Logic and Foundation II

Part 7. Theory of reals and Reverse Mathematics

Kazuyuki Tanaka

BIMSA

April 16, 2024

北京雁栖湖应用数学研究院
Beijing Institute of Mathematical Sciences and Applications

Logic and Foundations II

- Part 5. Models of first-order arithmetic (continued) (5 lectures)
- Part 6. Real-closed ordered fields: completeness and decidability (4 lectures)
- Part 7. Theory of reals and reverse mathematics (9 lectures?)
- Part 8. Second order arithmetic and non-standard methods (6 lectures?)

Part 7. Schedule

- Apr. 16, (1) Introduction and the base system RCA_0
- Apr. 18, (2) Defining real numbers in RCA_0
- Apr. 23, (3) Completeness of the reals and ACA_0
- Apr. 25, (4) Continuous functions and WKL_0
- Apr. 30, (5) Knig's lemma and Ramsey's theorem
- May 9, (6) Determinacy of infinite games I
- May 14, (7) Determinacy of infinite games II
- to be continued

Recap

Reverse Mathematics: Which axioms are needed to prove a theorem?

The Reverse Mathematics Phenomenon

Many theorems of mathematics are either provable in RCA_0, *or logically equivalent (over* RCA_0*) to one of* WKL_0, ACA_0, ATR_0, Π^1_1-CA_0.

Definition 1.2 The system of **recursive comprehension axioms** (RCA_0) consists of:

(0) Axioms and inference rules of first-order logic with axioms of equality for numbers.

(1) Basic arithmetic axioms: Same as $\mathsf{Q}_<$ (Chapter 4).

(2) Δ^0_1 comprehension axiom (Δ^0_1-CA_0): $\forall n(\varphi(n) \leftrightarrow \psi(n)) \to \exists X \forall n(n \in X \leftrightarrow \varphi(n))$, where $\varphi(n)$ is Σ^0_1, $\psi(n)$ is Π^0_1, and neither includes X as a free variable.

(3) Σ^0_1 induction: $\varphi(0) \land \forall n(\varphi(n) \to \varphi(n+1)) \to \forall n \varphi(n)$, for any Σ^0_1 formula $\varphi(n)$.

Basic properties of RCA_0

RCA_0 is a conservative extension of first-order arithmetic $\mathsf{I}\Sigma_1$. (Lemma 1.3)

In RCA_0, the following holds:

- (1) Π^0_1 induction. (2) The class of Σ^0_1 formulas is closed under bounded quantification. (Lemma 1.4)
- The set of total functions is closed under primitive recursion. (Lemma 1.5)
- The set of (partial) functions is closed under minimization μ. (Lemma 1.6) Moreover, if $f : \mathbb{N}^{n+1} \to \mathbb{N}$ is total and $\forall \vec{x} \exists y f(\vec{x}, y) = 0$ is provable, then $\mu y(f(\vec{x}, y) = 0)$ exists as a total function.
- for any Σ^0_1 formula $\varphi(x)$, there exists a finite set X such that $\forall x(x \in X \leftrightarrow \varphi(x))$, or there exists a one-to-one function $f : \mathbb{N} \to \mathbb{N}$ such that $\forall y(\exists x f(x) = y \leftrightarrow \varphi(y))$. (Lemma 1.7)
- (Bounded Σ^0_1-CA) : $\forall x \exists X \forall y(y \in X \leftrightarrow (y < x \land \varphi(y)))$, where $\varphi(y)$ is a Σ^0_1 formula, not containing X as a free variable. (Lemma 1.8)

Natural numbers $\mathbb{N}$

In this lecture, we explore how real number theory is developed in RCA_0.

First, we denote the set of all natural numbers $\{n : n = n\}$ by $\mathbb{N}$.

This is formally defined within the system, and the interpretation of $\mathbb{N}$ relies on a model of RCA_0. In a model (M, S), the interpretation of $\mathbb{N}$ is nothing but its first-order part M.

We will use ω to denote the totality of standard natural numbers.

