Logic and Computation: I

Part 3 First order logic and decision problems

Kazuyuki Tanaka

BIMSA

December 27, 2022

北京雁栖湖应用数学研究院
YANQI LAKE BEIJING INSTITUTE OF MATHEMATICAL SCIENCES AND APPLICATIONS

Logic and Computation I

- **Part 1. Introduction to Theory of Computation**
- **Part 2. Propositional Logic and Computational Complexity**
- **Part 3. First Order Logic and Decision Problems**

Part 3. Schedule

- Dec. 8, (1) What is first-order logic?
- Dec.13, (2) Skolem's theorem
- Dec.15, (3) Gödel's completeness theorem
- Dec.20, (4) Ehrenfeucht-Fraïssé's theorem
- Dec.22, (5) Presburger arithmetic
- Dec.27, (6) Peano arithmetic and Gödel's first incompleteness theorem

Peano arithmetic and Gödel's first incompleteness theorem

Recap

- By the EF theorem, DLO is decidable.
- DLO is PSPACE-complete. TQBF is polynomial-time reducible to DLO.
- (Gurevich) For any $m > 0$, for any two finite linear sequences L_1, L_2 of length 2^m or greater, $L_1 \equiv_m L_2$.
- For finite linear orders, there is no first-order formula expressing the parity of its length.
- The connectivity of a graph cannot be defined by a first-order formula.
- For every formula $\varphi(x_1, x_2, \ldots, x_s)$ in Presburger arithmetic, we can construct an automaton accepting the language of words representing s-tuples $(n_1, n_2, \ldots, n_s)$ that satisfy the formula $\varphi(x_1, x_2, \ldots, x_s)$.
- Presburger arithmetic is decidable.

- So-called "**Peano's postulates**" (1889) is famous as an axiomatic treatment of the natural numbers. However, it is not a formal system in the sense of modern logic, since its underlying logic is ambiguous. Moreover, we should also notice previous advanced studies by C.S. Peirce (1881) and R. Dedekind (1888).
- It was Hilbert who began to consider natural number theory as a formal theory in first-order logic.
- In fact, Peano arithmetic PA as a strict formal system were established through Gödel's arguments of his incompleteness theorem.

G. Peano

C.S. Peirce

R. Dedekind

Peano arithmetic is a first-order theory in the language of ordered rings $\mathcal{L}_{\mathrm{OR}} = \{+, \cdot, 0, 1, <\}$, consists of the following mathematical axioms.

Definition

Peano arithmetic (PA) has the following formulas in $\mathcal{L}_{\mathrm{OR}}$ as a mathematical axiom.

Successor:	$\neg(x+1=0)$,	$x+1=y+1 \to x=y$.
Addition:	$x+0=x$,	$x+(y+1)=(x+y)+1$.
Multiplication:	$x \cdot 0 = 0$,	$x \cdot (y+1) = x \cdot y + x$.
Inequality	$\neg(x<0)$,	$x<y+1 \leftrightarrow x<y \lor x=y$.

Induction: $\varphi(0) \land \forall x(\varphi(x) \to \varphi(x+1)) \to \forall x \varphi(x)$.

- Induction is not a single formula, but an axiom schema that collects the formulas for all the $\varphi(x)$ in $\mathcal{L}_{\mathrm{OR}}$. Note that $\varphi(x)$ may include free variables other than x.
- In "Peano's postulates", induction is expressed in terms of sets, but Peano arithmetic does not presuppose set theory.

- In a modern formal system, to add a new function, it must be defined explicitly so that the extended system is a conservative extension.
- The primitive recursive definition is not an explicit definition. In fact, if we add the primitive recursive definition of multiplication to Presburger arithmetic (a system of only addition), the resulting system loses completeness and decidability, and it is not a conservative extension.
- In other words, multiplication is not definable from addition.
- On the other hand, the inequality $x < y$ can be defined from addition as abbreviation for $\exists z(y = (x + z) + 1)$. However, we prefer to include the inequality as a primitive symbol, because it allows us to define the hierarchy of formulas simply.
- Similarly, in the following, we assume that $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\forall$, $\exists$, etc. are all pre-set.

Arithmetical Hierarchy

- We inductively define hierarchical classes of formulas Σ_i and Π_i $(i \in \mathbb{N})$.

