Logic and Computation II

Part 5. Automata on infinite objects

Kazuyuki Tanaka

BIMSA

April 11, 2023

Logic and Computation II

- **Part 4. Formal arithmetic and Gödel's incompleteness theorems**
- **Part 5. Automata on infinite objects**
- **Part 6. Recursion-theoretic hierarchies**
- **Part 7. Admissible ordinals and second order arithmetic**

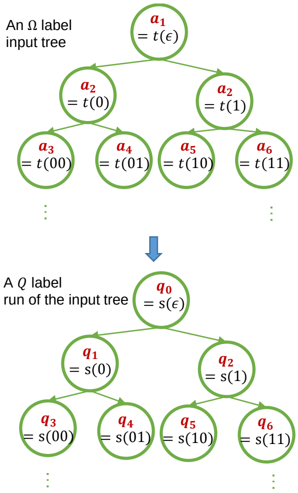
Part 4. Schedule

- Mar.28, (1) Automata on infinite strings
- Mar.30, (2) The decidability of S1S
- Apr. 4, (3) Tree automata
- Apr. 6, (4) The decidability of S2S
- Apr.11, (5) Finite model theory
- Apr.13, (6) Parity games

Today's topics

Recap

- The **tree automaton** $M = (Q, \Omega, \delta, Q_0, Acc)$:
  - $\delta \subseteq Q \times \Omega \times Q^2$: a transition relation,
  - Acc: an acceptance conditions.
- For an input Ω-labeled tree $t : \{0,1\}^* \to \Omega$, a run-tree of M is a Q-labeled tree $s : \{0,1\}^* \to Q$ such that
  - $s(\epsilon) \in Q_0$, where ϵ is the root of the tree.
  - for any $u \in \{0,1\}^*$, $(s(u), t(u), s(u0), s(u1)) \in \delta$.
- For a Q-labeled tree s and an infinite path α, $s(\alpha)$ denotes the ω-sequence of states on α in s. $\mathsf{Inf}(s(\alpha))$ denotes the set of states which appears infinitely often on $s(\alpha)$.
- An input tree t is accepted by a tree automaton M iff there is a run-tree s in which all its infinite paths $s(\alpha)$ satisfy:
  - For MTA M, Acc is $\mathcal{F}(\subseteq \mathcal{P}(Q))$: $\mathsf{Inf}(s(\alpha)) \in \mathcal{F}$.
  - For PTA M, Acc is $\pi : Q \to \{0, 1, \ldots, k\}$: $\min\{\pi(q) : q \in \mathsf{Inf}(s(\alpha))\}$ is even.



- PTA $\leftrightarrow$ MTA.
- The tree languages accepted by PTA's are closed under complement.
- It is decidable whether the accepted language of PTA is empty or not.
- Any S2S formula $\varphi(\vec{X})$ has an equivalent MTA M_φ, and vice versa.
- S2S is decidable.

Introduction

- Second-order logic is also very useful for describing classes of finite structures, and its hierarchy is closely linked to the computational complexity.
- We first review some popular classes of first-order formulas. Then, we discuss Fagin's famous theorem on the equivalence between Σ^1_1 formulas and NP problems.
- Let FO be the set of all first-order sentences in $\mathcal{L}$. For simplicity, assume that $\mathcal{L}$ is finite. Also, we do not discriminate between a formula and its Gödel number.
- Now, define the following subsets of FO.
  - $\mathrm{Sat} := \{\varphi \in \mathrm{FO} : \varphi$ has a model (satisfiable)$\}$.
  - $\mathrm{FinSat} := \{\varphi \in \mathrm{FO} : \varphi$ has a finite model$\}$.
  - $\mathrm{InfSat} := \mathrm{Sat} - \mathrm{FinSat} = \{\varphi \in \mathrm{FO} : \varphi$ has only infinite models$\}$.
  - $\mathrm{Valid} := \{\varphi \in \mathrm{FO} : \varphi$ is true for all structures$\}$.
  - $\mathrm{FinVal} := \{\varphi \in \mathrm{FO} : \varphi$ is true for all finite structures)$\}$.

