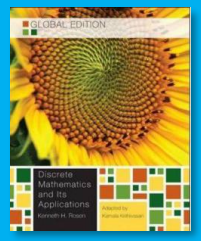
ITP20002-01 Discrete Mathematics

Proof

18 September 2018



- Taken from the instructor's resource of *Discrete Mathematics and Its Applications,* 7/e
- Edited by Shin Hong hongshin@handong.edu

Chapter 1. Logic and Proofs

- ~~Propositional logic (1.1, 1.2)~~
- ~~Logical equivalence and satisfiability (1.3)~~
- ~~Predicate logic (1.4, 1.5)~~
- Inference (1.6, 1.7)
- Proof basics (1.8, 1.9)

How can we find whether his argument is true or not?

Proof and Inference

- An argument is a sequence of propositions
  - a proposition is derived from the preceding propositions by an inference rule
  - the last proposition is called *conclusion*

- A proof is a sequence of premises and valid arguments
  - a premise is a proposition known/accepted to be true
  - an argument is valid if it is based on premises and the conclusions of valid arguments and follows inference rules

- Example
  1. If you have a current password, you can log onto the net
  2. You have a current password
  3. You can log onto the net

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

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

Rules of Inferences

premise$_1$
premise$_2$
…
---
conclusion

p $p \rightarrow q$ $\therefore q$	Modus ponens
$\neg q$ $p \rightarrow q$ $\therefore \neg p$	Modus tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	Disjunctive syllogism
p $\therefore p \vee q$	Addition
$p \wedge q$ $\therefore p$	Simplification
p q $\therefore p \wedge q$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	Resolution

Intuitive Examples

- If one is a man, the one dies (i.e., every man dies).
  Socrates is a man.
  Thus, Socrates dies.

- Fire alarm rings if there's fire.
  There is no fire alarm.
  Thus, there is no fire.

- If one is a man, the one dies.
  If one is a professor, the one is a man.
  Thus, every professor dies.

- I will take a taxi tonight if it rains.
  Otherwise, I will take a bus tonight.
  Thereby, I will take a taxi or bus tonight.

Handling Quantified Statements

- Valid arguments for quantified statements are a sequence of statements. Each statement is either a premise or follows from previous statements by rules of inference which include:
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Quantified Statements
- The rules of inference for quantified statements are introduced in the next several slides.

Universal Instantiation (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Example:

Our domain consists of all dogs and Fido is a dog.

"All dogs are cuddly."

"Therefore, Fido is cuddly."

Universal Generalization (UG)

$$\frac{P(c) \text{ for an arbitrary } c}{\therefore \forall x P(x)}$$

Used often implicitly in Mathematical Proofs.

Existential Instantiation (EI)

$$\frac{\exists x P(x)}{\therefore P(c) \text{ for some element } c}$$

Example:

"There is someone who got an A in the course."
"Let's call her *a* and say that *a* got an A"

Existential Generalization (EG)

$$\frac{P(c) \text{ for some element } c}{\therefore \exists x P(x)}$$

Example:

"Michelle got an A in the class."
"Therefore, someone got an A in the class."

Using Rules of Inference

Example 1: Using the rules of inference, construct a valid argument to show that

"John Smith has two legs"

is a consequence of the premises:

"Every man has two legs." "John Smith is a man."

Solution: Let $M(x)$ denote "x is a man" and $L(x)$ " x has two legs" and let John Smith be a member of the domain.

Valid Argument:

Step	**Reason**
1. $\forall x(M(x) \rightarrow L(x))$	Premise
2. $M(J) \rightarrow L(J)$	UI from (1)
3. $M(J)$	Premise
4. $L(J)$	Modus Ponens using (2) and (3)

Using Rules of Inference

Example 2: Use the rules of inference to construct a valid argument showing that the conclusion

"Someone who passed the first exam has not read the book."

follows from the premises

"A student in this class has not read the book."

"Everyone in this class passed the first exam."

Solution: Let $C(x)$ denote "x is in this class," $B(x)$ denote "x has read the book," and $P(x)$ denote "x passed the first exam."

First we translate the premises and conclusion into symbolic form.

