Logic and Foundation I

Part 2. First-order logic

Kazuyuki Tanaka

BIMSA

December 14, 2023

北京雁栖湖应用数学研究院
Beijing Institute of Mathematical Sciences and Applications

Logic and Foundations I

- **Part 1. Equational theory**
- **Part 2. First order theory**
- **Part 3. Model theory**
- **Part 4. First order arithmetic and incompleteness theorems**

Part 2. Schedule

- Dec. 07, (1) Peano arithmetic and representation theorems
- Dec. 14, (2) The first incompleteness theorem
- Dec. 21, (3) The second incompleteness theorem
- Dec. 28, (4) Presburger arithmetic

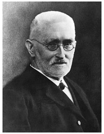
Today's topics

Peano arithmetic

- 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.
- Today we will introduce Peano arithmetic PA and its representative subsystems PA^-, $\mathrm{I}\Sigma_n$, Q, etc., and investigate its fundamental properties.

G. Peano

C.S. Peirce



R. Dedekind

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

Definition

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

Successor:	A1. $\neg(x + 1 = 0)$,	A2. $x + 1 = y + 1 \to x = y$.
Addition:	A3. $x + 0 = x$,	A4. $x + (y + 1) = (x + y) + 1$.
Multiplication:	A5. $x \cdot 0 = 0$,	A6. $x \cdot (y + 1) = x \cdot y + x$.
Inequality	A7. $\neg(x < 0)$,	A8. $x < y + 1 \leftrightarrow x < y \vee x = y$.

Induction: A9. $\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(x + 1)) \to \forall x \varphi(x)$.

- 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.

- Peano's postulates include A1 and A2, but not A3 $\sim$ A8, since addition, multiplication and inequality are regarded as definable notions.
- However, from a modern axiomatic perspective, functions (and relations) can be added by definition, only if the system is extended conservatively. That is, we can add a new symbol f and $\forall x \forall y(\varphi(x,y) \leftrightarrow f(x) = y)$ to a theory T if $T \vdash \forall x \exists y \varphi(x,y)$ holds.
- The primitive recursive definition is not an explicit definition. A system without multiplication ($\mathrm{PA} - \{$A5, A6$\}$), the relation $x \bullet y = z$ cannot be expressed by a formula $\varphi(x,y,z)$ such that $\forall x \forall y \exists z \varphi(x,y,z)$ is provable. Thus $\mathrm{PA} - \{$A5, A6$\}$ is a properly weaker system than PA.
- On the other hand, even if inequality axioms A7 and A8 are removed, $<$ can be introduced as follow.

  A7.5 $\quad \forall x \forall y(x < y \leftrightarrow \exists z(z + (x+1) = y))$.

  However, to classify the formulas of $\mathcal{L}_{\mathrm{OR}}$ according to their forms, we want to treat $<$ as a primitive symbol. It would be inappropriate to think it as an abbreviation for the right-hand side of A7.5.
- If A7.5 is used instead of A7 and A8, it must be assumed as an axiom at the beginning.

- The structure of natural numbers $\mathfrak{N} = (\mathbb{N}, +, \bullet, 0, 1, <)$ is the **standard model** of PA.
- There also exist models of $\mathrm{Th}(\mathfrak{N})$ non-isomorphic to $\mathfrak{N}$, called **nonstandard models** of arithmetic.
- The structure $(\omega^\omega, +, \bullet, 0, 1, <)$, which has ordinal addition and multiplication on ordinal numbers $< \omega^\omega$, is a model of A1 $\sim$ A8.

  In set theory, a transfinite ordinal is identified with a set of smaller ordinals. ω^ω is the next ordinal of ω closed under $+$ and $\cdot$.
- Let $\mathbb{Z}[X]$ be the ring of polynomials of integer coefficients with X as a variable. For $p \in \mathbb{Z}[X]$, define $p > 0$ when its highest order coefficient is positive, and $p > q \Leftrightarrow p - q > 0$ defines an order between the two polynomials p, q.

