上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

计算复杂性　习题课

第 1、2 章习题

助教：郑扬珞

2025 年 12 月 1 日

第一章：计算理论

第 1 题

设计一个计算两个自然数相乘的图灵机。

- 编码：二进制或一进制

第 2 题

在第 7 页，定义了何谓一台图灵机 $\mathbb{M}$ 解决一个问题 $f : \{0,1\}^* \to \{0,1\}^*$。证明绝大部分问题是不可计算的。

- 什么是“绝大部分”?
- 可数 v.s. 不可数

第 3 题

设计一台将一进制数 1^n 转换成二进制数 $\llcorner n \lrcorner$ 的图灵机。你设计的图灵机的时间函数是什么？将二进制数转换成一进制数呢？

- 均摊分析
- 时间函数是关于输入长度的函数

第 4 题

函数 $\log^*(x)$ 定义如下:

$$\begin{aligned} \log^*(1) &= 0, \\ \log^*(x) &= 1 + \log^*(\log(x)), \quad 若 x > 1。 \end{aligned}$$

设计计算 $\log^*(x)$ 的图灵机。你设计的图灵机的时间复杂性是多少?

- $\log^* = \text{tower}^{-1}$，其中 $\text{tower}(n+1) = 2^{\text{tower}(n)}$

第 5 题

证明符号集为 $\{0, 1, \square, \triangleright\}$ 的多带图灵机可以模拟如下类型的图灵机，并且模拟过程中使用的额外计算是多项式时间的：

1. 带子是双向无限的，符号集可以任意大小。证明模拟可以在线性时间内完成。
2. 将带子换成三维坐标定义的第一象限体，符号存放在整数坐标点上。
3. 证明具有一条读写带的图灵机可以模拟 k 带图灵机。

- 配对函数：$\pi_2(x, y) = \frac{1}{2}(x + y)(x + y + 1) + y$
- $\pi_3(x, y, z) = \pi_2(\pi_2(x, y), z)$

第 6 题

有一台“厉害的”双带图灵机，该机有三个特殊的状态 $q_?, q_=, q_\neq$。当机器处于状态 $q_?$ 时，进行如下计算：若两个读写头处于同一位置（比如都处于所在带子的第 7 格），机器进入状态 $q_=$，若两个读写头处于不同位置，机器进入状态 $q_\neq$。设计一台多带图灵机模拟这台“厉害的”的图灵机的计算。

第 7 题

设 $T(n), T'(n)$ 为时间可构造。证明 $T(n)+T'(n)$、$T(n)\cdot T'(n)$、$T(n)^{T'(n)}$ 均为时间可构造。能证明 $T(n)/T'(n)$ 是时间可构造吗？$\log T(n)$ 呢？

- 时间可构造 v.s. 完全时间可构造

ON PROVING TIME CONSTRUCTIBILITY OF FUNCTIONS

Kojiro KOBAYASHI

Department of Information Science, Tokyo Institute of Technology, Oh-okayama, Meguro-ku, Tokyo, Japan 152

Communicated by R.V. Book
Received March 1984
Revised June 1984

Abstract. We formalize the techniques that have been used to prove time constructibility of functions by means of two theorems. The first theorem gives one sufficient condition for time constructibility of $f_1(n)+f_2(n)$ and $f_2(n)$ to imply that of $f_1(n)$. As an application of this theorem, we show that, for a function $f(n)$ such that $(\exists \varepsilon > 0)(\forall^{\infty} n) f(n) \geq (1+\varepsilon)n$, $f(n)$ is time constructible if and only if it is computable by a Turing machine within $O(f(n))$ steps. The second theorem concerns time constructibility of functions $f(n)$ for which there are no $\varepsilon > 0$ such that $(\forall^{\infty} n)$ $f(n) \geq (1+\varepsilon)n$.

第 8 题

考虑第 12 页的定理 1.2: 存在通用图灵机 $\mathbb{U}$ 和多项式 c，使得对任意长度为 n 的输入串 x，若 $\mathbb{M}_\alpha(x)$ 在 $T(n)$ 步内停机，则 $\mathbb{U}(\alpha, x)$ 在 $c(|\alpha|)T(n)\log T(n)$ 步内停机。
如果在定理 1.2 的证明中，我们让 $|R_i| = 2{\cdot}2^{i^2}$。证明在哪一步会出问题？如果没有问题的话，我们会得到一个更高效的通用图灵机!

$$2^{3^2} = 512 \gg 2^{0^2} + 2^{1^2} + 2^{2^2} = 19$$

第 10 题

证明**第 24 页的推论 1.3:** 设 $T(n) = \omega(n)$，设图灵机 $\mathbb{M}$ 在 $T(n)$ 步内判定 L。对任意 $\epsilon > 0$，存在图灵机 $\mathbb{M}'$，$\mathbb{M}'$ 能在 $\epsilon T(n)$ 步内判定 L。