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

Continued on next slide →

Using Rules of Inference

Valid Argument:

Step	**Reason**
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	EI from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	UI from (4)
6. $P(a)$	MP from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conj from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	EG from (8)

Returning to the Socrates Example

$$\forall x(Man(x) \rightarrow Mortal(x))$$

$$\frac{Man(Socrates)}{\therefore \quad Mortal(Socrates)}$$

Proof

- A theorem is an important proposition that can be shown true
  - A theorem (or fact) is a proposition that is true
  - A lemma is a less important proposition that is true
  - A corollary is a theorem directly established from a main theorem

- A proof is a valid argument that establishes the truth of a theorem
  - A proof can include axioms (postulates) which are statement assumed / believed to be true
  - A proof can include proven theorems
  - A proof can include premises
  - A proof include a conclusion from valid assertions by a valid inference rule

- A conjecture is a statement proposed to be true without a proof

Proving Methods

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Exhaustive proof
- Existence proof

Direct Proofs

- A direct proof of $p \rightarrow q$ is constructed as follows:
  - first step is the assumption that p is true
  - subsequent steps are constructed by rules of inferences
  - final step shows that q is true under the assumption

- Example: prove that n^2 is odd if n is an odd integer

1.	x is odd iff there is a positive integer y s.t. x=2y -1	theorem
2.	n is odd	premise
3.	there is a positive integer m s.t. n = 2m - 1	MP 1L,2
4.	$n^2 = (2m-1)^2 = 4m^2 - 2m + 1$	arithem.
5.	$n^2 = 2(4m^2 - 2m) + 1$	arithem.
6.	n^2 is odd	MP 1R,5

Proof by Contraposition

- Use the fact that $p \rightarrow q$ is equivalent to $\neg q \rightarrow \neg p$

- Example: prove that an integer n is odd if $3n$+2 is odd

  CP = if n is not an odd integer, then $3n$+2 is not odd

1.	if an integer is not odd, the integer is even	theorem
2.	*n* is not an odd integer	premise
3.	*n* is even	MP 2,1
4.	if *x* is even, there is an integer y s.t. *x* = 2*y*	theorem
5.	there is an integer m s.t. $n = 2m$	MP 3, 4
6.	3n+2 = 3(2m) + 2 = 2(3m + 1)	arithm.
7.	if there is an integer y s.t. x = 2y, x is even	theorem
8.	3n+2 is even	MP 6,7

Proof by Contradiction

- Proving p by contradiction
  1. show that $\neg p \rightarrow q$ is true for a statement q
  2. show that q is always false (i.e., unsatisfiable or contradiction)
  3. conclude that p is true by Modus Tollens 1, 2

- Example: prove that $\sqrt{2}$ is irrational.
  1. assume that $\sqrt{2}$ is rational
  2. there are two integers a and b such that $\sqrt{2} = \frac{a}{b}$, and a and b have no common factor
  3. $2b^2 = a^2$
  4. a^2 is even, and there is an integer c such that $2c = a$
  5. $2b^2 = (2c)^2 = 4c^2$
  6. b^2 is even as $b^2 = 2c^2$
  7. a and b have a common factor as 2
  8. it is a contradiction that statements 2 and 7 hold at the same time

Exhaustive Proof

- An exhaustive proof of a conditional statement $p \rightarrow q$ first divides the condition into multiple cases (i.e., $p = p_1 \vee p_2 \ldots \vee p_n$) and then proves that the conclusion holds for every case (i.e., $\bigwedge_{i=1}^{n} p_i \rightarrow q$)

- Proof by cases
  - A proof must cover all possible cases that arise in a theorem exhaustively.