Arithmetical operations on $\mathbb{N}$ such as $+$ and $\cdot$ are simply taken as the corresponding operations in RCA_0. Then, $(\mathbb{N}, +, \cdot, 0, 1, <)$ represents the standard model of arithmetic in a model of RCA_0 whose first order part is just the standard model of arithmetic.

In the following, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are all formally introduced and so they coincide with their standard counterparts in the real world only if they are interpreted in the special models of RCA_0.

Integers $\mathbb{Z}$

First, the equivalence relation $=_{\mathbb{Z}}$ on $\mathbb{N} \times \mathbb{N}$ is defined by

$$(k, l) =_{\mathbb{Z}} (m, n) \leftrightarrow k + n = l + m.$$

Here, the pair (k, l) intuitively represents the integer $k - l$.

Then, we select a pair with the smallest code from each equivalence class of $=_{\mathbb{Z}}$ to be the representative, called an **integer**. We denote the set of all such representatives by $\mathbb{Z}$.

The operations on $\mathbb{Z}$ are defined as

$$(k, l) + (m, n) =_{\mathbb{Z}} (k + m, l + n),$$

$$(k, l) \cdot (m, n) =_{\mathbb{Z}} (km + ln, kn + lm), \text{ etc.}$$

Note that even if (k, l) and (m, n) belong to $\mathbb{Z}$, $(k + m, l + n)$ may not belong to $\mathbb{Z}$.

Strictly, $+$ on $\mathbb{Z}$ is induced by taking the representatives of equivalent classes as follows:

$$[(k, l)] + [(m, n)] = [(k + m, l + n)].$$

Then, it can be verified that $\mathbb{Z}$ satisfies the basic properties of an integer ring.

Rational numbers $\mathbb{Q}$

Next, the equivalence relation $=_{\mathbb{Q}}$ on $\mathbb{Z} \times (\mathbb{Z} - \{(0,0)\})$ is defined by

$$(k,l) =_{\mathbb{Q}} (m,n) \leftrightarrow kn = lm.$$

Here, the pair (k,l) intuitively means the rational number $\dfrac{k}{l}$.

Then, we select a pair with the smallest code from each equivalence class of $=_{\mathbb{Q}}$ as a **rational number**, and denote the set of all such representatives by $\mathbb{Q}$.

The operations on $\mathbb{Q}$ are defined as

$$(k,l) + (m,n) =_{\mathbb{Q}} (kn + lm, ln),$$

$$(k,l) \cdot (m,n) =_{\mathbb{Q}} (km, ln), \text{ etc.}$$

Thus, $\mathbb{Q}$ satisfies the basic properties of a field of rational numbers.

We will next define a real number as a infinite sequence of rational numbers, that is, a function $\subset \mathbb{N} \times \mathbb{Q} \subset \mathbb{N} \times \mathbb{Z}^2 \subset \mathbb{N} \times \mathbb{N}^4 = \mathbb{N}^5$, coded as a subset of $\mathbb{N}$ after all.

Real numbers $\mathbb{R}$

A sequence of rational numbers $\{q_n\}$ is called a **real number**, $\{q_n\} \in \mathbb{R}$, if it satisfies

$$\forall n \forall i (|q_n - q_{n+i}| \leq 2^{-n}).$$

Note that $\mathbb{Q}$ is a set in second-order arithmetic, whereas $\mathbb{R}$ is a predicate about sets.
The equality $=$ and inequality $<$ on real numbers are defined as

$$\{p_n\} = \{q_n\} \leftrightarrow \forall n (|p_n - q_n| \leq 2^{-n+1}),$$
$$\{p_n\} < \{q_n\} \leftrightarrow \exists n (q_n - p_n > 2^{-n+1}).$$

It is easy to see that for any two reals $\{p_n\}$ and $\{q_n\}$, exactly one of the following holds:

$$\{p_n\} = \{q_n\}, \{p_n\} < \{q_n\} \text{or } \{q_n\} < \{p_n\}.$$

The **sum** of two real numbers $\{p_n\}$ and $\{q_n\}$ is defined as follows:

$$\{p_n\} + \{q_n\} = \{p_{n+1} + q_{n+1}\}.$$

Here, $\{p_{n+1} + q_{n+1}\}$ is a real, since

$$\begin{aligned} |(p_{n+1} + q_{n+1}) - (p_{n+1+i} + q_{n+1+i})| &\leq |p_{n+1} - p_{n+1+i}| + |q_{n+1} - q_{n+1+i}| \\ &\leq 2^{-n-1} + 2^{-n-1} \leq 2^{-n} \end{aligned}$$

