Foundations of Computability Theory (14)

Nan Fang

Institute of Software, Chinese Academy of Sciences

Peking University

2025 Autumn Semester

Language and Terms

Definition 14.1

The *language* $\mathcal{L}_{\text{PA}}$ of Peano arithmetic consists of the following symbols:

1. Variable symbols $x, y, z, \ldots$: they represent natural numbers.
2. Parentheses ( ) and symbols of logical connectors: $\wedge, \vee, \rightarrow, \neg$.
3. Quantifier symbols: $\forall, \exists$.
4. The following symbols of binary functions: $+, \times$.
5. The following symbols of binary relations: $=, <$.
6. Constant symbols $\dot{0}$, $\dot{1}$.

Definition 14.2

The *terms* of predicate calculus for arithmetic are inductively defined as follows.

1. A variable or a constant symbol is a term.
2. If t_1, t_2 are terms, then $(t_1 + t_2)$ and $(t_1 \times t_2)$ are terms.

A term is *closed* if it does not contain any variable and therefore only constants and the operations $+$ and $\times$.

Formulas and Theories

Definition 14.3

The *arithmetic formulas* are defined as follows:

1. For all terms t_1, t_2, $t_1 = t_2$ and $t_1 < t_2$ are formulas. These formulas are called *atomic formulas*.
2. For all formulas F_1, F_2, then $(F_1 \wedge F_2)$, $(F_1 \vee F_2)$, $(F_1 \rightarrow F_2)$ and $\neg F_1$ are formulas.
3. For any formula F, then $\forall x F$ and $\exists x F$ are formulas.

A *closed formula* or a *statement* is a formula in which no variable is free.

For any formula F, let $\#F \in \mathbb{N}$ be a Gödel number (effective code) of F.

Definition 14.4

1. A *theory* T in a language $\mathcal{L}$ is a collection of closed formulas of that language. We also often use the term *axiomatic system* or more simply *system* to denote a theory.
2. A theory T is *consistent* if there is no formula F such that $T \vdash F \wedge \neg F$.
3. A theory T is *complete* if $T \vdash F$ or $T \vdash \neg F$ for any closed formula F in the language of T.

Axioms of Peano arithmetic

The theory of Peano arithmetic, denoted by PA, is the theory in the language $\mathcal{L}_{\mathrm{PA}}$ whose axioms are the following:

1. $\forall x \neg(x + \dot{1} = \dot{0})$: $\dot{0}$ has no predecessor.
2. $\forall x\,(x = \dot{0} \vee \exists y\,(x = y + \dot{1}))$: Any integer other than $\dot{0}$ has a predecessor.
3. $\forall x \forall y\,(x + \dot{1} = y + \dot{1} \to x = y)$: The successor function for integers is injective.
4. $\forall x\,(x + \dot{0} = x)$;
5. $\forall x \forall y\,(x + (y + \dot{1}) = (x + y) + \dot{1})$;
6. $\forall x\,(x \times \dot{0} = \dot{0})$;
7. $\forall x \forall y\,(x \times (y + \dot{1}) = (x \times y) + x)$;
8. $\forall x \forall y\,(x < y \leftrightarrow (\exists z\,(z \neq \dot{0} \wedge x + z = y)))$;
9. For any arithmetic formula $F(x)$: $(F(\dot{0}) \wedge (\forall x\,(F(x) \to F(x + \dot{1})))) \to \forall x F(x)$.

The theory composed of axioms (1) - (8) is called *Robinson arithmetic* and denoted by **Q**.

Hierarchy of Arithmetic Formulas

Definition 14.5

1. A formula of Peano arithmetic is Δ_0 if the quantifications it comprises are all bounded, that is to say of the form $\exists x < t$ and $\forall x < t$, with t a term where the variable x does not appear freely.
2. A formula $F(x_1, \ldots, x_m)$ of Peano arithmetic is Σ_n if

$$F(x_1, \ldots, x_m) \equiv \exists y_1 \forall y_2 \ldots Q y_n \, G(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

   for a Δ_0 formula $G(x_1, \ldots, x_m, y_1, \ldots, y_n)$, where Q is $\exists$ if n is odd, and $\forall$ if n is even.
3. A formula $F(x_1, \ldots, x_m)$ of Peano arithmetic is Π_n if

$$F(x_1, \ldots, x_m) \equiv \forall y_1 \exists y_2 \ldots Q y_n \, G(x_1, \ldots, x_m, y_1, \ldots, y_n)$$

   for a Δ_0 formula $G(x_1, \ldots, x_m, y_1, \ldots, y_n)$, where Q is $\forall$ if n is odd, and $\exists$ if n is even.

