# Logic and Computation I

## Part 3a. Formal Arithmetic

Kazuyuki Tanaka

BIMSA

November 28, 2024

北京雁栖湖应用数学研究院
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 3a. Formal Arithmetic**

## Part 3a. Schedule (subject to change)

- Nov.21, (6) Presburger arithmetic
- Nov.26, (7) Peano arithmetic
- Nov.28, (8) **Gödel's first incompleteness theorem**
- Dec. 3, (9) Gödel's second incompleteness theorem
- Dec. 5, (10) Second order logic
- Dec.10, (11) Second order arithmetic

# Recap: Peano Arithmetic

## Definition 3.38 (**Peano arithmetic** PA)

PA is a first-order theory in the language $\mathcal{L}_{\mathrm{OR}} = \{+, \cdot, 0, 1, <\}$ consisting of:

| | | |
|---|---|---|
| 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: $\varphi(0) \land \forall x(\varphi(x) \to \varphi(x + 1)) \to \forall x \varphi(x)$, for all formula $\varphi(x)$.

## Definition 3.39 (**Arithmetical Hierarchy**)

- A formula is **bounded ($\Sigma_0$, $\Pi_0$)** if its quantifiers are bounded $\forall x < t, \exists x < t$.
- If $\varphi$ is a $\Sigma_i$ formula, then $\forall x_1 \cdots \forall x_k \varphi$ is a $\Pi_{i+1}$ formula,
- If $\varphi$ is a $\Pi_i$ formula, then $\exists x_1 \cdots \exists x_k \varphi$ is a $\Sigma_{i+1}$ formula.
- A $\Sigma_i$ formula equivalent to some $\Pi_i$ formula is called a $\Delta_i$ formula.

## Definition 3.40 ($\mathsf{I}\Gamma$)

$\mathrm{I}\Gamma$ is a subsystem of PA obtained by restricting induction to a class $\Gamma$ of formulas .

## Definition 3.41 (**Robinson's system** Q)

Q is obtained from PA by removing inequality and induction, and instead adding:
Predecessor: $\forall x(x \neq 0 \to \exists y(y+1=x))$.
It is in language $\mathcal{L}_{\mathrm{R}} = \{+,\cdot,0,1\}$. Let $\mathsf{Q}_<$ be Q plus the explicit definition of $<$.

## Lemma 3.42 (**theory of discrete ordered semirings** $\mathsf{PA}^-$)

In $\mathrm{IOpen}$, the following axioms of $\mathsf{PA}^-$ can be proved.

(1) Ordered semirings (commutative ordered rings with no additive inverses).
(2) Difference: $x < y \to \exists z(z+(x+1)=y)$.
(3) Discreteness: $0 < x \leftrightarrow 1 \leq x$.

## Corollary 3.43

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

# Gödel's first incompleteness theorem

## Theorem 3.44 ($\Sigma_1$-**completeness of** $\mathsf{Q}_<$)

$\mathsf{Q}_<$ proves all true $\Sigma_1$ sentences.

**Proof**

- If a $\Sigma_1$ sentence $\exists x_1 \exists x_2 \ldots \exists x_k \varphi(x_1, x_2, \ldots, x_k)$ is true, there exist concrete numbers $n_1, n_2, \ldots, n_k$ such that $\varphi(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k})$ is true. Since $\varphi(\overline{n_1}, \overline{n_2}, \ldots, \overline{n_k})$ is a bounded sentence, it is provable if 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. □

- All the arithmetic systems we will discuss are extensions of $\mathsf{Q}_<$, and thus $\Sigma_1$-complete.
- Another condition for the first incompleteness theorem is **1-consistency**, also known as $\Sigma_1$-**soundness**. A theory is said to be $\Sigma_n$-**sound** if all provable $\Sigma_n$ sentences are true.

- We first look at the first incompleteness theorem from the viewpoint of computability theory. Then, we will reexamine the proof more syntactically.
- Recall that $X \subseteq \mathbb{N}^n$ is called **CE** (computably enumerable) if it is the domain (or range) of some partial recursive function. By Lemma 1.49, any CE relation $R(\vec{x})$ can be expressed by $\exists y S(\vec{x}, y)$ for some primitive recursive relation $S$.

