Logic and Foundation I

Part 4. First order arithmetic and incompleteness theorems

Kazuyuki Tanaka

BIMSA

December 15, 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 4. 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

1. Recap
2. $\mathrm{I}\Sigma_1$ and primitive recursive functions
3. CE sets and the first incompleteness
4. Formalizing metamathematics
5. The first incompleteness theorem and its variations

Recap

Peano arithmetic PA 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.

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.

Let us define subsystems of PA by restricting its induction axiom.

Definition

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

- The main subsystems of PA are $\mathrm{I}\Sigma_1 \supset \mathrm{I}\Sigma_0 \supset \mathrm{IOpen}$, 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: $\forall x(x \neq 0 \to \exists y(y + 1 = x))$.
So, it is a theory in the language of ring $\mathcal{L}_{\mathrm{R}} = \{+, \cdot, 0, 1\}$.

Let $\mathrm{Q}_<$ be the system Q plus axiom A7.5 $\forall x \forall y(x < y \leftrightarrow \exists z(z + (x + 1) = y))$.

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 $x < y \to x + z < y + z \wedge (x \cdot z < y \cdot z \vee z = 0)$.

Corollary

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

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

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

Theorem (Σ_1-completeness of R)

R proves all true Σ_1 sentences. Therefore, $\mathsf{Q}_<$, 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 $\varphi(\overline{0}) \lor \varphi(\overline{1})) \lor \cdots \lor \varphi(\overline{n-1})$ 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. $\square$

$\mathrm{I}\Sigma_1$ and related systems

We investigate some basic properties of $\mathrm{I}\Sigma_1$, especially the definability of primitive recursive functions.

Definition

For a formula $\varphi(x, y_1, \ldots, y_k)$ of $\mathcal{L}_{\mathrm{OR}}$, the following formula is called the **collection principle** or **bounding principle** of φ, denoted $(\mathrm{B}\varphi)$:

$$\forall x < u \exists y_1 \cdots \exists y_k \varphi(x, y_1, \ldots, y_k) \to \exists v \forall x < u \exists y_1 < v \cdots \exists y_k < v \varphi(x, y_1, \ldots, y_k),$$

where $\varphi(x, y_1, \ldots, y_k)$ may include undisplayed variables other than u, v. If the collection principle should be treated as a sentence, we consider its universal closure. For a class Γ of formulas, we let

$$\mathbf{B\Gamma} = \mathrm{I}\Sigma_0 \cup \{(\mathrm{B}\varphi) : \varphi \in \Gamma\}.$$

For any n, the collection principle of a Σ_{n+1} formula

$$\varphi(x, y_1, \ldots, y_k)(\equiv \exists z_1 \cdots \exists z_l \theta(x, y_1, \ldots, y_k, z_1, \ldots, z_l))$$

can be obtained from the collection principle of a Π_n formula $\theta(x, y_1, \ldots, y_k, z_1, \ldots, z_l)$ with $k + l$ variables. Therefore, $\mathrm{B}\Sigma_{n+1} \Leftrightarrow \mathrm{B}\Pi_n$.

Lemma

In $B\Sigma_n (n \geq 1)$, adding bounded quantifiers $\forall x < t$, $\exists x < t$ in front of a Σ_n formula produces a formula that is equivalent to a Σ_n formula. Similarly for a Π_n formula.

Proof. By meta-induction on n.

- The case $n = 1$.
  Take any Σ_1 formula $\exists y_1 \cdots \exists y_k \varphi(x, y_1, \ldots, y_k)$. By $B\Sigma_1$, we have

$$\forall x < t \exists y_1 \cdots \exists y_k \varphi(x, y_1, \ldots, y_k) \to \exists v \forall x < t \exists y_1 < v \cdots \exists y_k < v \varphi(x, y_1, \ldots, y_k),$$

  and obviously the converse $\leftarrow$ also holds. Thus, adding $\forall x < t$ in front of the Σ_1 formula is equivalent to a Σ_1 formula of the right-hand side. If $\exists x < t$ is added before a Σ_1 formula, it can be converted into a Σ_1 formula by shifting $\exists x < t$ to the end of the block of existential quantifiers of the formula.
  Π_1 formulas can be treated similarly.
- For $n > 1$, by the same argument as above, we exchange the order of a bounded quantifier $\forall x < t$ and an existential quantifier in front of a Σ_n formula. Then, by induction hypothesis, we can transform the Π_{n-1} formula preceded by a bounded quantifier into an equivalent Π_{n-1} formula.
  Π_n formulas can be treated similarly.