Hierarchy of Arithmetic Formulas

Proposition 14.6

Let $F(\bar{a},x)$, $F_1(\bar{a},x)$, $F_2(\bar{a},x)$ be Σ_n (resp. Π_n) formulas. Then, each of the following formulas is provably equivalent (using the axioms of arithmetic) to a Σ_n (resp. Π_n) formula:

- $F_1(\bar{a},x) \wedge F_2(\bar{a},x)$, $F_1(\bar{a},x) \vee F_2(\bar{a},x)$
- $\exists x < b\, F(\bar{a},x)$, $\forall x < b\, F(\bar{a},x)$
- $\exists x\, F(\bar{a},x)$ (resp. $\forall x\, F(\bar{a},x)$)

Proof.

Let $F(\bar{a},x) \equiv \exists y\, G(\bar{a},x,y)$, $F_1(\bar{a},x) \equiv \exists y_1\, G_1(\bar{a},x,y_1)$ and $F_2(\bar{a},x) \equiv \exists y_2\, G_2(\bar{a},x,y_2)$. Then, we have the following equivalences:

$$\begin{aligned}
F_1(\bar{a},x) \wedge F_2(\bar{a},x) &\quad\Leftrightarrow\quad \exists y\, \exists y_1, y_2 < y\, (G_1(\bar{a},x,y_1) \wedge G_2(\bar{a},x,y_2)) \\
F_1(\bar{a},x) \vee F_2(\bar{a},x) &\quad\Leftrightarrow\quad \exists y\, (G_1(\bar{a},x,y) \vee G_2(\bar{a},x,y)) \\
\exists x < b\, F(\bar{a},x) &\quad\Leftrightarrow\quad \exists y\, \exists x < b\, G(\bar{a},x,y) \\
\forall x < b\, F(\bar{a},x) &\quad\Leftrightarrow\quad \exists z\, \forall x < b\, \exists y < z\, G(\bar{a},x,y) \\
\exists x\, F(\bar{a},x) &\quad\Leftrightarrow\quad \exists z\, \exists x < z\, \exists y < z\, G(\bar{a},x,y)
\end{aligned}$$

Now the proposition follows by induction on n. □

Gödel's Representation Theorem

Given a Σ_1 formula of Peano arithmetic $\exists y\, F(x_1,\ldots,x_n,y)$ where F is Δ_0, the set $\{(x_1,\ldots,x_n) \in \mathbb{N} : \exists y\, F(x_1,\ldots,x_n,y)\}$ is computably enumerable: we test the formula F little by little on all $(n+1)$-tuples $x_1,\ldots,x_n,y$ and when we find one for which F is true, we enumerate $(x_1,\ldots,x_n)$. Gödel showed that any computably enumerable set could in fact be represented in this form.

Theorem 14.7 (Gödel)

A set of integers $A \subseteq \mathbb{N}$ is c.e. iff there exists a Σ_1 formula $F(x)$ of $\mathcal{L}_{\mathrm{PA}}$ such that $n \in A$ iff $\mathbb{N} \models F(\dot{n})$.

We will show that any partial computable function $f : \mathbb{N}^k \to \mathbb{N}$ is represented by a Σ_1 formula of arithmetic $F(n_1,\ldots,n_k)$, i.e. ,

$$\{\overline{n} \in \mathbb{N}^k : f(\overline{n})\downarrow\} = \{\overline{n} \in \mathbb{N}^k : \mathbb{N} \models F(\overline{n})\}.$$

As any c.e. set is the domain of a partial computable function, this proves the theorem.