  Let $\mathbb{Z}[X]^+ = \{p \in \mathbb{Z}[X] : p \geq 0\}$. Then it is a model of A1 $\sim$ A8 and more (indeed PA$^-$ as we will explain).

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.
- Note that $\forall x > t$ or $\forall x(x > t \to \cdots)$ and $\exists x > t$ or $\exists x(x > t \land \cdots)$ are not bounded.

- In the above definition, there are many formulas that do not belong to any class. However, by De Morgan's rule, any formula can be transformed to an equivalent formula that belongs to the above classification. 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

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

Also, it can be expressed as a Π_1 formula (exercise).

Let us define subsystems 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.

Definition

Robinson's system Q is obtained from PA by removing the axioms of inequality and induction, and instead adding the following axiom:

Predecessor: A10: $\forall x(x \neq 0 \rightarrow \exists y(y+1=x))$.

So, it is a theory in the language of ring $\mathcal{L}_{\mathrm{R}} = \{+, \cdot, 0, 1\}$.

Let Q$_<$ be the system Q plus axiom A7.5.

Problem 1-1: Show that Q $\vdash 0+1=1$

- First, we show Q $\vdash 1 \neq 0$. If $1=0$, then $0+1=0+0$. On the other hand, we have $0+1 \neq 0$ according to the successor axiom, and $0+0=0$ according to the axiom of addition. So it is a contradiction.
- Then we have y such that $y+1=1$ by applying the predecessor axiom.
- Next we show $y=0$. Assume $y \neq 0$. Then, by axiom of addition $0+1=0+(y+1)=(0+y)+1$, we have $0=0+y$. Again by the predecessor axiom, there is z such that $z+1=y$. Thus $0=0+(z+1)=(0+z)+1$, a contradiction.

Problem 1-2 (Exercise): Show that Q $-\{A10\} \nvdash 0+1=1$.

- We construct a model of Q-A10 which does not satisfy $0+1=1$.
- The domain of our model consists of two types of elements $\tilde{n}$ and $0+\tilde{n}$ for each natural number $n \geq 1$. It also contains 0 as a special element of the latter type.
- Addition and multiplication are performed as usual if we ignore types. The type of the result is defined to be the same as that of the left element. So, for instance,

$$\tilde{m}+\tilde{n}=\tilde{m}+(0+\tilde{n})=\widetilde{m+n},$$

$$(0+\tilde{m})+\tilde{n}=(0+\tilde{m})+(0+\tilde{n})=0+(\widetilde{m+n}).$$

Multiplication is defined similarly, but we have $\tilde{n} \bullet 0 = 0$.

Problem 1-3 (Homework): Show that Q $\nvdash \forall x(0+x=x)$.

- (Hint) Consider a non-standard model of Peano arithmetic PA in which only the non-standard part is divided into two kinds of numbers in the same way as Problem 1-2. Show it satisfies Q but does not satisfy $\forall x(0+x=x)$.

Lemma

In IOpen, the following axioms of **theory of discrete ordered semirings** PA^- are provable.

(1) Semiring axioms (excluding the additive inverses from the commutative ring).
(2) difference axiom $x < y \to \exists z(z + (x + 1) = y)$.
(3) a linear order with the minimum element 0 and discrete $(0 < x \leftrightarrow 1 \leq x)$.
(4) Order preservation $x < y \to x + z < y + z \wedge (x \cdot z < y \cdot z \vee z = 0)$.

Proof. ▶ (1) is a collection of equations (preceded by the universal symbol $\forall$). For instance, the associative law of addition $(x + y) + z = x + (y + z)$ can be easily shown by induction on z. Other equations can also be proven by induction on one variable, leaving the other variables as free variables.

▶ To show (2), $x < y \to \exists z < y(z + x + 1 = y)$ is a Σ_0 formula, which can be proved easily by Σ_0 induction on y. To show it by open induction, we prove it by contradiction. Consider a model of IOpen in which (2) does not hold. So, there are two elements $a < b$ such that $\forall z(z + a + 1 \neq b)$. Define an open formula $\varphi(z)$ as $z + (a + 1) > b$. Then we have $\neg\varphi(0)$ and $\varphi(b)$. By open induction, there exists c such that $\neg\varphi(c)$ and $\varphi(c + 1)$. Thus, $c + (a + 1) < b < c + (a + 1) + 1$, which contradicts with A8.

