Logic and Computation I

Part 3. First order logic and decision problems

Kazuyuki Tanaka

BIMSA

November 12, 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

- Any formula φ can be transformed into an equivalent **PNF** $Q_1x_1 \ldots Q_nx_n\theta$. Removing all $\exists x$ and replace x in θ with a new function f, we obtain a **SNF**. For instance, a PNF formula $\varphi \equiv \forall w \exists x \forall y \exists z \theta(w, x, y, z)$ is transformed into a SNF $\varphi^S \equiv \forall w \forall y \theta(w, \mathrm{f}(w), y, \mathrm{g}(w, y))$.
- For a formula φ in $\mathcal{L}$ (i.e., with no Skolem functions), $T \models \varphi \Leftrightarrow T^S \models \varphi$. Namely, $T^S = \{\sigma^S : \sigma \in T\}$ is a **conservative extension** of T (Theorem 3.9).
- **Löwenheim-Skolem's downward theorem**. For a structure $\mathcal{A}$ in a countable language $\mathcal{L}$, there exists a countable $\mathcal{A}' \subset \mathcal{A}$ s.t. $\mathcal{A}' \models \varphi \Leftrightarrow \mathcal{A} \models \varphi$ for any $\mathcal{L}_{A'}$-sentence φ. $\mathcal{A}'$ is called an **elementary substructure** of $\mathcal{A}$, $\mathcal{A}' \prec \mathcal{A}$.
- (Proof) Let A' be the smallest subset of A that includes an element a and is closed under the functions of $\mathcal{L}$ and all Skolem functions. A' is countable. Let $\mathcal{A}'^S$ be a substructure of $\mathcal{A}^S$ obtained by restricting the domain A to A'. Then, $\mathcal{A}'^S \equiv \mathcal{A}^S$. Since each element of A' can be expressed as a term in $\mathcal{L}$ with Skolem functions, $\mathcal{A}' \models \varphi \Leftrightarrow \mathcal{A} \models \varphi$ for any $\mathcal{L}_{A'}$ sentence φ. So $\mathcal{A}' \preccurlyeq \mathcal{A}$.

- **Herbrand's theorem** (Skolem version). In first-order logic (without equality), ∃-sentence $\exists\vec{x}\varphi(\vec{x})$ is valid if and only if there exist n-tuples of terms, $\vec{t}_1,\dots,\vec{t}_k$, from $\mathcal{L}(\varphi)$ such that $\varphi(\vec{t}_1)\vee\cdots\vee\varphi(\vec{t}_k)$ is a tautology.
- What happens if equality "=" is considered? Let $\mathrm{Eq}(\sigma)$ be the finite set of the following axioms of equation for $\mathcal{L}(\sigma)$: the reflexivity, symmetricity, and transitivity of "=", and for each symbol $f, R \in \mathcal{L}(\sigma)$,

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

- Since each sentence of $\mathrm{Eq}(\sigma)$ is a ∀ sentence, their conjunction can also be regarded as a ∀-sentence, also denoted as $\mathrm{Eq}(\sigma)$.
- Therefore, an ∃-sentence σ is valid in first-order logic with "=" iff

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

is valid without the equality axioms. Since the above formula is an ∃-sentence, applying the Herbrand's theorem to this, we obtain the equivalent condition as a tautology.

Decision problem solved by F.Ramsey et al.

- For a quantifier-free formula $\theta(\vec{x},\vec{y})$, a formula in the form $\forall\vec{x}\exists\vec{y}\theta(\vec{x},\vec{y})$ is called a $\forall\exists$ formula; $\exists\vec{x}\forall\vec{y}\theta(\vec{x},\vec{y})$ is called a $\exists\forall$ formula.
  Now, we assume a formula contains no function symbols except constants.
- Then, we can check in finite steps the $\forall\exists$ sentence σ (with $=$) is valid or not. Let $\vec{a}$ be Skolem functions (constants) for $\neg\sigma \equiv \exists\vec{x}\forall\vec{y}\neg\theta(\vec{x},\vec{y})$. Then,
  $$\begin{aligned} \sigma \text{ is valid} \quad &\Leftrightarrow \quad \exists\vec{y}\ \theta(\vec{a},\vec{y}) \text{ is valid} \\ &\Leftrightarrow \quad \mathrm{Eq}(\theta(\vec{a},\vec{y})) \to \exists\vec{y}\theta(a,\vec{y}) \text{ is valid without } =. \end{aligned}$$
- Let $\exists\vec{z}\ \varphi(\vec{z})$ denote $\mathrm{Eq}(\theta(\vec{a},\vec{y})) \to \exists\vec{y}\theta(a,\vec{y})$. The Herbrand domain of $\mathcal{L}(\varphi(\vec{z}))$ consists of a finite number of constants.
- We substitute all combinations of these constants for $\vec{z}$ in $\varphi(\vec{z})$, combine them with disjunction $\vee$. We check whether the proposition is a tautology or not.
- The decision problem of $\forall\exists$ sentences is known to be NEXPTIME complete.

