Logic and Computation: I

Chapter 1 Introduction to theory of computation

Kazuyuki Tanaka

BIMSA

November 15, 2022

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 1. Schedule

- Oct.27, (1) Automata and monoids
- Nov. 1, (2) Turing machines
- Nov. 3, (3) Computable functions and primitive recursive functions
- Nov. 8, (4) Computability and incomputability
- Nov.10, (5) Partial recursive functions and computable enumerable sets
- Nov.15, (6) Rice's theorem and many-one reducibility

Recap

- If a partial computable function $f : \mathbb{N}^k \longrightarrow \mathbb{N}$ is realized by a TM $\mathcal{M}$ with index e, f is denoted by $\{e\}^k$ (or simply $\{e\}$). When e is not an index of TM, $\{e\}$ is regarded as a partial function with empty domain.
- Enumeration theorem: For any $n \geq 0$, there exists a natural number e_n such that

$$\{e_n\}^{n+1}(d, x_1, \ldots, x_n) \sim \{d\}^n(x_1, \ldots, x_n), \quad \text{for any } d, x_1, \ldots, x_n.$$

  $f(x_1, \ldots, x_n) \sim g(x_1, \ldots, x_n)$ means either both sides are not defined or they are defined with the same value.
- A set $X \subset \mathbb{N}^n$ is said to be computably enumerable or CE if $\{1^{x_1}0 \cdots 01^{x_n} : (x_1, \ldots, x_n) \in X\}$ is 0-type, i.e., the domain of a partial recursive function.
- X is said to be computable if both X and X^c are CE.
- A halting program $\mathrm{K} = \{e : \{e\}(e) \downarrow\}$ is CE but not computable.

Recap

- The partial recursive functions are the smallest class that contains the constant 0, the successor function, projections, and closed under composition, primitive recursion and minimalization.
- Kleene normal form theorem: There are a primitive recursive function $U(y)$ and a primitive recursive relation $T_n(e, x_1, \cdots, x_n, y)$ such that for any e, there exists d s.t.

$$\{e\}(x_1, \cdots, x_n) \sim U(\mu y T_n(d, x_1, \cdots, x_n, y)).$$

- Parameter theorem: There exists a primitive recursive function $S_n^m : \mathbb{N}^{m+1} \to \mathbb{N}$ s.t.

$$\{e\}^{m+n}(x_1, \cdots, x_n, y_1, \cdots, y_m) \sim \{S_n^m(e, y_1, \cdots, y_m)\}^n(x_1, \cdots, x_n).$$

- Recursion theorem: For any d, there exists e such that $\{e\}^n(x_1, \cdots, x_n) \sim \{d\}(x_1, \cdots, x_n, e)$.

Recap

- Ackermann function is a (total) recursive function by the recursion theorem. However, it is not a primitive recursive function, though its graph is primitive recursive.
- Definition of recursively enumerable relation and its equivalent statements.

(1) R is the domain of a partial recursive function.

(2) R the range of a partial recursive function (a recursive 1-to-1 function or a primitive recursive function).

(3) There exists a primitive recursive relation S such that

$$R(x_1, \cdots, x_n) \Leftrightarrow \exists y S(x_1, \cdots, x_n, y).$$

Rice's theorem and many-one reducibility

- A set C is called an **index set** $\Leftrightarrow$ if $e \in C$ and $\{e\} \sim \{d\}$ then $d \in C$.
- **Rice's theorem** asserts that for a nontrivial class of partial recursive functions $\mathcal{C}$, its index set $C = \{e : \{e\} \in \mathcal{C}\}$ is not computable.

Theorem (Rice's theorem [1])

Any nontrival (neither $\mathbb{N}$ nor $\varnothing$) index set is noncomputable.

CLASSES OF RECURSIVELY ENUMERABLE SETS AND THEIR DECISION PROBLEMS(1)

BY

H. G. RICE

1. **Introduction.** In this paper we consider classes whose elements are recursively enumerable sets of non-negative integers. No discussion of recursively enumerable sets can avoid the use of such classes, so that it seems desirable to know some of their properties. We give our attention here to the properties of complete recursive enumerability and complete recursiveness (which may be intuitively interpreted as decidability). Perhaps our most interesting result (and the one which gives this paper its name) is the fact that no nontrivial class is completely recursive.

We assume familiarity with a paper of Kleene [5](2), and with ideas which are well summarized in the first sections of a paper of Post [7].

[1] Henry Gordon Rice, Classes of recursively enumerable sets and their decision problems, Trans. Amer. Math. Soc. 74 (1953), 358-366.
Rice proved in his doctoral dissertation of 1951 at Syracuse University.

Proof.