□

Lemma

For any $n \geq 1$, $\mathrm{B}\Sigma_n$ is a subsystem of $\mathrm{I}\Sigma_n$.

Proof. We use meta-induction on n.

- Let $\exists z_1 \cdots \exists z_l \varphi(x, y_1, \ldots, y_k, z_1, \ldots, z_l)$ be Σ_n and $\varphi(x, y_1, \ldots, y_k, z_1, \ldots, z_l)$ Π_{n-1}.
- Suppose $\forall x < u \exists y_1 \cdots \exists y_k \exists z_1 \cdots \exists z_l \varphi(x, y_1, \ldots, y_k, z_1, \ldots, z_l)$. [1]
- By the induction hypothesis $\mathrm{B}\Sigma_{n-1}$ (obvious for $n = 1$) and the above lemma, the following formula $\psi(w)$ is Σ_n.

$$\psi(w) :\equiv (\exists v \forall x < w \exists y_1 < v \cdots \exists y_k < v \exists z_1 < v \cdots \exists z_l < v \varphi) \vee u < w.$$

- Now, we want to prove $\forall w \psi(w)$ by induction.
- Clearly, $\psi(0)$ holds.
- Assume $\psi(w)$ and we will show $\psi(w+1)$.

[1] In the following, we may treat u as a constant.

- If $u < w+1$, $\psi(w+1)$ is obvious.
- So, assume $w < u$. By the first assumption, there exist $y'_1, \ldots, y'_k, z'_1, \ldots, z'_l$ such that $\varphi(w, y'_1, \ldots, y'_k, z'_1, \ldots, z'_l)$. By the induction hypothesis $\psi(w)$, there is v such that

$$\forall x < w \exists y_1 < v \cdots \exists y_k < v \exists z_1 < v \cdots \exists z_l < v \varphi.$$

- If we put
$$v' = \max\{v, y'_1 + 1, \ldots, y'_k + 1, z'_1 + 1, \ldots, z'_l + 1\},$$
then $\forall x < w+1 \exists y_1 < v' \cdots \exists y_k < v' \exists z_1 < v' \cdots \exists z_l < v' \varphi$, which implies $\psi(w+1)$.
- So by Σ_n induction, $\psi(w)$ holds for all w. In particular, if $w = u$,

$$\exists v \forall x < u \exists y_1 < v \cdots \exists y_k < v \exists z_1 < v \cdots \exists z_l < v \varphi,$$

which implies $\exists v \forall x < u \exists y_1 < v \cdots \exists y_k < v \exists z_1 \cdots \exists z_l \varphi$. □

By the above two lemmas, we have

Lemma

For any n, $\mathrm{I}\Sigma_n$ and $\mathrm{I}\Pi_n$ are equivalent.

Proof.

- We show that $\mathrm{I}\Pi_n$ is provable in $\mathrm{I}\Sigma_n$. The other cases can be treated in a similar way.
- Let $\varphi(x)$ be a Π_n formula and assume $\varphi(0) \land \forall x(\varphi(x) \to \varphi(x+1))$.
- By way of contradiction, we assume $\neg\varphi(c)$. Note that free variables included in $\varphi(c)$ should be replaced with constants.
- Roughly, we use induction on the Σ_n formula $\neg\varphi(c-x)$. That is, $\neg\varphi(c-0)$ and $\neg\, \varphi(c-x) \to \neg\varphi(c-(x+1))$ imply $\neg\varphi(0)$.
- More strictly, it is proved by using the following formula.

$$\psi(x) \equiv \exists y \le c(x+y=c \land \neg\varphi(y)) \lor c < x.$$

- It is a Σ_n formula by the lemma in Page 10.
- Similarly, $\mathrm{I}\Sigma_n$ is provable in $\mathrm{I}\Pi_n$.

