UC Davis
ECS20, Winter 2019

Discrete Mathematics for Computer Science

Prof. Raissa D'Souza
(slides adopted from Michael Frank and Haluk Bingöl)

Lecture 6 & 7

Foundations of Logic: Overview

- Introduction to Proofs (§1.5-1.6):
  - Nested Quantifiers. (§1.5)
  - Rules of Inference. (§1.6)

- More Proofs (§1.7)
  - Terminology.
  - Proof Methods.
  - Common Proof Mistakes.

Nature & Importance of Proofs

- Proof is a
  - *Correct* (well-reasoned, logically valid)
  - *Complete* (clear, detailed)

  argument that rigorously, undeniably establishes the truth of a mathematical statement.

- Why correct **AND** complete?
  - *Correctness* prevents us from fooling ourselves.
  - *Completeness* allows anyone to verify the result.

- *High standard* for correctness and completeness of proofs is demanded

Proof

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.

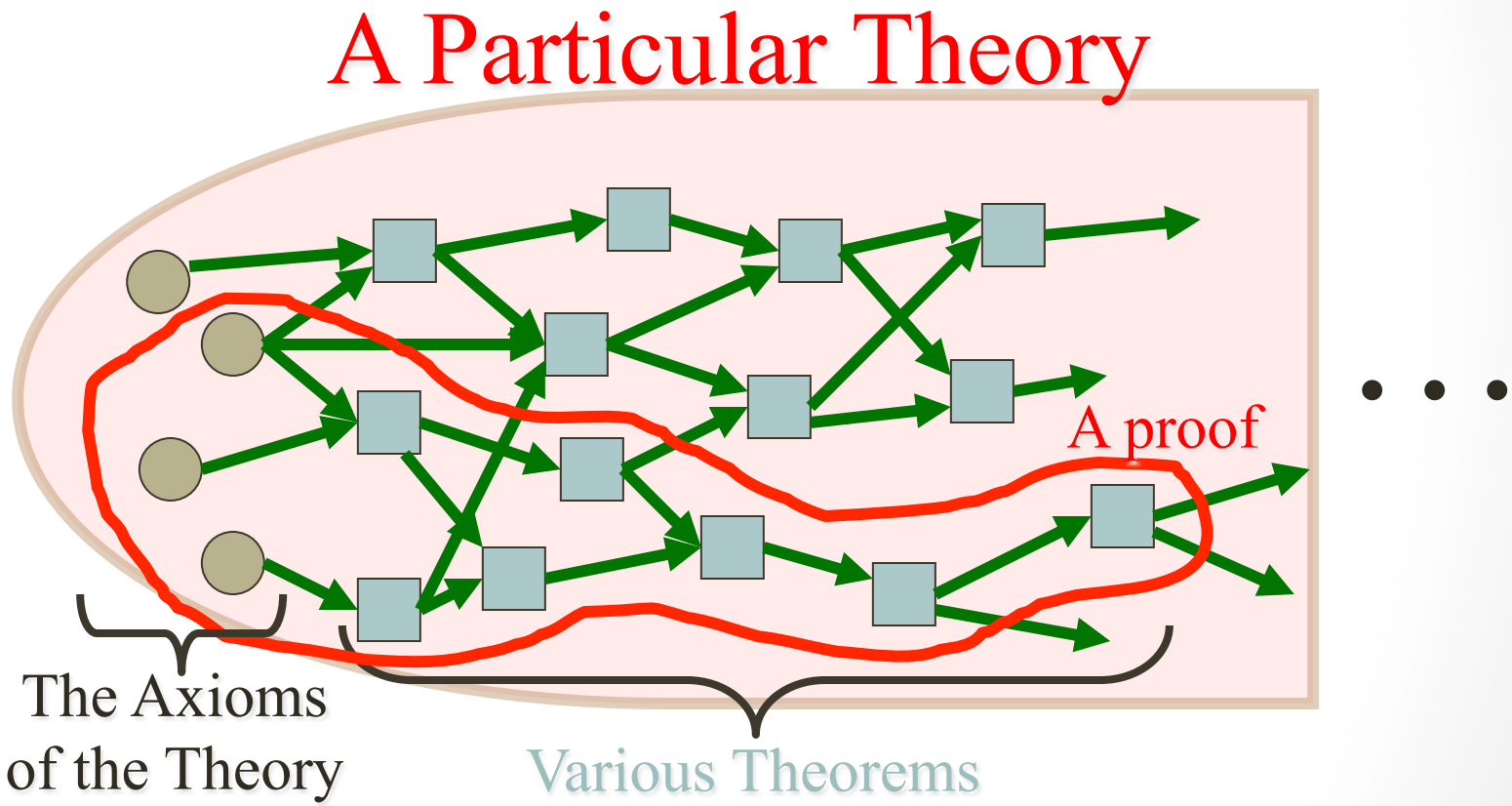
Proof Terminology

- *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

Inference Rules - General Form

- Def. 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
…
antecedent n

- ∴ *consequent*

The antecedents are postulated to all be TRUE

"∴" means "therefore"

