 is even.
- **Attempted proof:** "Assume n^2 is even. Then $n^2=2k$ for some integer k. Dividing both sides by n gives $n = (2k)/n = 2(k/n)$. So there is an integer j (namely k/n) such that $n=2j$. Therefore n is
  – Circular reaso

How do you show that $j=k/n=n/2$ is an integer, without ***first*** *assuming that n is even?*

A Correct Proof

We know that n must be either odd or even. If n were odd, then n^2 would be odd, since an odd number times an odd number is always an odd number. Since n^2 is even, it is not odd, since no even number is also an odd number. Thus, by modus tollens, n is not odd either. Thus, by disjunctive syllogism, n must be even. ■

This proof is correct, but not quite complete, since we used several lemmas without proving them. Can you identify what they are?

A More Verbose Version

- Suppose n^2 is even $\therefore 2|n^2 \;\therefore\; n^2$ mod 2 = 0.
- Of course n mod 2 is either 0 or 1.
- If it's 1, then $n \equiv 1 \pmod{2}$, so $n^2 \equiv 1 \pmod{2}$
- Now $n^2 \equiv 1 \pmod{2}$ implies that n^2 mod 2 = 1. So by the hypothetical syllogism rule,
  - (n mod 2 = 1) implies (n^2 mod 2 = 1).
- Since we know n^2 mod 2 = 0 $\neq$ 1, by *modus tollens* we know that n mod 2 $\neq$ 1.
- So by disjunctive syllogism we have that
  - n mod 2 = 0 $\therefore 2|n \;\therefore\; n$ is even. Q.E.D.

Proof Methods for Implications

For proving implications $p \rightarrow q$, we have:

- *Direct* proof: Assume p is true, and prove q.
- *Indirect* proof: Assume $\neg q$, and prove $\neg p$.
- *Vacuous* proof: Prove $\neg p$ by itself.
- *Trivial* proof: Prove q by itself.
- Proof by cases:
  Show $p \rightarrow (a \vee b)$, and $(a \rightarrow q)$ and $(b \rightarrow q)$.

Direct Proof Example

- **Theorem:** (For all numbers *n*) If *n* is an odd integer, then n^2 is an odd integer.
- **Proof:** If *n* is odd, then $n = 2k+1$ for some integer *k*. Thus, $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Therefore n^2 is of the form $2j + 1$ (with *j* the integer $2k^2 + 2k$), thus n^2 is odd. □

Indirect Proof Example

- **Theorem:** (For all integers *n*)
  If $3n+2$ is odd, then *n* is odd.
- **Proof:** Suppose that the conclusion is false, *i.e.*, that *n* is even. Then $n=2k$ for some integer *k*. Then $3n+2 = 3(2k)+2 = 6k+2 = 2(3k+1)$. Thus $3n+2$ is even, because it equals $2j$ for integer $j = 3k+1$. So $3n+2$ is not odd. We have shown that $\neg(n \text{ is odd}) \rightarrow \neg(3n+2 \text{ is odd})$, thus its contrapositive $(3n+2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. □

Vacuous Proof Example

- **Theorem:** (For all *n*) If *n* is both odd and even, then $n^2 = n + n$.
- **Proof:** The statement "*n* is both odd and even" is necessarily false, since no number can be both odd and even. So, the theorem is vacuously true. □

Trivial Proof Example

- **Theorem:** (For integers *n*) If *n* is the sum of two prime numbers, then either *n* is odd or *n* is even.
- **Proof:** *Any* integer *n* is either odd or even. So the conclusion of the implication is true regardless of the truth of the antecedent. Thus the implication is true trivially. □

Proof by Contradiction

- A method for proving *p*.
- Assume $\neg p$, and prove both *q* and $\neg q$ for some proposition *q*. (Can be anything!)
- Thus $\neg p \rightarrow (q \wedge \neg q)$
- $(q \wedge \neg q)$ is a trivial contradiction, equal to **F**
- Thus $\neg p \rightarrow \mathbf{F}$, which is only true if $\neg p = \mathbf{F}$
- Thus *p* is true.

Proof by Contradiction Example

- **Theorem:** $\sqrt{2}$ is irrational.
  - **Proof:** Assume $2^{1/2}$ were rational. This means there are integers i,j with no common divisors such that $2^{1/2} = i/j$. Squaring both sides, $2 = i^2/j^2$, so $2j^2 = i^2$. So i^2 is even; thus i is even. Let $i=2k$. So $2j^2 = (2k)^2 = 4k^2$. Dividing both sides by 2, $j^2 = 2k^2$. Thus j^2 is even, so j is even. But then i and j have a common divisor, namely 2, so we have a contradiction. □

Review: Proof Methods So Far

- *Direct*, *indirect*, *vacuous*, and *trivial* proofs of statements of the form $p \to q$.
- *Proof by contradiction* of any statements.
- Next: *Constructive* and *nonconstructive existence proofs*.

