Logic and Computation I

Part 3a. Formal Arithmetic

Kazuyuki Tanaka

BIMSA

December 5, 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

Second order logic: Introduction

- In **first-order logic** (**FO**), quantifiers $\forall$ and $\exists$ range over the elements of a structure.
- To describe "first-order logic", the Tarski School often uses the term "**elementary**" (e.g., elementary equivalence), in which elementary also means "by means of the elements".

- **Second-order logic** (**SO**) enables us to use quantifiers over relations and functions on the elements.
- Especially, **monadic second-order logic** (**MSO**) uses quantification over the sets of elements. There are many MSO theories which are expressive and yet decidable.

- In the following, we only consider the quantifiers over relations.
- Consider a first-order language $\mathcal{L}$ and an n-ary relation symbol R ($\notin \mathcal{L}$). For a formula $\varphi(\mathrm{R}) \in \mathcal{L} \cup \{\mathrm{R}\}$, by considering R as variable R, we can introduce formulas with second order quantifiers such as $\forall R \varphi(R)$ and $\exists R \varphi(R)$.
- Then, for a structure $\mathcal{A}$ in $\mathcal{L}$, the satisfiability of $\forall R \varphi(R)$ and $\exists R \varphi(R)$ is determined as follows.

Definition 4.1

Consider a first-order language $\mathcal{L}$ and an n-ary relation symbol R ($\notin \mathcal{L}$). For a formula $\varphi(\mathrm{R}) \in \mathcal{L} \cup \{\mathrm{R}\}$, the satisfiability of $\forall R \varphi(R)$ and $\exists R \varphi(R)$ in a structure $\mathcal{A}$ of $\mathcal{L}$ is defined as follows.

$$\mathcal{A} \models \forall R \varphi(R) \Leftrightarrow \text{for any } \dot{\mathrm{R}} \subseteq A^n, (\mathcal{A}, \dot{\mathrm{R}}) \models \varphi(\mathrm{R}) \text{ holds.}$$

$$\mathcal{A} \models \exists R \varphi(R) \Leftrightarrow \text{there exists } \dot{\mathrm{R}} \subseteq A^n \text{ such that } (\mathcal{A}, \dot{\mathrm{R}}) \models \varphi(\mathrm{R}).$$

- In the following, we do not strictly distinguish among the relation variable R, relation $\dot{\mathrm{R}}$, and relation constant (symbol) R.
- The concepts of free and bound variables can be introduced for second-order formulas as those in first-order formulas.
- The problem is how to define the domain of second-order variables.
- In the above interpretation, we use "any $\dot{\mathrm{R}} \subseteq A^n$" to mean that all the subsets of A^n. A structure with such an interpretation is called a **standard structure** of second-order logic.
- However, this interpretation is not rigorous, since it leaves to the meta-standpoint what are all the subsets of A^n are.
- In fact, it is impossible to formalize this interpretation as we will explain soon.

Theorem 4.2 (Gödel)

The validity of (M)SO in terms of standard structures is not axiomatizable (CE), hence not decidable.

Proof.

- Assume MSO were axiomatized. We can define second-order Peano Arithmetic PA_2 by adding arithmetic axioms to MSO. In a model (M, S) of PA_2, any subset of the first-order domain M belongs to the second-order domain $S = \mathcal{P}(M)$.
- Then, let N be the minimum subset of M containing 0 and closed under $+1$. This is isomorphic to $\mathbb{N}$, and exists in the second-order domain S.
- Since induction for $\varphi(x) \equiv x \in \mathbb{N}$ holds in (M, S), $\mathbb{N}$ must agree with the whole M. Thus, M is isomorphic to $\mathbb{N}$.
- Therefore, the unique model for PA_2 is $\mathbb{N} \cup \mathcal{P}(\mathbb{N})$, which implies that there is no sentence independent from PA_2. This condradicts with Gödel's first incompleteness theorem.