Product of real numbers

Next, the **product** of two real numbers $\{p_n\}$ and $\{q_n\}$ is defined as follows:

$$\{p_n\} \cdot \{q_n\} = \{p_{n+m} \cdot q_{n+m}\},$$

where m is the smallest natural number such that $\max(|p_0|, |q_0|) + 1 \leq 2^{m-1}$. Then,

$$\begin{aligned}
&|p_{n+m} \cdot q_{n+m} - p_{n+m+i} \cdot q_{n+m+i}| \\
&\qquad \leq |q_{n+m}| \cdot |p_{n+m} - p_{n+m+i}| + |p_{n+m+i}| \cdot |q_{n+m} - q_{n+m+i}| \\
&\qquad \leq (|q_0| + 1) \cdot 2^{-n-m} + (|p_0| + 1) \cdot 2^{-n-m} \\
&\qquad \leq 2 \cdot (\max(|p_0|, |q_0|) + 1) \cdot 2^{-n-m} \\
&\qquad \leq 2 \cdot 2^{m-1} \cdot 2^{-n-m} = 2^{-n}.
\end{aligned}$$

Thus, $\{p_n\} \cdot \{q_n\}$ is also a real number.

Problem 2

In RCA_0, show the existence of a real $y = 1/x$ for any real $x \neq 0$.

Summary

It is provable in RCA_0 that $(\mathbb{R}, +, \cdot, 0, 1, <, =)$ becomes an **Archimedean ordered field**.

Remark 1. The above relation $=$ is not the equality but an equivalent relation. In ordinary mathematics, the definition of real numbers $\mathbb{R}$ is finished by dividing by the equivalence relation $=$. But in RCA_0, we cannot construct equivalence classes of sets, or choose representatives for them.

Remark 2. There is another way to define reals from rationals by so-called "Dedekind cuts". In this definition, a real r is identified with the unique set $\{q \in \mathbb{Q} : q < r\}$. Arithmetical operations on such reals can be defined easily. However, it is difficult to handle infinite sequences of such reals. In fact, it is not provable in RCA_0 that the element-wise sum of two sequence of such reals exists.

Sequences of real numbers

We define a **sequence of real numbers** as a function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{Q}$ such that:

for each n, letting $f_n(m) = f(n, m)$, $f_n : \mathbb{N} \to \mathbb{Q}$ is a real number.

The sequence of real numbers is denoted by $\{f_n\}$, and for each n, f_n represented as $\{f_{nm}\}$. Furthermore, the **limit** of a sequence of real numbers $\{f_n\}$, denoted $\lim_{n\to\infty} f_n$, is defined as the unique real number a such that

$$\forall \varepsilon > 0 \exists n \forall i (|a - f_{n+i}| < \varepsilon).$$

Under this definition, the next theorem can be proved in RCA_0.

Theorem 2.1 (Nested interval property of $\mathbb{R}$)

The following is provable in RCA_0. Let $\{a_n\}$ and $\{b_n\}$ be two sequences of real numbers such that

$$a_n \leq a_{n+1} \leq b_{n+1} \leq b_n (\text{for all } n), \text{ and } \lim_{n\to\infty} |a_n - b_n| = 0.$$

Then, there exists a real number c such that $c = \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$.

