Discrete Mathematics

Chih-Wei Yi

Dept. of Computer Science
National Chiao Tung University

March 9, 2009

Overview of Basic Proof Methods (§1.5-§1.7, ~2 hours)

- 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 correct & fallacious inference rules, & several proof methods.

§1.5 Rules of Inference

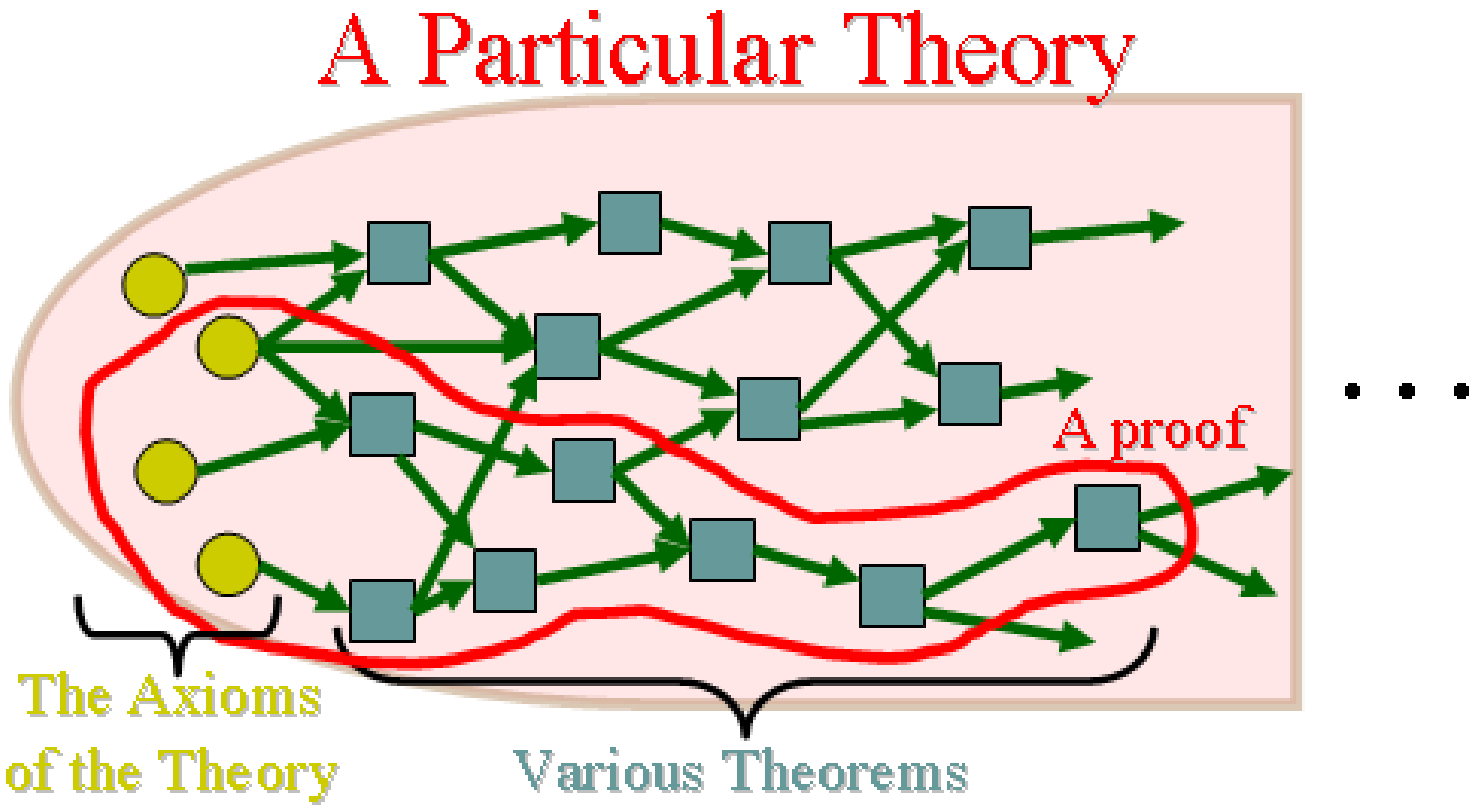
Proof Terminology

- *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

- Inference Rule
  - Pattern establishing that if we know that a set of antecedent statements of certain forms are all true, then a certain related consequent statement is true.

