Logic and Computation

K. Tanaka

Logic and Computation: I

Part 3 First order logic and decision problems

Kazuyuki Tanaka

BIMSA

December 13, 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

Skolem's theorem

Recap

- 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's 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 $\forall \mathcal{A}(\mathcal{A} \models T \rightarrow \mathcal{A} \models \varphi)$.

Introduction

- In the original proof of K. Gödel's completeness theorem, he reduced the nesting depth of quantifiers by introducing new relation symbols. Finally, the satisfiability of first-order logic is reduced to that of propositional logic.
- Before Gödel's, T. Skolem performed a similar operation using function symbols instead of relation symbols.
- Since Skolem did not consider formal deductive systems, he did not derive the completeness theorem, but his results are equivalent to those of the completeness theorem and its applications in model theory.
- Conversely, J. Herbrand, in the same era, obtained a result equivalent to the completeness theorem independent from the viewpoint of the model.
- In this lecture, we will review Skolem's arguments by adding Herbrand's perspective.

K. Gödel's

T. Skolem

J. Herbrand

In the following, unless otherwise stated, the language $\mathcal{L}$ is arbitrarily fixed.

Definition

Let φ be a formula without quantifiers and Q_i be quantifiers ($\forall$ or $\exists$).

$$Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \varphi$$

is in **prenex normal form**, abbreviated as PNF.
In particular, if all Q_i are $\forall$, we call it **$\forall$-formula** (universal formula); if all Q_i are $\exists$, we call it **$\exists$-formula** (existential formula).

Theorem (1)

For any formula φ, there exists an equivalent PNF formula φ', that is, the universal closure of $\varphi \leftrightarrow \varphi'$ (i.e., $(\varphi \to \varphi') \wedge (\varphi' \to \varphi)$) is valid.

Proof idea of Thm (1).

- For any formula φ, we perform the following transformation to push an inner quantifier in φ outside one by one.
- For example, consider a formula $\varphi \equiv \theta \land \forall x \xi(x)$.
- If θ does not have x as a free variable, we have the following equivalent transformation.

$$\theta \land \forall x \xi(x) \leftrightarrow \forall x(\theta \land \xi(x)).$$

- To show the equivalence, we take an arbitrary $\mathcal{L}$-structure and any assignment of its elements to free variables other than x. Then check the equivalence. Since θ does not have x as a free variable, it has the same truth value on both sides. Although the positions of $\forall x$ are different, both sides require $\xi(a)$ to hold for all elements a.
- If θ has x as a free variable, we replace the bound variable x of $\forall x \xi(x)$ by a new variable y and then obtain the following equivalent transformation.

$$\theta \land \forall x \xi(x) \leftrightarrow \forall y(\theta \land \xi(y)).$$

- For other combinations of logical symbols, we also have a similar equivalent transformation.

In the following, assume that in a PNF formula $Q_1x_1Q_2x_2\ldots Q_nx_n\theta$, all the variables x_i's are distinct. In fact, in $\cdots Qx \cdots Q'x \cdots \varphi$, the outer Qx is meaningless and is automatically deleted.

Definition

Given a formula φ, we first transform it into a equivalent PNF formula

$$\varphi' \equiv Q_1x_1Q_2x_2\ldots Q_nx_n\theta.$$

Then, by repeating the following operations as much as possible, we finally obtain a $\forall$-formula, which is called the **Skolem normal form** of φ, abbreviated as SNF.

- Let Q_i be the outermost (leftmost) existential symbol in φ'. Remove Q_ix_i and replace all occurrences of x_i on its right side (inside) of Q_ix_i with $\mathrm{f}(x_1,\ldots,x_{i-1})$, where f is a new function symbol and is called a **Skolem function**.

In the above definition, when Q_1 is existential, x_1 is replaced by a "constant" (or a 0-ary function symbol). In this lecture, constants are treated as 0-ary function symbols.

