Logic and Computation

K. Tanaka

Recap

Introducing second-order arithmetic

Summary

Logic and Computation I

Part 3a. Formal Arithmetic

Kazuyuki Tanaka

BIMSA

December 10, 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

- In first-order logic (**FO**), quantifiers $\forall$ and $\exists$ range over the elements of a structure.
- Second-order logic (**SO**) allows quantifiers over relations and functions on the elements. Thus, a **general structure** of SO is a pair of a first-order structure and a second-order domain which satisfies given conditions (comprehension, choice, etc.). The **standard** structure of SO equips with any interpretations of relations and functions (in the naïve sense).
- **Theorem**: The validity of SO in the standard structures is not axiomatizable.
- Monadic second-order logic (**MSO**) uses quantification over the sets of elements. Some MSO theories with standard structures are computable, e.g., S1S $=$ MSO$(\mathbb{N}, S(x))$, S2S $=$ MSO$(2^{<\omega}, x^\frown 0, x^\frown 1)$.
- **Lindström theorem**: FO is the strongest logic that satisfies both the compactness theorem and the downward LS theorem.

Second-order arithmetic

- **Second-order arithmetic** Z_2 is a monadic second-order theory, or a two-sorted first-order theory dealing with natural numbers and sets of natural numbers under the condition of full comprehension.
- An original version of Z_2 was formulated by Hilbert around 1920 as a comprehensive deductive system encompassing real numbers, sequences of real numbers, continuous functions and etc. Then, he proposed so-called **Hilbert's program** aiming at establishing the consistency of Z_2 finitistically. Regretfully, Gödel's second incompleteness theorem blocked its progress.
- However, a considerable breadth of mathematics can be developed within weak subsystems of Z_2, whose consistency can be shown finitistically.
- From the mid-1970's, H. Friedman, S. Simpson, and others started research to investigate which subsystem is needed to prove a popular theorem of mathematics in the framework of second order arithmetic. This research program has evolved into a significant field known as **reverse mathematics**.

Formulas of second-order arithmetic

- The language $\mathcal{L}^2_{\mathrm{OR}}$ of second-order arithmetic is the language of first-order arithmetic $\mathcal{L}_{\mathrm{OR}} = \{+, \cdot, 0, 1, <\}$ plus a symbol $\in$ for the membership relation.
- The **formulas** of second-order arithmetic are constructed from atomic formulas $(t_1 = t_2,\ t_1 < t_2,\ t \in X)$ by propositional connectives such as $\neg$, $\vee$, etc., and quantifiers over arithmetic $\forall x$, $\exists x$, as well as over sets $\forall X$, $\exists X$.
- A formula can be rewritten in the prenex normal form by shifting quantifiers to the head of formula. Moreover, all second-order quantifiers can be placed outside of the scopes of any first-order quantifier. The following transformation is possible even in a very weak theory,

$$\forall x \exists Y \varphi(x, Y) \Leftrightarrow \forall X \exists Y (\exists! x (x \in X) \to \forall x (x \in X \to \varphi(x, Y))).$$

If the axiom of choice is available, the places of quantifiers are exchanged as:

$$\forall x \exists Y \varphi(x, Y) \Leftrightarrow \exists Y' \forall x \varphi(x, Y'_x),$$

where Y' is a set-valued choice function, i.e., $Y'(x) = Y'_x = \{y : (x, y) \in Y'\}$.

Hierarchy of formulas

We inductively define the hierarchy of $\mathcal{L}^2_{\mathrm{OR}}$-formulas, Σ^i_j and Π^i_j $(i = 0, 1,\ j \in \mathbb{N})$.

Definition 4.5

- The **bounded** formulas are constructed from atomic formulas $t_1 = t_2, t_1 < t_2, t \in X$ by propositional connectives and bounded quantifiers $\forall x < t$, $\exists x < t$.
  The class of such formulas is written as Π^0_0 or Σ^0_0.
- For each $j \geq 0$, if $\varphi \in \Sigma^0_j$, then $\forall x_1 \cdots \forall x_k \varphi \in \Pi^0_{j+1}$;
  if $\varphi \in \Pi^0_j$, then $\exists x_1 \cdots \exists x_k \varphi \in \Sigma^0_{j+1}$.
  All formulas in Σ^0_j and Π^0_j are called **arithmetical**.
  The class of arithmetical formulas is also denoted as Π^1_0 or Σ^1_0.
- For each $j \geq 0$, if $\varphi \in \Sigma^1_j$, then $\forall X_1 \cdots \forall X_k \varphi \in \Pi^1_{j+1}$;
  if $\varphi \in \Pi^1_j$ then $\exists X_1 \cdots \exists X_k \varphi \in \Sigma^1_{j+1}$.
  All formulas in Σ^1_j and Π^1_j are called **analytical**.