- Let C be a nontrivial index set. Thus there exist indices e_0, e_1 such that $e_0 \in C$ and $e_1 \notin C$.
- Suppose C is computable.
- We define the following function:

$$\sigma(x) \stackrel{\text{def}}{=} \begin{cases} e_0, & \text{if } x \notin C \\ e_1, & \text{if } x \in C \end{cases}$$

  which is computable.
- Then for all x, $x \in C \Leftrightarrow \sigma(x) \notin C$, so σ has no point e such that $\{e\}(x) \sim \{\sigma(e)\}(x)$.
- This contradicts the fixed point theorem.

□

Applications of Rice's theorem

Example

The following are nontrivial index sets and hence incomputable from Rice's theorem.

$$\mathrm{K}_1 = \{e : \mathrm{dom}(\{e\}) \neq \varnothing\},$$

$$\mathsf{TOTAL} = \{e : \{e\} \text{ is a (total) recursive function}\},$$

$$\{e : \{e\} \sim \{d\}\} \ (d \text{ is fixed}).$$

Example

$\{\langle e, d\rangle : \{e\} \sim \{d\}\}$ is not computable, where $\langle e, d\rangle = \dfrac{(e+d)(e+d+1)}{2} + e$.

Definition

A sequence (or set) of partial recursive functions $\varphi_0, \varphi_1, \varphi_2, \ldots$ (with repetition) is called a CE numbering, if $\varphi(e, x) := \varphi_e(x)$ is a partial recursive function.

Example

Let F be a co-finite subset of $\mathbb{N}$, i.e., $\mathbb{N} - F$ is finite. Then, F is not an index set, but the set $\{\{e\} : e \in F\}$ is a CE-numbering consisting of all partial recursive functions.

- There is no CE numbering consisting of all recursive functions.

  $\because$ For contradiction, let $\{\varphi_e\}$ be a CE numbering consists of all recursive functions. Then, $\varphi_x(x)$ is partial recursive since $\{\varphi_e\}$ is a CE numbering, and it is total since φ_e's are total. Therefore, $\varphi_x(x) + 1$ is also total recursive, and so there is an e such that $\varphi_e(x) = \varphi_x(x) + 1$. Letting $x = e$, we obtain $\varphi_e(e) = \varphi_e(e) + 1$, which is a contradiction.

Definition

A sequence of CE sets $A_0, A_1, A_2, \ldots$, is called a CE numbering if $\{\langle e, x\rangle : x \in A_e\}$ is CE.

- There is no CE numbering consisting of all recursive sets.

  $\because$ For contradiction, let $\{A_e\}$ be a CE numbering consists of all recursive sets. Then, $\{x : x \notin A_x\}$ is also recursive, and so it is equal to A_e for some e. Considering $e \in A_e$, we get a contradiction.

Definition

The CE numbering of partial recursive functions $\varphi_0, \varphi_1, \varphi_2, \ldots$ is called a Gödel numbering if for any CE numbering $\psi_0, \psi_1, \psi_2, \ldots$, there exists a recursive function σ such that for any e,

$$\psi_e(x) \sim \varphi_{\sigma(e)}(x).$$

Lemma

$\{\{e\} : e \in \mathbb{N}\}$ is a Gödel numbering.

Proof.
Let $\psi_0, \psi_1, \psi_2, \ldots$ be a CE numbering. Then, there is d such that $\{d\}(e, x) \sim \psi_e(x)$. By the parameter theorem, $\{S^1_1(d, e)\}(x) \sim \{d\}(e, x) \sim \psi_e(x)$. So, letting $\sigma(e) = S^1_1(d, e)$, we have shown that $\{\{e\} : e \in \mathbb{N}\}$ is a Gödel numbering. $\square$.

The Gödel numbering is a general idea for a universal coding system of certain functions or sets. Most of the theorems w.r.t. $\{e\}$ we proved in the last two lectures (e.g., the parameter theorem and the recursion theorem) also hold w.r.t. any Gödel numbering. We now prove a new theorem w.r.t. a Gödel numbering.

Lemma (Padding lemma)

Let $\{\varphi_e\}$ be a Gödel numbering. There is a computable function π such that for any x, $\pi(x) > x$ and $\varphi_e \sim \varphi_{\pi(e)}$.

Proof.

- We construct a computable function π as follows. Given an x, we will obtain $y > x$ such that $\varphi_y \sim \varphi_x$ by the following calculation, and let $\pi(x) := y$.
- During the calculation, we collect $y \leq x$ such that $\varphi_y \sim \varphi_x$ and define B as the set of such a y. Thus, B is expanding until we obtain $y > x$ by the calculation.