Problem 2

(1) The following formula is called the **least number principle** for a formula φ and denoted as $\mathrm{L}\varphi$,

$$\exists x \varphi(x) \to \exists x(\varphi(x) \land \forall y < x \neg\varphi(y)).$$

$\mathbf{L}\Sigma_n$ stands for $\{\ \mathrm{L}\varphi : \varphi \text{ is } \Sigma_n\}$. Then, show that $\mathrm{I}\Sigma_n$ is equivalent to $\mathrm{L}\Sigma_n$.
(2) For any n, show $\mathrm{B}\Sigma_{n+1} \supset \mathrm{I}\Sigma_n$.

It is also known that the relation $\mathrm{I}\Sigma_{n+1} \supset \mathrm{B}\Sigma_{n+1} \supset \mathrm{I}\Sigma_n$ is strict.[2] [3].

[2] Petr Hájek and Pavel Pudlák. Metamathematics of first-order arithmetic. Springer, 1993
[3] Kaye R. Models of Peano arithmetic, Oxford Univesity Press, 1991.

Next we discuss the definability of primitive recursive functions in $\mathrm{I}\Sigma_1$. The following lemma is a basic tool for uniquely assigning natural numbers to finite sets and finite sequences in $\mathrm{I}\Sigma_1$.

Lemma

In $\mathrm{I}\Sigma_1$, for a Σ_1 formula $\varphi(x)$ and a Π_1 formula $\psi(x)$, we can prove

$$\forall x(\varphi(x) \leftrightarrow \psi(x)) \to \forall u \exists m, n > 0 \forall x < u(\varphi(x) \leftrightarrow m(x+1)+1 \text{ is a divisor of } n \text{).}$$

Proof.

- First, fix u. The existence of a number m which divides all $i < u$ can be easily shown by Σ_1 induction.
- Then, for all $i < u$, $m(i+1)+1$ are mutually prime. $\because$ If $m(i+1)+1$ and $m(j+1)+1$ $(i < j < u)$ are both multiples of a prime number d, $(m(j+1)+1) - (m(i+1)+1) = m(j-i)$ should also be a multiple of d. But d is never a divisor of m because it devises $m(i+1)+1$. Also, d is not a divisor of $m(j-i)$ since $d \geq u > j-i$.

- Next, let $\varphi(x)$ be Σ_1 formula, and $\psi(x)$ be a Π_1 formula. Assume $\forall x(\varphi(x) \leftrightarrow \psi(x))$.
- Then, by Σ_1 induction on j, we prove the following.

$$\exists n \forall x < j \Big[(\psi(x) \to m(x+1)+1 \text{ is a divisor of } n\ ) \\ \wedge (m(x+1)+1 \text{ is a divisor of } n\ \to \varphi(x))\Big] \vee u < j.$$

- It is obvious when $j = 0$.
- Let n_j be the minimum n that satisfies the above condition for j (See the least number principle, Problem 3).
- Now, if $\varphi(j)$, then $n_{j+1} = n_j \bullet (m(j+1)+1)$, otherwise $n_{j+1} = n_j$.
- Note that for all $i < u$, $m(i+1)+1$ are mutually prime, and n_j does not contain any factor of $m(j+1)+1$ due to its minimality.
- Then, n_{j+1} satisfies the above condition for $j+1 \leq u$, which completes the induction step.
- Thus, the lemma holds as $j = u$. □

- In the above lemma, the triple (u, m, n) satisfying

$$\forall x < u \left(\varphi(x) \leftrightarrow m(x+1)+1 \text{ is a divisor of } n \right)$$

is called a u-**piece code** of a Δ_1 set $\{x \mid \varphi(x)\}$ defined by a Σ_1 formula $\varphi(x)$ and a Π_1 formula $\psi(x)$.

- We will extend the above to n-dimensional sets. First, we code a pair of natural numbers (x, y) by a natural number $\langle x, y\rangle = \frac{(x+y)(x+y+1)}{2} + x$. Note that if $u = \langle u_1, u_2\rangle$, then $\langle x, y\rangle < u$ for any $x < u_1$, $y < u_2$.

- Then, from the lemma in Page 15, for a Δ_1 formula $\varphi(x, y)$, there exist u, m, n s.t.

$$\forall x < u_1 \forall y < u_2 (\varphi(x, y) \leftrightarrow m(\langle x, y\rangle + 1) + 1 \text{ is a divisor of } n\ )$$

The triple $c = (u, m, n)$ is called a (u_1, u_2)-piece code of the Δ_1 set.