## Definition 3.45

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 $\Sigma_i$ if there exists a $\Sigma_i$ formula $\varphi(x_1, \ldots, x_l)$ s.t.

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

- Similarly, $\Pi_i$ sets can be defined by $\Pi_i$ formulas.
- A set that is both $\Sigma_i$ and $\Pi_i$ is called $\Delta_i$.

## Lemma 3.46

The graph $\{(\vec{x}, y) : f(\vec{x}) = y\}$ of a primitive recursive function $f$ is a $\Delta_1$ set.

**Proof**

- By induction on the construction of primitive recursive functions. For example, consider the following definition of a function $f(x)$:

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

- Let $\gamma(x, m, n)$ be a $\Sigma_0$ formula "$m(x+1)+1! \mid n$". Then, for any finite set $A$ (with $\max A < u$), there exist $m, n$ s.t. $\forall x < u(x \in A \Leftrightarrow \gamma(x, m, n))$.
- Fix such $m, n$. Define a $\Sigma_0$ formula $\delta(\langle u_1, u_2\rangle) \Leftrightarrow \forall y < u_1 \exists z < u_2\ f(y) = z$ (with $m, n$ as hidden parameters) as follows: for any $u = \langle u_1, u_2\rangle$,

$$\begin{aligned}\delta(u) \equiv\ & \forall y < u_1 \exists z < u_2\ \gamma(\langle y, z\rangle) \wedge \forall z < u_2(\gamma(\langle 0, z\rangle) \leftrightarrow z = c) \\ & \wedge \forall y < u_1 - 1 \forall z < u_2(\gamma(\langle y+1, z\rangle) \leftrightarrow \exists z' < u_2(z = h(y, z') \wedge \gamma(\langle y, z'\rangle)))).\end{aligned}$$

- Then $\forall u_1 \exists u_2 \exists m \exists n \delta(\langle u_1, u_2\rangle, m, n)$ holds. Thus, we obtain a $\Delta_1$ relation:

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

□

### Lemma 3.47

The CE sets are exactly the same as the $\Sigma_1$ sets. Hence, the computable (recursive) sets are exactly the same as the $\Delta_1$ sets.

**Proof** By Lemma 1.49, 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, $S$ can be expressed by a $\Sigma_1$ formula, and so $\exists y S(\vec{x}, y)$ is still $\Sigma_1$. □

### Theorem 3.48 ((Weak) Representation Theorem for CE sets)

Suppose that a theory $T$ is $\Sigma_1$-complete and 1-consistent. Then, for any CE set $C$, there exists a $\Sigma_1$ formula $\varphi(x)$ s.t. for any $n$, $\quad n \in C \Leftrightarrow T \vdash \varphi(\overline{n})$.

**Proof.**

- By the above Lemma, for any CE set $C$, there exists a $\Sigma_1$ formula $\varphi(x)$ such that $n \in C \Leftrightarrow \mathfrak{N} \models \varphi(\overline{n})$.
- Since $T$ is $\Sigma_1$-complete, $\mathfrak{N} \models \varphi(\overline{n}) \Rightarrow T \vdash \varphi(\overline{n})$.
- Also since $T$ is 1-consistent, $T \vdash \varphi(\overline{n}) \Rightarrow \mathfrak{N} \models \varphi(\overline{n})$. □

## Theorem 3.49 ((Strong) Representation Theorem for Computable Sets)

Assume a theory $T$ is $\Sigma_1$-complete. For any computable set $C$, there exists a $\Sigma_1$ formula $\varphi(x)$ s.t. for any $n$, $\quad n \in C \Rightarrow T \vdash \varphi(\overline{n}), \quad n \notin C \Rightarrow T \vdash \neg\varphi(\overline{n})$.