Inference Rules & Implications

- Each valid logical inference rule corresponds to an implication that is a tautology.

$$\begin{array}{c} p_1 \\ p_2 \\ \ldots \\ p_n \\ \hline \therefore q \end{array}$$

Inference rule

Corresponding tautology:
$(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$

- Remark. $p \rightarrow q \equiv \neg p \vee q$

Some Inference Rules

$$\frac{p}{\therefore\ p \vee q}$$

Rule of Addition

$$\frac{p \wedge q}{\therefore\ p}$$

Rule of Simplification

$$\frac{\begin{array}{c} p \\ q \end{array}}{\therefore\ p \wedge q}$$

Rule of Conjunction

Modus Ponens & Tollens

$$\begin{array}{l} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$$

Rule of *modus ponens*
(a.k.a. *law of detachment*)
$(p \wedge (p \rightarrow q)) \rightarrow q$

"the mode of affirming"

$$\begin{array}{l} \neg q \\ \underline{p \rightarrow q} \\ \therefore \neg p \end{array}$$

Rule of *modus tollens*
$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$

"the mode of denying"

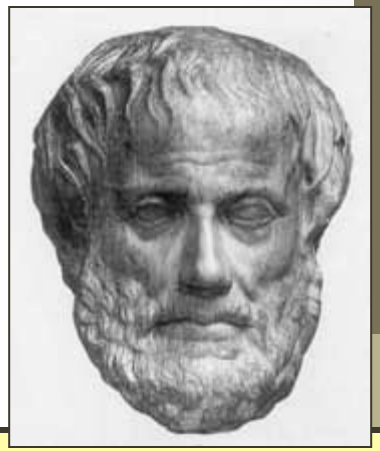
Syllogism Inference Rules

$$\begin{array}{c} p \rightarrow q \\ q \rightarrow r \\ \hline \therefore p \rightarrow r \end{array}$$

Rule of hypothetical syllogism

$$\begin{array}{c} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Rule of disjunctive syllogism



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

Rosen text
Sec 1.6,
Table 1

TABLE 1 **Rules of Inference.**

Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$(p \wedge (p \to q)) \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$(\neg q \wedge (p \to q)) \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \to (p \to r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \to q$	Disjunctive syllogism
p $\therefore p \vee q$	$p \to (p \vee q)$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \to p$	Simplification
p q $\therefore p \wedge q$	$((p) \wedge (q)) \to (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \to (q \vee r)$	Resolution

Formal Proofs

Formal Proofs

- A formal proof of a conclusion *C*,
  - given premises $p_1, p_2, \ldots, p_n$
  - sequence of *steps*
  - apply inference rule to premises or previously-proven statements (*antecedents*)
  - Yield new true statement (the *consequent*).
- A proof: *if* the premises are true, *then* the conclusion is true.

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.

Formal Proof
Example ...

- 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) $canoe \rightarrow early$

Formal Proof
Example ...

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*)

- $\dfrac{P(g)}{\therefore \forall x\, P(x)}$ **Universal generalization**
  (for *g* a *general* element of u.d.)

- $\dfrac{\exists x\, P(x)}{\therefore P(c)}$ **Existential instantiation**
  (substitute a *new constant c*)

- $\dfrac{P(o)}{\therefore \exists x\, P(x)}$ **Existential generalization**
  (substitute any extant object *o*)

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 **F**$\rightarrow$**T** is true.)

- 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.)

Review: Introduction to Proofs (§1.5-1.6)

- "Methods of mathematical argument" (proof methods) formalized with *rules of logical inference*.
- Proofs represented as discrete structures.
- Correct inference rules
- Fallacious inference rules
- (You can now do problems 12-14 on HW2)

Proof Methods

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

- Def. An integer n is called *odd* iff
  $n=2k+1$ for some integer k;
  n is *even* iff
  $n=2k$ for some k.
- Thm. Every integer is either odd or even.
  - This can be proven from even simpler axioms.
- Thm. (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

- Thm. (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 contra-positive $(3n+2 \text{ is odd}) \rightarrow (n \text{ is odd})$ is also true. □

Vacuous Proof Example

- Thm. (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

- Thm. (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 $\neg p \rightarrow$ **F**, which is only true if $\neg p$=**F**
- Thus p is true.

Proof by Contradiction Example

Thm. $\sqrt{2}$ 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 $p \rightarrow q$.
- *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

- Thm. 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

- Thm. For any integer $n>0$, there exists a sequence of n consecutive composite integers.

- Same statement in predicate logic:

- Thm. $\forall n>0\ \exists x\ \forall i\ (1\leq i\leq n)\rightarrow(x+i \text{ is composite})$

The proof…

- Thm. $\forall n>0\ \exists x\ \forall i\ (1\le i\le n)\rightarrow(x+i$ is composite)

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

Nonconstructive Existence Proof

- Thm. 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, ∃ a larger prime.
- Formally: Show $\forall n\ \exists p>n : p$ is prime.

The proof, using *proof by cases*…

- Thm. Given $n>0$, there is a prime $p>n$.

- Proof. 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 $x \bmod p = 1$. Contradiction.
  So $p>n$, and we're done.