- In general, by coding an n-tuple $(x_1, x_2, \cdots, x_n)$ by a natural number $\langle\langle \cdots \langle x_1, x_2\rangle, \ldots\rangle, x_n\rangle$, we can define a $(u_1, u_2, \cdots, u_n)$-piece code of a Δ_1 n-dimensional set.

Theorem (Definability of primitive recursive functions)

In $I\Sigma_1$, (the graph of) a primitive recursive function f can be represented by a Δ_1 formula $\varphi(x_1, \ldots, x_l, y, z)$, and the following are provable

$$\forall x_1 \cdots \forall x_l \forall y \exists! z \varphi(x_1, \ldots, x_l, y, z).$$

Proof.

- We will prove this by induction on the construction of primitive recursive functions. The essential step is 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.
- If f can be expressed by a Δ_1 formula φ, it will be easily derived in $I\Sigma_1$ that $\forall \overrightarrow{x} \forall y \exists! z \varphi(\overrightarrow{x}, y, z)$.

- First, let $\gamma(x, m, n)$ be a Σ_0 formula expressing "$m(x+1)+1$ is a divisor of n", that is, $\exists d < n\ (m(x+1)+1) \cdot d = n$.
- We define a predicate $\delta(u, m, n)$ such that

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

by the following Σ_0 formula: 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, by $I\Sigma_1$, we can show $\forall u_1 \exists u_2 \exists m \exists n \delta(\langle u_1, u_2 \rangle, m, n)$
- Therefore, we have

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

- Thus, $f(y) = z$ is expressed by a Δ_1 formula.

□

- The above theorem shows that adding a symbol for a primitive recursive function and its definition to $\mathrm{I}\Sigma_1$, we obtain a conservative extension.
- Furthermore, even if primitive recursive function symbols are involved, the classes of Σ_n and Π_n formulas $(n > 0)$ do not essentially change. In other words, for a Σ_n formula containing primitive recursive function symbols, we can construct an equivalent Σ_n formula that includes no primitive recursive function symbols by replacing a primitive recursive function symbol with a Σ_1 formula or Π_1 formula that defines it.
- In the lemma in Page 15, we showed the existence of a u-piece code for a Δ_1 set. Also, a finite sequence of natural numbers $s = (s_0, \ldots, s_{n-1})$ can be coded as a natural number c. Then, we identify s and c, and write c_i for s_i.
Note that $(c, i) \mapsto c_i$ is primitive recursive.

Recap: Partial computable functions and CE sets

- 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.
- 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.

Theorem

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

- 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.

Among many conditions equivalent to CE, some basic ones are following.

Lemma

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

(1) R is CE.

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

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

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

Definition

Let $\mathfrak{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$ be the 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

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

- 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

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.

Proof.

- Any CE relation $R(\vec{x})$ can be expressed by $\exists y S(\vec{x}, y)$ for some primitive recursive relation S.
- By the definability theorem of prim. rec. functions, any primitive recursive relation S can be expressed by a Σ_1 formula, and so $\exists y S(\vec{x}, y)$ is still Σ_1.
- Conversely, a Σ_1 formula is expressed in the form $\exists y \theta(\vec{x}, y)$ with $\theta(\vec{x}, y) \in \Sigma_0$. Since a Σ_0 formula is a primitive recursive, a Σ_1 formula is CE.

From now on, we assume that all theories are given in the language $\mathcal{L}_{\mathrm{OR}}$ and contain at least R, so Σ_1-complete. We will prove a version of Gödel's first incompleteness theorem

Definition

Theory T is **1-consistent** if, for any Σ_1 sentence σ, $T \vdash \sigma \Rightarrow \mathfrak{N} \models \sigma$.

- Ordinary theories T of arithmetic such as Q and PA have the standard model $\mathfrak{N}$, so they are naturally 1-consistent, and indeed ω-consistent (i.e., for any formula $\varphi(x)$, if $T \vdash \varphi(\bar{n})$ for all $n \in \mathbb{N}$ then $T \nvdash \exists x \neg\varphi(x)$.)
- 1-consistency is properly stronger than consistency. E.g., Q $+\exists x(0 + x \neq x)$ is consistent but not 1-consistent.

Theorem ((Weak) Representation Theorem for CE sets, reposted)

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,

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

Theorem (Gödel's first incompleteness theorem, a naïve version)

Let T be a Σ_1-complete and 1-consistent Σ_1 theory. Then T is incomplete, that is, there is a sentence σ such that T cannot prove or disprove.