- Formulas belonging to Σ^i_j or Π^i_j are referred to as Σ^i_j or Π^i_j formulas, resp.
- Σ^0_i (or Π^0_i) formulas without set variables are nothing but Σ_i (or Π_i) formulas of first-order arithmetic.
- A formula that is equivalent to a Σ^i_j (or Π^i_j) formula on a given base system is also called Σ^i_j (or Π^i_j).
- If a Σ^i_j formula is equivalent to a Π^i_j formula, each of them is called a Δ^i_j formula. More formally, if the formulas are equivalent over a base theory T, Δ^i_j is denoted as $(\Delta^i_j)^T$.

Examples:

- "X is an infinite set" is represented by a Π^0_2 formula $\forall x \exists y (x < y \land y \in X)$.
- "A linear order $\preceq$ is a well-ordering", that is, "every non-empty set has the least element", can be represented by the following Π^1_1 formula
  $\forall X(\exists z(z \in X) \to \exists x(x \in X \land \forall y \in X(x \preceq y)))$,
  or rewritten as $\forall X \forall z \exists x(z \notin X \lor (x \in X \land \forall y \in X(x \preceq y)))$.

The system of recursive comprehension axioms (RCA_0) is a weak base system of second-order arithmetic, which serves as foundation for our subsequent observation.

Definition 4.6 (recursive comprehension axioms)

The system of recursive comprehension axioms RCA_0 consists of the following:

(0) Axioms and inference rules of first-order logic with axioms of equality for numbers. Equality between sets $X = Y$ is defined as $\forall n(n \in X \leftrightarrow n \in Y)$.

(1) Basic arithmetic axioms: Same as $Q_<$.

(2) Δ^0_1 comprehension axiom (Δ^0_1-CA):

$$\forall n(\varphi(n) \leftrightarrow \psi(n)) \to \exists X \forall n(n \in X \leftrightarrow \varphi(n)),$$

where $\varphi(n)$ is a Σ^0_1 formula, $\psi(n)$ is a Π^0_1 formula, and neither includes X as a free variable. This axiom ensures the existence of set $X = \{n : \varphi(n)\}$.

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

- Since the Δ^0_1 comprehension axiom asserts the existence of recursive sets (=computable sets) in the standard model $\mathbb{N}$, it is also called the **recursive comprehension axiom**.
- More precisely, since $\psi(x)$ and $\varphi(x)$ in the axiom may include set variables (other than X) as parameters, this axiom indeed asserts that there exists a set that can be computed with the parameters as oracle. But notice that it does not assert the non-existence of a non-recursive set.
- RCA_0 is a conservative extension of first-order arithmetic $\mathsf{I}\Sigma_1$.

Definition 4.7 (**arithmetical comprehension axioms**)

The system of arithmetical comprehension axioms ACA_0 is obtained from RCA_0 by replacing the Δ^0_1 comprehension with the Σ^0_1 comprehension [1].

- ACA_0 is a conservative extension of first-order arithmetic PA.

[1] Σ^1_0 comprehension can be achieved by repeatedly applying the Σ^0_1 comprehension axiom to the parameters.

Lemma 4.8

RCA_0 is a conservative extension of first-order arithmetic $\mathsf{I}\Sigma_1$, that is, any theorem of $\mathsf{I}\Sigma_1$ is provable in RCA_0, and any sentence in $\mathcal{L}_{\mathrm{OR}}$ provable in RCA_0 is already provable in $\mathsf{I}\Sigma_1$.