$$\frac{\begin{array}{l}\textit{antecedent } 1\\ \textit{antecedent } 2\ldots\end{array}}{\therefore \textit{consequent}}$$

PS. "$\therefore$" means "therefore"

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

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

How to Prove Inference Rules

- Truth tables.
  - The consequent statement must be true if all antecedent statements are ture.
- Prove the corresponding implication proposition is a tautology.

Some Inference Rules

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

Modus Ponens & Tollens

- $$\frac{p \quad p \rightarrow q}{\therefore q}$$

  Rule of modus ponens
  (a.k.a. law of detachment)
  "the mode of affirming"

- $$\frac{\neg p \quad p \rightarrow q}{\therefore \neg p}$$

  Rule of modus tollens
  "the mode of denying"

Syllogism Inference Rules

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

  Rule of hypothetical syllogism

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

  Rule of disjunctive syllogism

Formal Proofs

- A formal proof of a conclusion, 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 to previously-proven statements (as antecedents) to yield a new true statement q (the consequent).
- A proof demonstrates that *if* the premises are true, *then* the conclusion is true
- In other words, $p_1 \wedge p_2 \wedge \cdots \wedge p_n \rightarrow q$ is a tautology.

Formal Proof Example

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 of the Example

- Let us adopt the following abbreviations:
  1. $sunny$ = "*It is sunny*";
  2. $cold$ = "*It is cold*";
  3. $swim$ = "*We will swim*";
  4. $canoe$ = "*We will canoe*";
  5. $early$ = "*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 (cont.)

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

Inference Rules for Quantifiers

- $\dfrac{\forall x\ P(x)}{\therefore P(o)}$ Universal instantiation (substitute *any* 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.
  - 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.)
- Fallacy of *denying the hypothesis*:
  - "$p \rightarrow q$ is true, and p is false, so q must be false." (No, again because $\mathbf{F} \rightarrow \mathbf{T}$ is true.)

§1.6 Introduction to Proofs

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

Definition

An integer n is called odd iff $n = 2k + 1$ for some integer k; n is even iff $n = 2k$ for some k.

Fact (Axiom)

Every integer is either odd or even.

Theorem

($\forall n$) 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 $n^2 = 2j + 1 (j = 2k^2 + 2k)$, 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 is odd) $\rightarrow \neg$ ($3n+2$ is odd), thus its contra-positive ($3n+2$ is odd) $\rightarrow$ (n 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.
- Thus $\neg p \longrightarrow (q \wedge \neg q)$
- $(q \wedge \neg q)$ is a trivial contradiction, equal to **F**
- Thus $\neg p \longrightarrow \mathbf{F}$, which is only true if $\neg p = \mathbf{F}$
- Thus p is true.

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 even." □

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

Removing the Circularity

Suppose n^2 is even $\therefore 2|n^2 \therefore n^2 \bmod 2 = 0$. Of course $n \bmod 2$ is either 0 or 1. If it's 1, then $n \equiv 1 (\bmod 2)$, so $n^2 \equiv 1 (\bmod 2)$, *using the theorem that if* $a \equiv b (\bmod m)$ *and* $c \equiv d (\bmod m)$ *then* $ac \equiv bd (\bmod m)$, *with* $a = c = n$ *and* $b = d = 1$. Now $n^2 \equiv 1 (\bmod 2)$ implies that $n^2 \bmod 2 = 1$. So *by the hypothetical syllogism rule,* $(n \bmod 2 = 1)$ implies $(n^2 \bmod 2 = 1)$. Since we know $n^2 \bmod 2 = 0 \neq 1$, *by modus tollens* we know that $n \bmod 2 \neq 1$.So *by disjunctive syllogism* we have that $n \bmod 2 = 0$ $\therefore 2|n \therefore n$ is even.