Proof.

- We know 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.

□

Formalizing metamathematics

We prepare some useful prim. rec. functions for coding things.

Lemma

For a primitive recursive function $h(\vec{x})$, $\mu y < h(\vec{x}) A(\vec{x}, y)$ is primitive recursive.

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.

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

- A finite sequence of natural numbers $(x_0, \ldots, x_{n-1})$ can be represented by a single natural number x as follows,

$$x = p(0)^{x_0+1} \cdot p(1)^{x_1+1} \cdot \cdots \cdot p(n-1)^{x_{n-1}+1}$$

- Fixing n, such a mapping from $\mathbb{N}^n$ to $\mathbb{N}$ is a primitive recursive function.
- Conversely, for a natural number x, the function $c(x, i)$ takes the ith element x_i from x,

$$x_i = c(x, i) = \mu y < x\ (\neg\exists z < x\, (p(i)^{y+2} \cdot z = x)).$$

- The length of the sequence represented by x is

$$\mathrm{leng}(x) = \mu i < x\ (\neg\exists z < x\, (p(i) \cdot z = x)).$$

- Furthermore, we define a primitive recursive relation $\mathrm{Seq}(x)$ to denote that a natural number x is the code of such a sequence as follows:

$$\mathrm{Seq}(x) \Leftrightarrow \forall i < x \forall z < x\ (p(i) \cdot z = x \to i \leq \mathrm{leng}(x)).$$

Gödel numbers

Definition

Let Ω be a finite (or countably infinite) set of symbols, and an injection $\phi : \Omega \to \mathbb{N}$. For a string $s = a_0 \cdots a_{n-1}$, the following natural number $\psi(s)$ is called the **Gödel number** of s, denoted by $\ulcorner s \urcorner$.

$$\psi(s) = p(0)^{\phi(a_0)+1} \cdot p(1)^{\phi(a_1)+1} \cdot \cdots \cdot p(n-1)^{\phi(a_{n-1})+1}.$$

The mapping $\ulcorner \quad \urcorner$ is an injection from the set of all symbols Ω^* to $\mathbb{N}$.

Example

Let $\Omega = \{0, 1, +, (,)\}$, $\phi(0) = 0$, $\phi(1) = 1$, $\phi(+) = 3$, $\phi(\,(\,) = 5$ and $\phi(\,)\,) = 6$.
Then,

$$\ulcorner (1 + 0) + 1 \urcorner = 2^6 \cdot 3^2 \cdot 5^4 \cdot 7^1 \cdot 11^7 \cdot 13^4 \cdot 17^2$$

Problem 5

Show that $\mathrm{Term}(x)$ expressing "x is the Gödel number of a term" is primitive recursive.

Definition

A theory T is Σ_i ($\Pi_i/\Delta_i/$primitive recursive, etc.) if the set of Gödel numbers of its axioms $\{\ulcorner\sigma\urcorner : \sigma \in T\}$ is Σ_i ($\Pi_i/\Delta_i/$primitive recursive, etc.).

- Ordinary theories in mathematics are finite or at most primitive recursive.
- The theories of arithmetic introduced so far (PA, IΣ_1, etc.) are all primitive recursive.
- To derive the incompleteness theorem, we need to assume that a theory 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 Σ_1 set of axioms can be always be replaced by a primitive recursive set.

Theorem (Craig's lemma)

For any CE theory T, there exists a primitive recursive theory T' that proves the same theorems.

Proof. Let T be a 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 $\vdash \sigma \leftrightarrow \sigma \wedge \sigma \wedge \cdots \wedge \sigma$. Thus T' is primitive recursive. □

Because Gödel numbers and their decodings are heavily used in T', T' cannot be easily expressed in Σ_0.

Based on Craig's lemma, a Σ_1 theory is primitive recursively axiomatizable. Then, "a finite sequence (or finite tree) P of formulas is a proof in T" can be defined in a primitive recursive way (with T as a parameter).