Proof: It is obvious that any theorem of $\mathsf{I}\Sigma_1$ can be proved in RCA_0, since all axioms of $\mathsf{I}\Sigma_1$ are included in RCA_0.
To prove the converse, consider a sentence σ in $\mathcal{L}_{\mathrm{OR}}$ such that $\mathsf{I}\Sigma_1 \nvdash \sigma$. By the completeness theorem, there exists a model $\mathfrak{M} = (M, +, \cdot, 0, 1, <)$ of $\mathsf{I}\Sigma_1$ where $\mathfrak{M} \models \neg\sigma$. For a Σ_1 formula $\varphi(x, y_1, \ldots, y_k)$, a Π_1 formula $\psi(x, y_1, \ldots, y_k)$ and $b_1, \ldots, b_k \in M$, if $\mathfrak{M} \models \forall x(\varphi(x, b_1, \ldots, b_k) \leftrightarrow \psi(x, b_1, \ldots, b_k))$ holds, then we put

$$A_{\varphi,\psi,b_1,\ldots,b_k} = \{a \in M : \mathfrak{M} \models \varphi(a, b_1, \ldots, b_k)\}.$$

Otherwise, we let $A_{\varphi,\psi,b_1,\ldots,b_k} = \emptyset$. Finally, let S be the set of such Δ_1 definable subsets of M, namely

$$S = \{A_{\varphi,\psi,b_1,\ldots,b_k} : \varphi \in \Sigma_1, \psi \in \Pi_1, \text{ and } b_1, \ldots, b_k \in M\}.$$

To show that $(\mathfrak{M}, S) = (M \cup S, +, \cdot, 0, 1, <, \in)$ forms a model of RCA_0, it suffices to prove that any Σ^0_1 formula with set parameters from S can be rewritten as an equivalent Σ^0_1 formula without set parameters. If so, Σ^0_1 induction of $(\mathfrak{M}, S)$ can be derived from Σ_1 induction of $\mathfrak{M}$. Also, $(\mathfrak{M}, S)$ satisfies Δ^0_1 comprehension, since any set Δ^0_1 (i.e., Σ^0_1 and Π^0_1) definable with set parameters can be Δ^0_1 definable without set parameters, and so already belongs to S.

Now, consider a Σ^0_1 formula $\theta(x, b_1, \ldots, b_k, A_{\varphi_1,\psi_1,\bar{c}}, \ldots, A_{\varphi_l,\psi_l,\bar{c}})$ with $b_i \in M$ and $A_{\varphi_j,\psi_j,\bar{c}} \in S$. In the formula, replace $t \in A_{\varphi_j,\psi_j,\bar{c}}$ with either $\varphi_i(t, \bar{c})$ or $\psi_i(t, \bar{c})$ so that the whole formula keeps in Σ^0_1. Thus, we obtain a Σ^0_1 formula $\theta'(x, b_1, \ldots, b_k, \bar{c})$, which is equivalent to $\theta(x, b_1, \ldots, b_k, A_{\varphi_1,\psi_1,\bar{c}}, \ldots, A_{\varphi_l,\psi_l,\bar{c}})$. The same for Π^0_1 formulas. Thus, $(\mathfrak{M}, S)$ is a model of RCA_0.

Finally, since σ does not contain set variables, its truth value is independent of S, and hence $(\mathfrak{M}, S) \models \neg\sigma$. Therefore, $\mathsf{RCA}_0 + \neg\sigma$ is consistent, which implies $\mathsf{RCA}_0 \nvdash \sigma$. This completes the proof. $\square$

The various properties of $\mathsf{I}\Sigma_1$ also hold true in RCA_0. In particular, the following fact is frequently used.

Lemma 4.9

In RCA_0, the following holds:
(1) Π^0_1 induction.
(2) The class of Σ^0_1 formulas is closed under bounded quantification.

Proof ideas. (1) Let $\varphi(x)$ be a Π^0_1 formula and assume $\varphi(0) \land \forall x(\varphi(x) \to \varphi(x+1))$. By way of contradiction, we assume $\neg\varphi(c)$. Use induction for a Σ^0_1 formula $\neg\varphi(c-x)$. Then, $\neg\varphi(c-0)$ and $\neg\varphi(c-x) \to \neg\varphi(c-(x+1))$ imply $\neg\varphi(0)$, a contradiction.

(2) Suppose $\forall x < u \exists y \varphi(x,y)$ with $\varphi(x,y)$ bounded. Let $\psi(w)$ be a Σ^0_1 formula $\exists v \forall x < w \exists y < v \varphi(x,y) \lor u < w$. By Σ^0_1 induction, we have $\forall w \psi(w)$, in particular, $\exists v \forall x < u \exists y < v \varphi(x,y)$. □

Let X, Y be sets of natural numbers. $X \subseteq Y$ is an abbreviation for $\forall n(n \in X \to n \in Y)$, and $X = Y$ is defined as $X \subseteq Y \land Y \subseteq X$. The equality of terms $t_1 = t_2$ is a Π^0_0 formula, but the equality of sets $X = Y$ is a Π^0_1 formula.