Example 1

For a PNF formula

$$\forall w \exists x \forall y \exists z \theta(w, x, y, z),$$

first remove $\exists x$ and replace x with $\mathrm{f}(w)$,

$$\forall w \forall y \exists z \theta(w, \mathrm{f}(w), y, z).$$

Remove $\exists z$, replace z with $\mathrm{g}(w, y)$,

$$\forall w \forall y \theta(w, \mathrm{f}(w), y, \mathrm{g}(w, y)).$$

This is a $\forall$-formula and thus the SNF of the given formula.

We here note that the following implications holds:

$$\forall w \forall y \theta(w, \mathrm{f}(w), y, \mathrm{g}(w, y)) \to \forall w \forall y \exists z \theta(w, \mathrm{f}(w), y, z) \to \forall w \exists x \forall y \exists z \theta(w, x, y, z).$$

- The equivalence between φ and its SNF formula φ^S does not hold in general.
- $\varphi^S \to \varphi$ is always true, while $\varphi \to \varphi^S$ is not. $(\because)$ A Skolem function of φ^S can be interpreted arbitrarily.
- But φ is satisfiable $\Leftrightarrow \varphi^S$ is satisfiable.

Theorem (2)

Let T be a theory in $\mathcal{L}$ and T^S be the collection of SNF σ^S for a sentence σ of T. For a formula φ in $\mathcal{L}$ (i.e., not containing a skolem function),

$$T \models \varphi \Leftrightarrow T^S \models \varphi.$$

Remark 1

- Let T be a theory in $\mathcal{L}$ and T' be a theory of an extended language $\mathcal{L}' \supset \mathcal{L}$.
- T' is said to be a **conservative extension** of T if for any formula φ in $\mathcal{L}$,

$$T \models \varphi \Leftrightarrow T' \models \varphi.$$

- The above theorem asserts that T^S is a conservative extension of T.

Proof of Thm(2).

$\Rightarrow$ is obvious because $\sigma^S \to \sigma$.
To show $\Leftarrow$

- Assume $T^S \models \varphi$ and let $\mathcal{A}$ be any model of T. We want to show $\mathcal{A} \models \varphi$.
- Choose any sentence σ in T. We suppose that it is of the form $\forall w \exists x \forall y \exists z \theta(w, x, y, z)$. (General cases can be treated similarly).
- Since this sentence σ holds in $\mathcal{A}$, then by the axiom of choice, we construct a functions $\mathrm{f}^{\mathcal{A}}(w)$ and $\mathrm{g}^{\mathcal{A}}(w, y)$ such that $(\mathcal{A}, \mathrm{f}^{\mathcal{A}}, \mathrm{g}^{\mathcal{A}})$ satisfies $\forall w \forall y \theta(w, \mathrm{f}(w), y, \mathrm{g}(w, y))$, namely, σ^S.
- Similarly, we can extend $\mathcal{A}$ to a model $\mathcal{A}^S$ by giving an appropriate interpretation to every Skolem function in every sentence σ in T. Then, obviously $\mathcal{A}^S \models T^S$.
- Since $T^S \models \varphi$, $\mathcal{A}^S \models \varphi$. So, we get $\mathcal{A} \models \varphi$ because φ contains no Skolem functions. Thus, $T \models \varphi$ since $\mathcal{A}$ is an arbitrary model of T. $\square$

- In Theorem (2), if φ is a contradiction $\bot$,

$$\text{“ } T \text{ is not satisfiable”} \Leftrightarrow \text{“ } T^S \text{ is not satisfiable”}$$

- So “ T is satisfiable” $\Leftrightarrow$ “ T^S is satisfiable”.
- For any sentence σ,

$$\models \neg\sigma \;\Leftrightarrow\; \text{“}\sigma \text{ is not satisfiable”} \Leftrightarrow \text{“}\sigma^S \text{ is not satisfiable”} \;\Leftrightarrow\; \models \neg\sigma^S.$$

Lemma (3)

In a countable language, if a formula φ holds in a structure $\mathcal{A}$, it holds in some countable substructure $\mathcal{A}' \subset \mathcal{A}$.

Proof.