Definition

- Let T be a Σ_1 theory and T' its p.r. counterpart. A proof in T' is a finite sequence of formulas where each formula is either a logical axiom, an equality axiom, or an axiom of T', or obtained by applying MP or quantification rules from formulas appearing before. The formula that appears at the end of the proof is the theorem of T.
- Now, we define the primitive recursive predicate Proof_T as follows.

$$\mathrm{Proof}_T(\ulcorner P \urcorner, \ulcorner \sigma \urcorner) \Leftrightarrow P \text{ is a proof of formula } \sigma \text{ in } T'.$$

- By Proof_T, we also denote a Δ_1 formula expressing the above Proof_T in $\mathrm{I}\Sigma_1$. A Σ_1 formula Bew_T is defined as

$$\mathrm{Bew}_T(x) \equiv \exists y \; \mathrm{Proof}_T(y, x).$$

The formula $\mathrm{Bew}_T(x)$ expresses that "x is the Gödel number of a theorem of T". "Bew" stands for the German beweisbar (provable).

Theorem ((Strong) Representation Theorem for Computable Sets, reposted)

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

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

Theorem (Representation Theorem for Computable Function)

Let T be Σ_1-complete. For any computable function $f(\vec{x})$, there exists a Σ_1 formula $\varphi(\vec{x}, y)$ which represents $f(\vec{x}) = y$ and satisfies, for all natural numbers $m_1, \ldots, m_l$,

$$T \vdash \forall y \forall y' (\varphi(\overline{m_1}, \ldots, \overline{m_l}, y) \land \varphi(\overline{m_1}, \ldots, \overline{m_l}, y') \to y = y').$$

Proof. For simplicity, we assume that $l = 1$. Suppose $f(x) = y$ is represented by a Σ_1 formula $\varphi(x, y) \equiv \exists z \theta(x, y, z)$ with $\theta(x, y, z) \in \Sigma_0$. We define a Σ_0 formula $\psi(x, y, z)$ as

$$\theta(x, y, z) \land \forall y', z' \leq y + z(\theta(x, y', z') \to y + z \leq y' + z').$$

Then, $\exists z \psi(x, y, z)$ also represents $f(x) = y$. To show, the functional property of this representation. Take any m and let $n = f(m)$. Then the minimal k such that $\theta(\overline{m}, \overline{n}, \overline{k})$ satifies $\psi(\overline{m}, \overline{n}, \overline{k})$. By the definition, no other y, z satisfy ψ. So, we are done. □

Lemma (Diagonalization lemma)

Let T be Σ_1-complete. For any formula $\psi(x)$ in which x is the unique free variable, there exists a sentence σ such that $T \vdash$ "$\sigma \leftrightarrow \psi(\overline{\ulcorner \sigma \urcorner})$" .

Proof.

- A formula with only x as a free variable is computably enumerated as $\varphi_0(x), \varphi_1(x), \ldots$, and then $f(n) = \ulcorner \varphi_n(\overline{n}) \urcorner$ is also a computable function. By the functional representation theorem, there exists a Σ_1 formula χ such that

$$f(m) = n \Rightarrow T \vdash \chi(\overline{m}, \overline{n}) \wedge \forall y \neq \overline{n}\ \chi(\overline{m}, y).$$

- The formula $\exists y(\chi(x, y) \wedge \psi(y))$ must be listed as $\varphi_k(x)$ for some k. Now, let $\sigma \equiv \varphi_k(\overline{k})$. Since $f(k) = \ulcorner \sigma \urcorner$, $T \vdash \chi(\overline{k}, \overline{\ulcorner \sigma \urcorner})$. Thus, in T, $\psi(\overline{\ulcorner \sigma \urcorner}) \to \exists y(\chi(\overline{k}, y) \wedge \psi(y))$ $(\equiv \varphi_k(\overline{k}) \equiv \sigma)$.
- On the other hand, since $T \vdash \forall y \neq \overline{\ulcorner \sigma \urcorner}\ \neg\chi(\overline{k}, y)$, in T,

$$\neg\psi(\overline{\ulcorner \sigma \urcorner}) \to \forall y(\chi(\overline{k}, y) \to \neg\psi(y)) \to \neg\exists y(\chi(\overline{k}, y) \wedge \psi(y))\ (\equiv \neg\sigma).$$

- Therefore, $T \vdash \sigma \leftrightarrow \psi(\overline{\ulcorner \sigma \urcorner})$, that is, σ is a fixed point of ψ. □

Homework

(1) T is called ω-consistent if for any formula $\varphi(x)$, if $T \vdash \varphi(\bar{n})$ for all $n \in \mathbb{N}$ then $T \nvdash \exists x \neg\varphi(x)$.