Lemma

About the five subsets of FO, the following hold.

(1) Valid is CE (Σ_1).
(2) Sat is co-CE (Π_1).
(3) FinSat is CE.
(4) InfSat is co-CE.
(5) FinVal is co-CE.

Proof

(1) By the completeness theorem, $\varphi \in \mathrm{Valid} \Leftrightarrow \vdash \varphi$, and by the theorem on p.17 of Slide 04-03, the right-hand side is CE, so is the left-hand side.

(2) It follows from $\varphi \in \mathrm{Sat} \Leftrightarrow \neg\varphi \notin \mathrm{Valid}$.

(3) Enumerate the finite structures, and sequentially check whether φ holds in a finite structure. If one finds a model of φ, the algorithm terminates successfully. Otherwise, it does not halt. Thus, FinSat is CE.

(4) The complement of InfSat is $(\mathrm{FO} - \mathrm{Sat}) \cup \mathrm{FinSat}$, which is CE.

(5) Clear from $\varphi \in \mathrm{FinVal} \Leftrightarrow \neg\varphi \notin \mathrm{FinSat}$. □

- Let $\mathcal{L}$ be a finite (or recursive) language containing $\mathcal{L}_{\mathrm{OR}}$. Then we will show that none of the above five classes are decidable (computable, recursive).
- Since the provability of first-order logic is undecidable, Valid and Sat are also undecidable by the completeness theorem.
- To simplify the discussion for the remaining three classes, we assume that $\mathcal{L}$ has sufficiently (but finitely) many relation symbols.
- The proof of the following theorem is almost the same as Turing's proof of the undecidability of first-order logic, and the details also overlap with the proof of Cook's theorem.

Theorem (Trakhtenbrot's theorem (1950)[1])

FinSat is not decidable.

[1] Boris Trakhtenbrot. Born in Moldova, Eastern Europe. He taught in Russia and lived in Israel in his later years.

Proof

- Let $M = (Q, \Omega, \delta, Q_0, F)$ be a universal Tm with one tape, and $Q = \{q_0, q_1, \ldots, q_{m-1}\}$, $Q_0 = \{q_0\}$ and $\Omega = \{0, 1\}$.
- In the following, we will define a first-order sentence Ψ_w which means "M accepts $w \in \Omega^*$ " and then show $w \in L(M) \Leftrightarrow \Psi_w \in \mathrm{FinSat}$. Since $w \in L(M)$ is undecidable as a halting problem, FinSat is also undecidable.
- The sentence Ψ_w is constructed by encoding the computation process of M on input w and embedding it in a finite structure $\mathcal{A}$.
- First, assume that the language of $\mathcal{A}$ contains the symbol $<$, and add the assertion that "$<$ is a linear order on A" to Ψ_w.
- Then, if $|A| = n$, then A can be identified with $\{0, 1, \ldots, n-1\}$.
- We do not rule out the possibility of $|A| = \infty$ in the definition of Ψ_w, but since we only treat finite structures, we do not need to think about the infinite case.

- We consider the elements $0, 1, \ldots, n-1$ of A represent both the time (steps) of the computation and the position of the tape.
- Then, $\mathcal{L}$ is assumed to have the relational symbols $T_i(t,p)$ $(i = 0, 1, B)$, which indicates that i is written on the tape in position p at time t, and also the relation symbols $H_q(t,p)$ $(q \in Q)$, which means "at time t, the head is at position p and the internal state is q".
- We can describe the transition function δ as first-order relations among $T_i(t,p)$ and $H_q(t,p)$ (see the proof of Cook's theorem), and put them into Ψ_w. Also, add the initial configuration $\forall p T_{w(p)}(0,p) \wedge H_{q_0}(0,0)$ and the accepting condition $\exists t \exists p\ \exists q_f \in F H_{q_f}(t,p)$ to Ψ_w.
- Then it is clear that w is accepted by M if and only if Ψ_w has a finite model $\mathcal{A}$. $\square$

The language $\mathcal{L}$ of Ψ_w in the above proof includes $\{<, T_0, T_1, T_B, H_{q_0}, \ldots, H_{q_{n-1}}\}$. But it is known that if $\mathcal{L}$ has a binary function, then Trakhtenbrot's theorem holds. A related fact is that group theory and finite group theory are undecidable (Tarski, Mal'cev).

