Logic and Computation: I

Part 3 First order logic and decision problems

Kazuyuki Tanaka

BIMSA

December 20, 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

Ehrenfeucht-Fraïssé's theorem

Recap

- **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
- If a sentence σ can be proved from the set of sentences T, then σ is called a **theorem** of T, and written as $T \vdash \sigma$.
- A sentence φ is **true** in $\mathcal{A}$, written as $\mathcal{A} \models \varphi$ is defined by Tarski's clauses. $\mathcal{A}$ is a **model** of T, denoted by $\mathcal{A} \models T$, if $\forall\varphi \in T\ (\mathcal{A} \models \varphi)$.
- φ holds in T, written as $T \models \varphi$, if $\forall\mathcal{A}(\mathcal{A} \models T \to \mathcal{A} \models \varphi)$.
- **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 cannot be expressed as a first-order formula.

Introduction

- Model-theoretical research on first-order logic developed rapidly with the new proof of the completeness theorem by Henkin in 1949.
- One of the most important concepts is **elementary equivalence**. Two structures are elementary equivalent if they satisfy the same formulas.
- In the early 1950s, R. Fraïsse studied elementary equivalences using the back-forth argument. In the late 1950s, A. Ehrenfeucht, a student of A. Mostowski's, further reformulated it in terms of games.
- We refer the Ehrenfeucht-Fraïsse game and related theorems as **EF games** and **EF theorems**. Their results have been attracting a great deal of attention since the 1980s in relation to theory of computation.

Relational languages

- In this section we assume that the language have no function symbols (other than constants).
- Because with function symbols, to make a substructure, we must pay attention to the closedness of its domain under the functions.
- However, the lack of functions is not a strong restriction. For example, addition $+$ of $(\mathbb{N},+)$ can replaced by the following relation R.

$$R(n, m, k) \Leftrightarrow n + m = k$$

- Then, for any set $A \subset \mathbb{N}$, $(A, R \cap A^3)$ is always a substructure of $(\mathbb{N}, +)$.
- Note that for the set A of odd numbers, $(A, +)$ is no longer a (sub)structure.

- We will consider a language of finitely many relation symbols and constants. So, let $\mathcal{L}$ be $\{\mathrm{R}_0, \ldots, \mathrm{R}_{n-1}\}$, and consider its extensions by adding constants.
- The structure $\mathcal{A}$ in $\mathcal{L}$ can be expressed as

$$\mathcal{A} = (A, \mathrm{R}_0^{\mathcal{A}}, ..., \mathrm{R}_{n-1}^{\mathcal{A}}).$$

- Then, for any $B \subset A$, we define a substructure

$$\mathcal{A} \upharpoonright B = (B, \mathrm{R}_0^{\mathcal{A}} \cap B^{k_0}, \ldots, \mathrm{R}_{n-1}^{\mathcal{A}} \cap B^{k_{n-1}}).$$

- By naming $\vec{a} = (a_1, \cdots, a_k)$ of A^k by constants $\vec{c}$, we obtain a structure $(\mathcal{A}, \vec{a})$ in language $\mathcal{L} \cup \{\vec{c}\}$.

The following definition applies to any language $\mathcal{L}$ possibly with function symbols.

Definition (Quantifier Rank)

For a formula φ, the **(quantifier) rank** of φ, denoted as $\mathrm{qr}(\varphi)$, is defined recursively as follows,

- $\mathrm{qr}(\text{atomic formulas}) = 0$,
- $\mathrm{qr}(\neg\varphi) = \mathrm{qr}(\varphi)$, $\qquad \mathrm{qr}(\varphi \land \psi) = \max\{\mathrm{qr}(\varphi), \mathrm{qr}(\psi)\}$,
- $\mathrm{qr}(\forall x\varphi) = \mathrm{qr}(\exists x\varphi) = \mathrm{qr}(\varphi) + 1$.