§3.3 Gödel's completeness theorem

- Before discussing Gödel's completeness theorem, we introduce a formal deductive system of first-order logic.
- Among the various formal systems, we consider an formal system by extending that of propositional logic in part 2 of this course.

Axioms

P1. $\varphi \to (\psi \to \varphi)$

P2. $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$

P3. $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$

P4. $\forall x \varphi(x) \to \varphi(t)$ (the quantification axiom)

Inference rules

(1) If φ and $\varphi \to \psi$ are theorems, so is ψ

(2) If $\psi \to \varphi(x)$ (where ψ does not include x) is a theorem, then so is $\psi \to \forall x \varphi(x)$ (the generalization rule)

- The **existential quantifier** $\exists$ is defined as $\exists x\varphi(x) \equiv \neg\forall x\neg\varphi(x)$.
- In languages with equality, we assume the axioms **Eq** (reflexive, symmetrical, transitive, and for each symbol f or R, its value is preserved with equality).
- If a sentence σ can be proved from a theory T, then σ is called a **theorem** of T, and written as $T \vdash \sigma$.
- The quantification axiom and the axioms Eq hold trivially in any structure, and the generalization rule also clearly preserves truth (because the free variable x of a formula is interpreted by universal closure).
- So, if $T \vdash \sigma$ then $T \models \sigma$. This is called the **soundness theorem**, since it means that the deductive system does not derive any strange theorems.
- The **completeness theorem** asserts the opposite, which means that the formal system derives all true propositions.

Exercise 3.3.1

(1) For any formula $\varphi(x_1, \ldots, x_n)$, prove the following formula, which means that the truth value must be preserved with equality:

$$(x_1 = y_1 \land \cdots \land x_n = y_n) \to (\varphi(x_1, \ldots, x_n) \leftrightarrow \varphi(y_1, \ldots, y_n)).$$

(2) Let $\psi(\varphi)$ be the formula obtained by replacing a relation symbol $\mathrm{R}(\vec{x})$ (all occurrences) in formula ψ with a formula $\varphi(\vec{x})$. Prove the following:

$$\forall \vec{x}(\varphi_1(\vec{x}) \leftrightarrow \varphi_2(\vec{x})) \to (\psi(\varphi_1) \leftrightarrow \psi(\varphi_2)).$$

Completeness theorem (a weak version)

For any sentence σ, if $\models \sigma$ then $\vdash \sigma$.

Proof.

- Assuming $\models \neg\sigma$, we will show $\vdash \neg\sigma$.
- Let $\forall\vec{x}\varphi(\vec{x})$ be the $\mathrm{SNF}\sigma^S$ of σ. By Skolem's fundamental theorem, for a valid $\neg\sigma$, there are n tuples of terms $\vec{t_i}$ s.t. $\neg\varphi(\vec{t_1}) \vee \cdots \vee \neg\varphi(\vec{t_k})$ is a tautology.
- By the completeness theorem of propositional logic, the tautology is a theorem of propositional logic. So, it is also a theorem of first-order logic.
- Since $\neg\varphi(\vec{t_i}) \to \exists\vec{x}\neg\varphi(\vec{x})$ can be proved in first-order logic, we can deduce $\exists\vec{x}\neg\varphi(\vec{x})$ from the theorem $\neg\varphi(\vec{t_1}) \vee \cdots \vee \neg\varphi(\vec{t_k})$. Thus, $\neg\sigma$ is provable. □

Other proofs

- To prove the completeness theorem, Gödel introduced new relation symbols instead of Skolem functions, and transformed any sentence into a $\forall\exists$ sentence.
- Subsequently, L. Henkin introduced a constant $c_{\exists x\varphi(x)}$ (**Henkin constant**) for each sentence $\exists x\varphi(x)$, and assume the following formula as an axiom.

$$\exists x\varphi(x) \to \varphi(c_{\exists x\varphi(x)}) \qquad \text{Henkin axiom.}$$

  By the Henkin axioms, any sentence can be rewritten without quantifiers.
- To obtain the general completeness theorem ($T \vdash \varphi \Leftrightarrow T \models \varphi$), we need the compactness theorem of first order logic, which is also deduced from the compactness of propositional logic.