**Proof.**

- For computable $C$, by Lemma 3.47 there exist $\Sigma_0$ formulas $\theta_1(x, y), \theta_2(x, y)$ such that $\quad n \in C \Leftrightarrow \mathfrak{N} \models \exists y \theta_1(\overline{n}, y), \quad n \notin C \Leftrightarrow \mathfrak{N} \models \exists y \theta_2(\overline{n}, y)$.
- Let $\varphi(x)$ be a $\Sigma_1$ formula $\exists y(\theta_1(\overline{n}, y) \land \forall z \leq y \neg\theta_2(\overline{n}, z))$. By the $\Sigma_1$-completeness of $T$, $\quad n \in C \Rightarrow T \vdash \varphi(\overline{n})$.
- To show $n \notin C \Rightarrow T \vdash \neg\varphi(\overline{n})$, take any $n \notin C$. Since $\mathfrak{N} \models \exists y \theta_2(\overline{n}, y)$, there exists an $m$ s.t. $\mathfrak{N} \models \theta_2(\overline{n}, \overline{m})$. Again by $\Sigma_1$ 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 $l$, $\mathfrak{N} \models \neg\theta_1(\overline{n}, \overline{l})$, i.e., $T \vdash \neg\theta_1(\overline{n}, \overline{l})$. Therefore, if $\theta_1(\overline{n}, a)$ holds 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, $T \vdash \neg\varphi(\overline{n})$. $\square$

- To derive the incompleteness theorem, we need one more condition on a formal system of arithmetic, that is, the set of axioms is CE.
- From the following theorem, a CE set of axioms can be also expressed as a primitive recursive set.

## Theorem 3.50 (Craig's lemma)

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

**Proof.** Let $T$ be a CE theory, defined by $\Sigma_1$ formula $\varphi(x) \equiv \exists y \theta(x, y)$ ($\theta$ is $\Sigma_0$). That is, $\sigma \in T \Leftrightarrow \mathfrak{N} \models \varphi(\overline{\ulcorner \sigma \urcorner})$. $\ulcorner \sigma \urcorner$ is the Gödel number of a sentence $\sigma$. 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 $\vdash \sigma \leftrightarrow \sigma \wedge \sigma \wedge \cdots \wedge \sigma$. □

- $T'$ may not be $\Sigma_0$ since it includes the Gödel numbers, etc.

## Theorem 3.51

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 $\mathrm{MP}$ 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 whether (the Gödel number of) a finite sequence of formulas is a proof of $T$.
- A sentence $\sigma$ is a theorem of $T$ iff there exists a proof (i.e., a sequence that satisfies the primitive recursive relation) such that $\sigma$ is the last formula of the proof. Thus, the set of theorems of $T$ is CE. □

Gödel's first incompleteness theorem easily follows from The halting problem $\mathrm{K}$.

**Theorem 3.52 (Gödel's first incompleteness theorem)**

Let $T$ be a $\Sigma_1$-complete and 1-consistent CE theory. Then $T$ is incomplete, that is, there is a sentence that cannot be proved or disproved.

**Proof.**

- Suppose $\mathrm{K}$ 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, which contradicts with the 1-consistency assumption.
  - In the latter case, $T$ is incomplete because $\varphi(\overline{d})$ cannot be proved or disproved.

## Exercise

(1) In a $\Sigma_1$ complete theory $T$, show that $\Sigma_1$-soundness of $T$ is equivalent to the following: for any $\Sigma_0$ 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 $\Sigma_1$-complete. Show that there exists a $\Sigma_1$ 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.21.) In particular, $\{\ulcorner\sigma\urcorner : T \vdash \sigma\}$ is not computable.

From now, we will reconsider the proof of the first incompleteness theorem more rigorously in $\mathsf{I}\Sigma_1$, which leads us to the second incompleteness theorem.

To begin with, we remark that $\mathsf{I}\Sigma_1$ actually enables the use of induction for the boolean combinations of $\Sigma_1$ formulas. For instance, to use induction for $\neg\varphi(x)$, one may use induction for $\varphi(a - x)$ with any constant $a$.

## Lemma 3.53 (Formal representation for primitive recursive functions)

For any p.r. function, there is a $\Delta_1$ formula $\varphi(x, y)$ which expresses its graph, and in $\mathsf{I}\Sigma_1$, it is provable that $\forall x \exists! y \varphi(x, y)$, where $\exists!$ means "unique existence".

**Proof.** By Lemma 3.46, the graph of a primitive recursive (p.r.) function $f$ is expressed as a $\Delta_1$ formula $\varphi(x, y)$. Then, $\forall x \exists! y \varphi(x, y)$ is rewritten as

$$\forall x \exists y \varphi(x, y) \ \wedge \ \forall x \forall y \forall z (\varphi(x, y) \wedge \varphi(x, z) \to y = z),$$

which can be shown by $\mathsf{I}\Sigma_1$, and by induction on the construction of $\varphi(x, y)$. □

From the above lemma, we can see that $\mathrm{I}\Sigma_1$ is a conservative extension even if we add the symbols of the p.r. function and its definable formulas.