- Initially, set $B = \{x\}$.
- To consider the next step, we define the following computable function

$$f(z) = \begin{cases} x+1 & \text{if } z \in B, \\ x & \text{if } z \notin B. \end{cases}$$

- By the fixed point theorem, there is a fixed point y of f, *i.e.*, $\varphi_y \sim \varphi_{f(y)}$.
- If $y > x$, $\varphi_y \sim \varphi_{f(y)} \sim \varphi_x$, so the process is completed with $\pi(x) = y$.
- In the case $y \in B$, letting $\pi(x) = x + 1$ we have $\varphi_{\pi(x)} \sim \varphi_{f(y)} \sim \varphi_y \sim \varphi_x$, which completes the process.
- Suppose $y < x$ and $y \notin B$. Since $f(y) = x$, we have $\varphi_y \sim \varphi_x$. So, we change B to $B \cup \{y\}$ and then continue the calculation for another y.
- Eventually, we get a fixed point $y > x$ and let $\pi(x) := y$. □

Remark

- There exists a CE numbering $g_0, g_1, g_2, \ldots$, which is not a Gödel numbering.
- R. Friedberg shows the existence of a CE numbering that lists all partial recursive functions without repetition. [2] This is also not a Gödel numbering.
- In this way, there are various CE numberings that are not Gödel numbering, but Gödel numbering is uniquely determined in the sense of the following theorem.

[2] A.H. Lachlan (Annals of Math. 91(2), 1970) and A. Shen (CiE, 2012) give another proof using games.

Theorem (Rogers' isomorphism theorem)

Let $f_0, f_1, f_2, \ldots$ and $g_0, g_1, g_2, \ldots$ be two Gödel numberings pf partial recursive functions. Then, there is a total recursive bijection $\rho : \mathbb{N} \to \mathbb{N}$ such that $f_e \sim g_{\rho(e)}$ for any e.

Proof.
Since both $f_0, f_1, f_2, \ldots$ and $g_0, g_1, g_2, \ldots$ are Gödel numberings, there exists a recursive function σ, τ such that

$$f_e(x) \sim g_{\sigma(e)}(x), \quad g_e(x) \sim f_{\tau(e)}(x).$$

In the following, we will construct a bijection $\rho : \mathbb{N} \to \mathbb{N}$ by combining σ and τ in the so-called back-and-forth method.

Proof.(continued)

- Suppose that a finite bijection $\rho : A_n \to B_n$ is constructed at the nth stage, where A_n,B_n ($\subset \mathbb{N}$) consists of n elements such that for all $e \in A_n$, $f_e \sim g_{\rho(e)}$.
- If n is even, let m be the smallest number in $\mathbb{N} - A_n$. Using the padding lemma repeatedly, let k be the first $\pi^i(\sigma(m)) \in \mathbb{N} - B_n$.
- Similarly, if n is odd, let k be the smallest number in $\mathbb{N} - B_n$. Using the padding lemma repeatedly, let m be the first $\pi^i(\tau(k)) \in \mathbb{N} - A_n$.
- Let $A_{n+1} = A_n \cup \{m\}, B_{n+1} = B_n \cup \{k\}$. Then, $\rho \cup \{(m, k)\}$ is a bijection from A_{n+1} to B_{n+1}.
- By repeating the above process, a recursive bijection $\rho : \mathbb{N} \to \mathbb{N}$ such that $f_e \sim g_{\rho(e)}$ is constructed.

Many-one reducibility

- In recursion theory, various methods have been developed to compare the complexity of two sets.
- In general, if a set A is "reducible to" a set B, then B has more information than A and hence is "more complex".
- The most basic notion of reducibility is "many-one reducibility".

Definition

- A set A is **many-one reducible** to a set B (written $A \leq_{\mathrm{m}} B$) if there exists a recursive function f s.t. for any x

$$x \in A \Leftrightarrow f(x) \in B.$$

- The set A is **one-one reducible** to the set B (written $A \leq_1 B$) if there exists a recursive injection f s.t. for any x

$$x \in A \Leftrightarrow f(x) \in B.$$

- If $A \leq_{\mathrm{m}} B$ and $B \leq_{\mathrm{m}} A$, we write $A \equiv_m B$.
- The class $\{B : B \equiv_m A\}$ is called the **many-one degree** of A.

- $\leq_{\mathrm{m}}$ (and $\leq_1$) are transitive and reflexive relations. Therefore $\equiv_m$ is an equivalence relation.
- $\leq_{\mathrm{m}}$ is often treated as a partial order over the equivalence classes of $\equiv_m$.

Theorem

For any $A \subset \mathbb{N}$, the following statements are equivalent.
(1) $A \leq_{\mathrm{m}} \mathrm{K}$
(2) $A \leq_1 \mathrm{K}$
(3) A is CE.

