Logic and Computation I

Part 3. First order logic and decision problems

Kazuyuki Tanaka

BIMSA

November 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 4. Modal logic**

Part 3. Schedule

- Nov. 5, (1) What is first-order logic?
- Nov. 7, (2) Skolem's theorem
- Nov.12, (3) Gödel's completeness theorem
- Nov.14, (4) Ehrenfeucht-Fraïssé's theorem
- Nov.19, (5) Presburger arithmetic
- Nov.21, (6) Peano arithmetic and Gödel's first incompleteness theorem
- Nov.26, (7) Gödel's second incompleteness theorem

Recap: Computational complexity

- A **decision problem** belongs to **P** (**NP**) or **PSPACE** (**NPSPACE**) if there is a (non-)deterministic TM and a polynomial $p(x)$ s.t. for an input of size n, it returns the correct answer within $p(n)$ steps or $p(n)$ cells of tape, respectively.
- By **Savitch's theorem**, PSPACE $=$ NPSPACE. It is not known that the following inclusions are proper: P $\subseteq$ NP $\subseteq$ PSPACE.
- A problem Q is **NP-hard** (**PSPACE-hard**) if any NP (PSPACE) problem is polynomial-time reducible to Q. An NP-hard NP problem is **NP-complete**. Similarly for **PSPACE**.
- **The Cook-Levin theorem**: SAT is NP-complete. Here, **SAT** is a problem to determine whether a given Boolean formula is satisfiable or not.
- **Theorem**: TQBF is PSPACE-complete. Here, **TQBF** is to determine whether a quantified Boolean formula without free variables is true or not.

Review: Propositional logic

- Propositional logic is the study of logical connections between propositions.
- $\Gamma \models \varphi$ means that φ is a tautological consequence of Γ, i.e., any truth-value function V satisfying all propositions in Γ also satisfies φ.
- $\Gamma \vdash \varphi$ means that φ is a **theorem** in Γ, i.e., Γ is deducible from Γ by means of axioms and rules of propositional logic.
- **Completeness theorem**: $\Gamma \vdash \varphi \quad \Leftrightarrow \quad \Gamma \models \varphi$.
- **Completeness theorem (another version)**: Γ is consistent $\quad \Leftrightarrow \quad$ Γ is satisfiable.
- **Compactness theorem**:
  If any finite subset of Γ is satisfiable, then Γ is also satisfiable.

Part 3. First order logic and decision problems

§3.1. What is first-order logic?

- First order logic is obtained from propositional logic by adding symbols: $\forall, \exists$.
  - a quantifier $\forall x$ expresses "for **a**ny element x (of the underlying set)",
  - a quantifier $\exists x$ expresses "there **e**xists an element x (of the set)".
- Historically, first order logic was tailored by D. Hilbert from Russell's type theory to capture mathematical theories in algebraic-style formulations.
- He describes the satisfiability problem of first-order logic as "**the main problem (Hauptproblem) of mathematical logic** " (1928).
- In this part, we will discuss first-order logic, especially from this point of view.

(2,3,4) Skolem's theorem, Gödel's completeness theorem, Ehrenfeucht-Fraïssé's thm.

(5) Presburger arithmetic: a decidable fragment of first-order arithmetic.

(6,7) Peano arithmetic and Gödel's incompleteness theorems: negative answers to the "main problem".

First order logic

- In order to develop a formal argument, we first specify the symbols involved.

Symbols of first-order logic

- Common logical symbols:
  1. **propositional connectives**: $\neg$ (not), $\land$ (and), $\lor$ (or), $\to$ (implies),
  2. **quantifiers**: $\forall$ (for any $\cdots$), $\exists$ (there exists $\cdots$).
  3. **variables**: x_0, x_1, $\cdots$
  4. **equality**: $=$, and auxiliary symbols such as parentheses $($,$)$.
- Mathematical symbols of a specific theory:
  constants $\mathrm{c}, \cdots$; **function symbols** $\mathrm{f}, \cdots$; **relation symbols** $\mathrm{R}, \cdots$.

- The latter set of symbols is called the **language**[1] $\mathcal{L}$ of the theory. $\mathcal{L}$ may be infinite, though in an ordinary theory, at most five or six symbols are used.

[1] "Langauge" here is different from that in Part 1 and 2 of this course.