▶ (3) and (4) are open formulas (with universal symbol $\forall$ in front), we can select appropriate variables and use induction. □

Corollary

$Q_<$ is a subsystem of the theory PA^-.

Proof. We prove the following axioms by using PA^-.

A7.5 $\forall x \forall y(x < y \leftrightarrow \exists z(z + (x + 1) = y))$.

A10: $\forall x(x \neq 0 \to \exists y(y + 1 = x))$.

For A10, $x \neq 0 \to x > 0$ is an assertion contained in condition (3) of the last lemma. So, if we use this and condition (2) of the last lemma, we immediately obtain A10.

For A7.5, since $\to$ is condition (2) of the last lemma, we only need to show $\leftarrow$. Assuming $\exists z(z + x + 1 = y)$, we derive a contradiction by denying $x < y$. Since the axiom of linear order holds from condition (3) of the last lemma, $x = y$ or $x > y$.

- If $x = y$, $z + y + 1 = y$, but since $z + 1 > 0$, $z + y + 1 > y$, a contradiction.
- If $x > y$, $\exists z'(z' + y + 1 = x)$ from $\to$, so $z + z' + y + 1 + 1 = y$, which is also a contradiction.

□

Corollary

$\mathsf{Q}_< \subset \mathsf{PA}^- \subset \mathrm{IOpen} \subset \mathrm{I}\Sigma_0 \subset \mathrm{I}\Sigma_1 \subset \mathsf{PA}$.

- Since $\mathsf{Q}_<$ lacks induction, it cannot prove many propositions that something holds for all x (eg, $\forall x(0 + x = x)$).
- However, it proves correct equalities and inequalities consisting of only concrete numbers. In other words, an atomic formula $s = t$ or $s < t$ without variables can be proved if true, and its negation can be proved if false.
- Furthermore, propositional connectives and bounded quantifiers preserve the correspondence between truth and provability. That is, a bounded sentence can be proved/disproved in $\mathsf{Q}_<$ if it is true/false.
- A system is said to be Σ_1-**complete** if it proves all true Σ_1 sentences. This seems to be very strong condition, but indeed $\mathsf{Q}_<$ is Σ_1-complete.
- There is even a weaker system with Σ_1 completeness. The system R of Mostowski-Robinson-Tarski is one of such. It has an infinite number of axioms and lacks simplicity as a formal system, but it is important for exploring the essence of the incompleteness theorem.

A standard formal representation of a natural number $n > 0$ in $\mathcal{L}_{\mathrm{R}}$ is $\overline{n} = \overbrace{1 + \cdots + 1}^{n \text{ times}}$. If $n = 0$, we also set $\overline{0} = 0$. Then, a term $\overline{n}$ is called the **numeral** of number n.

Definition (Mostowski-Robinson-Tarski's system R)

R is a theory in the language of ordinal rings, consisting of the following axiom schemes.

R1. $\overline{m} \neq \overline{n}$ (when $m \neq n$).

R2. $\neg(x < \overline{0})$.

R3. $x < \overline{n+1} \leftrightarrow x = \overline{0} \vee \cdots \vee x = \overline{n}$.

R4. $x < \overline{n} \vee x = \overline{n} \vee \overline{n} < x$.

R5. $\overline{m} + \overline{n} = \overline{m+n}$.

R6. $\overline{m} \bullet \overline{n} = \overline{m \bullet n}$.

Lemma

$\mathrm{Q}_<$ proves all axioms of R.

