Recap
Introduction
Languages and Structures
Terms and Formulas
Variables and Constants
Truth and Models
Summary

Logic and Computation: I

Part 3 First order logic and decision problems

Kazuyuki Tanaka

BIMSA

December 8, 2022

北京雁栖湖应用数学研究院
YANQI LAKE 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 3. Schedule

- Dec. 8, (1) What is first-order logic?
- Dec.13, (2) Skolem's theorem
- Dec.15, (3) Gödel's completeness theorem
- Dec.20, (4) Ehrenfeucht-Fraïssé's theorem
- Dec.22, (5) Presburger arithmetic
- Dec.27, (6) Peano arithmetic and Gödel's first incompleteness theorem

Recap
Introduction
Languages and Structures
Terms and Formulas
Variables and Constants
Truth and Models
Summary

First order logic

1. Recap
2. Introduction
3. Languages and Structures
4. Terms and Formulas
5. Variables and Constants
6. Truth and Models
7. Summary

Recap: 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.

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 string of length n, it returns the correct answer within $p(n)$ steps or $p(n)$ cells of the tape, respectively.
- By **Savitch's theorem**, PSPACE $=$ NPSPACE. It is not known that the following inclusions are proper: P $\subseteq$ NP $\subseteq$ PSPACE.
- Q is NP-hard (PSPACE-hard) if any NP (PSPACE) problem Q′ is polynomial-time reducible to Q. An NP-hard NP problem is NP-complete. Similarly for PSPACE.
- **SAT** is a problem to determine whether a given proposition (or a Boolean formula) is satisfiable or not.
- **The Cook-Levin theorem**: SAT is NP-complete.
- **TQBF** is a problem to determine whether a given QBF (quantified Boolean formula without free variables) is true or not.
- **Theorem**: TQBF is PSPACE-complete.

Introduction

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

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

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

(6) Peano arithmetic and Gödel's first incompleteness theorem: undecidability and incompleteness theorems as negative answers to the "main problem".

☺ In next semester, we will introduce more details.

First order logic

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

Symbols

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

- The latter set of symbols is called the **language**[1] $\mathcal{L}$ of the theory. Note that $\mathcal{L}$ 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, a $\mathcal{L}$-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 do not make a strict distinction between the set A and the structure $\mathcal{A}$ 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 here a constant 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 simplicity, we often omit a superscipt such as ${}^{\mathcal{R}}$ 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.

Fix a language $\mathcal{L}$ and define a "term" of $\mathcal{L}$ to denote a specific element of $\mathcal{L}$-structure $\mathcal{A}$.

Definition (Terms)

The **terms** of the language $\mathcal{L}$ are symbol strings 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 variable, 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 (Formulas)

A **formula** of language $\mathcal{L}$ is a sequence of symbols 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

$$\neg(\varphi),\ (\varphi) \land (\psi),\ (\varphi) \lor (\psi),\ (\varphi) \to (\psi),$$

$$\forall x(\varphi),\quad \exists x(\varphi),$$

where x is any variable.

As in propositional logic, parentheses in a formula are appropriately omitted.
$\forall x(\varphi)$ means "for all x, φ holds", $\exists x(\varphi)$ means "some x exists and φ holds".

Example 2

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

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

Homework 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.

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

$$(\forall w(w \leq y)) \to (\exists z(x \leq z)).$$

- 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, a sentence of the form $\forall x_1 \cdots \forall x_n \varphi$ (i.e. all free variables appearing in φ are in $\{x_1, \ldots, x_n\}$) 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. We prepare a name (constant) c_a for each element a of structure $\mathcal{A}$. Then for $B \subseteq A$, by $\mathcal{L}_B$ we denote the language $\mathcal{L}$ extended with the new constant c_a for each element a of B.
- An $\mathcal{L}$-structure $\mathcal{A}$ is naturally extended to the structure in $\mathcal{L}_B$ by interpreting c_a as a, denoted $\mathcal{A}_B$.
- This kind of expansion is often made implicitly. Unless a serious confusion occurs, we may write $\mathcal{A}$ for $\mathcal{A}_B$, and a and c_a are indiscriminate.

Definition (Tarski's truth definition clauses)

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

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

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

Definition

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 $a_0, \ldots, a_{n-1} \in A$,

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

- 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,

$$\underbrace{\mathcal{A} \models \varphi \Leftrightarrow \mathcal{B} \models \varphi \quad \text{for any formula } \varphi.}_{\mathcal{A} \equiv \mathcal{B}, \text{ elementary equivalence}}$$

- However, the converse, namely, $\mathcal{A} \equiv \mathcal{B} \Rightarrow \mathcal{A} \cong \mathcal{B}$ does not hold in general (See the Löwenheim-Skolem theorem in the next lecture)

Definition

- The set T 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 all the sentence 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, written as $T \models \varphi$, if any model $\mathcal{A}$ of T is also a model of φ.
- In particular, given $T = \varnothing$, φ satisfying $\models \varphi$ is said to be **valid**.

- The formal system of first-order logic will be introduced in the next lecture.
- 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.

Homework 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: Sum-product operations cannot be used).

2. In the structure $(\mathbb{R}, <, f)$, show that there is no formula that expresses "$f(x)$ is differentiable with respect to $x = a$" (A. Padoa's method).

Summary

- First-order logic is developed in the common logical symbols and specific mathematical symbols. Major logical symbols are propositional connectives, quantifiers $\forall x$ and $\exists x$ and equality $=$. 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' clauses. The truth of a formula with free variables is defined by the truth of its universal closure.
- 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 next lecture, we will introduce a proof system for first-order logic. Later, we will prove the completeness theorem: $\vdash \varphi \Leftrightarrow \models \varphi$.

Further readings

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

Thank you for your attention!