Discrete Structures

Inference Rules and Proof Methods

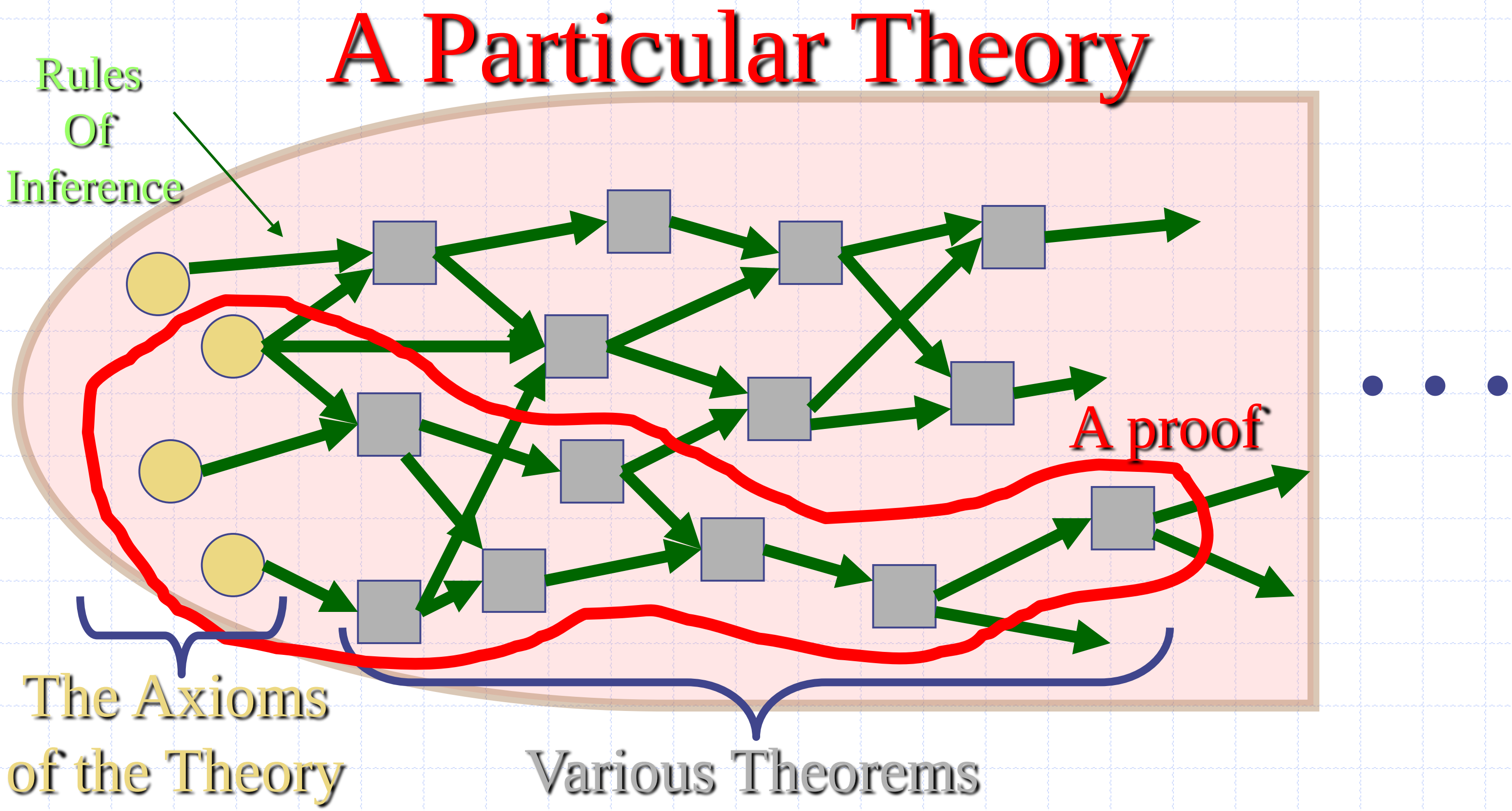
Nature & Importance of Proofs

- In mathematics, a *proof* is:
  - *A sequence of statements that form an argument.*
  - Must be *correct* (well-reasoned, logically valid) and *complete* (clear, detailed) 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.

Rules of Inference

- Rules of inference are patterns of logically valid deductions from hypotheses to conclusions.
- We will review “inference rules” (i.e., correct & fallacious), and “proof methods”.

Visualization of Proofs



Inference Rules - General Form

- *Inference Rule* –
  - Pattern establishing that if we know that a set of *hypotheses* are all true, then a certain related *conclusion* statement is true.

Hypothesis 1
Hypothesis 2 …
$\therefore$ *conclusion*

"$\therefore$" means "therefore"

Inference Rules & Implications

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

- *Hypothesis 1*
  Hypothesis 2 …
  ∴ *conclusion*

  Inference rule

- Corresponding tautology:
  $((Hypoth.\ 1) \wedge (Hypoth.\ 2) \wedge \ldots) \rightarrow conclusion$

Some Inference Rules

- $$\frac{p}{\therefore\ p \lor q}$$

  Rule of Addition

  "It is below freezing now. Therefore, it is either below freezing or raining now."