- A **structure** in language $\mathcal{L}$ (simply, an $\mathcal{L}$-structure) is defined as a non-empty set A equipped with an interpretation of the symbols in $\mathcal{L}$, denoted as

$$\mathcal{A} = (A, \mathrm{c}^{\mathcal{A}}, \cdots, \mathrm{f}^{\mathcal{A}}, \cdots, \mathrm{R}^{\mathcal{A}}, \cdots).$$

- A is called the **domain** of the structure $\mathcal{A}$. We often denote a structure $\mathcal{A}$ simply by its domain A if it is clear from the context.
- Each function symbol has a predetermined number of arguments, called its **arity**. If the arity of f is n, then $\mathrm{f}^{\mathcal{A}} : A^n \to A$.
- Each relation symbol also has an **arity**. If the arity of R is n, then $\mathrm{R}^{\mathcal{A}} \subseteq A^n$.
- A **constant** could be regarded as a function symbol with no argument (0-ary function), but a constant often plays a special role distinct from a function.

Example 1

- The ordered field of real numbers $\mathcal{R} = (\mathbb{R}, 0, 1, +, \cdot, <)$ is a structure in the language $\mathcal{L}_{\mathrm{OR}} = \{0, 1, +, \cdot, <\}$, where 0 and 1 are constants, $+$ and $\cdot$ are binary function symbols, and $<$ is a binary relation symbol.
- Rigorously, $\mathcal{R}$ should be written as $(\mathbb{R}, 0^{\mathcal{R}}, 1^{\mathcal{R}}, +^{\mathcal{R}}, \cdot^{\mathcal{R}}, <^{\mathcal{R}})$. For instance, $+^{\mathcal{R}}$ is a function corresponding to a function symbol $+$. However, we often omit a superscipt ${}^{\mathcal{R}}$ unless a serious confusion might occur.
- The subscript OR of $\mathcal{L}_{\mathrm{OR}}$ stands for ordered rings, since a typical structure in this language is an ordered ring (e.g., integers). However, a structure in $\mathcal{L}_{\mathrm{OR}}$ is not necessarily an ordered ring. E.g., $(\mathbb{N}, 0, 1, +, \cdot, <)$ is not a ring.

A "term" of a language $\mathcal{L}$ is a symbol string to denote an element of $\mathcal{L}$-structure $\mathcal{A}$.

Definition 3.1 (Terms)

The **terms** of a language $\mathcal{L}$ are defined inductively as follows.

1. variables and constants in $\mathcal{L}$ are terms of $\mathcal{L}$.
2. If $t_0, \cdots, t_{n-1}$ are terms and f is an n-ary function symbol of $\mathcal{L}$, then $\mathrm{f}(t_0, \cdots, t_{n-1})$ is a term of $\mathcal{L}$.

For a term t with no variables, its **value** in a structure $\mathcal{A}$, denoted $t^{\mathcal{A}}$, is defined inductively as follows.

1. the value of constant c in $\mathcal{L}$ is $\mathrm{c}^{\mathcal{A}}$.
2. the value of term $\mathrm{f}(t_0, \cdots, t_{n-1})$ is $\mathrm{f}^{\mathcal{A}}(t_1^{\mathcal{A}}, \cdots, t_{n-1}^{\mathcal{A}})$.

A formula is introduced as a symbol string to describe a property of a structure.

Definition 3.2 (Formulas)

The **formulas** of language $\mathcal{L}$ are inductively defined as follows.

(1) $s, t, t_0, \cdots, t_{n-1}$ are terms of $\mathcal{L}$, and R is an n-ary relation symbol of $\mathcal{L}$, then

$$s = t \quad \text{and} \quad \mathrm{R}(t_0, \cdots, t_{n-1})$$

are formulas of $\mathcal{L}$, which are called **atomic** formulas.

(2) If φ, ψ are formulas of $\mathcal{L}$, then so are the followings

$$\neg(\varphi),\ (\varphi) \wedge (\psi),\ (\varphi) \vee (\psi),\ (\varphi) \to (\psi),\ \ \forall x(\varphi),\ \ \exists x(\varphi),$$

where x is any variable.

As in propositional logic, parentheses in a formula are appropriately omitted.
$\forall x(\varphi)$ means "for any x, φ holds", $\exists x(\varphi)$ means "there exists an x s.t. φ holds".