- Let $\mathrm{f}_i(x_1, \ldots, x_{k_i})(1 \leq i \leq n)$ be the Skolem functions of φ.
- Let $\mathcal{A} \cup \{\mathrm{f}_i^{\mathcal{A}}\}$ be a model of SNF φ^S of φ. Note that this model is equipped with countable many functions.
- Choose an element $a \in A$, and construct the smallest subset A' of A that includes a and is closed under all functions. Then A' is a countable subset of A.
- Let $\mathcal{A}' \cup \{\mathrm{f}_i^{\mathcal{A}'}\}$ be a substructure of $\mathcal{A} \cup \{\mathrm{f}_i^{\mathcal{A}}\}$ obtained by restricting the domain to A'.
- Since φ^S is a $\forall$-formula, if it holds in $\mathcal{A} \cup \{\mathrm{f}_i^{\mathcal{A}}\}$, then also holds in $\mathcal{A}' \cup \{\mathrm{f}_i^{\mathcal{A}'}\}$. Thus φ also holds for $\mathcal{A}'$. □

The theorem above holds even if we replace a formula φ with a set of formulas. Thus we obtain the following theorem.

Theorem (Countable version of Löwenheim-Skolem's downward theorem)

For a structure $\mathcal{A}$ in a countable language $\mathcal{L}$, there exists a countable substructure $\mathcal{A}' \subset \mathcal{A}$ such that

$$\mathcal{A}' \models \varphi \Leftrightarrow \mathcal{A} \models \varphi, \quad \text{for any } \mathcal{L}_{A'} \text{ sentence } \varphi.$$

Such $\mathcal{A}'$ is called an **elementary substructure** of $\mathcal{A}$, denoted as $\mathcal{A}' \prec \mathcal{A}$.

Proof.

- Let T be the theory of $\mathcal{A}$, that is, the set of sentences true in $\mathcal{A}$.
- The set of Skolem functions (without duplication) for all sentences in T is a countable set. Therefore, there exists a countable set $A_1 \subset A$ which is closed under the functions of $\mathcal{L}$ and all Skolem functions.
- Let $\mathcal{A}_1$ be a substructure of $\mathcal{A}$ obtained by restricting the domain A to A_1. Then, $\mathcal{A}_1 \models T^S$ and so $\mathcal{A}_1 \models T$.
- Let T_{A_1} be the $\mathcal{L}_{A_1}$-theory of $\mathcal{A}$, that is, the set of $\mathcal{L}_{A_1}$-sentences true in $\mathcal{A}$.
- Construct a countable $\mathcal{A}_2 \subset \mathcal{A}$ such that $\mathcal{A}_2 \models T_{A_1}$.Then $\mathcal{A}_1 \prec \mathcal{A}_2$.
- Similarly, there is a countable $\mathcal{A}_3 \subset \mathcal{A}$ such that $\mathcal{A}_2 \prec \mathcal{A}_3 \models T_{A_2}$.
- By repeating this ω times and taking the limit sum, we obtain a countable substructure $\mathcal{A}'$ of $\mathcal{A}$ such that $\mathcal{A}_n \prec \mathcal{A}'$ for all n.
- Then any $\mathcal{L}_{A'}$ sentence φ is a $\mathcal{L}_{A_n}$ sentence for some n, so

$$\mathcal{A}' \models \varphi \Leftrightarrow \mathcal{A}_n \models \varphi \Leftrightarrow \mathcal{A} \models \varphi.$$

- Thus $\mathcal{A}'$ is a countable elementary substructure of $\mathcal{A}$. □

- By the countable version of Löwenheim-Skolem's downward theorem, real number theory and set theory, if they are described by countably many axioms, have a countable model. This fact is known as **Skolem's paradox**.
- Skolem also considered a structure, which is later be called the "Herbrand model".
- For simplicity, we assume that every language has at least one constant.
- **Herbrand domain** U is the collection of terms (without variables) constructed by function symbols, including Skolem functions.
- **Herbrand structure** $\mathcal{U}$ is defined by interpreting each function symbol on U: for $t_1, \ldots, t_n \in U$,
$$\mathrm{f}^{\mathcal{U}}(t_1, \ldots, t_n) \equiv \text{term “}\mathrm{f}(t_1, \ldots, t_n)\text{”}.$$
- There are no restrictions on the interpretation of relational symbols, except for the equality symbol $=$. We first consider a language without equality.

