Logic and Decidability

CS 81: Computability and Logic

December 2, 2010

Recall:

Provability:

$$A_1, \ldots, A_n \vdash B$$

Validity

$$A_1, \ldots, A_n \models B$$

Decidability

$$A_1, \ldots, A_n \vdash B$$

Key question:

Given $A_1, \ldots, A_n$, is B provable using a fixed set of logical rules?

E.g., is there a decision algorithm?

Propositional Logic is Decidable

Proof: Truth tables, completeness.

Predicate Logic is <u>not</u> decidable

Proof: Reduce the PCP to Predicate Logic!

Given a PCP instance in binary, produce a formula that is provable iff the instance has a solution.

Setup

On the logic side, we will use

- a constant symbol e
- Two unary functions f_0 and f_1
- A binary predicate P

We will use f_0, f_1, and e to encode binary strings.

We will force P to be true when the two arguments could the top and bottom of a sequence of dominos.

Encoding Binary Strings into Logic (by example)

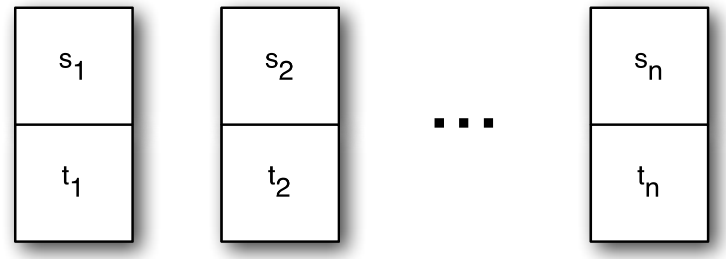
$$w = 000111$$

$$\downarrow$$

$$f_w(e) = f_1(f_1(f_1(f_0(f_0(f_0(e))))))$$

Translation

The PCP instance



The formula

$$P(f_{s_1}(e), f_{t_1}(e)) \;\wedge\; \cdots \;\wedge\; P(f_{s_n}(e), f_{t_n}(e))$$

$$\wedge$$

$$(\forall u, v.\ P(u,v) \;\rightarrow\; P(f_{s_1}(u), f_{t_1}(v)) \wedge \cdots \wedge P(f_{s_n}(u), f_{t_n}(v)))$$

$$\rightarrow$$

$$\exists z.\ P(z,z)$$

Completeness and Incompleteness

Theories

Theory:

A collection of formulas derivable from a set Γ of axioms.

Implicitly or explicitly specifies constants, functions, relations.

Γ might be infinite

Any proof can only use a finite subset of Γ

We normally expect recognizable/enumerable axioms.

Extending a theory means adding more axioms.

Hence, more things might be provable!

Peano Axioms

$\forall x.\ \neg(S(x) = 0)$

$\forall x,y.\ \ S(x) = S(y) \rightarrow x{=}y$

$A[0/x] \wedge (\forall n.\ \ A[n/x] \ \rightarrow\ A[S(n)/x])$

$\rightarrow$

For every formula A!

$(\forall n.\ \ A[n/x])$

Semigroup Theory

$\forall x,y,z.\ \ x + (y + z) = (x + y) + z$

Monoid Theory

$\forall x,y,z.\;\; x + (y + z) = (x + y) + z$

$\forall x.\;\; (x+0) = x$

Group Theory

$\forall x,y,z.\ \ x + (y + z) = (x + y) + z$

$\forall x.\ \ \ (x+0) = x$

$\forall x.\ \exists y.\ \ x+y = 0$

Commutative Group Theory

$\forall x,y,z.\ \ x + (y + z) = (x + y) + z$

$\forall x.\ \ \ (x+0) = x$

$\forall x.\ \exists y.\ \ x+y = 0$

$\forall x,y.\ \ x + y\ \ = y + x$

Linear Order Theory

$\forall x.\ \neg(x < x)$

$\forall x,y.\ (x < y) \vee (x = y) \vee (y < x)$

$\forall x,y,z.\ ((x < y) \wedge (y < z)) \rightarrow (x < z)$

Dense Linear Order Theory

$\forall x.\ \neg(x < x)$

$\forall x,y.\ \ (x < y) \vee (x = y) \vee (y < x)$

$\forall x,y,z.\ \ ((x < y) \wedge (y < z)) \rightarrow (x < z)$

$\exists x,y.\ \ x < y$

$\forall x,y.\ \ (x < y) \rightarrow \exists z.\ (x < z) \wedge (z < y)$

Dense Linear Order Theory without Endpoints

$\forall x.\ \neg(x < x)$

$\forall x,y.\ (x < y) \vee (x = y) \vee (y < x)$

$\forall x,y,z.\ ((x < y) \wedge (y < z)) \rightarrow (x < z)$

$\exists x,y.\ x < y$

$\forall x,y.\ (x < y) \rightarrow \exists z. (x < z) \wedge (z < y)$

$\forall x.\ \exists z. (z < x)$

$\forall x.\ \exists z. (x < z)$

Recall:
Predicate Logic

... is Sound.

$$\text{If } \Gamma \vdash B \text{ then } \Gamma \models B$$

... is Complete (Gödel's <u>Completeness</u> Theorem)

$$\text{If } \Gamma \models B \text{ then } \Gamma \vdash B$$

Validity Revisited

If B is a closed formula, then either:

$\Gamma \vDash B$

$\Gamma \vDash \neg B$

Neither.

