

Mathematical Logic (XI)

Yijia Chen

1. Theories and Decidability

Definition 1.1. A set $T \subseteq L_0^S$ of L-sentences is a *theory* if

- T is satisfiable,
- and T is closed under consequences, i.e., for every $\varphi \in L_0^S$, if $T \vdash \varphi$, then $\varphi \in T$. +

Example 1.2. Let \mathfrak{A} be an S-structure. Then

$$\text{Th}(\mathfrak{A}) := \{\varphi \in L_0^S \mid \mathfrak{A} \models \varphi\}$$

is a theory. +

Definition 1.3. Let $\mathfrak{N} := (\mathbb{N}, +, \cdot, 0, 1)$. Then $\text{Th}(\mathfrak{N})$ is called (*elementary arithmetic*). +

Definition 1.4. Let $T \subseteq L_0^S$. We define

$$T^{\models} := \{\varphi \in L_0^S \mid T \models \varphi\}. \quad +$$

Lemma 1.5. *All the following are equivalent.*

- T^{\models} is a theory.
- T is satisfiable.
- $T^{\models} \neq L_0^S$. +

Definition 1.6. The *Peano Arithmetic* Φ_{PA} consists of the following S_{ar} -sentences, where $S_{\text{ar}} = \{+, \cdot, 0, 1\}$:

$$\begin{array}{ll} \forall x \neg x + 1 \equiv 0, & \forall x \forall y (x + 1 \equiv y + 1 \rightarrow x \equiv y), \\ \forall x x + 0 \equiv x, & \forall x \forall y x + (y + 1) \equiv (x + y) + 1, \\ \forall x x \cdot 0 \equiv 0, & \forall x \forall y x \cdot (y + 1) \equiv x \cdot y + x, \end{array}$$

and for all $n \in \mathbb{N}$, all variables x_1, \dots, x_n, y , and all $\varphi \in L^{S_{\text{ar}}}$ with

$$\text{free}(\varphi) \subseteq \{x_1, \dots, x_n, y\}$$

the sentence

$$\forall x_1 \dots \forall x_n \left(\left(\varphi \frac{0}{y} \wedge \forall y \left(\varphi \rightarrow \varphi \frac{y+1}{y} \right) \right) \rightarrow \forall y \varphi \right). \quad +$$

Remark 1.7. It is easy to see that $\mathfrak{N} \models \Phi_{\text{PA}}$, i.e., $\Phi_{\text{PA}}^{\models} \subseteq \text{Th}(\mathfrak{N})$. We will show that $\Phi_{\text{PA}}^{\models} \subsetneq \text{Th}(\mathfrak{N})$. +

Definition 1.8. Let $T \subseteq L_0^S$ be a theory.

(i) T is *R-axiomatizable* if there exists an R-decidable $\Phi \subseteq L_0^S$ with $T = \Phi^{\models}$.

(ii) T is *finitely axiomatizable* if there exists a finite $\Phi \subseteq L_0^S$ with $T = \Phi^{\models}$.

Clearly any finitely axiomatizable T is R-axiomatizable. ⊣

Theorem 1.9. *Every R-axiomatizable theory is R-enumerable.*

Proof: Let $T = \Phi^{\models}$ where $\Phi \subseteq L_0^S$ is R-decidable. We can effectively generate all derivable sequent proofs and check for each proof whether all the used assumptions belong to Φ (by the R-decidability of Φ). □

Remark 1.10. There are R-axiomatizable theories that are not R-decidable, e.g., for $S = S_\infty$ and $\Phi = \emptyset$

$$\Phi^{\models} = \{\varphi \in L^{S_\infty} \mid \models \varphi\}. \quad \dashv$$

Definition 1.11. A theory $T \subseteq L_0^S$ is *complete* if for any $\varphi \in L_0^S$, either $\varphi \in T$ or $\neg\varphi \in T$. ⊣

Remark 1.12. Let \mathfrak{A} be an S -structure. Then the theory $\text{Th}(\mathfrak{A})$ is complete. ⊣

Theorem 1.13. (i) *Every R-axiomatizable complete theory is R-decidable.*

(ii) *Every R-enumerable complete theory is R-decidable.* ⊣

2. The Undecidability of Arithmetic

Theorem 2.1. $\text{Th}(\mathfrak{N})$ is not R-decidable.

Again, for the alphabet $\mathcal{A} = \{\}\}$ we consider the halting problem

$$\Pi_{\text{halt}} := \{\mathcal{W}_{\mathbb{P}} \mid \mathbb{P} \text{ a program over } \mathcal{A} \text{ and } \mathbb{P} : \square \rightarrow \text{halt}\}.$$

For any program \mathbb{P} over \mathcal{A} we will construct effectively an S_{ar} -sentence $\varphi_{\mathbb{P}}$ (i.e., $\varphi_{\mathbb{P}}$ can be computed by a register machine) such that

$$\mathfrak{N} \models \varphi_{\mathbb{P}} \iff \mathbb{P} : \square \rightarrow \text{halt}.$$

Assume that \mathbb{P} consists of instructions $\alpha_0, \dots, \alpha_k$. Let n be the maximum index i such that R_i is used by \mathbb{P} . Recall that a configuration of \mathbb{P} is an $(n+2)$ -tuple

$$(L, m_0, \dots, m_n),$$

where $L \leq k$ and $m_0, \dots, m_n \in \mathbb{N}$, meaning that α_L is the instruction to be executed next and every register R_i contains m_i , i.e., the word $\underbrace{|\dots|}_{m_i \text{ times}}$.