□

- L. Henkin introduced a **general structure** of second-order logic, whose second-order part varies similarly to the first-order logic domain. In other words, such a logic can be regarded as two-sorted first-order logic.
- Such a logic captures the same theorems as first-order logic, e.g., the completeness theorem.
- For simplicity, we only consider **monadic second-order logic** (**MSO**), which restricts second-order variables to unary relations, namely subsets of the first-order domain.
- The monadic second-order variables (also called **set variables**) are denoted by $X, Y, Z, \dots,$ and the atomic formula $X(t)$ is also written as $t \in X$.
- We define the general structure of monadic second-order logic as follows.

Definition 4.3

A **general structure** of monadic second-order logic $\mathcal{B} = (\mathcal{A}, \mathcal{S})$ consists of first-order logic structure $\mathcal{A}$ and set $\mathcal{S} \subset \mathcal{P}(A)$. The set quantifiers range over $\mathcal{B}$ as follows.

$$\mathcal{B} \models \forall X \varphi(X) \Leftrightarrow \text{for any } S \in \mathcal{S}, \mathcal{B} \models \varphi(S) \text{ holds,}$$

$$\mathcal{B} \models \exists X \varphi(X) \Leftrightarrow \text{there exists } S \in \mathcal{S} \text{ such that } \mathcal{B} \models \varphi(S).$$

- A general structure can also be viewed as a first-order structure with two domains (A and $\mathcal{S}$) (or split into two domains).
- The formalization is almost the same as first-order logic, just by preparing two kinds of variables. Therefore, fundamental theorems such as the completeness theorem can be proved in a similar way.
- Henkin assumed that the general structure should satisfy certain amounts of comprehension axiom and axiom of choice. **Comprehension axiom** asserts that for a formula $\varphi(x)$ with no free occurrence of X, $\exists X \forall x(x \in X \leftrightarrow \varphi(x))$, i.e., the set $\{x : \varphi(x)\}$ exists in the second-order domain.
  Note that if $\varphi(x)$ contains a second-order quantifier $\forall Y$ (or $\exists Y$), the range of the variable Y already includes the set $\{x : \varphi(x)\}$ to be defined.
  Although such comprehension axiom does not lead to contradiction, we often restrict the use of second-order quantifiers in the principal formula $\varphi(x)$ of the comprehension axiom.
- Similarly, there are various versions of the **axiom of choice**, and it is desirable to assume only what is necessary for the discussion (- Remove unnecessary hypotheses by Occam's razor).

Theorem 4.4 (Completeness theorem of MSO)

An MSO formula is provable from appropriate comprehension and other axioms in two-sorted first-order system if and only if it is true in any general structure that satisfies those axioms.

This theorem can be proved in the same way as in first-order logic.
It can also be generalized to higher-order logics.
In fact, Henkin's proof for the completeness theorem of first-order logic was made with such a generalization scheme.

MSO examples and Lecture 03-04

- We consider a first-order language of finitely many relation symbols and constants.
- The (quantifier) rank of a formula measures the entanglement of quantifiers appearing in it. For example, the rank of $\forall y(\forall x \exists y(x = y) \wedge \forall z(z > 0))$ is 3.
- By $\mathcal{A} \equiv_n \mathcal{B}$, we mean structures $\mathcal{A}, \mathcal{B}$ satisfy the same formulas with rank $\leq n$.
- Given an $\mathcal{A}$ and n, there is the **Scott-Hintikka sentence** $\varphi^n_{\mathcal{A}}$ of rank n such that $\mathcal{B} \models \varphi^n_{\mathcal{A}} \Leftrightarrow \mathcal{B} \equiv_n \mathcal{A}$.
- By $\mathcal{A} \simeq^n \mathcal{B}$, we mean that player II has a winning strategy in $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$, where n is the round of the game.
- **EF theorem** For all $n \geq 0$, $\mathcal{A} \equiv_n \mathcal{B}$ iff $\mathcal{A} \simeq^n \mathcal{B}$.
- **Corollary** $\mathcal{A} \equiv \mathcal{B}$ iff $\mathcal{A} \simeq^n \mathcal{B}$ for all $n \geq 0$.

Example

- First-order logic FO cannot distinguish $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$.