- $$\frac{p \land q}{\therefore\ p}$$

  Rule of Simplification

  "It is below freezing and raining now. Therefore, it is below freezing now.

Some Inference Rules

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

Rule of Conjunction

- *"It is below freezing.*
- *It is raining now.*
- *Therefore, it is below freezing and it is raining now.*

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*)

  "If it is snows today, then we will go skiing" <u>and</u> *"It is snowing today"* <u>imply</u> *"We will go skiing"*

- $$\begin{array}{l} \neg q \\ \underline{p \rightarrow q} \\ \therefore \neg p \end{array}$$ Rule of *modus tollens*

Syllogism Inference Rules

- $$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$
  Rule of hypothetical syllogism

- $$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$
  Rule of disjunctive syllogism

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 to previously-proven statements (as hypotheses) to yield a new true statement (the conclusion).
- A proof demonstrates that *if* the premises are true, *then* the conclusion is true (i.e., valid argument).

Formal Proof - Example

- Suppose we have the following premises:
  "It is not sunny and it is cold."
  "if it is not sunny, we will not swim"
  "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) $\neg sunny \rightarrow \neg swim$
  (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. $\neg sunny \rightarrow \neg swim$	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.

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 **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.)

Common Fallacies - Examples

"If you do every problem in this book, then you will learn discrete mathematics. You learned discrete mathematics."

p: "You did every problem in this book"

q: "You learned discrete mathematics"

- Fallacy of *affirming the conclusion*:
  - $p \to q$ *and* q does not imply p
- Fallacy of *denying the hypothesis*:
  - $p \to q$ and $\neg p$ does not imply $\neg q$

Inference Rules for Quantifiers

Universal instantiation

- $\dfrac{\forall x\, P(x)}{\therefore P(c) \text{ for } \textit{any} \text{ element } c}$

Universal generalization

- $\dfrac{P(c) \text{ for an arbitrary } c}{\therefore \forall x\, P(x)}$

Existential instantiation

- $\dfrac{\exists x\, P(x)}{\therefore P(c) \text{ for some element } c}$

Existential generalization

- $\dfrac{P(c) \text{ for some element } c}{\therefore \exists x\, P(x)}$

Example

"*Everyone in this discrete math class has taken a course in computer science*" <u>and</u> "*Marla is a student in this class*" <u>imply</u> "*Marla has taken a course in computer science*"

D(x): "*x is in discrete math class*"
C(x): "*x has taken a course in computer science*"

$$\begin{array}{l} \forall x\,(D(x) \rightarrow C(x)) \\ D(\text{Marla}) \\ \hline \therefore\ C(\text{Marla}) \end{array}$$

Example – cont.

Step	Proved by
1. $\forall x\,(D(x) \rightarrow C(x))$	Premise #1.
2. $D(Marla) \rightarrow C(Marla)$	Univ. instantiation.
3. $D(Marla)$	Premise #2.
4. $C(Marla)$	Modus ponens on 2,3.

Another Example

"*A student in this class has not read the book*" and "*Everyone in this class passed the first exam*" imply "*Someone who passed the first exam has not read the book*"

C(x): "*x is in this class*"
B(x): "*x has read the book*"
P(x): "*x passed the first exam*"

$$\begin{array}{l} \exists x(C(x) \land \neg B(x)) \\ \forall x\,(C(x) \rightarrow P(x)) \\ \hline \therefore\ \exists x(P(x) \land \neg B(x)) \end{array}$$

Another Example – cont.

Step	Proved by
1. $\exists x(C(x) \wedge \neg B(x))$	Premise #1.
2. $C(a) \wedge \neg B(a)$	Exist. instantiation.
3. $C(a)$	Simplification on 2.
4. $\forall x\,(C(x) \rightarrow P(x))$	Premise #2.
5. $C(a) \rightarrow P(a)$	Univ. instantiation.
6. $P(a)$	Modus ponens on 3,5
7. $\neg B(a)$	Simplification on 2
8. $P(a) \wedge \neg B(a)$	Conjunction on 6,7
9. $\exists x(P(x) \wedge \neg B(x))$	Exist. generalization

More Examples...

- 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.

Answer

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: $\forall x,\ T(x) \rightarrow E(x)$

Answer cont…

- Premise #2: Ramesh is a TA.
  - Let R :≡ Ramesh
  - Then Premise #2 says: $T(R)$
- Conclusion says: $E(R)$
- The argument is correct, because it can be reduced to a sequence of applications of valid inference rules, as follows:

The Proof in Detail

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

Another example

- Correct or incorrect? At least one of the 105 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) $\exists x\, InClass(x) \wedge Intelligent(x)$
    (2) InClass(Y)
  - Conclusion: Intelligent(Y)

Answer

- No, the argument is invalid; we can disprove it with a counter-example, as follows:

- Consider a case where there is only one intelligent student X in the class, and X≠Y.
  - Then the premise ∃*x* **InClass(*x*)** ∧ **Intelligent(*x*)** is true, by existential generalization of **InClass(X)** ∧ **Intelligent(X)**
  - But the conclusion **Intelligent(Y)** is false, since X is the only intelligent student in the class, and Y≠X.