Example 2

In $(\mathbb{N}, 0, 1, +, \cdot, <)$, the following formula $\varphi(x)$ denotes "x is prime".

$$\varphi(x) \;\equiv\; \forall y \forall z (x = y \cdot z \to (y = 1 \lor z = 1)) \land x > 1.$$

Exercise 3.1.1

In the structure $\mathbb{N}$ of natural numbers in the language $\mathcal{L}_{\mathrm{OR}} = \{0, 1, +, \cdot, <\}$, express the following statements by a first-order formula.

(1) There are infinitely many prime numbers.

(2) Every even number greater than 2 can be written as the sum of two primes.

For in-depth discussion on formulas, we must clarify the role of variables in them.

- Let Q denote $\exists$ or $\forall$. Assume φ contains a subformula of the form $Qx(\psi)$, where no quantifier of the form Qx appears in ψ. Then each occurrence of x in (Qx and ψ) is said to be **bound** in φ. An occurrence of the variable x in the formula φ is said to be **free** when it is not bound.
- A variable may have both bound and free occurrences in a formula. E.g., in
$$(\forall x(x \leq y)) \to (\exists y(x \leq y)),$$
the first two of the three occurrences of x are bound, and last one is free.
- If a variable occurs both bound and free in a formula, we often automatically replace the bound occurrence with another variable to avoid unnecessary misreading. For example, the above formula can be rewritten as
$$(\forall w(w \leq y)) \to (\exists z(x \leq z)).$$
Then, the variables in a formula can be separated into free variables and bound variables.

- A formula without free variables is called a **sentence**.
- For a formula φ with free variables among $\{x_1, \ldots, x_n\}$, a sentence of the form $\forall x_1 \cdots \forall x_n \varphi$ is called the **universal closure** of φ.

- We often add new constants to a given language $\mathcal{L}$ to handle some elements of a structure $\mathcal{A}$. Let c_a be a constant (name) for an element a of $\mathcal{A}$. Then for $B \subseteq A$, by $\mathcal{L}_B$ we denote the language $\mathcal{L}$ extended with new constants c_a for all elements a of B. By $\mathcal{A}_B$, we denote an $\mathcal{L}_B$-structure obtained from the $\mathcal{L}$-structure $\mathcal{A}$ by interpreting c_a as a for each element a of B.
- This kind of expansion is often made implicitly. Unless a serious confusion occurs, we may write $\mathcal{A}$ for $\mathcal{A}_A$, and a and c_a are indiscriminate.

Definition 3.3 (Tarski's truth definition clauses)

For a sentence φ in $\mathcal{L}_A$, "φ is **true** in $\mathcal{A}$" (denote $\mathcal{A} \models \varphi$) is defined as follows.

$$\begin{aligned}
\mathcal{A} \models s = t &\Leftrightarrow s^{\mathcal{A}} = t^{\mathcal{A}}, \\
\mathcal{A} \models \mathrm{R}(s_0, \cdots, s_{n-1}) &\Leftrightarrow \mathrm{R}^{\mathcal{A}}(s_0^{\mathcal{A}}, \ldots, s_{n-1}^{\mathcal{A}}), \\
\mathcal{A} \models \neg\varphi &\Leftrightarrow \mathcal{A} \models \varphi \text{ does not hold}, \\
\mathcal{A} \models \varphi \wedge \psi &\Leftrightarrow \mathcal{A} \models \varphi \text{ and } \mathcal{A} \models \psi, \\
\mathcal{A} \models \varphi \vee \psi &\Leftrightarrow \mathcal{A} \models \varphi \text{ or } \mathcal{A} \models \psi, \\
\mathcal{A} \models \varphi \to \psi &\Leftrightarrow \text{ if } \mathcal{A} \models \varphi, \text{ then } \mathcal{A} \models \psi, \\
\mathcal{A} \models \forall x \varphi(x) &\Leftrightarrow \text{for any constant } a, \mathcal{A} \models \varphi(a), \\
\mathcal{A} \models \exists x \varphi(x) &\Leftrightarrow \text{there exists a constant } a \text{ s.t. } \mathcal{A} \models \varphi(a).
\end{aligned}$$

The truth of a formula with free variables is defined by the truth of its universal closure.

Definition 3.4

For $\mathcal{L}$-structures $\mathcal{A}$, $\mathcal{B}$, a function $\phi : A \to B$ satisfying the following conditions is called a **homomorphism**:

(1) For all constants c, $\phi(\mathrm{c}^{\mathcal{A}}) = \mathrm{c}^{\mathcal{B}}$.