Corollary

FinVal is not decidable.

Proof $\varphi \in \mathrm{FinVal} \Leftrightarrow \neg\varphi \notin \mathrm{FinSat}$ and so Trakhtenbrot's theorem implies the corollary. □

Before dealing with InfSat, let us define the following useful concepts.

Definition

$T \subset \mathrm{FO}$ is said to have the **finite model property** if $T \cap \mathrm{Sat} = T \cap \mathrm{FinSat}$.

Lemma

If $T \subset \mathrm{FO}$ is decidable and has the finite model property, then $T \cap \mathrm{Sat}$ is decidable.

Proof If T is decidable, by lemma in Page 7 of this slides, $T \cap \mathrm{Sat}$ is co-CE and $T \cap \mathrm{FinSat}$ is CE. By the f.m.p., $T \cap \mathrm{Sat} = T \cap \mathrm{FinSat}$, and so it is decidable. □

Corollary

InfSat is not decidable.

Proof

- B.W.O.C., assume that InfSat is decidable.
- Then its complement $\mathrm{FO} - \mathrm{InfSat}$ is also decidable. Since

$$(\mathrm{FO} - \mathrm{InfSat}) \cap \mathrm{Sat} = \mathrm{FinSat},$$

  $\mathrm{FO} - \mathrm{InfSat}$ has finite model property. By the lemma in Page 11 of this slides, FinSat is also decidable.
- However, this contradicts the Trakhtenbrot's theorem, which denies our assumption. That is, InfSat is not decidable. $\square$

- Trachtenbrot's theorem means that in the world of finite structures, the validity cannot be formalized as a deductive system.
- As can be expected from this fact, most properties of ordinary first-order logic does not hold in that world.

Lemma (Noncompactness of finite model theory)

There exists a theory $T(\subset \mathrm{FO})$ such that any finite part $S \subset T$ has a finite model, but the whole T does not have a finite model.

Proof Let σ_n be the following formula which means that there are at least n elements

$$\sigma_n := \exists x_0 \ldots \exists x_{n-1} \bigwedge_{i<j<n} x_i \neq x_j.$$

Obviously, the theory $T := \{\sigma_n : n \in \mathbb{N}\}$ satisfies the lemma. □

In addition, fundamental theorems of first-order logic, such as E. Beth's definability theorem and W. Craig's interpolation theorem, do not hold.

- Next we consider the following problem: for a fixed formula, to decide whether or not a given finite structure satisfies the formula.
- To do this, we must code a finite structure as a string. Let n be the number of elements in a finite structure. Then a subset of the domain can be encoded with a binary sequence of length n, and general relations and functions on the domain with sequences of length n^k, where k is an arbitrary constant. In sum, the code size of a finite structure with n elements is about n^k.
- On the other hand, in order to evaluate a logical expression, it is necessary to memorize the values of variables during the computation, which requires the space in a constant multiple of $\log n$, which is the same as a constant multiple $\log$ of input length n^k. So, the computational complexity is the deterministic log-space L. This claim is often is represented as

$$\mathsf{FO} \subset \mathsf{L}$$

- Now we consider finite model theory of second-order logic SO.
- A second-order logical expression $\exists R_1 \ldots \exists R_n \varphi(R_1, \ldots, R_n)$ (with first-order φ) is called **existential second-order formula** (ESO for short) or Σ^1_1.
- Similarly, the formula obtained by binding with universal second-order quantifiers is called **universal second-order formula** (USO for short) or Π^1_1.
- If all quantified relations (variables) are unary (set variables), they are called m-Σ^1_1 and m-Π^1_1, respectively, where m stands for *monadic*.
- We start with investigating properties of graphs. A graph $G = (V, E)$, either finite or infinite, can be viewed as a first-order structure in which the set of vertices V is a domain and the set of edges E is a binary relation on it. The property of the following example cannot be expressed by a first-order formula, but can be expressed by a second-order formula.