Gödel's β function

We will show Theorem 14.7 based on the model of general recursive functions which coincide with computable functions. The main difficulty lies in the management of the primitive recursion scheme, for which we need to encode lists of integers by arithmetic formulas.

Lemma 14.8 (Gödel's β function)

There exists a function $\beta : \mathbb{N}^3 \to \mathbb{N}$ represented by a Δ_0 formula, such that for all n and any sequence of integers $(a_0, \dots, a_n)$, there exist integers $a, b \in \mathbb{N}$ for which $\beta(a, b, i) = a_i$ for all $i \leq n$.

The following Chinese Remainder Theorem will allow Gödel to code lists of integers of arbitrary size.

Lemma 14.9 (Chinese Remainder Theorem)

Let $(a_0, \dots, a_n)$ be an arbitrary sequence of integers. Let $(p_0, \dots, p_n)$ be a sequence of pairwise prime integers with $p_i \geq a_i$ for $i \leq n$. Then, there exists an integer b such that a_i is the remainder of the Euclidean division of b by p_i, for all i.

Proof of Lemma 14.8

The formula $B(a,b,i,r)$ which represents β is as follows: "r is the remainder of the Euclidean division of b by $a(i+1)+1$". The formula is indeed Δ_0:

$$r < a \times (i+1) + 1 \wedge \exists c < b \; c \times (a \times (i+1) + 1) + r = b.$$

Let $(a_0, \ldots, a_n)$ be a sequence of integers. Let us show the existence of integers a, b such that this formula defines the function $(a,b,i) \mapsto a_i$.
Let m be such that $m > \max\{a_i : i \leq n\}$ and $m > n$. Let $a = m!$ and $p_i = a(i+1)+1$. Let us show that $\{p_i\}_{i \leq n}$ are pairwise prime. Suppose absurdly that a prime number p divides p_i and p_j with $i < j$. So p also divides $p_j - p_i = a(j-i)$. Since p is prime then p divides a or p divides $j-i$. As $a = m!$ with $m > n \geq j > i$ then $j-i$ divides a and therefore in all cases p divides a. So p divides $a(i+1)$. Since p also divides $a(i+1)+1$, then p divides $a(i+1)+1-a(i+1) = 1$ which is a contradiction. So the numbers p_i are mutually prime.

We have $p_i = a(i+1)+1 > m > a_i$ for all i. According to the Chinese Remainder Theorem, there exists an integer b such that for all i, the integer a_i is the remainder of the Euclidean division of b by $a(i+1)+1$. $\square$

General Recursive Functions

Definition 14.10

The class of primitive recursive functions is the least class C of functions closed under the following Schemes (I)–(V).

(I) The successor function $f(x) = (x + 1)$ is in C.

(II) For $m, n \geq 0$, the constant functions $f(x_1, \ldots, x_n) = m$ are in C.

(III) The projection functions $f(x_1, x_2, \ldots, x_n) = x_i$, $1 \leq i \leq n$, are in C.

(IV) (Composition) If $g_1, g_2, \ldots, g_m, h \in C$, then

$$f(\bar{x}) = h(g_1(\bar{x}), \ldots, g_m(\bar{x}))$$

is in C, where $\bar{x} = (x_1, \ldots, x_n)$, $g_1, \ldots, g_m$ are functions of n variables, and h is a function of m variables.

(V) (Primitive Recursion) If $g, h \in C$ and $n \geq 1$, then $f \in C$ where

$$f(0, \bar{x}) = g(\bar{x})$$
$$f(x_1 + 1, \bar{x}) = h(x_1, f(x_1, \bar{x}), \bar{x})$$

where $\bar{x} = (x_2, \ldots, x_n)$, the $n - 1$ variables treated as parameters, assuming g and h are functions of $n - 1$ and $n + 1$ variables, respectively, and f is a function of n variables. (In case $n = 1$, a 0-ary function is a constant function which is in C by Scheme (II).)

Definition 14.11

The class C of general recursive (partial) functions is the least class obtained by closing under Schemes (I)–(V) for the primitive recursive functions and the following Scheme (VI).