Example 1: MSO is more expressive than FO

In MSO, let π be the following formula (rank 4) which expresses "a bounded set $X (\neq \varnothing)$ has a least upper bound".

$$\forall X(\exists x \in X \wedge \exists y \forall x \in X(x \leq y) \to$$
$$\exists z(\forall x \in X(x \leq z) \wedge \forall y(\forall x \in X(x \leq y) \to z \leq y))).$$

π holds not only for the standard structure of $(\mathbb{R}, <)$, but also for any general structure of $(\mathbb{R}, <)$.

- As for $(\mathbb{Q}, <)$, π holds meaninglessly in special general structures with second-order domains consisting of unbounded sets and finite sets.

π does not hold in structures with second-order domain containing a set with an irrational supremum.

- $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$ are distinguishable by MSO (in the standard structures).

Example 2: MSO is more expressive than FO

• FO can not express the parity (even or odd) of the length of a finite linear order. In fact, a sentence with rank m can not distinguish linear orders with length $\geq 2^m$ (Lecture 03-05).

• MSO can express the parity (even or odd) of the length of a finite linear order. First we put

$$\mathrm{succ}(x, y) \equiv (x < y) \land \forall z(z \leq x \lor y \leq z)$$
$$\mathrm{succ2}(x, y) \equiv \exists z(\mathrm{succ}(x, z) \land \mathrm{succ}(z, y)).$$

In addition, $\mathrm{first}(x) \equiv \neg\exists y\ \mathrm{succ}(y, x)$, and $\mathrm{last}(x) \equiv \neg\exists y\ \mathrm{succ}(x, y)$.
Finally, we define σ as the following formula

$$\exists X(\exists x \in X(\mathrm{first}(x)) \land \exists z \notin X(\mathrm{last}(z)) \land \forall u, v(u \in X \land \mathrm{succ2}(u, v) \to v \in X))$$

which means "there is a set X that does not reach the last by skipping every other points from the start". So it expresses that the length is even (in the standard structure).

Example 3: SO is more expressive than MSO

- The MSO theory of $(\mathbb{N}, x+1, 0)$ is decidable due to Büchi. (We will study this result in the next semester.)
- The SO theory of $(\mathbb{N}, x+1, 0)$ is not, since addition $m+n=k$ is defined by

$$\forall R([R(0,m) \wedge \forall x, y(R(x,y) \to R(x+1, y+1))] \to R(n,k),$$

and multiplication can be defined in a similar way, which means that first-order arithmetic is embedded into the theory.

Exercise

Show that multiplication is definable in a second-order theory of $(\mathbb{N}, x+1, 0)$, and prove that this theory is undecidable.

The relations between arithmetic theories are summarized as follows.

$$\begin{array}{ccccc} \mathsf{FO}(\mathbb{N}, S(x)) \subset & \mathsf{FO}(\mathbb{N}, S(x), +) \subset & \mathsf{FO}(\mathbb{N}, S(x), +, \cdot) \\ & \Cap * & \Cap \\ & \mathsf{MSO}(\mathbb{N}, S(x)) \subset & \mathsf{MSO}(\mathbb{N}, S(x), +) \\ & & \Cap \\ & & \mathsf{SO}(\mathbb{N}, S(x)) \end{array}$$

Here, $S(x)$ denotes $x+1$, and $\mathsf{FO}(\mathbb{N}, S(x))$ is the FO theory of $(\mathbb{N}, S(x))$. Similarly for $\mathsf{MSO}(\mathbb{N}, S(x))$, etc. $A \subset B$ is the usual set inclusion, $A \Cap B$ a relation via a formula translation, $A \Cap^* B$ a formula translation with coding.

S1S $=$ $\mathsf{MSO}(\mathbb{N}, S(x))$ is decidable.
Büchi (1960)'s proof relied on ω-automata with a Büchi condition, which accept an infinite word if a final state appears infinitely many times during reading the input.