Proving Existentials

- A proof of a statement of the form $\exists x\, P(x)$ is called an *existence proof*.
- If the proof demonstrates how to actually find or construct a specific element a such that $P(a)$ is true, then it is a *constructive* proof.
- Otherwise, it is *nonconstructive*.

Constructive Existence Proof

- **Theorem:** There exists a positive integer n that is the sum of two perfect cubes in two different ways:
  - equal to $j^3 + k^3$ and $l^3 + m^3$ where j, k, l, m are positive integers, and $\{j,k\} \neq \{l,m\}$
- **Proof:** Consider $n = 1729$, $j = 9$, $k = 10$, $l = 1$, $m = 12$. Now just check that the equalities hold.

Another Constructive Existence Proof

- **Theorem:** For any integer $n>0$, there exists a sequence of n consecutive composite integers.
- Same statement in predicate logic: $\forall n>0\ \exists x\ \forall i\ (1 \leq i \leq n) \rightarrow (x+i \text{ is composite})$
- Proof follows on next slide…

The proof...

- Given $n>0$, let $x = (n + 1)! + 1$.
- Let $i \geq 1$ and $i \leq n$, and consider $x+i$.
- Note $x+i = (n + 1)! + (i + 1)$.
- Note $(i+1)|(n+1)!$, since $2 \leq i+1 \leq n+1$.
- Also $(i+1)|(i+1)$. So, $(i+1)|(x+i)$.
- $\therefore$ $x+i$ is composite.
- $\therefore$ $\forall n\ \exists x\ \forall 1 \leq i \leq n : x+i$ is composite. Q.E.D.

Nonconstructive Existence Proof

Principle of extremum

- **Theorem:**
  "There are infinitely many prime numbers."
- **Any finite set of numbers must contain a maximal element**, so we can prove the theorem if we can just show that there is *no* largest prime number.
- *i.e.*, show that for any prime number, there is a larger number that is *also* prime.
- More generally: For *any* number, $\exists$ a larger prime.
- Formally: Show $\forall n\ \exists p>n : p$ is prime.

The proof, using *proof by cases*...

- Given $n>0$, prove there is a prime $p>n$.
- Consider $x = n!+1$. Since $x>1$, we know (x is prime)$\vee$(x is composite).
- **Case 1:** x is prime. Obviously $x>n$, so let $p=x$ and we're done.
- **Case 2:** x has a prime factor p. But if $p\leq n$, then x mod p = 1. So $p>n$, and we're done.

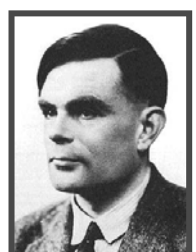
Proof by contradiction

- Assume a largest prime number exists; call it p. Form the product of the finite number of prime numbers,
  – r=2.3.5.7…p
- Now inspect r+1: It cannot be divisible by any of the above prime numbers
- So, either r+1 is a prime or divisible by a prime greater than p **(There is a fallacy in Stanat's proof).**
- Thus, in either case there is a prime greater than p, and hence we have a contradiction
- Thus, there is no maximum prime number and the set is infinite.

Adaptive proofs

- *Adapt the previous proof to prove that there are infinite prime numbers of the form 4k+3, where k is a non-negative integer.*

The Halting Problem (Turing'36)



Alan Turing
1912-1954

- The *halting problem* was the first mathematical function proven to have *no* algorithm that computes it!
  - We say, it is *uncomputable.*
- The desired function is *Halts*(*P*,*I*) :≡ the truth value of this statement:
  - *"Program P, given input I, eventually terminates."*
- **Theorem:** *Halts* is uncomputable!
  - I.e., There does *not* exist *any* algorithm *A* that computes *Halts* correctly for *all* possible inputs.
- Its proof is thus a *non*-existence proof.
- **Corollary:** General impossibility of predictive analysis of arbitrary computer programs.

The Proof

Absurd makes a liar out of *HALT*, by doing the opposite of whatever *HALT* predicts.

- Given any *arbitrary* program *HALT*(*P*)
- Consider algorithm Absurd, defined as:

  procedure *Absurd:*
  if HALT(Absurd)==T
  while T begin end

- Note that Absurd halts iff H(Absurd) = **F**.
- So *H* does **not** compute the function *Halts*!

Limits on Proofs

- Some very simple statements of number theory haven't been proved or disproved!
  - *E.g. Goldbach's conjecture*: Every integer $n \geq 2$ is exactly the average of some two primes.
  - $\forall n \geq 2$ $\exists$ primes p,q: $n=(p+q)/2$.
- There are true statements of number theory (or any sufficiently powerful system) that can *never* be proved (or disproved) (Gödel).