Proof. We reason within RCA_0.
Let $\{a_n\}$ and $\{b_n\}$ be two sequences of real numbers such that

$$a_n \le a_{n+1} \le b_{n+1} \le b_n (\text{for all } n), \text{ and } \lim_{n\to\infty} |a_n - b_n| = 0.$$

Now, suppose $a_n = \{p_{nm}\}$ and $b_n = \{q_{nm}\}$. We set $p'_{nm} = p_{n(m+1)} - 2^{-m-1}$ and $q'_{nm} = q_{n(m+1)} + 2^{-m-1}$. Then $\{p'_{nm}\}$ and $\{q'_{nm}\}$ are also sequences of real numbers. In addition, for any n, $a_n = \{p'_{nm}\}$ and $b_n = \{q'_{nm}\}$, and for any m,

$$p'_{nm} \le a_n \text{ and } b_n \le q'_{nm}$$

.

Since $\lim_{n\to\infty} |a_n - b_n| = 0$, we have

$$\forall \varepsilon > 0 \exists n \forall m \ge n |a_m - b_m| < \varepsilon.$$

A simple calculation shows that

$$\forall \varepsilon > 0 \exists n \forall m \ge n |p'_{mm} - q'_{mm}| < \varepsilon$$

also holds.

We define an increasing sequence $\{p''_k\}$ by primitive recursion as follows: Let $p''_0 = p'_{00}$. For $k > 0$, set $p''_k = p'_{nn}$ with the smallest $n \geq k$ such that $|p'_{nn} - q'_{nn}| < 2^{-k}$ and $p''_{k-1} \leq p'_{nn}$.

Since $p''_k = p'_{nn} \leq p''_{k+i} \leq q'_{nn}$, it is clear that $\{p''_k\}$ becomes a real number.

Moreover, since $\forall k \exists n \forall m \geq n |a_m - p''_m| < 2^{-k}$, we have $\{p''_k\} = \lim_{n\to\infty} a_n$. Similarly, we have $\{p''_k\} = \lim_{n\to\infty} b_n$. So we are done. □

Although the nested completeness property of $\mathbb{R}$ is provable in RCA$_0$, the sequential compactness or completeness of $\mathbb{R}$ is not, which will be discussed in the next lecture. As an application of the above theorem, we prove that $\mathbb{R}$ is uncountable.

Theorem 2.2 (Uncountability of $\mathbb{R}$)

It is provable in RCA$_0$ that for any sequence of real numbers $\{a_n\}$, there exists a real number c such that $\forall n (a_n \neq c)$.

Proof. We reason within RCA_0.
First, let $a_n = \{p_{nm}\}$. Using primitive recursion, we define a sequence of shrinking closed intervals with rational endpoints $\{[q_n, r_n]\}$ as follows:

$$[q_0, r_0] = [0, 1],$$

$$[q_{n+1}, r_{n+1}] = \begin{cases} [\frac{q_n+3r_n}{4}, r_n] & \text{if } p_{n,2n+3} \leq \frac{q_n+r_n}{2}, \\ [q_n, \frac{3q_n+r_n}{4}] & \text{otherwise.} \end{cases}$$

The two sequences $\{q_n\}$ and $\{r_n\}$ clearly satisfy the conditions of Theorem 2.1, and thus there exists a real number c such that $c = \lim_{n\to\infty} q_n = \lim_{n\to\infty} r_n$.

Now, take any n. If $p_{n,2n+3} \leq \frac{q_n+r_n}{2}$, then
$a_n \leq p_{n,2n+3} + 2^{-2n-3} \leq \frac{q_n+r_n}{2} + 2^{-2n-3} < \frac{q_n+r_n}{2} + \frac{2^{-2n}}{4} = \frac{q_n+r_n}{2} + \frac{r_n-q_n}{4} = q_{n+1} \leq c$.

Otherwise, $a_n \geq \frac{q_n+r_n}{2} - 2^{-2n-3} > r_{n+1} \geq c$.

In either case, $a_n \neq c$ is shown. □

We will introduce continuous functions on $\mathbb{R}$ in RCA_0. [1]

Definition 2.3

A set $\Phi \subseteq \mathbb{Q}^4$ that satisfies the following conditions is called the **code** for a continuous function $f : \mathrm{dom}\ f(\subseteq \mathbb{R}) \to \mathbb{R}$.

(1) $(p, q, r, s) \in \Phi \to p < q \wedge r \leq s$,

(2) $(p, q, r, s), (p', q', r', s') \in \Phi, p' < q \wedge p < q' \ \to\ r' \leq s \wedge r \leq s'$.