Examples

(1) The non-connectivity of $G = (V, E)$ can be expressed by an m-Σ^1_1 formula as follows.

$$\exists S(\exists x S(x) \land \exists y \neg S(y) \land \forall x, y(S(x) \land \neg S(y) \to \neg E(x, y))).$$

Its negation, i.e., connectivity, cannot be represented by m-Σ^1_1.

(2) The fact that a (directed/undirected) graph $G = (V, E)$ has a Hamiltonian path can be represented by Σ^1_1 as follows.

$$\exists < (\text{“} < \text{is a linear order over } V\text{”} \land \forall x, y(\neg \exists z(x < z < y) \to E(x, y))).$$

This can not be expressed by m-Σ^1_1 nor any MSO.

Homework

Write an m-Σ^1_1 formula expressing that the vertices of the graph $G = (V, E)$ can be painted with k colors so that adjacent vertices have different colors.

Here are some basic facts about finite structures.

Lemma

The problem of whether or not a finite structure has a property represented by Σ^1_1 is NP.

Proof

- Let $\exists\vec{R}\varphi(\vec{R})$ be a Σ^1_1 formula.
- Given a finite structure $\mathcal{A}$, we nondeterministically choose a relation $\vec{R}$ on A and check whether $(\mathcal{A}, \vec{R})$ satisfies $\varphi(\vec{R})$ or not.
- Since FO $\subseteq$ L $\subseteq$ P and $\vec{R}$ (the code $\leq n^k$) is chosen nondeterministically, this problem is NP.

$\square$

Surprisingly, the converse of the above lemma also holds. The proof is similar to that of Trachtenbrot's theorem. The key point is that binary relations $<$, relations T_i and H_q appear as second-order existential quantifiers.

Theorem (Fagin's Theorem (1973))

An NP problem can be expressed as Σ_1^1 on finite structures .

Proof

- Let $M = (Q, \Omega, \delta, Q_0, F)$ determine an NP problem nondeterministically in TIME(n^k). Suppose $Q = \{q_0, q_1, \ldots, q_{m-1}\}$, $Q_0 = \{q_0\}$ and $\Omega = \{0, 1\}$.
- Given a finite structure $\mathcal{A}$, assume that there exists a linear order $<$ on A. So, if $|A| = n$ then A can be identified with $\{0, 1, \ldots, n-1\}$.
- Since M works within time n^k, the time can be represented by a k-tuple $\vec{t}$ of elements in the structure. Hence, the head position on the tape can also be represented by a k-tuple $\vec{p}$.
- Then, with these arguments, let $T_i(\vec{t}, \vec{p})$ represent "at time $\vec{t}$ and on the tape position $\vec{p}$, a symbol $i = 0, 1, B$ is written," and $H_q(\vec{t}, \vec{p})$ "at time $\vec{t}$, the head is on position $\vec{p}$ and the internal state is q."
- In addition, add the formulas describing the initial configuration and the accepting condition into Ψ (cf. Trakhtenbrot's theorem).
- Then, the NP problem can be decided by checking whether or not the Σ_1^1 formula $\exists < \exists(T_0, T_1, T_B)\exists(H_{q_0}, \ldots, H_{q_{n-1}})\Psi$ holds in $\mathcal{A}$.

The above theorem immediately leads to Cook's theorem.

Corollary

SAT is NP-complete.

Proof

- SAT can be viewed as ESO and so it is NP.
- By Fagin's theorem, any NP problem can be expressed by a fixed ESO formula on a finite structure. Since a first-order quantifier on a structure with n elements can be identified with a conjunction or disjunction of n components, a first-order formula on it can be converted to a Boolean formula of length n^k.
- Hence, ESO on a finite structure can be converted to SAT. Therefore, SAT is NP-hard. □

Thank you for your attention!