Lemma 2.2. *For every program \mathbb{P} over \mathcal{A} we can compute an S_{ar} -formula*

$$\chi_{\mathbb{P}}(x_0, \dots, x_n, z, y_0, \dots, y_n)$$

such that for all $\ell_0, \dots, \ell_n, L, m_0, \dots, m_n \in \mathbb{N}$

$$\mathfrak{N} \models \chi_{\mathbb{P}}[\ell_0, \dots, \ell_n, L, m_0, \dots, m_n]$$

if and only if \mathbb{P} , beginning with the configuration $(0, \ell_0, \dots, \ell_n)$, after finitely many steps, reaches the configuration (L, m_0, \dots, m_n) . ⊣

Using the formula $\chi_{\mathbb{P}}$ in Lemma 2.2, we define

$$\varphi_{\mathbb{P}} := \exists y_0 \cdots \exists y_n \exists \chi_{\mathbb{P}}(0, \dots, 0, \bar{k}, y_0, \dots, y_n),$$

where $\bar{k} := \underbrace{1 + \cdots + 1}_{k \text{ times}}$. Then By Lemma 2.2, we conclude $\mathfrak{N} \models \varphi_{\mathbb{P}}$ if and only if \mathbb{P} , beginning with the initial configuration $(0, 0, \dots, 0)$, after finitely many steps, reaches the configuration (k, m_0, \dots, m_n) , i.e., $\mathbb{P} : \square \rightarrow \text{halt}$. This finishes our proof of Theorem 2.1. \square

By Theorem 2.1, Theorem 1.13, and Remark 1.12:

Corollary 2.3. *Th(\mathfrak{N}) is neither R-axiomatizable nor R-enumerable. Thus*

$$\Phi_{\text{PA}}^{\text{f}} \subsetneq \text{Th}(\mathfrak{N}). \quad \dashv$$

Proof of Lemma 2.2. Recall that $\chi_{\mathbb{P}}$ expresses in \mathfrak{N} that there is an $s \in \mathbb{N}$ and a sequence of configurations C_0, \dots, C_s such that

- $C_0 = (0, x_0, \dots, x_n)$,
- $C_s = (z, y_0, \dots, y_n)$,
- for all $i < s$ we have $C_i \xrightarrow{\mathbb{P}} C_{i+1}$, i.e., from the configuration C_i the program \mathbb{P} will reach C_{i+1} in one step.

We slightly rewrite the above formulation as that there is an $s \in \mathbb{N}$ and a sequence of natural numbers

$$\underbrace{a_0, \dots, a_{n+1}}_{C_0} \underbrace{a_{n+2}, \dots, a_{(n+2)+(n+1)}}_{C_1} \cdots \underbrace{a_{s \cdot (n+2)}, \dots, a_{s \cdot (n+2)+(n+1)}}_{C_s} \quad (1)$$

such that

- $a_0 = 0, a_1 = x_0, \dots, a_{n+1} = x_n$,
- $a_{s \cdot (n+2)} = z, a_{s \cdot (n+2)+1} = y_0, \dots, a_{s \cdot (n+2)+(n+1)} = y_n$,
- for all $i < s$ we have

$$\left(a_{i \cdot (n+2)}, \dots, a_{i \cdot (n+2)+(n+1)} \right) \xrightarrow{\mathbb{P}} \left(a_{(i+1) \cdot (n+2)}, \dots, a_{(i+1) \cdot (n+2)+(n+1)} \right).$$

Observe that the length of the sequence (1) is unbounded, so we cannot quantify it directly in \mathfrak{N} . So we need the following beautiful (elementary) number-theoretic tool.

Lemma 2.4 (Gödel's β -function). *There is a function $\beta : \mathbb{N}^3 \rightarrow \mathbb{N}$ with the following properties.*

(i) For every $r \in \mathbb{N}$ and every sequence (a_0, \dots, a_r) in \mathbb{N} there exist $t, p \in \mathbb{N}$ such that for all $i \leq r$

$$\beta(t, p, i) = a_i.$$

(ii) β is definable in L^{Sar} . That is, there is an S_{ar} -formula $\varphi_{\beta}(x, y, z, w)$ such that for all $t, q, i, a \in \mathbb{N}$

$$\mathfrak{N} \models \varphi_{\beta}[t, q, i, a] \iff \beta(t, q, i) = a.$$

Proof: Let (a_0, \dots, a_r) be a sequence over \mathbb{N} . Choose a *prime*

$$p > \max\{a_0, \dots, a_r, r + 1\},$$

and set

$$\begin{aligned} t := 1 \cdot p^0 + a_0 \cdot p^1 + 2 \cdot p^2 + a_1 \cdot p^3 + \dots + (i + 1) \cdot p^{2i} + a_i \cdot p^{2i+1} \\ + \dots + (r + 1) \cdot p^{2r} + a_r \cdot p^{2r+1}. \end{aligned} \quad (2)$$

