

Mat 2345

Chapter Three

Mathematical Reasoning

Fall 2007

Chapter Three Overview

- ▶ 3.1 Methods of Proof
- ▶ 3.2 **Mathematical Induction**
- ▶ 3.3 Recursive Definitions
- ▶ 3.4 Recursive Algorithms
- ▶ 3.5 Program Correctness

Section 3.1 — Methods of Proof

Why bother?

We need to be able to answer questions such as:

When is an argument correct?

How can we construct a “mathematical” argument?

Applications to Computer Science include:

- ▶ Used to verify program correctness
- ▶ Establishing operating system security
- ▶ Making inferences in the area of artificial intelligence
- ▶ ...and many more

Propositional Logic

Rules of Inference — rules that provide justification of the steps used to show that a **conclusion** follows **logically** from a set of **premises**.

modus ponens or the **law of detachment** — the **tautology**
 $(p \wedge (p \rightarrow q)) \rightarrow q$

Notation used by book:

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

If an implication and its premises are true, then the conclusion of the implication is true.

Rules of Inference

Rule of Inference	Tautology	Name
$\frac{p}{\therefore p \vee q}$	$p \rightarrow (p \vee q)$	Addition
$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification
$\frac{p}{q} \\ \frac{q}{\therefore p \wedge q}$	$((p) \wedge (q)) \rightarrow (p \wedge q)$	Conjunction
$\frac{p}{p \rightarrow q} \\ \therefore q$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens

Rules of Inference

Rule of Inference	Tautology	Name
$\neg q$ $p \rightarrow q$ <hr/> $\therefore \neg p$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens
$p \rightarrow q$ $q \rightarrow r$ <hr/> $\therefore p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ <hr/> $\therefore q$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Disjunctive syllogism

Incorrect Arguments — Fallacies

There are several common errors in logic, based on contingencies rather than tautologies.

▶ **fallacy of affirming the conclusion**

$[(p \rightarrow q) \wedge q] \rightarrow p$ (false when p is false and q is true)

▶ **fallacy of denying the hypothesis**

$[(p \rightarrow q) \wedge \neg p] \rightarrow \neg q$ (false when p is false and q is true)

▶ **begging the question or circular reasoning**

One or more steps in a proof are based on the truth of the statement being proved

Rules of Inference for quantified statements

Given c is a member of the universe of discourse:

▶ **Universal Instantiation:**

If $\forall xP(x)$, then $P(c)$ is true

▶ **Universal generalization:**

If for arbitrary $cP(c)$ is true, then $\forall xP(x)$

▶ **Existential instantiation:**

If $\exists xP(x)$, then for some c , $P(c)$ is true
(c cannot be arbitrary)

▶ **Existential generalization:**

If for a particular $cP(c)$ is true, then $\exists xP(x)$

Methods of Proving Theorems

- ▶ **Direct proof**

Given $p \rightarrow q$, assume p is true and show q must also be true (using rules of inference and theorems)

- ▶ **Indirect proof**

Since $p \rightarrow q$ is equivalent to its contrapositive, $\neg q \rightarrow \neg p$, assume the conclusion is false and show the premise must be false

- ▶ **Vacuous proof**

Given $p \rightarrow q$, show p is false, then the implication is vacuously true

- ▶ **Trivial proof**

$p \rightarrow q$ is true when $T \rightarrow T$ or $F \rightarrow T$, so if q can be shown to be true, the implication is trivially true

More Methods of Proving Theorems

- ▶ **Proof by contradiction**

Assume $\neg q$ is true (i.e., $\neg p \rightarrow F$ is true), then $\neg p$ must be false, and hence p must be true

- ▶ **Proof by cases**

When an implication consists of a disjunction of propositions, p_i , each of the p_i can be proven individually to prove the original implication

- ▶ **Existential proof: constructive**

A proof of the proposition $\exists xP(x)$; find such an element

- ▶ **Existential proof: nonconstructive**

Show indirectly such a value exists, perhaps using proof by contradiction

More Methods of Proving Theorems

- ▶ **Counterexample**

Show \exists an a for which $P(a)$ is false; only one such example is necessary

- ▶ **Mathematical Induction**

Extremely important proof technique used extensively to prove results about a large variety of discrete objects.