Proof Most of the axioms of R can be easily proved in $\mathrm{Q}_<$ by meta-induction. We only show R3. The base $n = 0$ is obvious from A8. For induction step, assume it for n. Consider $x < \overline{n+2}$. If $x = 0$, we are done. Otherwise, use A10 to find y such that $y + 1 = x$. So, since $y < \overline{n+1}$, we can use the induction hypothesis for y and finish the induction step. □

Theorem (Σ_1-completeness of R)

R proves all true Σ_1 sentences. Therefore, $Q_<$, PA^-, IOpen, etc. are all Σ_1-complete.

Proof

- If a Σ_1 sentence $\exists x_1 \exists x_2 \ldots \exists x_k \varphi(x_1, x_2, \ldots, x_k)$ is true, there exist natural numbers $n_1, n_2, \ldots, n_k$ such that $\varphi(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k})$ holds.
- By virtue of R3, a bounded quantification $\exists x < t\ \varphi(x)$ can be rewritten as $\varphi(\overline{0}) \vee \varphi(\overline{1})) \vee \cdots \vee \varphi(\overline{n-1})$ if the value of close term t is n. Thus, by induction, a bounded sentence can be rewritten as a Boolean combination of atomic sentences. Since an atomic sentence can be proved/disproved in R if it is true/false, also can a bounded sentence.
- Therefore, $\varphi(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k})$ is provable since it is true. From the rule of first-order logic, $\exists x_1 \exists x_2 \ldots \exists x_k \varphi(x_1, x_2, \ldots, x_k)$ is also provable in R. □

- All the arithmetic systems we will discuss are extensions of R, and thus Σ_1-complete.
- Another condition for a theory to be needed for the first incompleteness theorem is **1-consistency**, also known as Σ_1-**soundness**. A theory is said to be Σ_n-**sound** if all provable Σ_n statements are true.

- We first look at the first incompleteness theorem from the viewpoint of computability theory. Then, we will reexamine the proof more syntactically.
- The most important class in computability theory is **CE** (computably enumerable).
- $X \subseteq \mathbb{N}^n$ is called **CE** if it is the domain (or range) of some partial recursive function. Also, any CE relation $R(\vec{x})$ can be expressed by $\exists y S(\vec{x}, y)$ for some primitive recursive relation S.
- So, we first review the basics of primitive recursive functions and relations.

Recap: Primitive recursive functions

Definition

The **primitive recursive functions** are defined as below.

1. Constant 0, **successor function** $\mathrm{S}(x) = x + 1$,
   projection $\mathrm{P}_i^n(x_1, x_2, \ldots, x_n) = x_i$ $(1 \leq i \leq n)$ are prim. rec. functions.
2. **Composition**.
   If $g_i (1 \leq i \leq m)$, h are prim. rec. functions, so is $f = h(g_1, \ldots, g_m)$ defined by:
   $$f(x_1, \ldots, x_n) = h(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)).$$
3. **Primitive recursion**.
   If g, h are prim. rec. functions, so is f defined by:
   $$f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n),$$
   $$f(x_1, \ldots, x_n, y + 1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)).$$

A primitive recursive function is a computable total function.

Example

$x + y$, $x \dot{-} y$, $x \cdot y$, x/y, x^y, $x!$, $\max\{x, y\}$, $\min\{x, y\}$ are primitive recursive functions.

Example

Let $p(x) =$ "$(x + 1)$-th prime number ", that is ,

$$p(0) = 2, p(1) = 3, p(2) = 5, \dots$$

Then, $p(x)$ is a primitive recursive function since it is defined as follows.

$$p(0) = 2, \quad p(x + 1) = \mu y < p(x)! + 2\ (p(x) < y \wedge \mathrm{prime}(y)).$$

Definition

An n-ary relation $R \subset \mathbb{N}^n$ is called primitive recursive, if its characteristic function $\chi_R : \mathbb{N}^n \to \{0,1\}$ is primitive recursive

$$\chi_R(x_1,\ldots,x_n) = \begin{cases} 1 & \text{if } R(x_1,\ldots,x_n) \\ 0 & \text{otherwise} \end{cases}$$

Primitive recursive relations are closed under Boolean operations and bounded quantifiers.