Lemma (4)

Let Σ be a set of sentences without quantifiers and equality. The following three statements are equivalent.

1. Σ is satisfiable in the first-order sense, *i.e.*, Σ has a model.
2. Σ is satisfiable in the sense of propositional logic (regarding atomic sentences as atomic propositions).
3. Σ has a Herbrand structure as its model.

Proof.
$(1 \Rightarrow 2)$ If the truth-value of atomic propositions is determined by the model given by 1, then we get a truth-value function that makes all propositions in Σ true.
$(2 \Rightarrow 3)$ Assume there exists a truth-value function V that makes all statements of Σ true. Then, the interpretation of the relation symbol R in the Herbrand structure $\mathcal{U}$ is determined as follows. For $t_1, \ldots, t_n \in U$,

$$\mathrm{R}^{\mathcal{U}}(t_1, \ldots, t_n) \Leftrightarrow V(\mathrm{R}(t_1, \ldots, t_n)) = \mathrm{T}(\mathrm{true}).$$

By induction on the complexity of formulas, we can say that all sentences that are true with V hold in $\mathcal{U}$. In particular, $\mathcal{U}$ is a model of Σ.
$(3 \Rightarrow 1)$ trivial

Let $\mathcal{L}(\varphi)$ denote the set of mathematical symbols of formula φ. For simplicity, let $\exists\vec{x}\varphi(\vec{x}) := \exists x_1 \ldots \exists x_n \varphi(x_1, \ldots, x_n)$. When we write $\exists\vec{x}\varphi(\vec{x})$, $\varphi(\vec{x})$ has no quantifiers.

Lemma (Herbrand's theorem (Skolem version))

In first-order logic without equality, $\exists$-formula $\exists\vec{x}\varphi(\vec{x})$ is valid if and only if

- there exist n-tuples $\vec{t_i} \in U^n$ $(i < k)$ from the Herbrand domain U of $\mathcal{L}(\varphi)$ and
- $\varphi(\vec{t_1}) \vee \cdots \vee \varphi(\vec{t_k})$ is a tautology.

If $\mathcal{L}(\varphi)$ does not have a constant, add a new constant to U.

Proof.

($\Leftarrow$) The tautology $\varphi(\vec{t_1}) \vee \cdots \vee \varphi(\vec{t_k})$ is also true in first-order logic. $\varphi(\vec{t_i}) \rightarrow \exists\vec{x}\varphi(\vec{x})$ is valid, so $\exists\vec{x}\varphi(\vec{x})$ is valid.

($\Rightarrow$) By contraposition.

- For any n-tuple $\vec{t_i}(i < k)$ of the Herbrand domain U, $\varphi(\vec{t_1}) \vee \cdots \vee \varphi(\vec{t_k})$ is not a tautology.
- Then $\neg\varphi(\vec{t_1}) \wedge \cdots \wedge \neg\varphi(\vec{t_k})$ is satisfiable in propositional logic.
- By the compactness theorem of propositional logic, $\Sigma = \{\neg\varphi(\vec{t}) : \vec{t} \in U^n\}$ is satisfiable.
- From Lemma (4), Herbrand structure $\mathcal{U}$ is a model of Σ. By the definition of Σ, $\mathcal{U} \models \neg\exists\vec{x}\varphi(\vec{x})$. So the given $\exists$ sentence $\exists\vec{x}\varphi(\vec{x})$ is not valid.

Theorem (Skolem Fundamental Theorem)

In first-order logic without equality, let $\sigma^S \equiv \forall\vec{x}\varphi(\vec{x})$ be a SNF of sentence σ. Then, $\neg\sigma$ is valid if and only if

- there exist n-tuples $\vec{t_i} \in U^n (i < k)$ from Herbrand domain U of $\mathcal{L}(\varphi)$, and
- $\neg\varphi(\vec{t_1}) \vee \cdots \vee \neg\varphi(\vec{t_k})$ is a tautology.

