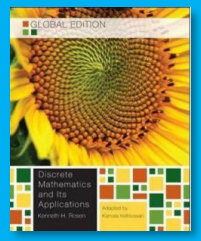
ITP20002-01 Discrete Mathematics

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

- 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)

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

c is a specific instance of the domain, or
c is a variable representing arbitrary value of the domain

Example:

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

“All dogs are cuddly.”

“Therefore, Fido is cuddly.”
"Therefore, dog *x* 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 J be an element representing John Smith.

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