Analysis

- Premises:
  - n^2 is even (and n is integer)
- Proof logic:
  - n is integer $\Longleftrightarrow n \equiv 0 (\mathrm{mod}\, 2) \vee n \equiv 1 (\mathrm{mod}\, 2)$ (enumerate)
  - We want to show "$n \equiv 1 (\mathrm{mod}\, 2)$ is False" (by contradiction)
    - $n \equiv 1 (\mathrm{mod}\, 2) \rightarrow n^2 \equiv 1 (\mathrm{mod}\, 2)$ is True (by calculation)
    - $n^2 \equiv 0 (\mathrm{mod}\, 2)$ is True (premises)
    - modus of tollens
  - So, $n \equiv 0 (\mathrm{mod}\, 2)$ is True (disjunctive syllogism)

Review: Proof Methods So Far

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

§1.7 Proof Methods and Strategy

Proving Existential

- 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.

- *In other words, n is 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...

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.
- $\therefore \forall n \exists x$ s.t. $\forall 1 \leq i \leq n : x + i$ is composite.

□

Nonconstructive Existence Proof

Theorem

There are infinitely many prime numbers.

- Ideas for proof:
  - 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.
  - In other words, 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 $x \bmod p = 1$. So $p > n$, and we're done. (Why?)

The Halting Problem (Turing'36, Skip)

- The halting problem was the first mathematical function proven to have no algorithm that computes it! We say, it is *uncomputable*.
- The function is $Halts(P, I) :\equiv$ "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.

Proof.

- Given any arbitrary program $H(P, I)$,
- Consider algorithm *Breaker*, defined as:
  procedure *Breaker*(P: a program)
  halts := $H(P, P)$
  if *halts* **then while T begin end**
- Note that *Breaker*(*Breaker*) halts iff H(*Breaker*, *Breaker*) = **F**.
- So H does **not** compute the function *Breaker*!

□

More Proof Examples

Example

Quiz question 1a: Is this argument correct or incorrect?

- "All TAs compose easy quizzes. Ramesh is a TA. Therefore, Ramesh composes easy quizzes."

- First, separate the premises from conclusions:
  - Premise #1: All TAs compose easy quizzes.
  - Premise #2: Ramesh is a TA.
  - Conclusion: Ramesh composes easy quizzes.

- Next, re-render the example in logic notation.
  - Premise #1: All TAs compose easy quizzes.
    - Let U.D. = all people
    - Let $T(x) :\equiv$ "x is a TA"
    - Let $E(x) :\equiv$ "x composes easy quizzes"
    - Then Premise #1 says: $\forall x,\ T(x) \longrightarrow E(x)$
  - Premise #2: Ramesh is a TA.
    - Let $R :\equiv$ Ramesh
    - Then Premise #2 says: $T(R)$
  - And the Conclusion says: $E(R)$

The Proof in Gory Detail

- The argument is correct, because it can be reduced to a sequence of applications of valid inference rules, as follows:

Proof.

Statement	How obtained
1. $\forall x,\ T(x) \rightarrow E(x)$	(Premise#1)
2. $T(Ramesh) \rightarrow E(Ramesh)$	(Universal instantiation)
3. $T(Ramesh)$	(Premise#2)
4. $E(Ramesh)$	(Modus Ponens from statements #2 and #3)

□

Another Example

Example (Quiz question 1b: Correct or incorrect?)

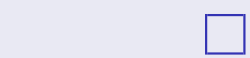
At least one of the 280 students in the class is intelligent. Y is a student of this class. Therefore, Y is intelligent.

- First: Separate premises/conclusion, & translate to logic:
  - Premises:
    1. $\exists x\ \mathit{InClass}(x) \wedge \mathit{Intelligent}(x)$
    2. $\mathit{InClass}(Y)$
  - Conclusion: $\mathit{Intelligent}(Y)$

- **No.** The argument is invalid. We can disprove it with a counter-example.