Example

The rank of the formula $\forall y(\forall x\exists y(x = y) \land \forall z(z > 0))$ is 3.

Lemma (1)

Consider a finite relational language $\mathcal{L} = \{\mathrm{R}_0, \ldots, \mathrm{R}_{l-1}\}$. For a fixed number n, there are essentially finitely many formulas with rank $\leq n$ in fixed free variables $x_1, ..., x_k$.

Proof.

- We prove by induction on quantifier rank n.
- Suppose $\mathbf{n = 0}$. Then a formula with rank 0 has no quantifiers.
- There are only essentially finitely many atomic formulas $\mathrm{R}(w_1, \ldots, w_i)$, since $\mathcal{L}$ is finite and $w_1, \ldots, w_i$ are chosen from $x_1, ..., x_k$.
- There are only finitely many clauses (disjunctions $\vee$ of atomic formulas and their negations).
- There are only finitely many CNF's (conjunctions $\wedge$ of clauses).
- Since any formula without quantifiers can be transformed into an equivalent CNF, there are essentially only finitely many formulas with rank 0 in $x_1, ..., x_k$.

- **Induction Step**. Assume that given k many variables (k is finite), there are only finitely many formulas with rank $\leq n$ in the variables.
- Let $\varphi(x_1, ..., x_k)$ be any formula with rank $n+1$ in free variables $x_1, ..., x_k$.
- Without loss of generality, we may assume that it is of the form $\mathrm{Q}x_{k+1}\theta(x_1, ..., x_k, x_{k+1})$, where x_{k+1} is a variable other than $x_1, ..., x_k$.
- Then, $\theta(x_1, ..., x_k, x_{k+1})$ is a formula of rank n in free variables $x_1, ..., x_k, x_{k+1}$. By induction hypothesis, there are only finitely many such $\theta(x_1, ..., x_k, x_{k+1})$.
- Therefore, there are only finitely many formulas of the form $\mathrm{Q}x_{k+1}\theta(x_1, ..., x_k, x_{k+1})$. Since the general formulas of rank $n+1$ in free variables $x_1, ..., x_k$ are obtained from formulas of the form $\mathrm{Q}x_{k+1}\theta(x_1, ..., x_k, x_{k+1})$ by propositional connectives, there are only finitely many formulas with rank $n+1$ in free variables $x_1, ..., x_k$, which can be shown in the same way as a CNF in the case of $n = 0$. □

The following definition also applies to a general language $\mathcal{L}$.

Definition

The **theory** of a structure $\mathcal{A}$ in $\mathcal{L}$, denoted $\mathrm{Th}(\mathcal{A})$, is the set of sentences in $\mathcal{L}$ that hold in $\mathcal{A}$. Two structures with the same theory are said to be **elementary equivalent**, denoted by $\mathcal{A} \equiv \mathcal{B}$. That is,

$$\mathcal{A} \equiv \mathcal{B} \quad \Leftrightarrow \quad \mathrm{Th}(\mathcal{A}) = \mathrm{Th}(\mathcal{B}) \quad \Leftrightarrow \quad \mathcal{B} \models \mathrm{Th}(\mathcal{A}).$$

- $\mathcal{A}$ is an elementary substructure of $\mathcal{B}$, denoted as $\mathcal{A} \prec \mathcal{B}$, iff $\mathrm{Th}(\mathcal{A}_A) = \mathrm{Th}(\mathcal{B}_A)$, which implies $\mathcal{A} \equiv \mathcal{B}$

Definition

Let $\mathrm{Th}_n(\mathcal{A})$ denote the subset of $\mathrm{Th}(\mathcal{A})$ consisting of sentences with $\leq n$. For structures $\mathcal{A}, \mathcal{B}$ in the same language $\mathcal{L}$, a relation $\equiv_n$ between them is defined as follows.

$$\mathcal{A} \equiv_n \mathcal{B} \Leftrightarrow \mathrm{Th}_n(\mathcal{A}) = \mathrm{Th}_n(\mathcal{B}).$$

Definition

Let $\mathcal{A}, \mathcal{B}$ be structures in $\mathcal{L}$. A partial function $f : A \to B$ is a **partial isomorphism** if $\mathcal{A} \restriction \mathrm{dom(f)}$ and $\mathcal{B} \restriction \mathrm{range(f)}$ are isomorphic via f.