Example: $x < y$ is primitive recursive

$$\chi_<(x,y) = (y \dot{-} x) \dot{-} \mathrm{M}(y \dot{-} x).$$

Example: $x = y$, prime(x) are primitive recursive

$$x = y \Leftrightarrow \neg(x < y) \wedge \neg(y < x).$$

$$\mathrm{prime}(x) \Leftrightarrow x > 1 \wedge \neg\exists y < x \exists z < x (y \cdot z = x).$$

Recap: Recursive functions

Definition

The set of **recursive** functions is the smallest class that contains the constant 0, successor function, projection, and closed under composition, primitive recursion and minimalization.

Minimalization (minimization).
Let $g : \mathbb{N}^{n+1} \to \mathbb{N}$ be a recursive function satisfying that $\forall x_1 \cdots \forall x_n \exists y\ g(x_1, \cdots, x_n, y) = 0$. Then, the function $f : \mathbb{N}^n \to \mathbb{N}$ defined by

$$f(x_1, \cdots, x_n) = \mu y(g(x_1, \cdots, x_n, y) = 0)$$

is recursive, where $\mu y(g(x_1, \cdots, x_n, y) = 0)$ denotes the smallest y such that $g(x_1, \cdots, x_n, y) = 0$.

Theorem

A recursive function is a computable total function, and vice versa.

Recap: Partial computable function

- If a partial computable function $f : \mathbb{N}^k \longrightarrow \mathbb{N}$ is realized by a TM $\mathcal{M}$ with index e, f is denoted by $\{e\}^k$ (or simply $\{e\}$). When e is not an index of TM, $\{e\}$ is regarded as a partial function with empty domain.
- Enumeration theorem: For any $n \geq 0$, there exists a natural number e_n such that

$$\{e_n\}^{n+1}(d, x_1, \ldots, x_n) \sim \{d\}^n(x_1, \ldots, x_n), \quad \text{for any } d, x_1, \ldots, x_n.$$

  $f(x_1, \ldots, x_n) \sim g(x_1, \ldots, x_n)$ means either both sides are not defined or they are defined with the same value.
- A set $X \subset \mathbb{N}^n$ is said to be computably enumerable or CE if $\{1^{x_1}0 \cdots 01^{x_n} : (x_1, \ldots, x_n) \in X\}$ is the domain of a partial computable function.
- X is said to be computable if both X and X^c are CE.
- A halting program $\mathrm{K} = \{e : \{e\}(e) \downarrow\}$ is CE but not computable.

Recap: Partial recursive function

- The **partial recursive functions** are the smallest class that contains the constant 0, the successor function, projections, and closed under composition, primitive recursion and minimalization.
- Kleene normal form theorem: There are a primitive recursive function $U(y)$ and a primitive recursive relation $T_n(e, x_1, \cdots, x_n, y)$ such that for any e, there exists d s.t.

$$\{e\}(x_1, \cdots, x_n) \sim U(\mu y T_n(d, x_1, \cdots, x_n, y)).$$

Theorem

A partial recursive function is a partial computable function, and vice versa.

Among many conditions equivalent to CE, some basic ones are summarized as follows.

Lemma

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

(1) R is CE.

(2) R is an empty set or the range of some primitive recursive function.

(3) R is a finite set or the range of a some recursive injection (1-to-1 function).

(4) R is an empty set or the range of some recursive function.

(5) R is the range of some partial recursive function.

(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.

- By Lemma (2) later, we will show that the Σ_1 sets are the CE sets.

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.

- We 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 $u = \langle u_1, u_2\rangle$,

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

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

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

- That is, $f(y) = z$ is a Δ_1 set. □

- As we saw in the revisited lemma on Slides p.25, 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.

Then, the following two formal 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 Computable Sets)

Assume a theory T is Σ_1-complete. For any computable 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 a computable 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 expressed 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.

□

Old Homework

(1) In a Σ_1 complete theory T, show that 1-consistency (Σ_1-soundness) 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.

(2) 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. In particular, $\{\ulcorner\sigma\urcorner : T \vdash \sigma\}$ is not computable.

Thank you for your attention!