A theory is said to be **negation-complete** (**complete** for short) if it always rules out the third case for all closed B.

That is, for every closed formula B, either $\Gamma \vDash B$ or $\Gamma \vDash \neg B$.

That is, for every closed formula B, either $\Gamma \vdash B$ or $\Gamma \vdash \neg B$.

Dense Linear Order Theory w/o Endpoints is (Negation-) Complete

$\forall x.\ \neg(x < x)$

$\forall x,y.\ (x < y) \lor (x = y) \lor (y < x)$

$\forall x,y,z.\ ((x < y) \land (y < z)) \rightarrow (x < z)$

$\exists x,y.\ x < y$

$\forall x,y.\ (x < y) \rightarrow \exists z.\ (x < z) \land (z < y)$

$\forall x.\ \exists z.\ (z < x)$

$\forall x.\ \exists z.\ (x < z)$

Presberger Arithmetic is Complete

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

$\forall x,y.\ x+1 = y+1 \rightarrow x=y$

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

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

$A[0/x] \wedge (\forall n.\ \ A[n/x] \ \rightarrow\ A[n+1/x])$

$\rightarrow$

$(\forall n.\ A[n/x]) + 1 = y + 1 \rightarrow x = y$

Linear Order Theory isn't complete.

$\forall x.\ \neg(x < x)$

$\forall x,y.\ (x < y) \lor (x = y) \lor (y < x)$

$\forall x,y,z.\ ((x < y) \land (y < z)) \rightarrow (x < z)$

Why Completeness Matters

Most theories aren't complete.

But completeness is a nice property.

- If the axioms can be enumerated, so can the theorems.
- "Is B provable" becomes <u>decidable</u>.
  - Enumerate theorems and wait for B or ¬B.
- (Of course, this assumes the theory is <u>consistent</u>.)

Gödel's First Incompleteness Theorem, 1931
(Refined by Rosser, 1936)

No consistent theory
with recognizable axioms
extending number theory
is (negation-)complete.

Consequence:

If you want to do math, you generally need <u>at least</u> addition, multiplication, and induction on natural numbers.

Any such theory will be (negation-) incomplete.

Number Theory?

Like Presburger Arithmetic + Multiplication

$\forall x.\ x \times 0 = 0$

$\forall x,y.\ (x \times (y+1)) = ((x \times y) + x)$

Gödel’s Proof Setup

Main idea: “Gödel Numbering”

- encode logical formulas (strings) as numbers.
- encode proofs (lists of formulas) as numbers.

Gödel's Proof Setup (continued)

He showed how to define a (big and complicated) formula $\Pi(p,f,a)$ true exactly when

- f encodes a formula $P(v)$ with one free variable v.
- p encodes a proof of $P(a)$

By the way:

- Π is built using partial recursive functions!
- These turn out to be the functions naturally definable in number theory.

The Proof Strategy(1)

- $\Pi(p,f,a)$ means that p is a proof of P(a), where f encodes P.
- Define $\Delta(f) := \forall p.\ \neg\Pi(p,f,f)$ [i.e., there is no proof of P(f)]
- Let d be the Gödel number of Δ.
- Is $\Delta(d)$ provable?
  - $\Delta(d) = \forall p.\ \neg\Pi(p,d,d)$ [i.e., there is no proof of $\Delta(d)$]
  - If it's provable then it's true, but then there's no proof.
  - So, no.

The Proof Strategy (2)

- $\Pi(p,f,a)$ means that p is a proof of P(a), where f encodes P.
- Define $\Delta(f) := \forall p.\ \neg\Pi(p,f,f)$ [i.e., there is no proof of P(f)]
- Let d be the Gödel number of Δ.
- Well, then, is $\neg\Delta(d)$ provable?
    - $\neg\Delta(d) = \neg\forall p.\ \neg\Pi(p,d,d)$ [i.e., there is a proof of $\Delta(d)$]
    - But we just showed there isn't a proof $\Delta(d)$.
    - So, no.

Gödel's Second Incompleteness Theorem

Within any consistent extension of number theory,

- there is a logical formula Con that expresses the consistency of the theory,
- but Con is not provable in the theory.

Corollary: In any extension of number theory,
Con is provable if and only if ...

Note: number theory can be proved consistent...if you're willing to believe set theory is consistent.

Decidability of Number Theory

Number Theory isn't complete.

- We can't decide whether A is a theorem by simply listing theorems and looking for A or $\neg$A.

But might theorem-hood still be decidable using some other algorithm?

Recall:

- We can encode TM configurations as numbers.
- Primitive Recursive functions exist
  - R(x) = configuration one step beyond configuration x.
  - T(i,x) = configuration i steps beyond configuration x.
  - P(x) = whether configuration x is halting (0 or 1)
- Computation length = $\mu i. [P(T(i, x_0)) = 0]$
- Final configuration = $T(\mu i. [P(T(i, x_0)) = 0], x_0)$

Number Theory is Undecidable

Number Theory is strong enough to define all primitive recursive functions.

Halting is then the logical formula

$$\exists i.\ P(T(i, x_0)) = 0$$