Definition

- The **bounded** formulas are constructed from atomic formulas by using propositional connectives and bounded quantifiers $\forall x < t$ and $\exists x < t$, where $\forall x < t$ and $\exists x < t$ are abbreviations for $\forall x (x < t \to \cdots)$ and $\exists x (x < t \land \cdots)$, respectively, and t is a term that does not includes x. A bounded formula is also called a Σ_0 $(=\Pi_0)$ formula.
- For any $i, k \in \mathbb{N}$:
  - if φ is a Σ_i formula, $\forall x_1 \cdots \forall x_k \varphi$ is a Π_{i+1} formula,
  - if φ is a Π_i formula, $\exists x_1 \cdots \exists x_k \varphi$ is a Σ_{i+1} formula.

- Σ_i / Π_i also denotes the set of all Σ_i / Π_i formulas.

- In the above definition, there are many formulas that do not belong to any class. So, the (lowest) class to which the equivalent formula belongs is regarded as the class of the formula.

Examples

- $\neg\exists y(y + y = x)$ does not belong to any of the above class.
- But it is logically equivalent to a Π_1 formula $\forall y \neg(y + y = x)$.
- So $\neg\exists y(y + y = x)$ is a Π_1 formula.

- If a Π_i formula is equivalent to some Σ_i formula or a Σ_i formula equivalent to some Π_i formula, such a formula is called a Δ_i formula.

Example

- The following $\Sigma_0(=\Pi_0))$ formula $\mathrm{P}(x)$ expresses "x is a prime number"

$$\mathrm{P}(x) \equiv \neg\exists d < x \exists e < x(d \cdot e = x) \land \neg(x = 0) \land \neg(x = 1).$$

- The proposition "every even number greater than or equal to 4 is the sum of two primes" (the "Goldbach conjecture") is expressed by the following Π_1 formula:

$$\forall x > 1 \exists p < 2x \exists q < 2x\ (2x = p + q \land \mathrm{P}(p) \land \mathrm{P}(q)).$$

- "There are infinitely many primes" can be expressed as a Π_2 formula

$$\forall x \exists y > x \mathrm{P}(y).$$

Let us define a subsystem of Peano arithmetic PA by restricting its induction axiom.

Definition

Let Γ be a class of formulas in $\mathcal{L}_{\mathrm{OR}}$. By I$\Gamma$, we denote a subsystem of PA obtained by restricting ($\varphi(x)$ of) induction to the class Γ.

- The main subsystems of PA are I$\Sigma_1 \supset$ I$\Sigma_0 \supset$ IOpen, where Open is the set of formulas without quantifiers.
- Another system weaker than IOpen is the system Q defined by R. Robinson, which has no induction axiom but instead has

$$\forall x(x \neq 0 \to \exists y(y+1=x)).$$

- Gödel proved two versions of the incompleteness theorems. The first incompleteness theorem is mostly based on the representation theorem of recursive functions, which can be proved in Q. On the other hand, the second incompleteness theorem needs the absoluteness of primitive recursive functions, which requires IΣ_1.

- In this lecture, we look at the first theorem from the viewpoint of computability theory. In the next semester, we will reexamine the proof more rigorously, and prove the second theorem.
- Recall that $X \subseteq \mathbb{N}^n$ is called CE (computably enumerable) if it is the domain of some partial recursive function. Then, from the lemma below, any CE relation $R(\vec{x})$ can be expressed by $\exists y S(\vec{x}, y)$ for some primitive recursive relation S.
- By Lemma (2) later, we will show that a CE relation $R(\vec{x})$ can be expressed by $\exists y S(\vec{x}, y)$ for some Σ_0 relation S, that is, a Σ_1 formula.

Recall, Lemma in Lecture-01-05 of this course

For the relation $R \subset \mathbb{N}^n$, the following conditions are equivalent.

(1) R is recursively enumerable (CE).

(6) There exists a primitive recursive relation S such that

$$R(x_1, \cdots, x_n) \Leftrightarrow \exists y S(x_1, \cdots, x_n, y).$$

(7) There exists a recursive relation S such that

$$R(x_1, \cdots, x_n) \Leftrightarrow \exists y S(x_1, \cdots, x_n, y).$$

Definition

Let $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$ be a standard model of PA.