In other words, (in $\mathrm{I}\Sigma_1$) a $\Sigma_1$ formula containing p.r. functions is rewritten as an equivalent $\Sigma_1$ formula without p.r. functions by replacing the functions with the corresponding $\Delta_1$ formulas. Similarly for a $\Delta_1$ formula.

## Lemma 3.54 (Diagonalization lemma)

Let $T$ be any extension of $\mathrm{I}\Sigma_1$. For any formula $\psi(x)$ in which $x$ is the only free variable, there exists a sentence $\sigma$ such that $T \vdash$ "$\sigma \leftrightarrow \psi(\overline{\ulcorner \sigma \urcorner})$" .

**Proof.**

- We first enumerate (primitively recursively) the formulas with only $x$ as a free variable as $\varphi_0(x), \varphi_1(x), \ldots$. Then define $f(n) = \ulcorner \varphi_n(\overline{n}) \urcorner$, which is also a p.r. function.
- By Lemma 3.53, there exists a $\Delta_1$ formula $\chi$ such that

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

**Proof (continued).**

- Now given a formula $\psi(x)$, consider a formula $\exists y(\chi(x,y) \wedge \psi(y))$. Since it only has a free variable $x$, it is $\varphi_k(x)$ for some $k$.
- Let $\sigma \equiv \varphi_k(\overline{k})$ for this $k$. Then, $f(k) = \ulcorner\sigma\urcorner$, so $T \vdash \chi(\overline{k}, \overline{\ulcorner\sigma\urcorner})$.
- 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 $T \vdash \forall x \exists ! y \chi(x,y)$, in $T$,

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

- Therefore, $\sigma$ is the fixed point of $\psi$ ($T \vdash \sigma \leftrightarrow \psi(\overline{\ulcorner\sigma\urcorner})$). $\square$

In theorem 3.51, we show that the set of theorems of a CE theory is also CE . We here consider a formal version of this statement.

## Definition 3.55

Let $T$ be a CE theory. Based on Craig's lemma, let $T'$ be its p.r. counterpart. Then, "a sequence of formulas $P$ is a proof in $T'$" can be defined in a p.r. way. Thus, we define a p.r. relation $\mathrm{Proof}_T$ as follows.

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

By $\mathrm{Proof}_T$, we also denote a $\Delta_1$ formula expressing the above $\mathrm{Proof}_T$ in $\mathsf{I}\Sigma_1$.

A $\Sigma_1$ formula $\mathrm{Bew}_T$ 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).

# Alternative proof of the first incompleteness

We give another proof for the first incompleteness theorem (with the additional assumption that a theory $T$ includes $\mathsf{I}\Sigma_1$).

**Proof.**

- By the diagonalization lemma, $\neg\mathrm{Bew}_T(x)$ has a fixed point, that is, there exists $\sigma$ such that $T \vdash \sigma \leftrightarrow \neg\mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$.
- We will show this $\sigma$ is neither provable nor disprovable in $T$ as follows.
- Let $T \vdash \sigma$. Then $\mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$ is true. Hence $T \vdash \mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$ from $\Sigma_1$ completeness. Since $\sigma$ is the fixed point of $\neg\mathrm{Bew}_T(x)$, we have $T \vdash \neg\sigma$, which means that $T$ is inconsistent.
- On the other hand, if $T \vdash \neg\sigma$, $T \vdash \mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$ because $\sigma$ is a fixed point. Here, using the 1-consistency of $T$, $\mathrm{Bew}_T(\overline{\ulcorner\sigma\urcorner})$ is true, and so $T \vdash \sigma$, which is a contradiction. □

The sentence $\sigma$ thus constructed "asserts its own unprovability" because "$\sigma \Leftrightarrow T \nvdash \sigma$" holds. This $\sigma$ is called the **Gödel sentence** of $T$.

# Summary

**Theorem 4.1 (Gödel's first incompleteness theorem)**

Any 1-consistent CE extension of $\mathsf{I}\Sigma_1$ is incomplete.

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.

# Thank you for your attention!