If $\mathcal{L}(\varphi)$ does not contain a constant, add a new constant to U.

Proof. By Remark 1 after Theorem (2), and Herbrand's theorem.

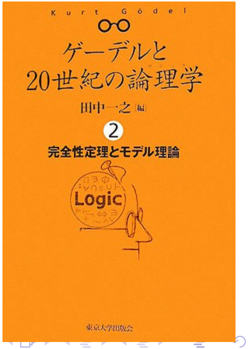
Example 3

$\exists w \forall x \exists y \forall z \neg\theta(w,x,y,z)$ is true $\Leftrightarrow$ $\exists w \exists y \neg\theta(w, f(w), y, g(w,y))$ is true $\Leftrightarrow$ there exist closed terms $s_1, \ldots, s_n$ and $t_1, \ldots, t_n$ such that

$$\neg\theta(s_1, f(s_1), t_1, g(s_1, t_1)) \vee \cdots \vee \neg\theta(s_n, f(s_n), t_n, g(s_n, t_n))$$

is a tautology.

- In response to Skolem's argument above, Herbrand presented a more constructive assertion by replacing validness with provability.
- In particular, there is Herbrand's Fundamental Theorem, which corresponds to Skolem's Fundamental Theorem.
- For the proof of Herbrand's Fundamental Theorem, *rf.* the Appendix of the right hand side book.



What happens if equality "=" is considered?

- Suppose we are given an arbitrary sentence σ with an equality "=".
- Let σ be a formula constructed with symbols $f, R \in \mathcal{L}(\sigma)$, and the conservation axiom for "="

$$\forall\vec{x}\,\forall\vec{y}\,(\vec{x}=\vec{y}\to f(\vec{x})=f(\vec{y})),\quad \forall\vec{x}\,\forall\vec{y}\,(\vec{x}=\vec{y}\to R(\vec{x})\leftrightarrow R(\vec{y})).$$

- Since each of the reflexivity, symmetricity, and transitivity of "=" can be expressed by a $\forall$ sentence, their conjunction, denote $\mathrm{Eq}(\sigma)$, can also be regarded as a $\forall$-sentence.
- Therefore, an $\exists$-sentence σ is valid in first-order logic with "=" iff

$$\mathrm{Eq}(\sigma)\to\sigma$$

  is valid without the equality axioms.
- Since the above expression is a $\exists$ statement, applying the Herbrand's theorem to this, we obtain the equivalent condition as a tautology.

Summary

- We first transform a formula φ into a equivalent PNF formula

$$\varphi' \equiv Q_1 x_1 Q_2 x_2 \dots Q_n x_n \theta.$$

  Then remove $\exists x$ and replace x in θ with a new function f. For a PNF formula $\forall w \exists x \forall y \exists z \theta(w, x, y, z)$, we obtain a SNF $\varphi^S \equiv \forall w \forall y \theta(w, \mathrm{f}(w), y, \mathrm{g}(w, y))$.

- Theorem (2). $T^S = \{\sigma^S : \sigma \in T\}$ is a **conservative extension** of T.

- Löwenheim-Skolem's downward theorem. For a structure $\mathcal{A}$ in a countable language $\mathcal{L}$, there exists a countable substructure $\mathcal{A}' \subset \mathcal{A}$ s.t. $\mathcal{A}' \models \varphi \Leftrightarrow \mathcal{A} \models \varphi$ for any $\mathcal{L}_{A'}$-sentence φ. Such $\mathcal{A}'$ is called an **elementary substructure** of $\mathcal{A}$, denote $\mathcal{A}' \prec \mathcal{A}$.

- Herbrand's theorem (Skolem version). In first-order logic (without equality), $\exists$-formula $\exists \vec{x} \varphi(\vec{x})$ is valid if and only if
  - there exist n-tuples of terms, $\vec{t}_1, \dots, \vec{t}_k$, from $\mathcal{L}(\varphi)$ and
  - $\varphi(\vec{t}_1) \vee \cdots \vee \varphi(\vec{t}_k)$ is a tautology.

Thank you for your attention!