Proof.

- (2) $\Rightarrow$ (1) is obvious.
- (1) $\Rightarrow$ (3). Since K is CE, there is a partial recursive function g whose domain is K. Now, suppose A is many-to-one reducible to K by a recursive function f. Then A is the domain of the recursive partial function $g(f(x))$, and so A is also CE.
- (3) $\Rightarrow$ (2). If A is CE then there is a recursive partial function f.

$$f(e,x) = \begin{cases} 1 & \text{if } e \in A; \\ \uparrow & \text{if } e \notin A. \end{cases}$$

By the parameter theorem and the padding lemma, for any e, x there is a recursive injection g such that $\{g(e)\}(x) = f(e,x)$. Then, $e \in A \Leftrightarrow \{g(e)\}(g(e)) \downarrow \Leftrightarrow g(e) \in \mathrm{K}$. That is, $A \leq_1 \mathrm{K}$. □

Definition

We say that a set A is **m-complete** (with respect to CE) if A is CE and $B \leq_{\mathrm{m}} A$ for any CE set B.
If we replace $\leq_{\mathrm{m}}$ with $\leq_1$, A is **1-complete**.

Example

K is an m-complete CE set.

Lemma

Any m-complete CE set is 1-complete.

Theorem (Myhill's isomorphism theorem)

If $A \leq_1 B$ and $B \leq_1 A$ then there exists a recursive bijection ρ such that for any x, $x \in A \Leftrightarrow \rho(x) \in B$.

Proof. There exist recursive injection σ, τ such that

$$x \in A \Leftrightarrow \sigma(x) \in B, \quad x \in B \Leftrightarrow \tau(x) \in A.$$

We construct a recursive bijection $\rho : \mathbb{N} \to \mathbb{N}$ from σ, τ by the back-and-forth method.

Suppose that a finite bijection $\rho : C_n \to D_n$ is constructed at the nth stage, where C_n and D_n are n element subsets of $\mathbb{N}$ and for every $x \in C_n$ $x \in A \Leftrightarrow \rho(x) \in B$.

Proof.(continued)

- If n is an even number, let m be the smallest number the $\mathbb{N} - C_n$. The value of $\rho(m)$, $k \in \mathbb{N} - D_n$, is determined as follows.
  - If $\sigma(m) \notin D_n$, let $k = \sigma(m)$.
  - For $\sigma(m) \in D_n$, let $m' = \rho^{-1}(\sigma(m)) \in C_n$ and if $\sigma(m') \notin D_n$, let $k = \sigma(m')$, otherwise, $m'' = \rho^{-1}(\sigma(m')) \in C_n$, and so on.

Since both σ and ρ^{-1} are injections, this operation does not fall into a loop. By comparing the cardinality (in $i \leq n+1$ steps), we get $\sigma(m^{(i)}) \notin D_n$. Thus, at every step i $m^{(i)} \in A \Leftrightarrow m \in A$, so $k \in B \Leftrightarrow m \in A$.

- If n is an odd number, let k be the smallest number in $\mathbb{N} - D_n$, and the value m of $\rho^{-1}(k)$ be the number when C_n goes outside by alternately applying τ and ρ.

Let $C_{n+1} = C_n \cup \{m\}, D_{n+1} = D_n \cup \{k\}$. Then ρ is a bijection from C_{n+1} to D_{n+1}, and for $x \in C_{n+1}$ $x \in A \Leftrightarrow \rho(x) \in B$ holds. By repeating this, the desired bijection $\rho : \mathbb{N} \to \mathbb{N}$ is obtained. □

Homework

Prove that there exist two disjoint CE sets $A, B \subset \mathbb{N}$ with the following property. There is no computable set C such that $A \subset C$ and $B \cap C = \varnothing$.

Such A and B are said to be **computably inseparable**

Summary

- Rice's theorem is a generalization of the undecidability of halting problems to all non-trivial properties of programs.
- It asserts that for a nontrivial class of partial recursive functions $\mathcal{C}$, its index set $C = \{e : \{e\} \in \mathcal{C}\}$ is not computable. It basically states that any nontrivial semantic properties of programs are algorithmically undecidable.
- $A \leq_{\mathrm{m}} B$ ($A \leq_1 B$) if there exists a recursive function (bijection) f s.t. for any x $x \in A \Leftrightarrow f(x) \in B$.
- Myhill isomorphism theorem. If $A \leq_1 B$ and $B \leq_1 A$ then there exists a recursive bijection ρ such that for any x, $x \in A \Leftrightarrow \rho(x) \in B$.

Further readings

H. Rogers. *Theory of Recursive Functions and Effective Computability*, MIT Press, Reprint of the 1967 edition.

Thank you for your attention!