- A set $A \subseteq \mathbb{N}^l$ is said to be Σ_i if there exists a Σ_i formula $\varphi(x_1, \ldots, x_l)$ satisfying

$$(m_1, \ldots, m_l) \in A \Leftrightarrow \mathfrak{N} \models \varphi(\overline{m_1}, \ldots, \overline{m_l}).$$

- Here, $\overline{m}$ is a term expressing number m, that is, $\overline{m} = \overbrace{(1 + 1 + \cdots + 1)}^{m}(m > 0)$, $\overline{0} = 0$.
- Similarly, Π_i sets can be defined by Π_i formulas.
- A set that is both Σ_i and Π_i is called Δ_i.

Lemma (1)

The graph $\{(\vec{x}, y) : f(\vec{x}) = y\}$ of a primitive recursive function f is a Δ_1 set.

Proof

- By induction on the construction of primitive recursive functions. The main part is to treat the definition by primitive recursion.
- For simplicity, we omit parameter variables $x_1, \ldots, x_l$, and consider the definition of a unary function f from a constant c and binary function h as follows:

$$f(0) = c, \quad f(y+1) = h(y, f(y)).$$

- From the induction hypothesis, h can be expressed in both Σ_1 and Π_1 formulas.
- First, let $\gamma(x, m, n)$ be a Σ_0 formula expressing "$m(x+1)+1$ is a divisor of n", that is, $\exists d < n \ (m(x+1)+1) \cdot d = n$. Then, for any finite set A (with $\max A < u$), there exist m, n such that $\forall x < u(x \in A \Leftrightarrow \gamma(x, m, n))$.
- In fact, assume $(u-1)! \mid m$. Then, $(m(i+1)+1)$ and $(m(j+1)+1)$ are mutually prime for any $i < j < u$. Thus, $n = \Pi_{i \in A}(m(i+1)+1)$ works.

- Now, we will define a Σ_0 formula $\delta(u,m,n)$ such that

$$\delta(\langle u_1,u_2\rangle,m,n) \Leftrightarrow \forall y < u_1 \exists z < u_2 \ f(y)=z.$$

- The formula $\delta(u,m,n)$ is formally constructed as follows: for any $u=\langle u_1,u_2\rangle$,

$$\delta(u,m,n) \equiv \forall y < u_1 \exists z < u_2 \ \gamma(\langle y,z\rangle,m,n) \wedge \forall z < u_2(\gamma(\langle 0,z\rangle,m,n) \leftrightarrow z=c)$$
$$\wedge \forall y < u_1 - 1 \forall z < u_2(\gamma(\langle y+1,z\rangle,m,n) \leftrightarrow \exists z' < u_2(z=h(y,z') \wedge \gamma(\langle y,z'\rangle,m,n))).$$

- Then $\forall u_1 \exists u_2 \exists m \exists n \delta(\langle u_1,u_2\rangle,m,n)$ holds. Thus, we obtain

$$\begin{aligned} f(y)=z &\Leftrightarrow \exists u \exists m \exists n(u_1=y+1 \wedge \delta(u,m,n) \wedge \gamma(\langle y,z\rangle,m,n)) \\ &\Leftrightarrow \forall u \forall m \forall n(u_1=y+1 \wedge \delta(u,m,n) \to \gamma(\langle y,z\rangle,m,n)). \end{aligned}$$

- That is, $f(y)=z$ is a Δ_1 set. $\square$

- As we saw in the revisited lemma on Slides p. 12, any CE relation $R(\vec{x})$ can be expressed by $\exists y S(\vec{x}, y)$ for some primitive recursive relation S.
- By the above lemma, the primitive recursive relation S can be expressed by a Σ_1 formula, and $\exists y S(\vec{x}, y)$ is still Σ_1. Thus, any CE relation can be expressed by a Σ_1 formula.
- Therefore, we have the following.

Lemma (2)

The CE sets are exactly the same as the Σ_1 sets. Hence, the computable (recursive) sets are exactly the same as the Δ_1 sets.

Before moving on to the incompleteness theorem, we introduce some notions of formal systems.

- A system is said to be Σ_1 **complete** if it proves all true Σ_1 sentences.
  - This condition seems very strong at the first glance. But in fact, a very weak subsystem of PA, such as Q(with $<$), satisfies this.
  - Indeed, all the true atomic sentences are provable (in a weak system). Also for their Boolean combinations. A bounded sentence $\forall x < t\theta(x)$ is equivalent to $\theta(0) \land \cdots \land \theta(t-1)$. So, all the true Σ_0 sentences are provable (in a weak system).
  - Now, suppose that a Σ_1 sentence $\exists x \varphi(x)$ is true. Then, there is $n \in \mathbb{N}$ such that the Σ_0 sentence $\varphi(\overline{n})$ holds. Hence, $\varphi(\overline{n})$ is provable, and also $\exists x \varphi(x)$.
- A system T is said to be 1-**consistent** if any Σ_1 sentence provable by T is true.
  - 1-consistency is strictly stronger than consistency. Gödel originally used ω-consistency, which is strictly stronger than 1-consistency.