Disprove by a counter example.

- Consider a case where there is only one intelligent student X in the class, and $X \neq Y$.
  - Then the premise $\exists x\ \mathit{InClass}(x) \wedge \mathit{Intelligent}(x)$ is true, by existential generalization of $\mathit{InClass}(X) \wedge \mathit{Intelligent}(X)$.
  - But the conclusion $\mathit{Intelligent}(Y)$ is false, since X is the only intelligent student in the class, and $Y \neq X$.
- Therefore, the premises do not imply the conclusion.



Another Example (Skip)

Example (Quiz question #2)

Prove that the sum of a rational number and an irrational number is always irrational.

- First, you have to understand exactly what the question is asking you to prove:
  - "For all real numbers x, y, if x is rational and y is irrational, then $x + y$ is irrational."
  - $\forall x, y : \mathit{Rational}(x) \wedge \mathit{Irrational}(y) \longrightarrow \mathit{Irrational}(x + y)$

An Example of Wrong Answers

- 1 is rational. $\sqrt{2}$ is irrational. $1 + \sqrt{2}$ is irrational. Therefore, the sum of a rational number and an irrational number is irrational. (Direct proof.)
- Why does this answer merit no credit?
  - The student attempted to use an example to prove a universal statement. **This is always wrong!**
  - Even as an example, it's incomplete, because the student never even proved that $1 + \sqrt{2}$ is irrational!

Direction of Proof

- Think back to the definitions of the terms used in the statement of the theorem:
  - $\forall$ reals r: $\begin{array}{l} Rational(r) \leftrightarrow \\ \exists Integer(i) \wedge Integer(j) : r = i \end{array}$.
  - $\forall$ reals r: $Irrational(r) \leftrightarrow \neg Rational(r)$.
- You almost always need the definitions of the terms in order to prove the theorem!
- Next, let's go through one valid proof:

What You Might Write

Theorem

$\forall x, y$: *Rational*$(x) \wedge$ *Irrational*$(y) \rightarrow$ *Irrational*$(x + y)$.

Proof.

- *Let x, y be any rational and irrational numbers, respectively. ...(universal generalization)*
- *Now, just from this, what do we know about x and y? You should think back to the definition of rational:*
- *...Since x is rational, we know (from the very definition of rational) that there must be some integers i and j such that $x = \frac{i}{j}$. So, let i_x, j_x be such integers...*
- *we give them unique names so we can refer to them later.*

□

What's Next?

- What do we know about y? Only that y is irrational:$\neg\exists$ integer i, j: $y = \frac{i}{j}$.
- But, it's difficult to see how to use a direct proof in this case. We could try indirect proof also, but in this case, it is a little simpler to just use proof by contradiction (very similar to indirect).
- So, what are we trying to show? Just that $x + y$ is irrational. That is, $\neg\exists i, j$: $(x + y) = \frac{i}{j}$.
- What happens if we hypothesize the negation of this statement?

Prove Continue ...

- Suppose that $x + y$ were not irrational. Then $x + y$ would be rational, so $\exists$ integers i, j: $x + y = \frac{i}{j}$. So, let i_s and j_s be any such integers where $x + y = \frac{i_s}{j_s}$.
- Now, with all these things named, we can start seeing what happens when we put them together.
- So, we have that $(\frac{i_x}{j_x}) + y = (\frac{i_s}{j_s})$.
- Observer! We have enough information now that we can conclude something useful about y, by solving this equation for it.

Finishing the Proof

- Solving that equation for y, we have:

$$y = \left(\frac{i_s}{j_s}\right) - \left(\frac{i_x}{j_x}\right) = \frac{(i_s j_x - i_x j_s)}{(j_s j_x)}$$

- Now, since the numerator and denominator of this expression are both integers, y is (by definition) rational. This contradicts the assumption that y was irrational. Therefore, our hypothesis that $x + y$ is rational must be false, and so the theorem is proved.