Theorem 3.15 (Compactness theorem)

If a set T of sentences of first order logic is not satisfiable, then there exists some finite subset of T which is not satisfiable.

Proof

- Let T^S be the collection of SNF σ^S for each sentence σ in T. (Notice that all the Skolem functions should be distinct. Regarding the equality, you can add the equality axiom Eq to T if necessary.)
- By Theorem 3.9, T^S is a conservative extension of T. In particular, the satisfiability of T is equivalent to the satisfiability of T^S.
- Let Σ be the set of quantifier-free sentences $\varphi(\vec{t})$ for all SNF $\forall\vec{x}\varphi(\vec{x})$ in T^S and all terms $\vec{t}$ (in the Herbrand domain U) which are constructed by function symbols used in T^S.
- Now, if Σ is satisfiable (in the sense of propositional logic or first-order logic), then from Lemma 3.12, Σ has a Herbrand structure $\mathcal{U}$ as its model.

- If $\mathcal{U} \models \Sigma$, then for any SNF $\forall \vec{x} \varphi(\vec{x})$ in T^S, all the substitution instances of $\varphi(\vec{x})$ hold in $\mathcal{U}$, hence also $\forall \vec{x} \varphi(\vec{x})$ holds in $\mathcal{U}$, which means that $\mathcal{U}$ is a model of T^S, hence also a model of T.
- Now, assume that T is not satisfiable. Then, Σ is not satisfiable. Here again, from Lemma 3.12, Σ is not satisfiable in the sense of propositional logic.
- By the compactness of propositional logic, some finite subset Σ' of Σ is not satisfiable, and it is also not satisfiable in the sense of first-order logic.
- Now, let T'^S be the finite set of SNF's $\forall \vec{x} \varphi(\vec{x})$ in T^S which correspond to $\varphi(\vec{t})$ in Σ'. Moreover, let T' be the finite sets of σ for σ^S in T'^S.
- In general, if T'^S has a model, then it is also a model of Σ'. Thus, T'^S is not satisfiable.
- Therefore, the finite subset T' of T is also not satisfiable. $\square$

From the compactness theorem, we can derive the general completeness theorem.

Theorem 3.16 (Gödel's completeness theorem)

In first order logic, $T \vdash \varphi \Leftrightarrow T \models \varphi$.

Proof.

- $\Rightarrow$ has been proved as above (page 7).
- To show $\Leftarrow$, assume $T \models \varphi$ and φ is a sentence.
- Then $T \cup \{\neg\varphi\}$ is not satisfiable.
- By the compactness theorem, there exists a finite set $\{\sigma_1, \ldots, \sigma_n\}$ of T such that $\{\sigma_1, \ldots, \sigma_n, \neg\varphi\}$ is not satisfiable.
- Then, $(\sigma_1 \wedge \cdots \wedge \sigma_n) \to \varphi$ is valid.
- From the completeness theorem (a weak version), $(\sigma_1 \wedge \cdots \wedge \sigma_n) \to \varphi$ is provable, and from MP, $\{\sigma_1, \ldots, \sigma_n\} \vdash \varphi$, hence $T \vdash \varphi$. □

Existence of non-standard models of arithmetic

- Let $\mathcal{N} = (\mathbb{N}, 0, 1, +, \cdot, <)$ be the standard model of arithmetic (natural number theory). Let Th($\mathcal{N}$) $:= \{\sigma : \mathcal{N} \models \sigma\}$. $\mathcal{N}$ is naturally a model of Th($\mathcal{N}$), but there also exist models of Th($\mathcal{N}$) that are not isomorphic to $\mathcal{N}$, which are called **nonstandard models** of arithmetic.
- Using the compactness theorem, we construct a nonstandard model of arithmetic as follows. First, with c as a new constant, for each $k \in \mathbb{N}$

$$T_k = \mathrm{Th}(\mathcal{N}) \cup \{0 < \mathrm{c}, 1 < \mathrm{c}, 1+1 < \mathrm{c}, 1+1+1 < \mathrm{c}, \ldots, \overbrace{1+1+\cdots+1}^{k \text{ times}} < \mathrm{c}\}$$