(Read about the famous Halting Problem mentioned earlier on page 181 in textbook.)

3.2 Mathematical Induction

- ▶ Similar to an infinite line of people, Person_1 , Person_2 , etc.
- ▶ A secret is told to Person_1 , and each person tells the secret to the next person in line — if the former person hears it.
- ▶ Let $P(n)$ be the proposition that Person_n knows the secret.
- ▶ Then $P(1)$ is true since the secret is told to Person_1 .
- ▶ $P(2)$ is true since Person_1 tells Person_2 , and so on.
- ▶ By the **Principle of Mathematical Induction**, every person in line learns the secret.

Mathematical Induction — Another Example

- ▶ Consider an infinite row of dominos labeled $1, 2, 3, \dots, n$, where each domino is positioned to knock the next one over when it falls.
- ▶ Let $P(n)$ be the proposition that domino n is knocked over.
- ▶ If the first domino is knocked over, i.e., $P(1)$ is true, and if whenever the n^{th} domino is knocked over, it also knocks over the $(n+1)^{\text{st}}$ domino (i.e., $P(n) \rightarrow P(n+1)$ is true), then all the dominos are knocked over.

Parts of an Induction Proof

- ▶ **Basis or Base Case (BC)**

Show the proposition is true for some small starting value

- ▶ **Inductive Hypothesis (IH)**

Assume the proposition is true for an arbitrary n

- ▶ **Inductive Step (IS)**

Show the proposition is true for $(n+1)$, using the inductive hypothesis

- ▶ give reasons for each step in the proof
- ▶ usually begin with the LHS and show logical steps to reach the RHS

Prove the theorem

$$\sum_{i=0}^n i = \frac{n(n+1)}{2}, \forall n \geq 0$$

Prove the theorem

$$\sum_{i=1}^n i(i+1)(i+2) = \frac{n(n+1)(n+2)(n+3)}{4}, \forall n \geq 1$$

Prove the theorem

$$\sum_{i=0}^n 2^i = 2^{n+1} - 1, \forall n \geq 1$$

Prove the theorem

$$n^5 - n \mid_5, \forall n \in \mathbb{N}$$

Prove the theorem

A plane divided into regions by any number of distinct straight lines, no three of which intersect at the same point (called **standard position**), can be painted with black and white paint in such a way that any two regions having a common boundary will be painted in different colors.

Prove the theorem

$$\sum_{i=0}^n i(i!) = (n+1)! - 1, \forall n \geq 1$$

Prove the theorem

$$8^n - 2^n \mid 6, \forall n \in \mathbb{N}$$

Prove the theorem

$$x^n - y^n \mid x - y, \forall n, x, y \in \mathbb{N}, \text{ and } y \geq 0, x \neq y$$

Prove the theorem

$n! > 2^n, \forall$ natural numbers $n \geq 4$

Prove the theorem

$$\sum_{i=0}^n r^i = \frac{r^{n+1}-1}{r-1}, \forall n \in \mathbb{N}, r \neq 0, r \neq 1$$

Prove the Pigeon-hole Principle

If $n + 1$ balls ($n \geq 1$) are put inside n boxes, then at least one box will contain more than one ball.

Example of Strong Induction

All integers $n \geq 2$ can be written as a product of prime numbers (and 1)

Suppose the sequence (s_0, s_1, s_2, \dots) satisfies the conditions $s_0 = a$ and $s_n = 2s_{n-1} + b$ for some constants a and b , and $\forall n \in \mathbb{N}$. Can we find a formula (closed form) to describe s_n ?