Home Page

Title Page

Contents

◀◀ ▶▶

◀ ▶

Go Back

Full Screen

Close

Quit

CS206 Lecture 04
Proof Procedures

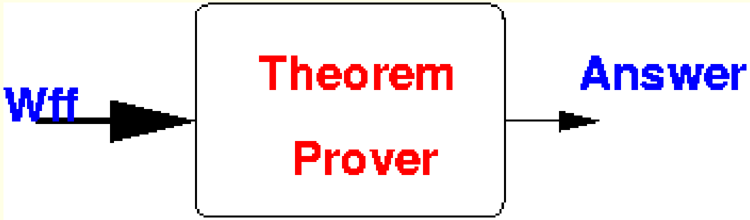
G. Sivakumar
Computer Science Department
IIT Bombay
siva@iitb.ac.in
http://www.cse.iitb.ac.in/∼siva

Mon, Jan 06, 2003

Plan for Lecture 04

- Proof Procedures
- Boolean Ring Method

Proof Procedure



Possible Answers

Satisfiable

Tautology

Contradiction

...

Don't know!

Doesn't Stop?

Decision Procedure

- A Proof procedure is a Decision Procedure (Algorithm) if it always halts with an answer in finite time.
- Soundness

  A proof procedure is *sound* if it never gives a wrong answer.

For Propositional Logic there are many sound decision procedures.

- Truth Table.
- Semantic Methods (Gentzen)
  - Natural Deduction
  - Sequent Calculus
- Syntactic Methods
  - Hilbert's Proof System
  - Simplification (Boolean Ring)
  - Resolution Theorem Proving
  - Binary Decision Diagrams (BDD)

Why so many methods? Efficiency.

Completeness

For some logics (we'll see later), it is not possible to give decision procedures.
That is, every theorem prover that is sound, will not halt on some inputs! (*a very non-intuitive and hard result to prove.*).
Completeness of a proof procedure is a weaker notion than termination.
Informal Definition

- A proof procedure is complete, if whenever the input is satisfiable, it answers correctly that it is satisfiable.

(Note: Nothing implied about behaviour when input is a contradiction).
This leads to the notion of a **semi-decision** procedure.

A Semi-Decision Procedure

A trivial example, to illustrate the concept.

Input: A polyonmial $P(x)$ (example: $3x^3 + 2x - 5$).

Problem: Does the polynomial have postive integer root? (that is, is there $x \geq 0$ such that $P(x) = 0$?).

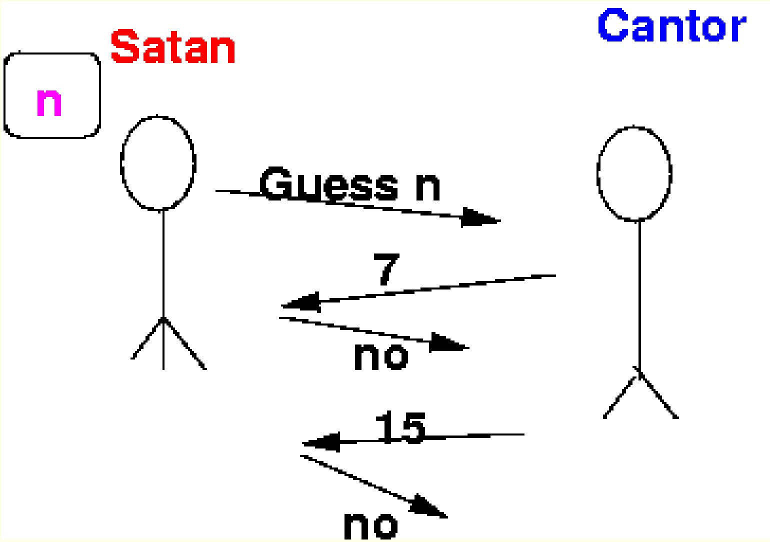
Semidecision Procedure

```
i = 0
repeat
  if P(i) = 0
 then print YES
      break
  else i = i + 1
end repeat
```

This method is **sound** and **complete**, but is not a **decision procedure**.

Satan-Cantor Puzzle

Very interesting formulation (Raymond Smullyan).



Satan-Cantor Variations

- Natural Numbers (0,1,2,3 ...)
- Integers (Negative numbers also)
- Pairs (,$\langle < 3, 8 > \rangle \langle < -4, 7 > \rangle$
- Triples, Quadruples, ...
- N-tuple with N unknown, but finite.
- Real Numbers

Notions of

- Countable
- Fair Enumeration

are very useful in proof procedures (and logic programming)

Booelan Ring Rewriting Method

Given a set R of rewriting rules, proceed as follows.

- Start with f as input formula f_0
- Repeat
  - If f "simplifies" to f_1 using R
    - then let $f = f_1$
    - else f is a normal form. Break
- If $f = 0$ print "Contradiction"
  - elseif $f = 1$ print "Tautology"
  - else print "Satisfiable"

Boolean Ring Rules

$$\boxed{\begin{array}{rcl} neg(x) & \longrightarrow & x+1 \\ x \vee y & \longrightarrow & x+y+xy \\ x1 & \longrightarrow & x \\ x0 & \longrightarrow & 0 \\ xx & \longrightarrow & x \\ x+x & \longrightarrow & 0 \\ x+0 & \longrightarrow & x \\ x(y+z) & \longrightarrow & xy+xz \\ (y+z)x & \longrightarrow & yx+zx \end{array}}$$

Just like **polynomials** we work with in algebra.

Associativity and Commutativity

Interesting properties (AC)

$$\boxed{\begin{array}{rcl} x + y & \rightarrow & y + x \\ (x + y) + z & \rightarrow & x + (y + z) \\ xy & \rightarrow & yx \\ x(yz) & \rightarrow & (xy)z \end{array}}$$

Can't use as rules. We will lose termination!

Sample Problems Again

How to formulate and solve?

> An island is inhabited by two classes of people: knights, who make only true statements, and knaves, who make only false statements. Three inhabitants are conversing. Ashok says, ''All of us are knaves.'' Balu says, ''Exactly one of us is a knight.'' What are Ashok, Balu, and Chandra?

> Either the program never terminates or the value of n is eventually zero. If the value of n is eventually zero then the value of m will also eventually be zero. The program does terminate. Therefore the value of m will eventually zero. (T: the program terminates; N: the value of n is zero; M: the value of n is zero.)

Course HomePage Ready.
http://www.cse.iitb.ac.in/~cs206/