- Therefore, the premises *do not* imply the conclusion.

Proof Methods

- Proving $p \to q$
  - *Direct* proof: Assume p is true, and prove q.
  - *Indirect* proof: Assume $\neg q$, and prove $\neg p$.
  - *Trivial* proof: Prove q true.
  - *Vacuous* proof: Prove $\neg p$ is true.
- Proving p
  - Proof by *contradiction:* Prove $\neg p \to (r \wedge \neg r)$

  ($r \wedge \neg r$ is a contradiction); therefore $\neg p$ must be false.
- Prove $(a \vee b) \to p$
  - Proof by cases: prove $(a \to p)$ and $(b \to p)$.
- More …

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.
- **Axiom:** Every integer is either odd or even.
- **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. □

Another Example

- **Definition:** A real number *r* is *rational* if there exist integers *p* and $q \neq 0$, with no common factors other than 1 (i.e., gcd(p,q)=1), such that $r=p/q$. A real number that is not rational is called *irrational*.

- **Theorem:** Prove that the sum of two rational numbers is rational.

Indirect Proof

- Proving $p \to q$
  - *Indirect* proof: Assume $\neg q$, and prove $\neg p$.

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

Another Example

- **Theorem:** Prove that if *n* is an integer and n^2 is odd, then *n* is odd.

Trivial Proof

- Proving $p \to q$
  - *Trivial* proof: Prove q 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 hypothesis. Thus the implication is true trivially. □

Vacuous Proof

- Proving $p \rightarrow q$
  - *Vacuous* proof: Prove $\neg p$ is 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. □

Proof by Contradiction

- Proving p
  - Assume $\neg p$, and prove that $\neg p \rightarrow (r \wedge \neg r)$
  - $(r \wedge \neg r)$ is a trivial contradiction, equal to **F**
  - Thus $\neg p \rightarrow$**F** is true only if $\neg p$=**F**

Contradiction Proof Example

- **Theorem:** Prove that $\sqrt{2}$ is irrational.

Another Example

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

Answer

- Next, think back to the definitions of the terms used in the statement of the theorem:
  - $\forall$ reals r: Rational(r) $\leftrightarrow$
    $\exists$ Integer(i) $\wedge$ Integer(j): $r = i/j$.
  - $\forall$ 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 $x = i/j$. So, let i_x, j_x be such integers …
- We give them unique names so we can refer to them later.

What next?

- What do we know about y? Only that y is irrational: $\neg\exists$ integers i,j: $y = i/j$.
- 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, $\neg\exists i,j$: $(x + y) = i/j$.
- What happens if we hypothesize the negation of this statement?

More writing…

- Suppose that $x+y$ were not irrational. Then $x+y$ would be rational, so $\exists$ integers i,j: $x+y = i/j$. So, let i_s and j_s be any such integers where $x+y = i_s/j_s$.
- Now, with all these things named, we can start seeing what happens when we put them together.
- So, we have that $(i_x/j_x) + y = (i_s/j_s)$.
- Observe! 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:

  $$y = (i_s/j_s) - (i_x/j_x)$$
  $$= (i_s j_x - i_x j_s)/(j_s j_x)$$

  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.

Proof by Cases

To prove $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$

we need to prove

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)$$

Example: Show that *|xy|=|x| |y|*, where *x,y* are real numbers.

Proof of Equivalences

To prove

$$p \leftrightarrow q$$

we need to prove

$$(p \rightarrow q) \land (q \rightarrow p)$$

<u>Example</u>: Prove that n is odd iff n^2 is odd.

Equivalence of a group of propositions

To prove

$$[p_1 \leftrightarrow p_2 \leftrightarrow \ldots \leftrightarrow p_n]$$

we need to prove

$$[(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \ldots (p_n \rightarrow p_1)]$$

Example

- Show that the statements below are equivalent:

  p_1: *n is even*

  p_2: *$n-1$ is odd*

  p_3: *n^2 is even*

Counterexamples

- When we are presented with a statement of the form $\forall x P(x)$ and we believe that it is false, then we look for a counterexample.

- Example
  - Is it true that "every positive integer is the sum of the squares of three integers?"

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 called a *constructive* proof.

- Otherwise, it is called a *non-constructive* proof.

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.

Existence Proof

- **Definition:** *A* composite is an integer which is not prime.
- **Theorem:** For any integer $n>0$, there exists a sequence of n consecutive composite integers.
- Same statement in predicate logic:
  $\forall n>0\ \exists x\ \forall i\ (1 \le i \le n) \rightarrow (x+i$ is composite$)$

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.

Non-constructive Existence Proof

- **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 <u>there is *no* largest prime number</u>.
- *i.e.*, **show that for any prime number, there is a larger number that is *also* prime.**
- <u>More generally:</u> 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 $(x \text{ is prime}) \vee (x \text{ is composite})$.
- **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 $p \bmod x = 1$. So $p>n$, and we're done.

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).

References

- *Sections 1.5 and 1.6 of the text book "Discrete Mathematics and its Applications" by Rosen, 6th edition.*
- The original slides were prepared by Bebis