Show that a Σ_1-complete theory T is 1-consistent iff it is ω-consistent with respect to the Σ_0 formulas $\varphi(x)$.

(2) T is called Σ_n-consistent if any Σ_n theorem of T is true. Similarly for Π_n-consistency.

Show that if a Σ_1-complete theory T is ω-consistent, then it is Π_3-consistent, but not necessarily Σ_3-consistent.

Theorem (Gödel's first incompleteness theorem, a formal version)

Let T be a Σ_1-complete and 1-consistent Σ_1 theory. Then T is incomplete, that is, there is a sentence σ such that $T \nvdash \sigma$ and $T \nvdash \neg\sigma$.

Proof. By the diagonalization lemma, there exists a fixed point σ of $\neg\mathrm{Bew}_T(x)$. In other words, $T \vdash \sigma \leftrightarrow \neg\mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$. We show that σ is such a sentence that T cannot prove or disprove as follows.

- Suppose $T \vdash \sigma$. Then $\mathrm{Bew}_T(\ulcorner\sigma\urcorner)$ holds, that is, $\mathfrak{N} \models \mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$. Therefore, by Σ_1 completeness, $T \vdash \mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$. Since σ is a fixed point of $\neg\mathrm{Bew}_T(x)$, we have $T \vdash \neg\sigma$ which implies the inconsistency of T, a contradiction.
- On the other hand, suppose $T \vdash \neg\sigma$. Since σ is a fixed point, $T \vdash \mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$. By 1-consistency of T, $\mathfrak{N} \models \mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$, that is, $T \vdash \sigma$, which also implies the inconsistency of T. □

- The sentence σ in the above proof "asserts its own unprovability" because "$\sigma \Leftrightarrow T \nvdash \sigma$" holds. This σ is called the **Gödel sentence** of T.
- Since $T \nvdash \sigma$, $\mathfrak{N} \models \neg\mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$, and so $\mathfrak{N} \models \sigma$ if $\mathfrak{N} \models T$. That is, a Gödel sentence of a theory which has $\mathfrak{N}$ as a model is a "true Π_1 sentence."
- As we will see later (if T contains $\mathrm{I}\Sigma_1$), such a Gödel sentence is equivalent to the statement expressing the consistency of T.

Rosser weakened the assumption of incompleteness theorem from 1-consistency to consistency. He modified $\mathrm{Bew}_T(x)$ as follows.

$$\mathrm{Bew}^*_T(x) \equiv \exists y(\mathrm{Proof}_T(y, x) \land \forall z < y \neg\mathrm{Proof}_T(z, \neg x)).$$

Here, $\neg x$ means the code of $\neg\varphi$ when x is the code of a formula φ.

$$\mathrm{Bew}^*_T(x) \equiv \exists y(\mathrm{Proof}_T(y,x) \land \forall z < y \neg \mathrm{Proof}_T(z, \neg x)).$$

Lemma

Let T be a Σ_1-complete Σ_1 theory. Then, for any sentence σ,
(1) $T \vdash \sigma \Rightarrow T \vdash \mathrm{Bew}^*_T(\overline{\ulcorner \sigma \urcorner})$,
(2) $T \vdash \neg\sigma \Rightarrow T \vdash \neg \mathrm{Bew}^*_T(\overline{\ulcorner \sigma \urcorner})$.

Proof. If T is inconsistent, the lemma holds trivially, so we assume T is consistent.
If $T \vdash \sigma$, it is easy to see that $\mathrm{Bew}^*_T(\overline{\ulcorner \sigma \urcorner})$ is true. Then (1) follows from Σ_1 completeness.
To show (2), assume $T \vdash \neg\sigma$. There exists $n \in \mathbb{N}$ such that the following holds in $\mathfrak{N}$

$$\mathrm{Proof}_T(\overline{n}, \overline{\ulcorner \neg\sigma \urcorner}) \land \forall z \leq \overline{n} \neg \mathrm{Proof}_T(z, \overline{\ulcorner \sigma \urcorner}).$$

By Σ_1 completeness, the above formula is provable in T. So, in T,
$\mathrm{Proof}_T(y, \overline{\ulcorner \sigma \urcorner}) \to y > \overline{n}$, and thus

$$\forall y(\mathrm{Proof}_T(y, \overline{\ulcorner \sigma \urcorner}) \to \exists z < y \mathrm{Proof}_T(z, \overline{\ulcorner \neg\sigma \urcorner}))$$

is provable. Therefore, $T \vdash \neg \mathrm{Bew}^*_T(\overline{\ulcorner \sigma \urcorner})$. □

The fixed point σ of $\neg\mathrm{Bew}^*_T(x)$, i.e., $T \vdash \sigma \leftrightarrow \neg\mathrm{Bew}^*_T(\overline{\ulcorner\sigma\urcorner})$ is called a **Rosser sentence**.