If $\mathrm{dom}(f) = \vec{a}$, then the above definition is equivalent to

$$(\mathcal{A}, \vec{a}) \equiv_0 (\mathcal{B}, f(\vec{a})).$$

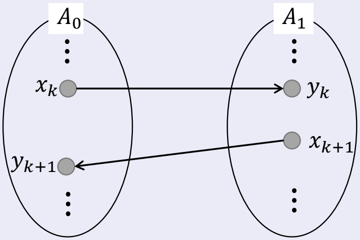
It is obvious that "if $\mathcal{A} \cong \mathcal{B}$, then $\mathcal{A} \equiv \mathcal{B}$". Fraïssé showed a weak version of its reversal by using quantifier ranks. Ehrenfeucht reformulated Fraïssé's argument in terms of games. Now such a technique is referred to as the Ehrenfeucht-Fraïssé game (EF game).

Definition

Let $\mathcal{A}_0$, $\mathcal{A}_1$ be structures of $\mathcal{L}$ and n be a natural number. In an n-round **EF game**, $\mathrm{EF}_n(\mathcal{A}_0, \mathcal{A}_1)$, player I (Spoiler) and player II (Duplicator) alternately choose from A_i $(i = 0, 1)$ obeying the rules described below, and the winner is determined according to the winning condition.

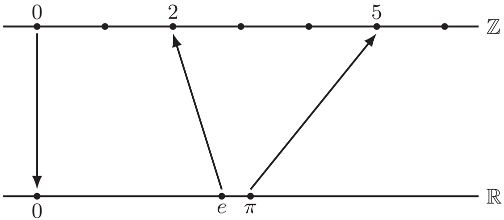
- **Rules**: if I chooses $x_i \in A_j$ $(j = 0, 1)$, II chooses $y_i \in A_{1-j}$.

- **Winning conditions**: If the correspondence $x_i \leftrightarrow y_i$ chosen by the players up to n rounds determines a partial isomorphism of $\mathcal{A}_0$ and $\mathcal{A}_1$, then II wins.



Example: $\mathrm{EF}_3((\mathbb{Z},<),(\mathbb{R},<))$

- Consider $\mathrm{EF}_3(\mathcal{A},\mathcal{B})$ where $\mathcal{A}=(\mathbb{Z},<),\mathcal{B}=(\mathbb{R},<)$.
- In the following, $e\in\mathbb{R}\to 2\in\mathbb{Z}$ represents that player I selects $e\in\mathbb{R}$ and then player II chooses $2\in\mathbb{Z}$.
- For example, if $e\in\mathbb{R}\to 2\in\mathbb{Z}$; $0\in\mathbb{Z}\to 0\in\mathbb{R}$; $\pi\in\mathbb{R}\to 5\in\mathbb{Z}$ are produced in the game, player II wins because $\{(0,0),(2,e),(5,\pi)\}$ is a partial isomorphism (order preserving).



Definition

$\mathcal{A} \simeq^n \mathcal{B}$ if player II has a winning strategy in $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$.

Note that if $\mathcal{A} \simeq^n \mathcal{B}$ then $\mathcal{B} \simeq^n \mathcal{A}$. We can easily show the following lemma.