(2) For each n-ary function symbol f, for any $a_0, \ldots, a_{n-1} \in A$,

$$\phi(\mathrm{f}^{\mathcal{A}}(a_0, \ldots, a_{n-1})) = \mathrm{f}^{\mathcal{B}}(\phi(a_0), \ldots, \phi(a_{n-1})).$$

(3) For each n-ary relation symbol R, for any $a_0, \ldots, a_{n-1} \in A$,

$$\mathrm{R}^{\mathcal{A}}(a_0, \ldots, a_{n-1}) \Longrightarrow \mathrm{R}^{\mathcal{B}}(\phi(a_0), \ldots, \phi(a_{n-1})).$$

In particular, a bijective homomorphism ϕ is called an **isomorphism**. If there is an isomorphism between $\mathcal{A}$ and $\mathcal{B}$, they are also called **isomorphic**, denoted by $\mathcal{A} \cong \mathcal{B}$.

- $\mathcal{A}$ is a **substructure** of $\mathcal{B}$, denoted by $\mathcal{A} \subset \mathcal{B}$, if $A \subset B$ and the inclusion function $i : A \to B$ (i.e., $i(a) = a$) is a homomorphism.

- If $\mathcal{A} \cong \mathcal{B}$, then it can be shown by simple induction that,

$$\underbrace{\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi \quad \text{for any sentence } \varphi.}_{\mathcal{A} \equiv \mathcal{B},\ \text{elementary equivalence (defined later)}}$$

- However, the converse $\mathcal{A} \equiv \mathcal{B} \Rightarrow \mathcal{A} \cong \mathcal{B}$ does not hold in general. (An counter example can be made by the Löwenheim-Skolem theorem in the next lecture.)

Definition 3.5

- A set T of sentences in a language $\mathcal{L}$ is called a **theory**.
- $\mathcal{A}$ is called a **model** of T, denote $\mathcal{A} \models T$, if all the sentences of T are true in $\mathcal{A}$. A theory is said to be **satisfiable** if it has a model.
- We say that φ **holds** in T, denote $T \models \varphi$, if any model $\mathcal{A}$ of T is also a model of φ. In particular, when $T = \varnothing$, we write $\models \varphi$ and such a φ is said to be **valid**.

- The formal system of first-order logic will be introduced in the folllowing lectures.
- We write $T \vdash \varphi$ if we have a proof of φ in T.
- **Gödel's completeness theorem** asserts

$$T \vdash \varphi \Leftrightarrow T \models \varphi.$$

- In the next lecture, we will focus on Skolem's theorem, which is the prototype of this theorem, and derive Gödel's completeness theorem from it.

Exercise 3.1.2

1. In the structure $(\mathbb{R}, <, f)$ of real numbers, construct a formula expressing "the function $f(x)$ is continuous at $x = a$".
   (Note: The structure is not equipped with any arithmetical operators).
2. In the structure $(\mathbb{R}, <, f)$, show that there is no formula that expresses "$f(x)$ is differentiable at $x = a$" (Padoa's method).

Summary

- First-order logic is developed in the common logical symbols (propositional connectives, quantifiers $\forall x$ and $\exists x$ and equality $=$) and specific mathematical symbols. The set of mathematical symbols to use is called a **language**.
- A **structure** in language $\mathcal{L}$ (simply, a $\mathcal{L}$-structure) is defined as a non-empty set A equipped with an interpretation of the symbols in $\mathcal{L}$.
- A **term** is a symbol string to denote an element of a structure. A **formula** is a symbol string to describe a property of a structure. A formula without free variables is called a **sentence**.
- "A sentence φ is **true** in $\mathcal{A}$", written as $\mathcal{A} \models \varphi$ is defined by Tarski's clauses.
- A set of sentences in the language $\mathcal{L}$ is called a **theory**. $\mathcal{A}$ is a **model** of T, denoted by $\mathcal{A} \models T$, if $\forall \varphi \in T \ (\mathcal{A} \models \varphi)$.
- We say that φ **holds** in T, written as $T \models \varphi$, if $\forall \mathcal{A}(\mathcal{A} \models T \to \mathcal{A} \models \varphi)$.

- In the following lectures, we will introduce a proof system for first-order logic. Later, we will prove the completeness theorem: $T \vdash \varphi \ \Leftrightarrow \ T \models \varphi$.

Further readings

E. Mendelson. *Introduction to Mathematical Logic*, CRC Press, 6th edition, 2015.

Thank you for your attention!