In (2), $p' < q \wedge p < q'$ is $(p, q) \cap (p', q') \neq \varnothing$, and $r' \leq s \wedge r \leq s'$ is $[r, s] \cap [r', s'] \neq \varnothing$. Intuitively, $(p, q, r, s) \in \Phi$ means $\forall x(p < x < q \to r \leq f(x) \leq s)$.
A real number x belongs to the **domain** of a continuous function f coded by Φ, if

$$\forall n \exists (p, q, r, s) \in \Phi(p < x < q \wedge s - r < 2^{-n}),\ \text{denoted } x \in \mathrm{dom} f.$$

It is provable in RCA_0 that if $x \in \mathrm{dom} f$, there exists a unique real y such that $\forall (p, q, r, s) \in \Phi(p < x < q \to r \leq y \leq s)$. (Exercise: Use the nested interval property of $\mathbb{R}$ to prove this.) We denote this y as $f(x)$.

Problem 3. Show in RCA_0 that $y = 1/x$ is a continuous function on $\mathbb{R} - \{0\}$.

[1] Continuous functions in separable metric spaces will be introduced at the end of Section 3.

Theorem 2.4 (Intermediate Value Theorem)

The following is provable in RCA_0. Given a continuous function f such that its domain includes $[0,1]$ and $f(0) < 0 < f(1)$, there exists an $x \in [0,1]$ such that $f(x) = 0$.

Proof. We reason in RCA_0. We may assume that $f(q) \neq 0$ for all rational numbers $q \in [0,1]$. Otherwise, the theorem already holds. For any rational number $q \in [0,1]$, if $\{p_n\}$ represents the real number $f(q)$, then for sufficiently large n, either $p_n < -2^{-n}$ or $2^{-n} < p_n$ holds, which allows us to determine whether $f(q) < 0$ or $f(q) > 0$. Therefore, we can recursively define a sequence of shrinking closed intervals with rational endpoints $\{[p_n, q_n]\}$ as follows:

$$[p_0, q_0] = [0,1],$$

$$[p_{n+1}, q_{n+1}] = \begin{cases} [\frac{p_n+q_n}{2}, q_n] & \text{if } f(\frac{p_n+q_n}{2}) < 0, \\ [p_n, \frac{p_n+q_n}{2}] & \text{if } f(\frac{p_n+q_n}{2}) > 0. \end{cases}$$

Then, by Theorem 2.1, there exists a real number $x \in [0,1]$ s.t. $x = \lim_{n\to\infty} p_n = \lim_{n\to\infty} q_n$. Finally, it is clear that $f(x) = 0$. □

One conclusion that can be drawn from the Intermediate Value Theorem is that $\mathbb{R}$ forms a real closed ordered field.

However, this does not immediately imply that all theorems of the theory of real closed ordered fields hold in $\mathbb{R}$. Since $\mathbb{R}$ is not a set but a formula in the sense of second-order arithmetic, treatment of quantifiers in $\mathbb{R}$ requires formal methods like quantifier elimination.

As a corollary of the Intermediate Value Theorem, it is provable in RCA_0 that any continuous function $f : [0, 1] \to [0, 1]$ has a fixed point. (Apply the Intermediate Value Theorem to $x - f(x)$.)

However, the empirical fact that this cannot be simply extended to dimensions two or higher is supported by a result in the next section, which claims that Brouwer's Fixed Point Theorem is equivalent to WKL_0.

Problem 4

Consider the following. Given an infinite sequence of continuous functions $\{f_n\}$ such that for each n, $\mathrm{dom} f_n$ includes $[0,1]$, and $f_n(0) < 0 < f_n(1)$. Can you show the existence of a sequence $\{x_n\} \subset [0,1]$ such that $f_n(x_n) = 0$ in RCA_0? (Hint: Use two Σ^0_1 sets that cannot be recursively separated in the minimal model of RCA_0, (ω, Rec), to construct a counterexample. Refer to Lemma 3.6 and Corollary 3.7 in the next section.)

Thank you for your attention!