Lemma (2)

Let $\mathcal{A}$ and $\mathcal{B}$ be structures of the same language.

$$
\begin{aligned}
(\mathcal{A}, \vec{a}) \simeq^0 (\mathcal{B}, \vec{b}) &\Leftrightarrow \ \vec{a} \mapsto \vec{b} \text{ is partial isomorphism.} \\
&\Leftrightarrow \ (\mathcal{A}, \vec{a}) \equiv_0 (\mathcal{B}, \vec{b}). \\
(\mathcal{A}, \vec{a}) \simeq^{n+1} (\mathcal{B}, \vec{b}) &\Leftrightarrow \ \forall a \in A \exists b \in B (\mathcal{A}, \vec{a}a) \simeq^n (\mathcal{B}, \vec{b}b) \text{ and} \\
&\qquad \forall b \in B \exists a \in A (\mathcal{A}, \vec{a}a) \simeq^n (\mathcal{B}, \vec{b}b)
\end{aligned}
$$

As you might expect from the above lemma, $\mathcal{A} \simeq^n \mathcal{B}$ and $\mathcal{A} \equiv_n \mathcal{B}$ are equivalent, which is the essence of the EF theorem. To this end, we introduce the Scott-Hintikka formulas.

Definition (Scott-Hintikka Formula)

For a structure $\mathcal{A}$ and a sequence of elements $\vec{a}$, the **Scott-Hintikka formula** of rank n, $\varphi^n_{\mathcal{A},\vec{a}}(\vec{x})$, is defined inductively as follows.

$$\varphi^0_{\mathcal{A},\vec{a}}(\vec{x}) = \bigwedge \{\theta(\vec{x}) : (\mathcal{A},\vec{a}) \models \theta(\vec{c}),\ \mathrm{qr}(\theta(\vec{x})) = 0\}.$$

$$\varphi^{n+1}_{\mathcal{A},\vec{a}}(\vec{x}) = \bigwedge_{a \in A} \exists x \varphi^n_{\mathcal{A},\vec{a}a}(\vec{x},x) \wedge \forall x \bigvee_{a \in A} \varphi^n_{\mathcal{A},\vec{a}a}(\vec{x},x).$$

- When we write $(\mathcal{A},\vec{a}) \models \theta(\vec{c})$, $\vec{c}$ are new constants interpreted as $\vec{a}$.
- In the above definition, even if A is infinite, by Lemma (1), there are finitely many formulas in the scopes of $\bigwedge, \bigvee$. So, the Scott-Hintikka formula can be defined as an first-order formula.

Lemma (3)

$(\mathcal{A}, \vec{a}) \models \varphi^n_{\mathcal{A},\vec{a}}(\vec{c})$.

Proof

- When $n = 0$, it is clear from the definition.
- Then, we want to show $(\mathcal{A}, \vec{a}) \models \varphi^{n+1}_{\mathcal{A},\vec{a}}(\vec{c})$ from the induction hypothesis. We first consider $\bigwedge_{a\in A} \exists x \varphi^n_{\mathcal{A},\vec{a}a}(\vec{c}, x)$, which is the left component of the definition formula of $\varphi^{n+1}_{\mathcal{A},\vec{a}}(\vec{c})$.
- For every $a \in A$, letting $x = a$, we have $\varphi^n_{\mathcal{A},\vec{a}a}(\vec{c}, c)$, which holds in $(\mathcal{A}, \vec{a}a)$ from the induction hypothesis. So, the left formula holds for $(\mathcal{A}, \vec{a}a)$.
- We next consider the right formula $\forall x \bigvee_{a\in A} \varphi^n_{\mathcal{A},\vec{a}a}(\vec{c}, x)$. Let x be an arbitrary $a \in A$, and then select the same a for the $\bigvee_{a\in A}$, we have $\varphi^n_{\mathcal{A},\vec{a}a}(\vec{c}, c)$, which also holds from the induction hypothesis. So, the right formula also holds for $(\mathcal{A}, \vec{a}a)$.
- Therefore, the conjunction of both formulas holds in $(\mathcal{A}, \vec{a}a)$. $\square$

Theorem (Ehrenfeucht-Fraïss theorem, EF theorem)

For all $n \geq 0$, the following are equivalent.
(1) $(\mathcal{A}, \vec{a}) \equiv_n (\mathcal{B}, \vec{b})$, (2) $(\mathcal{B}, \vec{b}) \models \varphi^n_{\mathcal{A},\vec{a}}(\vec{c})$, (3) $(\mathcal{A}, \vec{a}) \simeq^n (\mathcal{B}, \vec{b})$.