In other words, the *p-adic representation* of t is precisely

$$a_r(r + 1) \cdots a_i(i + 1) \cdots a_1 2 a_0 1.$$

Claim. Let $i \leq r$ and $a \in \mathbb{N}$. Then $a = a_i$ if and only if there are $b_0, b_1, b_2 \in \mathbb{N}$ such that:

$$(B1) \quad t = b_0 + b_1((i + 1) + a \cdot p + b_2 \cdot p^2),$$

$$(B2) \quad a < p,$$

$$(B3) \quad b_0 < b_1,$$

$$(B4) \quad b_1 = p^{2m} \text{ for some } m \in \mathbb{N}.$$

Proof of the claim. Assume $a = a_i$. We set

$$\begin{aligned} b_0 &:= 1 \cdot p^0 + a_0 \cdot p^1 + 2 \cdot p^2 + a_1 \cdot p^3 + \dots + i \cdot p^{2i-2} + a_{i-1} \cdot p^{2i-1} \\ b_1 &:= p^{2i} \\ b_2 &:= (i + 2) + a_{i+1} \cdot p + \dots + a_r \cdot p^{2(r-i)-1}. \end{aligned}$$

By (2) it is routine to verify that all (B1)–(B4) hold.

Conversely,

$$\begin{aligned} t &= (1 \cdot p^0 + a_0 \cdot p^1 + 2 \cdot p^2 + a_1 \cdot p^3 + \dots + i \cdot p^{2i-2} + a_{i-1} \cdot p^{2i-1}) \\ &\quad + (i + 1) \cdot p^{2i} + a \cdot p^{2i+1} \\ &\quad + ((i + 2) + a_{i+1} \cdot p + \dots + a_r \cdot p^{2(r-i)-1}) \cdot p^{2i+2} \\ &= b_0 + (i + 1) \cdot p^{2m} + a \cdot p^{2m+1} + b_2 \cdot p^{2m+2}. \end{aligned}$$

It is well known that the *p-adic representation* of any number is unique. Together with $b_0 < p^{2m}$, we conclude $a = a_i$. –

Since p is chosen to be a prime, it is easy to verify that (B4) is equivalent to

$$(B4') \quad b_1 \text{ is a square, and for any } d > 1 \text{ if } d \mid b_1, \text{ then } p \mid d.$$

Finally for every $t, q, i \in \mathbb{N}$ we define $\beta(t, q, i)$ to be *smallest* $a \in \mathbb{N}$ such that there are $b_0, b_1, b_2 \in \mathbb{N}$ such that

- $t = b_0 + b_1((i + 1) + a \cdot q + b_2 \cdot p^2),$
- $a < q,$
- $b_0 < b_1,$
- b_1 is a square, and for any $d > 1$ if $d \mid b_1$, then $q \mid d.$

If no such a exists, then we let $\beta(t, q, i) := 0$.

By the above argument, (i) holds by choosing q to be a sufficiently large prime. To show (ii) we define

$$\varphi_\beta(x, y, z, w) := \left(\psi(x, y, z, w) \wedge \forall w' (\psi(x, y, z, w') \rightarrow (w' \equiv w \vee w < w'^1)) \right) \\ \vee \left(\neg \psi(x, y, z, w) \wedge w \equiv 0 \right).$$

Here $\psi(x, y, z, w)$ expresses the properties (B1), (B2), (B3), and (B4'):

$$\psi(x, y, z, w) := \exists u_0 \exists u_1 \exists u_2 \left(x \equiv u_0 + u_1 \cdot ((z + 1) + w \cdot y + u_2 \cdot y \cdot y) \right. \\ \wedge w < y \wedge u_0 < u_1 \\ \left. \wedge \exists v u_1 \equiv v \cdot v \wedge \forall v (\exists v' u_1 \equiv v \cdot v' \rightarrow (v \equiv 1 \vee \exists v' v \equiv y \cdot v')) \right).$$

□

3. Exercises

Exercise 3.1. Prove that

$$\Phi_{\text{PA}} \models \forall x \forall y \ x + y \equiv y + x. \quad \dashv$$

Exercise 3.2. Let T be an R -enumerable theory. Show that T is R -axiomatizable. \dashv

Exercise 3.3. Construct an S_{ar} -formula $\varphi_{\text{exp}}(x, y, z)$ such that for every $a, b, c \in \mathbb{N}$

$$c = a^b \iff \mathfrak{N} \models \varphi_{\text{exp}}[a, b, c]. \quad \dashv$$

¹ $w < w'$ stands for the formula $\exists v (\neg v \equiv 0 \wedge w + v \equiv w')$.