Then, the following two representation theorems hold.

Theorem ((Weak) Representation Theorem for CE sets)

Suppose that a theory T is Σ_1-complete and 1-consistent. Then, for any CE set C, there exists a Σ_1 formula $\varphi(x)$ such that for any n,

$$n \in C \quad \Leftrightarrow \quad T \vdash \varphi(\overline{n}).$$

Proof.

- From the Lemma (2), for any CE set C, there exists a Σ_1 formula $\varphi(x)$ such that $n \in C \Leftrightarrow \mathfrak{N} \models \varphi(\overline{n})$.
- Since T is Σ_1-complete, $\mathfrak{N} \models \varphi(\overline{n}) \Rightarrow T \vdash \varphi(\overline{n})$.
- Also because T is 1-consistent, $T \vdash \varphi(\overline{n}) \Rightarrow \mathfrak{N} \models \varphi(\overline{n})$.

□

Theorem ((Strong) Representation Theorem for Recursive Sets)

Assume a theory T is Σ_1-complete. For any recursive set C, there exists a Σ_1 formula $\varphi(x)$ such that

$$n \in C \Rightarrow T \vdash \varphi(\overline{n}), \quad n \notin C \Rightarrow T \vdash \neg\varphi(\overline{n}).$$

Proof.

- For the recursive set C, from the Lemma (2) there exist Σ_0 formulas $\theta_1(x, y), \theta_2(x, y)$ such that

  $$n \in C \Leftrightarrow \mathfrak{N} \models \exists y \theta_1(\overline{n}, y), \quad n \notin C \Leftrightarrow \mathfrak{N} \models \exists y \theta_2(\overline{n}, y).$$

  Now, let $\varphi(x)$ be a Σ_1 formula $\exists y(\theta_1(\overline{n}, y) \wedge \forall z \leq y \neg\theta_2(\overline{n}, z))$. By the Σ_1-completeness of T, $n \in C \Rightarrow T \vdash \varphi(\overline{n})$.
- To show $n \notin C \Rightarrow T \vdash \neg\varphi(\overline{n})$, let $n \notin C$.
  Then, since $\mathfrak{N} \models \exists y \theta_2(\overline{n}, y)$, some m exists and $\mathfrak{N} \models \theta_2(\overline{n}, \overline{m})$. From the Σ_1 completeness of T, $T \vdash \theta_2(\overline{n}, \overline{m})$.
  Also, since $\mathfrak{N} \not\models \exists y \theta_1(\overline{n}, y)$, for all l, $\mathfrak{N} \models \neg\theta_1(\overline{n}, \bar{l})$, i.e., $T \vdash \neg\theta_1(\overline{n}, \bar{l})$.
  Therefore, if $\theta_1(\overline{n}, a)$ in some model of T, then a is not a standard natural number l.
  Thus, $T \vdash \forall y(\theta_1(\overline{n}, y) \to \exists z \leq y\ \theta_2(\overline{n}, z))$, that is, $T \vdash \neg\varphi(\overline{n})$. □

- To derive the incompleteness theorem, we need one more condition on a formal system, that is, the set of axioms is CE.
- Without this condition, for example, if we take all true arithmetic formulas as axioms, we would have a complete theory, but it would not be a formal system.
- From the following theorem, the CE set of axioms can be also express as a primitive recursive set.

Theorem (Craig's lemma)

For any CE theory T, there exists an equivalent (proving the same theorem) primitive recursive theory T'.