Proof. (1) ⇒(2). It is obvious from the Lemma (3), since qr$(\varphi^n_{\mathcal{A},\vec{a}}(\vec{x})) = n$.
To show (2) ⇒(3). By induction on n.For $n = 0$, (2)⇒ $(\mathcal{A}, \vec{a}) \equiv_0 (\mathcal{B}, \vec{b}) \Rightarrow (3)$.
For induction step, assume (2) ⇒(3) for n as well as $(\mathcal{B}, \vec{b}) \models \varphi^{n+1}_{\mathcal{A},\vec{a}}(\vec{c})$. From the definition of the Scott-Hintikka formula,

$$\forall a \in A \exists b \in B (\mathcal{B}, \vec{b}b) \models \varphi^n_{\mathcal{A},\vec{a}a}(\vec{c}, c) \ \wedge \ \forall b \in B \exists a \in A (\mathcal{B}, \vec{b}b) \models \varphi^n_{\mathcal{A},\vec{a}a}(\vec{c}, c)$$

By the induction hypothesis, we have

$$\forall a \in A \exists b \in B (\mathcal{A}, \vec{a}a) \simeq^n (\mathcal{B}, \vec{b}b) \ \wedge \ \forall b \in B \exists a \in A (\mathcal{A}, \vec{a}a) \simeq^n (\mathcal{B}, \vec{b}b).$$

By the Lemma (2), we obtain

$$(\mathcal{A}, \vec{a}) \simeq^{n+1} (\mathcal{B}, \vec{b}).$$

Thus, (3) also holds for $n + 1$.

To show (3) $\Rightarrow$(1). By induction on n.

- Case $n = 0$ follows from Lemma (2).
- For induction step, assume (3) $\Rightarrow$ (1) for n as well as $(\mathcal{A}, \vec{a}) \simeq^{n+1} (\mathcal{B}, \vec{b})$. To show $(\mathcal{A}, \vec{a}) \equiv_{n+1} (\mathcal{B}, \vec{b})$, the essential case to check is a formula $\varphi(\vec{x}) = \exists x \psi(\vec{x}, x)$ with qr$(\psi(\vec{x}, x)) = n$.
- Suppose $(\mathcal{A}, \vec{a}) \models \varphi(\vec{c})$. Then, there exists $a \in A$ such that $(\mathcal{A}, \vec{a}a) \models \psi(\vec{c}, c)$.
- Since $(\mathcal{A}, \vec{a}) \simeq^{n+1} (\mathcal{B}, \vec{b})$, by Lemma (2), there exists a $b \in B$ such that $(\mathcal{B}, \vec{b}b) \models \psi(\vec{c}, c)$.
- Thus $(\mathcal{B}, \vec{b}) \models \varphi(\vec{c})$. This proves $\mathrm{Th}_{n+1}(\mathcal{A}, \vec{a}) \subset \mathrm{Th}_{n+1}(\mathcal{B}, \vec{b})$. Similarly, we have $\mathrm{Th}_{n+1}(\mathcal{A}, \vec{a}) \supset \mathrm{Th}_{n+1}(\mathcal{B}, \vec{b})$, and so (1) holds. $\square$

Corollary

$\mathcal{A} \equiv \mathcal{B} \Leftrightarrow$ for any n, $\mathcal{A} \simeq^n \mathcal{B}$.

It is natural to extend the play of the EF game to infinity (ω-round). Such a game is denoted as $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$. We write $\mathcal{A} \simeq^\omega \mathcal{B}$ if player II has a winning strategy in $\mathrm{EF}_\omega(\mathcal{A}, \mathcal{B})$.