- The structure of $\mathcal{N}$ plus the interpretation of the constant c as $k+1$ is a model of T_k. Let $T = \bigcup_{k \in \mathbb{N}} T_k$. Any finite subset of T is contained in some T_k and so satisfiable. Hence, by the compactness theorem, T also has a model $\mathcal{M}$, where the value of c is larger than any standard natural number.
- By removing the constant c from the structure, $\mathcal{M}$ can be regarded as a non-standard model of arithmetic in the language $\mathcal{L}_{\mathrm{OR}}$.

Existence of arbitrarily large models

- If T has an arbitrarily large finite model, then T has a model of arbitrarily large infinite cardinality.
- Let $\{c_i : i \in \kappa\}$ be a set of constants with infinite cardinality κ. We consider

$$T' = T \cup \{c_i \neq c_j : i \neq j \text{ and } i, j \in \kappa\}$$

- For any finite subset of T', it is satisfiable if we take a finite model of T with at least the number of constants c_i in it, and interpret each constant as a distinct element.
- Therefore, from the compactness theorem, T' also has a model, which is a model of T with more than κ elements.
- To construct a model with exactly the same cardinality as T, we use a generalized version of the Löwenheim-Skolem's downward theorem.

Remark

- By the above example, there is no first-order theory that has arbitrarily large finite models and has no infinite models.
- Thus the relation $T \models_{\mathsf{finite}} \varphi$ asserting that a formula φ is true for any finite model $\mathcal{M}$ of theory T cannot be captured by the first order system (Trakhtenbrot theorem, which will be introduced in next semester).

Connectivity of graphs

- A graph $G = (V, E)$ consists of a set V of vertices and the relation $E \subset V \times V$ representing the edges.
  We consider an undirected graph (a directed graph can be treated similarly).
- Let c_1 and c_2 be constants. For each $n \in \mathbb{N}$, define φ_n as follows:

$$\varphi_n \equiv \neg \exists x_1 \exists x_2 \ldots \exists x_n (E(\mathrm{c}_1, x_1) \land E(x_1, x_2) \land \cdots \land E(x_n, \mathrm{c}_2)),$$

  meaning there is no path of length $n+1$ from c_1 to c_2, and φ_0 is $\neg E(\mathrm{c}_1, \mathrm{c}_2)$.
- Suppose there is a first order sentence σ expressing the connectivity of c_1 and c_2. Consider the following T, which has a model by compactness theorem.

$$T = \{\sigma\} \cup \{\varphi_n : n \in \mathbb{N}\} \cup \{\mathrm{c}_1 \neq \mathrm{c}_2\}$$

- But in that model there is no finite-length path from c_1 to c_2, which contradicts with the connectivity that σ represents.
- Therefore, there is no sentence of first-order logic expressing connectivity.

- In this way, for all graphs including infinite graphs, connectivity cannot be expressed by a first-order formula.
- But what if we restrict ourselves to finite graphs?
- Even in this case, connectivity cannot be formulated. For that purpose, the Ehrenfeucht-Fraïssé game introduced in the next lecture is effective.

Summary

- **Formal system** of first-order logic: formal system of propositional logic + $\forall x \varphi(x) \to \varphi(t)$ (the quantification axiom) + the generalization inference rule
- **Henkin axiom** $\exists x \varphi(x) \to \varphi(c_{\exists x \varphi(x)})$, by which any sentence can be rewritten as a formula without quantifiers.
- **Compactness theorem.** If a set T of sentences of first order logic is not satisfiable, then there exists some finite subset of T which is not satisfiable.
- **Gödel's completeness theorem.** In first order logic, $T \vdash \varphi \Leftrightarrow T \models \varphi$.
- Application of the compactness theorem
  - ▷ Existence of non-standard models of arithmetic.
  - ▷ Existence of arbitrarily large models.
  - ▷ Connectivity of graphs can not be exressed in a first-order formula.

Further readings

H.D.Ebbinghaus, et al., Mathematical Logic 3rd ed., Graduate Texts in Math, Springer 2021.

Thank you for your attention!