Proof. Let T be a CE theory, defined by Σ_1 formula $\varphi(x) \equiv \exists y \theta(x, y)$ (θ is Σ_0). That is, $\sigma \in T \Leftrightarrow \mathfrak{N} \models \varphi(\overline{\ulcorner \sigma \urcorner})$. $\ulcorner \sigma \urcorner$ is the Gödel number of a sentence σ.
Then, we define a primitive recursive theory T' as follows:

$$T' = \{\overbrace{\sigma \wedge \sigma \wedge \cdots \wedge \sigma}^{n+1 \text{ copies}} : \theta(\overline{\ulcorner \sigma \urcorner}, \overline{n})\}.$$

Then, T and T' are equivalent, since $\vdash \sigma \leftrightarrow \sigma \wedge \sigma \wedge \cdots \wedge \sigma$. □

In the proof above, the definition of T' is not Σ_0 since it includes the Gödel numbers, etc. The following can be shown about the CE theory.

Theorem

For any CE theory T, the set of its theorems $\{\ulcorner\sigma\urcorner : T \vdash \sigma\}$ is also CE.

Proof

- Recall that a proof in a formal system of first-order logic is a finite sequence of formulas, each formula being either a logical axiom, an equality axiom, or a mathematical axiom of a theory T, or obtained from previous formulas by applying MP or a quantification rule.
- From the Craig's Lemma, a CE theory T can be transformed into a primitive recursive theory. Thus, it is also a primitive recursive relation that (the Gödel number of) a finite sequence of formulas is a proof of T.
- The set of theorems of T is CE. Because a sentence σ is a theorem of T iff there exists a proof (i.e., a sequence that satisfies the primitive recursive relation) such that σ is the last formula of the proof. □

The halting problem K is CE, but its complement $\mathbb{N} - \mathrm{K}$ is not (part 1 of this course). Gödel's first incompleteness theorem easily follows from this fact.

Theorem (Gödel's first incompleteness theorem)

Let T be a Σ_1-complete and 1-consistent CE theory. Then T is incomplete, that is, there is a sentence that cannot be proved or disproved.

Proof.

- Suppose K is CE but not co-CE. By the weak representation theorem for CE sets, there exists a formula $\varphi(x)$ such that

$$n \in \mathrm{K} \Leftrightarrow T \vdash \varphi(\overline{n}).$$

- On the other hand, since $\mathbb{N} - \mathrm{K}$ is not a CE, there exists some d such that

$$d \in \mathbb{N} - \mathrm{K} \not\Leftrightarrow T \vdash \neg\varphi(\overline{d}).$$

  Thus, ($d \in \mathrm{K}$ and $T \vdash \neg\varphi(\overline{d})$) or ($d \notin \mathrm{K}$ and $T \nvdash \neg\varphi(\overline{d})$).
  - In the former case, since $d \in \mathrm{K}$ implies $T \vdash \varphi(\overline{d})$, T is inconsistent, contradicting with the 1-consistency assumption.
  - In the latter case, T is incomplete because $\varphi(\overline{d})$ cannot be proved or disproved.

Homework

(1) Prove Q $\vdash 0 + 1 = 1$. (See Slide p.11)

(2) In a Σ_1 complete theory T, show that 1-consistency of T is equivalent to the following: for any Σ_0 formula $\varphi(x)$, if $\varphi(\overline{n})$ is provable in T for all n, then $\exists x \neg\varphi(x)$ is not provable in T.

(3) Let A, B be two disjoint CE sets. Assume a theory T is Σ_1-complete. Show that there exists a Σ_1 formula $\psi(x)$ such that

$$n \in A \Rightarrow T \vdash \psi(\overline{n}), \quad n \in B \Rightarrow T \vdash \neg\psi(\overline{n}).$$

From this, deduce that $\{\ulcorner\sigma\urcorner : T \vdash \sigma\}$ and $\{\ulcorner\sigma\urcorner : T \vdash \neg\sigma\}$ are computably inseparable. (See Part 1-6, Slide p.25.) In particular, $\{\ulcorner\sigma\urcorner : T \vdash \sigma\}$ is not computable.

Summary

Theorem (Gödel's first incompleteness theorem)

Any Σ_1-complete and 1-consistent CE theory is incomplete, that is, there is a sentence that cannot be proved or disproved.

Further readings

- Theory of Computation, D.C. Kozen, Springer 2006.
- Mathematical Logic. H.-D. Ebbinghaus, J. Flum, W. Thomas, Graduate Texts in Mathematics 291, Springer 2021.

Next semester

- **Part 4. Formal arithmetic and Gödel incompletess theorems**
- **Part 5. Automata on infinite objects**
- **Part 6. Recursion-theoretic hierarchies**
- **Part 7. Admissible ordinals and second order arithmetic**

Thank you for your attention!