- Ex. Prove that if n is an integer, then $n^2 \geq n$ holds.
  - Case 1. $n = 0$: it is shown that $n^2 \geq n$ as $0^2 \geq 0$.
  - Case 2. $n > 0$: $n^2 \geq n$ as $n^2 \geq n \times 1$ and $n \geq 1$
  - Case 3. $n < 0$: $n^2 \geq n$ as $n^2 \geq 0 > n$

Existence Proof

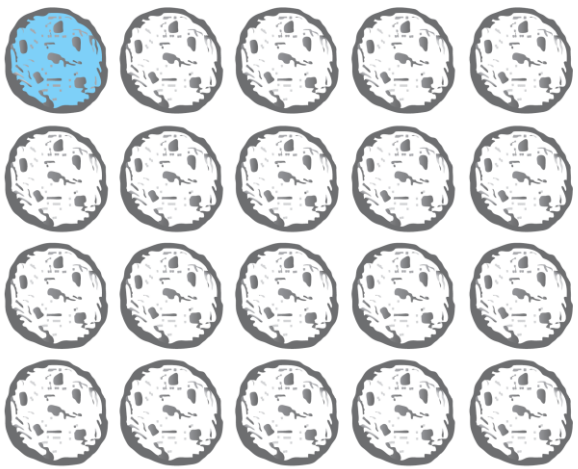
- An existence proof is to assert $\exists x P(x)$
- Strategies
  - Constructive proof: give a concrete case x that $P(x)$ holds
  - Nonconstructive proof: e.g., prove that $\neg\exists x P(x)$ is false

- Ex1 (constructive proof). show there is a positive integer that can be written as the sum of cubics of two positive integers in two different ways.
  - Proof. $1729 = 10^3 + 9^3 = 12^3 + 1^3$

- Ex2 (nonconstructive proof). show that there are two irrational numbers x and y such that x^y is a rational number.
  - $\sqrt{2}$ is an irrational number.
  - Case 1. $\sqrt{2}^{\sqrt{2}}$ is rational : the claimed statement holds for $x = \sqrt{2}$ and $y = \sqrt{2}$
  - Case 2. $\sqrt{2}^{\sqrt{2}}$ is irrational : the claimed statement holds for $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

    because $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$ is a rational number

Example 12. Chomp Game

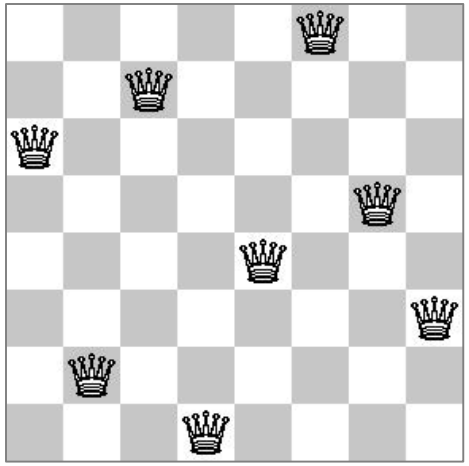


- Game setting
  - There are $m \times n$ cookies arranged as a m-by-n grid for $m > 1$ and $n > 1$
  - Turn-over game with two players: Player 1, Player 2, and repeat
  - In each turn, a player must pick a remaining cookie. Then the player takes the picked one and all the ones to the right and/or below the picked on
  - The loser is one who takes the cookie at the top left corner (i.e., the poisoned); the other one is the winner

- Theorem. There is no winning strategy for Player 2
  - There is no way that in any circumstance, Player 2 picks a cookie such that Player 2 has a chance to win the game over Player 1 in all subsequent cases

Solving Problems with SMT Solver

- A SMT solver is a tool that determine the satisfiability and find a solution of a certain kind of a given predicate formulas called *Satisfiability Modulo Theory* formula (e.g., propositional logic, linear integer arithmetic) by applying inference rules automatically
  - practical because search heuristics find results very quickly for most inputs
  - E.g., Microsoft Research Z3 (https://github.com/Z3Prover/z3)
- Once a problem can be represented as a satisfiability of a SMT formula, we can solve the problem quickly without having a specific algorithm for the problem
- Example: N-Queen Problems
  - Problem: find a placement of N number of queens on checkboard such that they do not conflict with each other
  - Modeling: assign an integer to every cell, which has 1 for having a queen and 0 otherwise
  - Constraint:
    - Each integer should be either 0 or 1
    - The sum of all integers should be the same as *N*
    - For each cell, the sum of the integers on the same row/column/diagonal-line should be less than or equal to 1



<One solution for N = 8>