CSCI 1900
Discrete Structures

Methods of Proof
Reading: Kolman, Section 2.3

Past Experience

Up to now we've used the following methods to write proofs:

- Used direct proofs with generic elements, definitions, and given facts
- Used proof by cases such as when we used truth tables

General Description of Process

- $p \Rightarrow q$ denotes "q logically follows from p"
- Implication may take the form $(p_1 \wedge p_2 \wedge p_3 \wedge \ldots \wedge p_n) \Rightarrow q$
- q logically follows from $p_1, p_2, p_3, \ldots, p_n$

General Description (continued)

The process is generally written as:

p_1
p_2
p_3
:
:
p_n
$\therefore q$

Components of a Proof

- The p_i's are called ***hypotheses*** or ***premises***
- q is called the ***conclusion***
- Proof shows that if all of the p_i's are true, then q has to be true
- If result is a tautology, then the implication $p \Rightarrow q$ represents a universally correct method of reasoning and is called a ***rule of inference***

Example of a Proof based on a Tautology

- If p implies q and q implies r, then p implies r

  $p \Rightarrow q$
  $\underline{q \Rightarrow r}$
  $\therefore p \Rightarrow r$

- By replacing the bar under $q \Rightarrow r$ with the "$\Rightarrow$", the proof above becomes $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
- The next slide shows that this is a tautology and therefore is universally valid.

Tautology Example (continued)

p	q	r	$p \Rightarrow q$	$q \Rightarrow r$	$(p \Rightarrow q) \wedge (q \Rightarrow r)$	$p \Rightarrow r$	$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Equivalences

- Some mathematical theorems are equivalences, i.e., $p \Leftrightarrow q$.
- The proof of such a theorem is equivalent with proving both $p \Rightarrow q$ and $q \Rightarrow p$

modus ponens form (the method of asserting):

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

- Example:
  - p: a man used the toilet
  - q: the toilet seat is up
  - $p \Rightarrow q$: If a man used the toilet, the seat was left up
- Supported by the tautology $(p \wedge (p \Rightarrow q)) \Rightarrow q$

modus ponens (continued)

p	q	$(p \Rightarrow q)$	$p \wedge (p \Rightarrow q)$	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Invalid Conclusions from Invalid Premises

- Just because the format of the argument is valid does not mean that the conclusion is true. A premise may be false. For example:

  Acorns are money
  <u>If acorns were money, no one would have to work</u>
  $\therefore$ No one has to work

- Argument is valid since it is in modus ponens form
- Conclusion is false because premise p is false

Invalid Conclusion from Invalid Argument

- Sometimes, an argument that looks like modus ponens is actually not in the correct form. For example:
- If tuition was free, enrollment would increase
  <u>Enrollment increased</u>
  $\therefore$ Tuition is free
- Argument is invalid since its form is:

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

Invalid Argument (continued)

- Truth table shows that this is not a tautology:

p	q	$(p \Rightarrow q)$	$(p \Rightarrow q) \wedge q$	$((p \Rightarrow q) \wedge q) \Rightarrow p$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	F	T

Indirect Method

- Another method of proof is to use the tautology:

$$(p \Rightarrow q) \Leftrightarrow (\sim q \Rightarrow \sim p)$$

- The form of the proof is:

$\sim q$
$\sim q \Rightarrow \sim p$
$\therefore p$

Indirect Method Example

- p: My e-mail address is available on a web site
- q: I am getting spam
- $p \Rightarrow q$: If my e-mail address is available on a web site, then I am getting spam
- $\sim q \Rightarrow \sim p$: If I am not getting spam, then my e-mail address must not be available on a web site
- This proof says that if I am not getting spam, then my e-mail address is not on a web site.

Another Indirect Method Example

- Prove that if the square of an integer is odd, then the integer is odd too.
- p: n^2 is odd
- q: n is odd
- $\sim q \Rightarrow \sim p$: If n is even, then n^2 is even.

- If n is even, then there exists an integer m for which $n = 2 \times m$. n^2 therefore would equal $(2 \times m)^2 = 4 \times m^2$ which must be even.

Proof by Contradiction

- Another method of proof is to use the tautology $(p \Rightarrow q) \wedge (\sim q) \Rightarrow (\sim p)$
- The form of the proof is:

$p \Rightarrow q$
$\sim q$
$\therefore \sim p$

Proof by Contradiction (continued)

p	q	$(p \Rightarrow q)$	$\sim q$	$(p \Rightarrow q) \wedge \sim q$	$\sim p$	$(p \Rightarrow q) \wedge (\sim q) \Rightarrow (\sim p)$
T	T	T	F	F	F	T
T	F	F	T	F	F	T
F	T	T	F	F	T	T
F	F	T	T	T	T	T

Proof by Contradiction (continued)

- The best application for this is where you cannot possibly go through a large number (such as infinite) of cases to prove that every one is true.

Proof by Contradiction Example

Prove that $\sqrt{(2)}$ is irrational, i.e., cannot be represented with m/n where m and n are integers.

- p: $\sqrt{(2)}$ is a rational number
- q: There exists integers m and n for every rational number such that the rational number can be expressed as m/n
- $p \Rightarrow q$: If $\sqrt{(2)}$ is a rational number, then we can find m and n
- The goal is to prove that we cannot find an m and an n, i.e., ~q is true.

Proof by Contradiction Example (continued)

- Assume $(m/n)^2 = 2$ and that m and n are in their most reduced form. This means that $m^2 = 2n^2$.
- Therefore, m must be even and m^2 must contain 2^2
- Therefore, n must be even too.
- Therefore, m/n is not in the most reduced form (we can pull a 2 out of both m and n).
- This is a contradiction! Cannot come up with m and n, i.e., ~q is true
- Therefore, ~p is true and $\sqrt{(2)}$ must not be a rational number