Corollary

Suppose $\mathcal{A}, \mathcal{B}$ are countable. Then, $\mathcal{A} \simeq^\omega \mathcal{B} \;\Leftrightarrow\; \mathcal{A} \simeq \mathcal{B}$.

Proof. $\Leftarrow$ is obvious because the isomorphism is a winning strategy for player II.
$\Rightarrow$ is shown by the **back-and-forth argument**. Let $A = \{a_0, a_1, \dots\}$, $B = \{b_0, b_1, \dots\}$. Player II follows the winning strategy, and Player I alternately chooses the smallest element that have not been selected from A and B, thus a bijection between $\mathcal{A}$ and $\mathcal{B}$ is produced, which is a desired isomorphism. □

Corollary

For each n, there are finitely many equivalence classes of $\mathcal{L}$-structure by $\equiv_n$.

Proof By Lemma (1), there are essentially finitely many Scott-Hintikka sentences $\varphi^n_{\mathcal{A},\varnothing}$ with rank n. By the EF theorem, each $\equiv_n$ equivalence class is characterized by such a sentence, and so there are only a finite number of them. □

Corollary

Let K be a set of $\mathcal{L}$-structures. The following are equivalent.

(1) For any n, there exist $\mathcal{A} \in K$ and $\mathcal{B} \notin K$ such that $\mathcal{A} \equiv_n \mathcal{B}$.

(2) K is not an elementary class (K cannot be defined by a first-order formula).

Proof.

- (1) $\Rightarrow$(2). By way of contraposition, assume K is defined by a first-order sentence φ. Let n be the rank of φ. If $\mathcal{A} \in K$ and $\mathcal{B} \notin K$ then $\mathcal{A} \not\equiv_n \mathcal{B}$.
- (2) $\Rightarrow$(1). By way of contraposition, assume that for some n, if $\mathcal{A} \equiv_n \mathcal{B}$ then $\mathcal{A} \in K \Leftrightarrow \mathcal{B} \in K$. Since there is a first-order (Scott-Hintikka) sentence $\varphi^n_{\mathcal{A}}$ of rank n such that $\mathcal{A} \equiv_n \mathcal{C} \Leftrightarrow \mathcal{C} \models \varphi^n_{\mathcal{A}}$, K is defined by $\varphi^n_{\mathcal{A}}$. □

Summary

- We consider a language of finitely many relation symbols and constants.
- The (quantifier) rank of a formula measures the entanglement of quantifiers appearing in it. For example, the rank of $\forall y(\forall x \exists y(x = y) \wedge \forall z(z > 0))$ is 3.
- By $\mathcal{A} \equiv_n \mathcal{B}$, we mean that structures $\mathcal{A}, \mathcal{B}$ satisfy the same formulas with rank $\leq n$.
- There are essentially finitely many formulas with rank $\leq n$ in fixed free variables $x_1, \ldots, x_k$. Thus we can define the **Scott-Hintikka sentence** $\varphi^n_{\mathcal{A}}$ of rank n such that $\mathcal{A} \equiv_n \mathcal{C} \Leftrightarrow \mathcal{C} \models \varphi^n_{\mathcal{A}}$.
- By $\mathcal{A} \simeq^n \mathcal{B}$, we mean that player II has a winning strategy in $\mathrm{EF}_n(\mathcal{A}, \mathcal{B})$.
- **EF theorem** For all $n \geq 0$, $\mathcal{A} \equiv_n \mathcal{B}$ iff $\mathcal{A} \simeq^n \mathcal{B}$.
- **Corollary** The following are equivalent.
  (1) For any n, there exist $\mathcal{A} \in K$ and $\mathcal{B} \notin K$ such that $\mathcal{A} \equiv_n \mathcal{B}$.
  (2) K is not an elementary class (K cannot be defined by a first-order formula).

Further readings

Jouko Väänänen, Models and Games, Cambridge University Press, 2011.

Thank you for your attention!