(VI) (Unbounded Search) If $\theta(\bar{x}, y) \in C$ is a partial function, and

$$\psi(\bar{x}) = (\mu y)\left[\theta(\bar{x}, y) \downarrow = 0 \quad \& \quad (\forall z < y)\left[\theta(\bar{x}, z) \downarrow \neq 0\right]\right],$$

then ψ is in C. (Here $\psi(\bar{x})$ diverges if there is no such y. Hence, ψ may be nontotal.)

Proof of Gödel's Representation Theorem

We show that any general recursive partial function is represented by a Σ_1 formula of arithmetic.

(I) The successor function $f(x) = x + 1$ is represented by the Δ_0 formula $F(x, r)$:

$$r = x + \dot{1}.$$

(II) The constant function $f(x_1, \ldots, x_n) = m$ is represented by the Δ_0 formula $F(x_1, \ldots, x_n, r)$:

$$r = \underbrace{\dot{1} + \dot{1} + \cdots + \dot{1}}_{m \text{ many}}.$$

(III) The projection function $f(x_1, \ldots, x_n) = x_i$ is represented by the Δ_0 formula $F(x_1, \ldots, x_n, r)$:

$$r = x_i.$$

(IV) (Composition) Let

$$f(\bar{x}) = g(h_1(\bar{x}), \ldots, h_k(\bar{x}))$$

for functions $g, h_1, \ldots, h_k$ represented by formulas $G, H_1, \ldots, H_k$. Then, f is represented by the formula $F(\bar{x}, r)$:

$$\exists y_1, \ldots, y_k \, H_1(\bar{x}, y_1) \wedge \cdots \wedge H_k(\bar{x}, y_k) \wedge G(y_1, \ldots, y_k, r).$$

Proof of Gödel's Representation Theorem

(V) (Primitive Recursion) Let

$$f(\bar{x},0) = g(\bar{x})$$
$$f(\bar{x},n+1) = h(\bar{x},n,f(\bar{x},n))$$

for functions g,h represented by formulas G,H. Let the formula B represent Gödel's β function. Then, f is represented by the following formula $F(\bar{x},n,r)$:

$$\exists a,b\, B(a,b,n,r) \wedge \exists a_0\, (B(a,b,0,a_0) \wedge G(\bar{x},a_0))$$
$$\wedge\, \forall i < n\, \exists a_i, a_{i+1}\, (B(a,b,i,a_i) \wedge B(a,b,i+1,a_{i+1}) \wedge H(\bar{x},i,a_i,a_{i+1})).$$

(VI) (Unbounded Search) Let

$$f(\bar{x}) = (\mu a)[g(\bar{x},a)\downarrow= 0 \quad \& \quad (\forall i < a)\ [g(\bar{x},i)\downarrow\neq 0]]$$

for g represented by a formula G. Then, f is represented by the formula $F(\bar{x},a)$:

$$G(\bar{x},a,0) \wedge \forall i < a\, \exists r \neq 0\, G(\bar{x},i,r).$$

Gödel's first incompleteness theorem

Theorem 14.12 (Gödel's first incompleteness theorem)

$\mathrm{Th}(\mathbb{N})$ *is undecidable, i.e., the set* $\#\mathrm{Th}(\mathbb{N}) := \{\#F : \mathbb{N} \models F\}$ *of all true statements of arithmetic is not computable.*

Proof.

According to Theorem 14.7 there exists a Σ_1 formula $F(x)$ of $\mathcal{L}_{\mathrm{PA}}$ defining the halting set K. For any $n \in \mathbb{N}$, we have

$$\begin{aligned} n \in K \quad &\Leftrightarrow \quad \mathbb{N} \models F(\dot{n}) \\ &\Leftrightarrow \quad F(\dot{n}) \in \mathrm{Th}(\mathbb{N}) \end{aligned}$$

It is straightforward to check that the function $n \mapsto \#F(\dot{n})$ is computable. Thus, if $\mathrm{Th}(\mathbb{N})$ was decidable, then $K = \{n \in \mathbb{N} : \#F(\dot{n}) \in \#\mathrm{Th}(\mathbb{N})\}$ would be computable, which is a contradiction. Therefore, $\mathrm{Th}(\mathbb{N})$ is undecidable. □