- In RCA_0, we encode the ordered pair of natural numbers (m, n) by $\frac{(m+n)(m+n+1)}{2} + m$.
- The **Cartesian product** $X \times Y$ is the set of all (codes of) pairs of an element of X and an element of Y:

$$n \in X \times Y \leftrightarrow \underbrace{\exists x \leq n \exists y \leq n (x \in X \land y \in Y \land (x, y) = n)}_{\Sigma^0_0}.$$

- A **function** $f : X \to Y$ is a unique set $F \subseteq X \times Y$ such that

  $\forall x \forall y_0 \forall y_1 ((x, y_0) \in F \land (x, y_1) \in F \to y_0 = y_1)$ and $\forall x \in X \exists y \in Y (x, y) \in F$.

  If $(x, y) \in F$, we write $f(x) = y$.
- In RCA_0, we can prove that the total functions are closed by primitive recursion. This is essentially from the poof of Lemma 3.46.
- A function f whose domain is $X = \{i : i < n\}$ is called a **finite sequence** with **length** n. In RCA_0, a finite sequence can be coded by a natural number, and this code (Gödel number) is often identified with the sequence itself.

Computable real numbers

Question 1

Any algebraic calculation of computable reals results in a computable real?
E.g., $1.41421356\cdots \times 3.14159265\cdots =?$

- This is not at all obvious. The difficulty comes from a fact that one can not determine whether a real r is zero or not by looking at the finite digits of r.

Question 2

$\mathbb{R} \models \sigma \Leftrightarrow$ Computable-$\mathbb{R} \models \sigma$ for any sentence σ in the language of fields?

- The above is more formally stated as $\mathsf{RCOF} \vdash \sigma \Leftrightarrow \mathsf{RCA}_0 \vdash (\mathbb{R} \models \sigma)$, where RCOF denotes the theory of real closed ordered fields. Thus, we also have

Question 3

$\mathsf{RCA}_0 \vdash \forall\sigma(\mathsf{RCOF} \vdash \sigma \Leftrightarrow \mathbb{R} \models \sigma)$?

Answering Question 3

- Question 3 was proved by Sakamoto and T., using the following theorem.

Strong Fundamental Theorem of Algebra (s-FTA),

Any monic complex polynomial has a unique factorization into linear terms,
$\mathsf{RCA}_0 \vdash \forall p(x) \in \mathbb{C}[x]\ \exists \overrightarrow{\alpha} \in \mathbb{C}^{<\mathbb{N}}\ p(x) = \prod_i (x - \alpha_i)$.

- Later, s-FTA is reproved by combining two metamathematical methods.

1. Conservation: Simpson-T.-Yamazaki (2002) proved

$$\mathsf{WKL}_0 \vdash \sigma \Rightarrow \mathsf{RCA}_0 \vdash \sigma \ \text{ for } \sigma \equiv \forall X \exists ! Y \varphi(X, Y) \text{ with } \varphi \text{ arithmetical.}$$

2. Non-standard models: s-FTA can be proved by a non-standard model in WKL_0 based on a self-embedding theorem (T. 1997, new proofs by Enayat 2013 and others).

Appendix: Reverse Mathematics Program

Reverse Mathematics

Which axioms are needed to prove a theorem?

Big Five in order of increasing strength: RCA_0, WKL_0, ACA_0, ATR_0, Π^1_1-CA_0

- RCA_0 stands for the Recursive Comprehension Axiom, and it only guarantees the existence of recursive (computable) sets. The subscript 0 indicates a restriction on induction, which will be discussed later.

- $\mathsf{WKL}_0 = \mathsf{RCA}_0 + \overbrace{\text{any infinite binary tree has an infinite path}}^{\text{Weak König Lemma}}$
  $= \mathsf{RCA}_0 + \Sigma^0_1\text{-SP}$

Σ^0_1-SP (Σ^0_1 *separation*):

$$\neg\exists x(\varphi_0(x) \land \varphi_1(x)) \to \exists X \forall x((\varphi_0(x) \to x \in X) \land (\varphi_1(x) \to x \notin X)),$$

where $\varphi_0(x)$ and $\varphi_1(x)$ are Σ^0_1 formulas.