Definition 3.32 for Lindström's theorem

- The essence of logic is the relation between sentences and models, "$\mathcal{A} \models_{\mathsf{S}} \varphi$".
- By a **logic**, we mean a set S of sentences together with a function $\mathrm{Mod}_{\mathsf{S}}$ such that for each sentence $\varphi \in \mathsf{S}$, $\mathrm{Mod}_{\mathsf{S}}(\varphi)$ intends to represent $\{\mathcal{A} : \mathcal{A} \models_{\mathsf{S}} \varphi\}$.
- Logic S is said to be **weaker than** logic S′ ($\mathsf{S} \leq \mathsf{S}'$) iff for any $\varphi \in \mathsf{S}$, there exists some $\varphi' \in \mathsf{S}'$ such that $\mathrm{Mod}_{\mathsf{S}}(\varphi) = \mathrm{Mod}_{S'}(\varphi')$. Obviously, $\mathsf{FO} \leq \mathsf{MSO} \leq \mathsf{SO}$.
- We say the (countable) **compactness theorem** holds for logic S iff for any countable $U \subset \mathsf{S}$, if $\bigcap\{\mathrm{Mod}_{\mathsf{S}}(\varphi) : \varphi \in U\} = \varnothing$, then there exists a finite $V \subset U$ such that $\bigcap\{\mathrm{Mod}_{\mathsf{S}}(\varphi) : \varphi \in V\} = \varnothing$.
- We say the (countable) **downward Löwenheim-Skolem theorem** holds for logic S iff for any countable $U \subset \mathsf{S}$, if $\bigcap\{\mathrm{Mod}_{\mathsf{S}}(\varphi) : \varphi \in U\}$ contains an infinite structure $\mathcal{A}$, then it has a countably infinite structure $\mathcal{B}$.
- The compactness theorem and the downward LS theorem hold for FO, but they fail for MSO and SO.
- Surprisingly, Lindström has shown that FO is the strongest logic that satisfies both the compactness theorem and the downward LS theorem.

We consider a language of finitely many relational symbols and constants, without functional symbols.

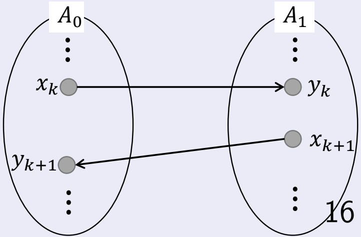
Definition 3.21

Let $\mathcal{A}, \mathcal{B}$ be structures in $\mathcal{L}$. A partial function $f : A \to B$ is a **partial isomorphism** if $\mathcal{A}\restriction\mathrm{dom(f)}$ and $\mathcal{B}\restriction\mathrm{range(f)}$ are isomorphic via f.

Definition 3.22 (Ehrenfeucht-Fraïssé games)

Let $\mathcal{A}_0$, $\mathcal{A}_1$ be structures in $\mathcal{L}$ and n be a natural number. In an n-round **EF game**, $\mathrm{EF}_n(\mathcal{A}_0, \mathcal{A}_1)$, player I (Spoiler) and player II (Duplicator) alternately choose from A_i $(i = 0, 1)$ following the rules described below, and the winner is determined according to the winning condition.

- **Rules**: if I chooses $x_i \in A_j$ $(j = 0, 1)$, II chooses $y_i \in A_{1-j}$.
- **Winning conditions**: If the correspondence $x_i \leftrightarrow y_i$ chosen by the players up to n rounds determines a partial isomorphism of $\mathcal{A}_0$ and $\mathcal{A}_1$, then II wins.



Definition 3.23

$\mathcal{A} \simeq^n \mathcal{B}$ if player II has a winning strategy in $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$.

The (quantifier) rank of a formula measures the entanglement of quantifiers appearing in it.

Definition 3.24

$\mathcal{A} \equiv_n \mathcal{B}$ if $\mathcal{A}, \mathcal{B}$ satisfy the same formulas with rank $\leq n$.

Theorem 3.27 (EF Theorem)

For all $n \geq 0$, $(\mathcal{A}, \vec{a}) \simeq^n (\mathcal{B}, \vec{b}) \Leftrightarrow (\mathcal{A}, \vec{a}) \equiv_n (\mathcal{B}, \vec{b})$.

- **Corollary 3.30** The following are equivalent.

(1) For any n, there exist $\mathcal{A} \in K$ and $\mathcal{B} \notin K$ such that $\mathcal{A} \equiv_n \mathcal{B}$.
(2) K is not an elementary class (K cannot be defined by a first-order formula).