Theorem (Gödel-Rosser)

If T is a consistent Σ_1-complete Σ_1 theory, then there exists a sentence σ such that $T \nvdash \sigma$ and $T \nvdash \neg\sigma$.

Proof.

- If $T \vdash \sigma$, then by the last lemma $T \vdash \mathrm{Bew}^*_T(\overline{\ulcorner\sigma\urcorner})$, and so by the definition of the fixed point σ, $T \vdash \neg\sigma$, which implies that T is inconsistent.
- If $T \vdash \neg\sigma$, then by the last lemma, $T \vdash \neg\mathrm{Bew}^*_T(\overline{\ulcorner\sigma\urcorner})$. By definition of the fixed point σ, we have $T \vdash \sigma$, which implies that T is inconsitent. $\square$

Let's look at more applications of the diagonalization lemma.

Lemma

In a consistent Σ_1-complete theory T, there exists no formula $\psi(x)$ such that for any sentence σ, $T \vdash \sigma \leftrightarrow \psi(\overline{\ulcorner \sigma \urcorner})$.

Proof. If there were such a $\psi(x)$, then a fixed point σ of $\neg\psi(x)$ clearly does not satisfy the condition. □

In the above lemma, letting T be $\mathrm{Th}(\mathfrak{N})$, we obtain the following theorem.

Theorem (Tarski's undefinability of truth)

There is no formula $\psi(x)$ such that $\mathfrak{N} \models \sigma \leftrightarrow \psi(\overline{\ulcorner \sigma \urcorner})$ for all sentence σ.

Lemma

For a consistent Σ_1-complete theory T, there is no formula $\psi(x)$ s.t. for any sentence σ,

$$(1)\ T \vdash \sigma \quad \Rightarrow \quad T \vdash \psi(\overline{\ulcorner \sigma \urcorner}),$$
$$(2)\ T \nvdash \sigma \quad \Rightarrow \quad T \vdash \neg\psi(\overline{\ulcorner \sigma \urcorner}).$$

Proof. Suppose there were such a $\psi(x)$, and let σ be a fixed point of $\neg\psi(x)$. Then, if $T \vdash \sigma$ then $T \vdash \neg\psi(\overline{\ulcorner \sigma \urcorner})$, which means (1) does not hold. If $T \nvdash \sigma$ then $T \nvdash \neg\psi(\overline{\ulcorner \sigma \urcorner})$, which means (2) does not hold. □

Lemma

For a consistent Σ_1-complete theory T, the set $\{\ulcorner \sigma \urcorner : T \vdash \sigma,\ \sigma \text{ is a sentence}\}$ is not computable.

Proof. If the set of theorems of T is computable, by the strong representation theorem, there would be such a $\psi(x)$ that satisfies the above lemma. □

Theorem (Church's undecidability of predicate calculus)

In the language $\mathcal{L}_{\mathrm{AR}}$ (or $\mathcal{L}_{OR}$), the set of Gödel numbers of sentences provable in first-order logic $\{\ulcorner\sigma\urcorner : \vdash \sigma, \sigma \text{ is a statement}\}$ is not computable.

Proof. Since Q consists of finitely many axioms, we can connect them all by $\wedge$ and denote it as ξ. By the deduction theorem,

$$\mathsf{Q} \vdash \sigma \;\Leftrightarrow\; \vdash \xi \to \sigma.$$

So if $\{\ulcorner\sigma\urcorner : \vdash \sigma\}$ is computable,

$$\{\ulcorner\sigma\urcorner : \vdash \xi \to \sigma\} = \{\ulcorner\sigma\urcorner : \mathsf{Q} \vdash \sigma\}$$

is also computable, which contradicts with the last lemma. □

Thank you for your attention!