- $\mathsf{ACA}_0 = \mathsf{RCA}_0 + \overbrace{\exists X \forall n \big(n \in X \leftrightarrow \varphi(n)\big) \text{ for all arithmetical } \varphi(n)}^{\text{Arithmetical Comprehension}}$
$= \mathsf{RCA}_0 + \Sigma^0_1\text{-}\mathsf{CA}$

- $\mathsf{ATR}_0 = \mathsf{RCA}_0 + \overbrace{\text{the existence of a transfinite hierarchy produced}}^{\text{Arithmetical Transfinite Recursion}}$ by interating arithemetic comprehension along a given well order

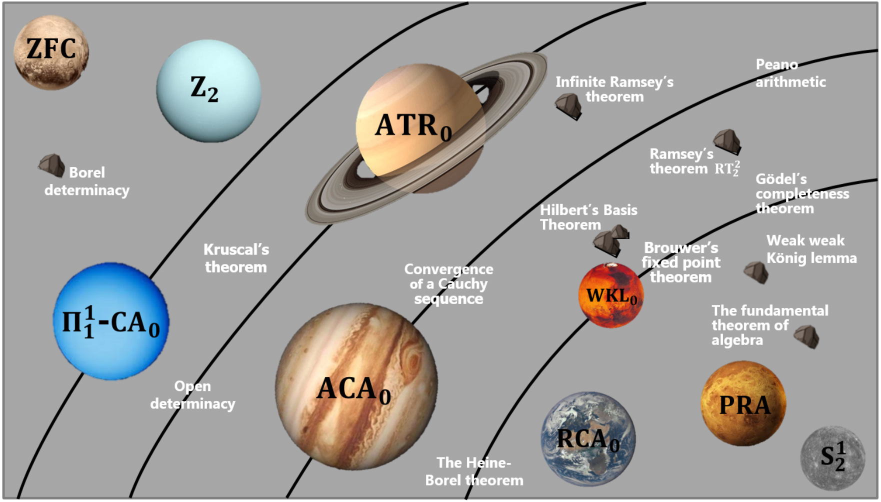
- $\Pi^1_1\text{-}\mathsf{CA}_0 = \mathsf{RCA}_0 + \overbrace{\exists X \forall n \big(n \in X \leftrightarrow \varphi(n)\big) \text{ for all } \Pi^1_1\ \varphi(n)}^{\Pi^1_1 \text{ Comprehension}}$
A formula in the form $\forall X \psi$ with ψ arithmetical is called a Π^1_1 formula.

The Reverse Mathematics Phenomenon

Many theorems of mathematics are either provable in RCA_0*, or logically equivalent* $($*over* $\mathrm{RCA}_0)$ *to one of the other four systems mentioned above.*

$$
\begin{aligned}
\mathrm{RCA}_0 &\Rightarrow \text{the intermediate value theorem} \\
&\Rightarrow \text{fundamental theorem of algebra} \\
\mathrm{WKL}_0 &\leftrightarrow \text{the maximum principle} \quad \leftrightarrow \quad \text{the Cauchy-Peano theorem} \\
&\leftrightarrow \text{Brouwer's fixed point theorem} \\
\mathrm{ACA}_0 &\leftrightarrow \text{the Bolzano-Weierstrass theorem} \quad \leftrightarrow \quad \text{the Ascoli-Arzela lemma} \\
\mathrm{ATR}_0 &\leftrightarrow \text{the Luzin separation theorem} \quad \leftrightarrow \quad \text{Open-determinacy} \\
\Pi^1_1\text{-}\mathrm{CA}_0 &\leftrightarrow \text{the Cantor-Bendixson theorem} \quad \leftrightarrow \quad (\text{Open} \wedge \text{Closed})\text{-determinacy}
\end{aligned}
$$

Planets and Reverse Mathematics



Next semester

Logic and Computation II

- **Part 4. Modal logic**
- **Part 5. Automata on infinite objects**
- **Part 6. Recursion-theoretic hierarchies**
- **Part 7. Admissible ordinals and advanced second order arithmetic**

Note. The theorem numbers in the last two lectures of Part 3a were provisional. Necessary statements will be restated with new numbers in the next semester.

Thank you for your attention!