Topics in Applied Math: Logic and Foundations of Mathematics

Part 4. First order arithmetic

Kazuyuki Tanaka

BIMSA

October 24, 2025

清華大学 求真书院
Qiuzhen College, Tsinghua University

Logic and Foundations

- **Part 1. Equational theory**
- **Part 2. First order theory**
- **Part 3. Basic Model theory**
- **Part 4. First order arithmetic and incompleteness theorems**
- **Part 5. Models of first-order arithmetic**
- **Part 6. Second order arithmetic and reverse mathematics**

Part 4. Schedule

- Oct. 24, (1) Peano arithmetic and representation theorems
- Oct. 29, (2) The first incompleteness theorem
- Oct. 31, (3) The second incompleteness theorem

§4.1. Peano arithmetic

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 1.1

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. $x<y+1 \leftrightarrow x<y \lor x=y$.

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

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

- 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 its definition $\forall x \forall y (f(x) = y \leftrightarrow \varphi(x, y))$ to a theory T if $T \vdash \forall x \exists y \varphi(x, y)$ holds.

- 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 A7 and A8 are removed, $<$ can be introduced as

  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, rather than an abbreviation for the right-hand side of A7.5.

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

  Here, ω^ω is the next ordinal after ω closed under $+$ and $\cdot$. In set theory, an ordinal is identified with the set of ordinals smaller than it.
- Let $\mathbb{Z}[X]$ be the ring of polynomials of integer coefficients with X as a variable. For $p, q \in \mathbb{Z}[X]$, we set $p > 0$ if its highest order coefficient is positive, and then $p > q$ if $p - q > 0$.

  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 1.2

- 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.

- The set of Σ_i/Π_i formulas is often denoted as Σ_i/Π_i, respectively.
- 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, many formulas do not belong to any class of the hierarchy. However, by de Morgan's rule, any formula can be transformed to an equivalent formula in the above classification. The (lowest) class to which the equivalent formula belongs is regarded as its hierarchical class.

Remark

- $\neg\exists y(y + y = x)$ 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 1

- 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 1.3

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 introduced by R. Robinson.

Definition 1.4

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 $-\{A10\} \nvdash 0+1=1$.

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

Lemma 1.5

In IOpen, the following axioms PA^- of **discrete ordered semirings** 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 ∀). For instance, the associative law of addition $(x + y) + z = x + (y + z)$ can be easily shown by induction on z. Similar for the other equations.

▶ 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 ∀ in front), we can select appropriate variables and use induction. □

Corollary 1.6

$Q_<$ 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.

□

Summary

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

- 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.

§4.2. The weakest system R

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 2.1 (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 2.2

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

Proof Most of the axioms of R can be easily proved in $\mathsf{Q}_<$ 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 2.3 (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 $\exists x_1 \exists x_2 \dots \exists x_k \varphi(x_1, x_2, \dots, x_k)$ is true, there exist natural numbers $n_1, n_2, \dots, n_k$ such that $\varphi(\overline{n_1}, \overline{n_2}, \dots, \overline{n_k})$ 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, $\varphi(\overline{n_1}, \overline{n_2}, \dots, \overline{n_k})$ is provable since it is true. From the rule of first-order logic, $\exists x_1 \exists x_2 \dots \exists x_k \varphi(x_1, x_2, \dots, x_k)$ is also provable in R. □

- All the arithmetic systems we will discuss are extensions of R, and thus Σ_1-complete.

Corollary 2.4

$Q_<$, PA^-, IOpen, etc. are all Σ_1-complete.

Representation

Definition 2.5 (Representation for Sets and Functions)

- A set $C \subset \mathbb{N}$ is **(strongly) representable** by a formula $\varphi(x)$ in a theory T, if

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

- A number-theoretic function $f(\vec{x})$ is **functionally representable** by a formula $\varphi(\vec{x}, y)$ in a theory T, if $\varphi(\vec{x}, y)$ represents $f(\vec{x}) = y$ and for all natural numbers $m_1, \ldots, m_l$,

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

Definition 2.6

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.

- Later, we will show that the Σ_1 sets are the CE sets, and the Δ_1 sets are the computable sets,

Theorem 2.7 ((Strong) Representation Theorem for Δ_1 Sets)

Assume a theory T is Σ_1-complete. For any Δ_1 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 Δ_1 set C, 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 $\exists y(\theta_1(\overline{n}, y) \land \forall z \leq y \neg\theta_2(\overline{n}, z))$. 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, $T \vdash \neg\varphi(\overline{n})$. □

Theorem 2.8 (Representation Theorem for Δ_1 Function)

Let T be Σ_1-complete. For any Δ_1 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. □

An important condition Gödel used to prove the first incompleteness theorem for a theory T is its **ω-consistency**, that is, for any 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. **1-consistency** is a weaker version obtained from ω-consistency by restricting $\varphi(x)$ to a Σ_0 (or Δ_1) formula.
A theory is said to be **Σ_n-sound** if all the Σ_n theorems of T are true.

Homework # 3-2

(1) Show that a Σ_1-complete theory T is 1-consistent iff it is Σ_1-sound.

(2) Show that any ω-consistent Σ_1-complete theory is Π_3-sound, but may not be Σ_3-sound.

Thank you for your attention!