CS21
Decidability and Tractability

Lecture 15

February 10, 2014

Outline

- Gödel Incompleteness Theorem

(midterm due Wednesday
at the beginning of class)

Gödel Incompleteness Theorem

Background

- Hilbert's program (1920's):
  - formalize mathematics in axiomatic form
  - derive all true statements "mechanically" from initial axioms
  - would put mathematicians out of business!
  - very influential proposal
- to start: try for all true statements about the natural numbers ("number theory")

Background:

- Kurt Gödel (1931): it is not possible!
- no formalization of number theory can prove all true statements
- stunning result
- considered one of greatest 20th century achievements in mathematics

Background

- We will prove using:
  - RE languages and non-RE languages
  - reductions
- Idea:
  - set of all theorems is RE
  - set of all true statements is not RE
- This kind of proof of Gödel's result attributed to Turing (1937).

Number Theory

- formal language to express properties of
  N = {0, 1, 2, 3, …}
- allowable symbols: parentheses, and
  - variables x,y,z,… ranging over **N**
  - operators + (addition) and * (multiplication)
  - constants 0 (additive id) and 1 (mult. identity)
  - relation = (equality)
  - quantifiers $\forall$ (for all) and $\exists$ (exists)
  - propositional operators $\wedge$ (and) $\vee$ (or) $\neg$ (not) $\Rightarrow$ (implies) $\Leftrightarrow$ (iff)

Number Theory

- can formalize syntax of allowable formulas (skip)
- defining comparison relations:
  - $x \leq y \equiv \exists z\ x + z = y$
  - $x < y \equiv \exists z\ x + z = y \wedge \neg (z = 0)$

Number Theory

- Other natural concepts we will need:
  - quotient q and remainder r when divide x by y
    $\text{INTDIV}(x, y, q, r) \equiv x = qy + r \wedge r < y$
  - y divides x
    $\text{DIV}(y, x) \equiv \exists\ q\ \text{INTDIV}(x,y,q,0)$
  - x is even
    $\text{EVEN}(x) \equiv \text{DIV}(1+1, x)$
  - x is odd
    $\text{ODD}(x) \equiv \neg\ \text{EVEN}(x)$

Number Theory

- Other natural concepts we will need:
  - x is prime
    $\text{PRIME}(x) \equiv x \geq (1+1) \wedge \forall y\ (\text{DIV}(y, x) \Rightarrow (y = 1 \vee y = x))$
  - x is a power of 2
    $\text{POWER}_2(x) \equiv \forall y\ (\text{DIV}(y, x) \wedge \text{PRIME}(y)) \Rightarrow y = (1+1)$
  - $y = 2^k$ and k^{th} bit of x is 1
    $\text{BIT}(x, y) \equiv \text{POWER}_2(y) \wedge \forall q\ \forall r\ (\text{INTDIV}(x, y, q, r) \Rightarrow \text{ODD}(q))$

Number Theory

- $y = 2^k$ and k^{th} bit of x is 1
  $\text{BIT}(x, y) \equiv \text{POWER}_2(y) \wedge \forall q\ \forall r\ (\text{INTDIV}(x, y, q, r) \Rightarrow \text{ODD}(q))$

$$y = 10000000000$$

$$x = \underbrace{10101110101}_{q}\underbrace{11001001001}_{r}$$

Number Theory

- A sentence is a formula with no un-quantified variables
  - every number has a successor:
    $\forall x\ \exists y\ y = x + 1$
    true
  - every number has a predecessor:
    $\forall x\ \exists y\ x = y + 1$
    false
  - not a sentence: $x + y = 1$
- "number theory" = set of true sentences
  - denoted Th(**N**)

Proof systems

- Proof system components:
  - axioms (asserted to be true)
  - rules of inference (mechanical way to derive theorems from axioms)
- axioms for manipulating symbols (e.g.):
  - $(\varphi \wedge \psi) \Rightarrow \varphi$
  - $(\forall x\ \varphi(x)) \Rightarrow \varphi(1+1+1)$
  - $\forall x\ \forall y\ \forall z\ (x = y \wedge y = z \Rightarrow x = z)$
  - others…

Peano Arithmetic

- Peano Arithmetic: proof system for number theory. Axioms:
  - 0 is not a successor

$$\forall x \neg (0 = x + 1)$$

  - the successor function is one-to-one

$$\forall x\ \forall y\ (x+1 = y+1 \Rightarrow x = y)$$

  - 0 is an identity for +

$$\forall x\ x + 0 = x$$

Peano Arithmetic

- + is associative

$$\forall x\ \forall y\ \ x + (y + 1) = (x + y) + 1$$

- multiplying by zero gives 0

$$\forall x\ x*0 = 0$$

- * distributes over +

$$\forall x\ \forall y\ \ x * (y + 1) = (x * y) + x$$

- induction axiom

$$(\varphi(0) \wedge \forall x\ (\varphi(x) \Rightarrow \varphi(x+1))) \Rightarrow \forall x\ \varphi(x)$$

Peano Arithmetic

- rules of inference:

modus ponens $\dfrac{\varphi \qquad\qquad \varphi \Rightarrow \psi}{\psi}$

generalization $\dfrac{\varphi}{\forall x\ \varphi}$

Proof systems

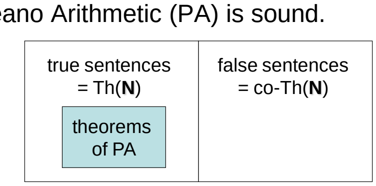
- a proof is a sequence of formulas

$$\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_n$$

  such that each φ_i is either
  - an axiom, or
  - follows from formulas earlier in list from rules of inference
- A sentence is a theorem of the proof system if it has a proof

Proof systems

- A proof system is sound if all theorems in that proof system are true (better have this)
- Peano Arithmetic (PA) is sound.



Proof systems

- A proof system is complete if all true sentences are theorems in that proof system
- hope to have this (recall Hilbert's program)

true sentences = Th(**N**)	false sentences = co-Th(**N**)
theorems of a complete proof system	

Incompleteness Theorem

Theorem: Peano Arithmetic is not complete.

(same holds for any reasonable proof system for number theory)

Proof outline:

- the set of theorems of PA is RE
- the set of true sentences (= Th(**N**)) is not RE

Incompleteness Theorem

- Lemma: the set of theorems of PA is RE.
- Proof:
  - TM that recognizes the set of theorems of PA:
  - systematically try all possible ways of writing down sequences of formulas
  - accept if encounter a proof of input sentence

  (note: true for any reasonable proof system)

Incompleteness Theorem

- Lemma: Th(**N**) is not RE
- Proof:
  - reduce from co-HALT (show co-HALT $\leq_m$ Th(**N**))
  - recall co-HALT is not RE
  - what should f(<M, w>) produce?
  - construct γ such that M loops on w $\Leftrightarrow$ γ is true

Incompleteness Theorem

- we will define

  $\text{VALCOMP}_{M,w}(v) \equiv \ldots$ (details to come)

  so that it is true iff v is a (halting) computation history of M on input w
- then define f(<M, w>) to be:

  $$\gamma \equiv \neg \exists v \ \text{VALCOMP}_{M,w}(v)$$
- YES maps YES?
  - $\langle M, w\rangle \in$ co-HALT $\Rightarrow \gamma$ is true $\Rightarrow \gamma \in$ Th(**N**)
- NO maps to NO?
  - $\langle M, w\rangle \notin$ co-HALT $\Rightarrow \gamma$ is false $\Rightarrow \gamma \notin$ Th(**N**)