Logic and Computation: I

Part 3 First order logic and decision problems

Kazuyuki Tanaka

BIMSA

December 16, 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

First order logic

Recap

- φ can be transformed into an equivalent PNF $\varphi' \equiv Q_1x_1Q_2x_2\dots Q_nx_n\theta$.
  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 $\varphi^S \equiv \forall w\forall y\theta(w,\mathrm{f}(w),y,\mathrm{g}(w,y))$.
- For a formula φ of $\mathcal{L}$ (i.e., not containing a skolem function), $T \models \varphi \Leftrightarrow T^S \models \varphi$.
  $T^S = \{\sigma^S : \sigma \in T\}$ 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 $\mathcal{A}$, denoted as $\mathcal{A}' \prec \mathcal{A}$.
- 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.

Application: P. Bernays, M. Shönfinkel, F. Ramsey

- Let $\theta(\vec{x}, \vec{y})$ be a formula without quantifiers. A formula of the form $\forall\vec{x}\exists\vec{y}\theta(\vec{x}, \vec{y})$ is called a $\forall\exists$ formula; a formula of the form $\exists\vec{x}\forall\vec{y}\theta(\vec{x}, \vec{y})$ is called a $\exists\forall$ formula. In this page, 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 $\mathrm{Eq}(\theta(\vec{a}, \vec{y})) \to \exists\vec{y}\theta(a, \vec{y})$. $\mathcal{L}(\varphi(\vec{z}))$ consists of a finite number of constants in the Herbrand domain.
- We substitute all combinations of these constants for $\vec{z}$ in $\varphi(\vec{z})$, combine them with disjunction $\vee$. We can check whether the proposition is a tautology or not.
- Such a decision problem is NEXPTIME complete.

Formal system of first-order logic

- Before introducing Gödel's completeness theorem, we define the the formal 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.

Axiom system

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

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

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 quantifiers $\exists x \varphi(x) := \neg \forall x \neg \varphi(x)$.
- In languages with equality, the axiom Eq is assumed (reflexive, symmetrical, transitive, and for each symbol f or R, its value is preserved with equality).
- If a sentence σ can be proved from the set of sentences T, then σ is called a **theorem** of T, and written as $T \vdash \sigma$.
- The quantification axiom and the equality axiom 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 means that the deductive system does not derive any strange theorems, and is called the **soundness theorem**.
- The completeness theorem (a weak version) asserts the opposite, that the system derives all true propositions.

Homework

(1) For any formula $\varphi(x_1, \dots, x_n)$, prove that the truth value must be preserved with equality $((x_1 = y_1 \land \cdots \land x_n = y_n) \to \varphi(x_1, \dots, x_n) \leftrightarrow \varphi(y_1, \dots, y_n))$.

(2) Let $\psi(\varphi)$ be the formula obtained by replacing the relation symbol $\mathrm{R}(\vec{x})$ in formula ψ with formula $\varphi(\vec{x})$. Show $\forall \vec{x}(\varphi_1(\vec{x}) \leftrightarrow \varphi_2(\vec{x})) \to (\psi(\varphi_1) \leftrightarrow \psi(\varphi_2))$.

Completeness theorem (a weak version)

- The theorem asserts that for any sentence σ, if $\models \sigma$ then $\vdash \sigma$. So, assuming $\models \neg\sigma$, we will show $\vdash \neg\sigma$.
- By Skolem's Fundamental Theorem, let $\forall\vec{x}\varphi(\vec{x})$ be the $\mathrm{SNF}\sigma^S$ of σ. If $\neg\sigma$ is valid, there are n pairs of terms $\vec{t_i}$ such that $\neg\varphi(\vec{t_1}) \vee \cdots \vee \neg\varphi(\vec{t_k})$ 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, by regarding the atomic propositions as atomic formulas 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.

Skolem Fundamental Theorem, revisited

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

- 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.

- To show 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 a axiom. By the Henkin axioms, any sentence can be rewritten as a formula without quantifiers.

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

- The compactness theorem of first order logic is also deduced from the compactness of propositional logic.

Theorem (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 of each sentence σ in T. (Notice that all the Skolem functions should be distinct. Regarding the equality, you can add the equality axiom Eq if necessary)
- From theorem below, we see that the satisfiability of T is equivalent to the satisfiability of T^S.

Recall: Theorem (2) of Lecture-03-02

For a formula φ in $\mathcal{L}$ (i.e., not containing a skolem function),

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

- Construct the Herbrand domain U using all function symbols contained in T^S.
- Let Σ be the set of all the sentences obtained from $\varphi(\vec{x})$ such that $\forall \vec{x} \varphi(\vec{x})$ in $T^S$by substituting terms in U to $\vec{x}$.

- Now, if Σ is satisfiable, then from the folowing lemma, Σ has a Herbrand structure $\mathcal{U}$ as its model.

Recall: Lemma (4) of Lecture-03-02

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.

- Since $\mathcal{U} \models \Sigma$, all the substitution instances of $\varphi(\vec{x})$ hold in $\mathcal{U}$, and so $\forall \vec{x} \varphi(\vec{x})$ also holds in $\mathcal{U}$, which means that $\mathcal{U}$ is a model of T^S, hence a model of T. Therefore, Σ is not satisfiable if T is not satisfiable.

- Now, assume that T is not satisfiable. Therefore, Σ is not satisfiable. Here again, from the Lemma (4) of Lecture-03-02, 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 $\overline{\sigma}^S$ denote the $\forall$ formula of T^S which is the source of formula σ of Σ', and let $\overline{\sigma}$ be the formula of T which is the source of formula $\overline{\sigma}^S$.
- Moreover, let T'^S and T' be the sets of $\overline{\sigma}^S$and $\overline{\sigma}$, respectively.
- In general, a model of T'^S is a model of Σ'. So $T'^S$is not satisfiable.
- Hence, the finite subset T' of T is also not satisfiable. □

From this we can derive the general completeness theorem.

Theorem (Gödel's completeness theorem)

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

Proof.

- $\Rightarrow$ has been proved as above.
- 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 $\mathrm{Th}(\mathcal{N}) := \{\sigma : \mathcal{N} \models \sigma\}$. $\mathcal{N}$ is naturally a model of $\mathrm{Th}(\mathcal{N})$, but there also exist models of $\mathrm{Th}(\mathcal{N})$ 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 $T = \bigcup_{k \in \omega} T_k$. 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.
- That is, $\mathcal{M}$ has elements that are not standard natural numbers.
- 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 $T \models_{\text{finite}} \varphi$ 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

- The graph $G = (V, E)$ consists of 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, and for each $n \in \mathbb{N}$, define φ_n as follows

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

  where φ_n means 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 a graph (there is a path between any two vertices).
- At this time, the following T 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.
- That is, there is no sentence of first-order logic expressing connectivity.

- In this way, for all graphs including infinite graphs, connectivity cannot be formulated by a first-order logic 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

Further readings

Mathematical Logic. H.-D. Ebbinghaus, J. Flum, w. Thomas, Springer New York, NY.

Thank you for your attention!