Mathematical Logic (XII)

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 $T \models \varphi$, then $\varphi \in T$. $\dashv$

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

$$\mathrm{Th}(\mathfrak{A}) := \left\{\varphi \in L_0^S \;\middle|\; \mathfrak{A} \models \varphi\right\}$$

is a theory. $\dashv$

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

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

$$T^{\models} := \left\{\varphi \in L_0^S \;\middle|\; T \models \varphi\right\}. \qquad \dashv$$

Lemma 1.5. *All the following are equivalent.*

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

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

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

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

$$\mathrm{free}(\varphi) \subseteq \{x_1, \ldots, x_n, y\}$$

the sentence

$$\forall x_1 \cdots \forall x_n \left(\left(\varphi \frac{0}{y} \wedge \forall y \left(\varphi \to \varphi \frac{y+1}{y}\right)\right) \to \forall y \varphi\right). \qquad \dashv$$

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

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 $\mathsf{T} = \Phi^{\models}$.

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

Clearly any finitely axiomatizable T is R-axiomatizable. ⊣

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

Proof: Let $\mathsf{T} = \Phi^{\models}$ 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 $\Phi = \emptyset$

$$\Phi^{\models} = \left\{\varphi \in L^{S_\infty} \;\middle|\; \models \varphi\right\}. \qquad ⊣$$

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

Remark 1.12. Let $\mathfrak{A}$ be an S-structure. Then the theory $\mathrm{Th}(\mathfrak{A})$ 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. $\mathrm{Th}(\mathfrak{N})$ *is not R-decidable.*

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

$$\Pi_{\text{halt}} := \left\{w_{\mathbb{P}} \;\middle|\; \mathbb{P} \text{ a program over } \mathcal{A} \text{ and } \mathbb{P} : \square \to \text{halt}\right\}.$$

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

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

Assume that $\mathbb{P}$ consists of instructions $\alpha_0, \ldots, \alpha_k$. 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

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

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

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

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

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

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

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

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

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

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 $(0, 0, \ldots, 0)$, after finitely many steps, reaches the configuration $(k, m_0, \ldots, m_n)$, i.e., $\mathbb{P} : \square \to$ halt. This finishes our proof of Theorem 2.1. $\square$

By Theorem 2.1, Theorem 1.13, and Remark 1.12:

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

$$\Phi_{\mathrm{PA}}^{\models} \subsetneq \mathrm{Th}(\mathfrak{N}). \qquad \dashv$$

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 $C_0, \ldots, C_s$ such that

- $C_0 = (0, x_0, \ldots, x_n)$,
- $C_s = (z, y_0, \ldots, y_n)$,
- 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

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

such that

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

$$\Big(a_{i\cdot(n+2)}, \ldots, a_{i\cdot(n+2)+(n+1)}\Big) \xrightarrow{\mathbb{P}} \Big(a_{(i+1)\cdot(n+2)}, \ldots, a_{(i+1)\cdot(n+2)+(n+1)}\Big).$$

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* $\beta : \mathbb{N}^3 \to \mathbb{N}$ *with the following properties.*

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

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

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

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

Equipped with the above β function and the formula φ_β, we define the desired $\chi_{\mathbb{P}}$ as follows.

$$\begin{aligned}\exists t \exists p \exists s \Big(& \varphi_\beta(t,p,0,0) \wedge \varphi_\beta(t,p,1,x_0) \wedge \cdots \wedge \varphi_\beta(t,p,\overline{n+1},x_n) \\ & \wedge \varphi_\beta(t,p,s\cdot\overline{n+2},z) \wedge \varphi_\beta(t,p,s\cdot\overline{n+2}+1,y_0) \\ & \qquad \wedge \cdots \wedge \varphi_\beta(t,p,s\cdot\overline{n+2}+\overline{n+1},y_n) \\ & \wedge \forall i \Big(i < s \to \forall u \forall u_0 \cdots \forall u_n \forall u' \forall u'_0 \cdots \forall u'_n \\ & \qquad (\varphi_\beta(t,p,i\cdot\overline{n+2},u) \wedge \varphi_\beta(t,p,i\cdot\overline{n+2}+1,u_0) \\ & \qquad\quad \wedge \cdots \wedge \varphi_\beta(t,p,i\cdot\overline{n+2}+\overline{n+1},u_n) \\ & \qquad \wedge \varphi_\beta(t,p,(i+1)\cdot\overline{n+2},u') \wedge \varphi_\beta(t,p,(i+1)\cdot\overline{n+2}+1,u'_0) \\ & \qquad\quad \wedge \cdots \wedge \varphi_\beta(t,p,(i+1)\cdot\overline{n+2}+\overline{n+1},u'_n) \\ & \qquad \to \text{“}(u,u_0,\ldots,u_n) \xrightarrow{\mathbb{P}} (u',u'_0,\ldots,u'_n)\text{”}) \Big) \Big).\end{aligned}$$

Here,

$$\text{“}(u,u_0,\ldots,u_n) \xrightarrow{\mathbb{P}} (u',u'_0,\ldots,u'_n)\text{”}$$

stands for a formula describing one-step computation of $\mathbb{P}$ from configuration $(u,u_0,\ldots,u_n)$ to configuration $(u',u'_0,\ldots,u'_n)$. Such a formula can be defined as a conjunction

$$\psi_0 \wedge \cdots \wedge \psi_{k-1}.$$

Recall that the program $\mathbb{P}$ consists of instructions $\alpha_0,\ldots,\alpha_k$ where the last α_k is the halt instruction. Thus, say α_j is

$$j \ \textbf{LET} \ R_1 = R_1 + |,$$

then we let

$$\psi_j := u \equiv \bar{j} \to \Big(u' \equiv u+1 \wedge u'_0 \equiv u_0 \wedge u'_1 \equiv u_1 + 1 \wedge u'_2 \equiv u_2 \wedge \cdots \wedge u'_n \equiv u_n \Big).$$

The remaining details are left to the reader. □

Proof of Lemma 2.4: Let $(a_0,\ldots,a_r)$ be a sequence over $\mathbb{N}$. Choose a *prime*

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

and set

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

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 $i \leqslant r$ 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) $t = b_0 + b_1\big((i+1) + a\cdot p + b_2 \cdot p^2\big)$,

(B2) $a < p$,

(B3) $b_0 < b_1$,

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

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

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

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

Conversely,

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

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′) b_1 is a square, and for any $d > 1$ if $d \mid b_1$, 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

- $t = b_0 + b_1\big((i+1) + a \cdot q + b_2 \cdot q^2\big)$,
- $a < q$,
- $b_0 < b_1$,
- 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

$$\begin{aligned} \varphi_\beta(x, y, z, w) := &\Big(\psi(x, y, z, w) \wedge \forall w'\big(\psi(x, y, z, w') \to (w' \equiv w \vee w < w'^1)\big)\Big) \\ &\vee \Big(\neg\psi(x, y, z, w) \wedge w \equiv 0\Big). \end{aligned}$$

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

$$\begin{aligned} \psi(x, y, z, w) := \exists u_0 \exists u_1 \exists u_2 \Big(&x \equiv u_0 + u_1 \cdot \big((z+1) + w \cdot y + u_2 \cdot y \cdot y\big) \\ &\wedge w < y \wedge u_0 < u_1 \\ &\wedge \exists v\, u_1 \equiv v \cdot v \wedge \forall v\big(\exists v' u_1 \equiv v \cdot v' \to (v \equiv 1 \vee \exists v' v \equiv y \cdot v')\big)\Big). \end{aligned}$$

□

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