We extend the play of the EF game to infinity (ω-round), denoted as $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$. We write $\mathcal{A} \simeq^\omega \mathcal{B}$ if player II has a winning strategy in $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$.

- **Corollary 3.31** Suppose $\mathcal{A}, \mathcal{B}$ are countable. Then, $\mathcal{A} \simeq^\omega \mathcal{B} \Leftrightarrow \mathcal{A} \simeq \mathcal{B}$.

Theorem 3.33 (Lindström's theorem)

For logic S such that FO $\leq$ S, the following are equivalent.
(1) Compactness theorem and downward LS theorem holds for S.
(2) S $\leq$ FO.

Proof. $(2) \Rightarrow (1)$ is obvious since (2) implies S $=$ FO.
To show $(1) \Rightarrow (2)$, assume S $\leq$ FO does not hold. There exists some $\varphi \in$ S such that $\mathrm{Mod}_{\mathsf{S}}(\varphi)$ is not defined by a first-order sentence. That is, for any $n \in \omega$, there exist $\mathcal{A} \in \mathrm{Mod}_{\mathsf{S}}(\varphi)$ and $\mathcal{B} \in \mathrm{Mod}_{\mathsf{S}}(\neg\varphi)$ such that $\mathcal{A} \equiv_n \mathcal{B}$, or equivalently $\mathcal{A} \simeq^n \mathcal{B}$ by the EF theorem. We express this condition as a logical expression θ_n of S for each n (so that $\theta_{n+1} \to \theta_n$). Namely, $(\mathcal{A}, \mathcal{B}, \sigma) \models_{\mathsf{S}} \theta_n$ means that "$\mathcal{A} \models_{\mathsf{S}} \varphi$ and $\mathcal{B} \models_{\mathsf{S}} \neg\varphi$ and σ is player II's winning strategy in $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$".
Since this holds for all $n \in \omega$, by the compactness theorem, $(\mathcal{A}, \mathcal{B}, \sigma) \models_{\mathsf{S}} \{\theta_n : n \in \omega\}$ holds, and thus σ is a winning strategy in $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$.
Moreover, $(\mathcal{A}, \mathcal{B}, \sigma)$ can be selected countable by downward LS theorem.
Therefore, $\mathcal{A}, \mathcal{B}$ are isomorphic, which contradicts with $\mathcal{A} \in \mathrm{Mod}_{\mathsf{S}}(\varphi)$ and $\mathcal{B} \in \mathrm{Mod}_{\mathsf{S}}(\neg\varphi)$. Thus S $\leq$ FO.

Examples of logic

Infinitary logic $\mathcal{L}_{\omega_1,\omega}$: allowing countable disjunctions and conjunctions, but including only finitely many free variables.

FO(Q_1): adding the quantifier Q_1 to the first-order logic. $Q_1 x\ \varphi(x)$ means "there are uncountably many x that satisfy $\varphi(x)$".

WMSO: Second-order quantifiers range over finite sets only.

Table: The compactness and downward LS property for various logic

Logic	Compactness	Downward LS property
FO	◯	◯
WMSO	×	◯
MSO, SO	×	×
FO(Q_1)	◯	×
$\mathcal{L}_{\omega_1,\omega}$	×	◯

Summary

- Second-order logic allows quantifiers over relations and functions on a domain.
- A general structure $(\mathcal{A}, \mathcal{S})$, where $\mathcal{S} \subset \mathcal{P}(A)$. A standard structure $(\mathcal{A}, \mathcal{P}(A))$.
- Theorem (Gödel): The validity of (M)SO in terms of standard structures is not axiomatizable (CE), hence not decidable.
- MSO has set variables ranging over subsets of the first-order domain.
- Completeness theorem of MSO: An MSO formula is provable from appropriate comprehension and other axioms in two-sorted first-order system if and only if it is true in any general structure that satisfies those axioms.
- Lindström theorem: FO is the strongest logic that satisfies both the compactness theorem and the downward LS theorem.

Further reading

Second-order and Higher-order Logic. From *Stanford Encyclopedia of Philosophy*, `https://plato.stanford.edu/entries/logic-higher-order/`

Thank you for your attention!