- 只能对足够大的 n 证明该结论。

第 11 题

利用分配律 $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ 和 $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$，是否可在多项式时间内将合（析）取范式转换成析（合）取范式？

- 不能假设 **NP** $\neq$ **P**

第 13 题

说明：若忽略不终止性，在第 28 页上定义的非确定的“通用”图灵机是正确的。

- “若忽略不终止性”= 停机时一定给出正确的结果

第 14 题

证明**第 44 页的命题 3:** 若 $A \leqslant_K B \leqslant_K C$，则 $A \leqslant_K C$。若若 $A \leqslant_C B \leqslant_C C$，则 $A \leqslant_C C$。

第 15 题

证明 $\mathrm{EXP}^{\mathrm{EXP}} = 2\text{-}\mathrm{EXP}$。

$$2^{2^n}/2^n = 2^{2^n - n}$$

第 16 题

证明 2SAT $\in \mathrm{P}$。

$$x \vee y \iff (\neg x \to y) \wedge (\neg y \to x)$$

第 17 题

写一段对数空间程序，解决在**第 46 页** (1.16.1) 中定义的问题 MULP:

$$\texttt{MULP} = \{(a, b, c) \mid a, b, c \text{ 为二进制数，且 } a \cdot b = c\}.$$

- “对数空间”是关于输入长度的对数
- 输入长度是其表示数值的对数

第 18 题

证明**第 46 页的定理 1.11(空间压缩定理):** 设图灵机 $\mathbb{M}$ 在 $S(n)$ 空间判定 L。对任意 $\epsilon > 0$，存在图灵机 $\mathbb{M}'$，$\mathbb{M}'$ 能在 $\epsilon S(n) + 1$ 空间内判定 L。

- 是否需要“+1”?

第 19 题

证明**第 51 页的引理 1.8:** 隐式对数空间可计算函数就是对数空间可计算函数。

Definition [隐式对数空间可计算函数]

1. $\exists c, \forall x, |f(x)| \leqslant c|x|^c$
2. $\{\langle x, i\rangle | i \leqslant |f(x)|\} \in \mathbf{L}$
3. $\{\langle x, i\rangle | f(x)_i = 1\} \in \mathbf{L}$

第 23 题

证明 $\mathrm{PSPACE}^{\mathrm{PSPACE}} = \mathrm{PSPACE}$。

上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

考虑第 59 页的定理 1.18(时空定理):

$$\mathrm{TIME}(S(n)) \subseteq \mathrm{SPACE}\left(\frac{S(n)}{\log(S(n))}\right)$$

将引理 1.10 的证明细节补上。

证明：即便 $S(n)$ 不是空间可构造的，定理 1.18 依然成立。

Simulating Time With Square-Root Space*

Ryan Williams†
MIT

February 24, 2025

Abstract

We show that for all functions $t(n) \geq n$, every multitape Turing machine running in time t can be simulated in space only $O(\sqrt{t \log t})$. This is a substantial improvement over Hopcroft, Paul, and Valiant's simulation of time t in $O(t/\log t)$ space from 50 years ago [FOCS 1975, JACM 1977]. Among other results, our simulation implies that bounded fan-in circuits of size s can be evaluated on any input in only $\sqrt{s} \cdot \mathrm{poly}(\log s)$ space, and that there are explicit problems solvable in $O(n)$ space which require $n^{2-\varepsilon}$ time on a multitape Turing machine for all $\varepsilon > 0$, thereby making a little progress on the P versus PSPACE problem.

Our simulation reduces the problem of simulating time-bounded multitape Turing machines to a series of implicitly-defined Tree Evaluation instances with nice parameters, leveraging the remarkable space-efficient algorithm for Tree Evaluation recently found by Cook and Mertz [STOC 2024].

第二章：难解性

第 1 题

证明：假定 NP $\neq$ P，不存在保持可满足性的多项式时间算法将合取范式转换成析取范式。

- NP $\neq$ NP-完全

第 2 题

证明：若 $A, B \in \mathbf{NP}$，则 $AB := \{ab \mid a \in A, b \in B\} \in \mathbf{NP}$。

- 输入中不包含分隔符

第 3 题

设 $A \in \mathbf{NPC}$ 和 $B \in \mathbf{P}$。证明：若 $A \cap B = \emptyset$，并且 $A \cup B \neq \{0,1\}^*$，则 $A \cup B \in \mathbf{NPC}$。

- **NP** 完全性是基于 Karp 归约定义的
- “归”约，而非“规”约

思考：如果 $\mathbf{NP} = \mathbf{P}$，空语言 $\emptyset$ 和全语言 $\{0,1\}^*$ 是不是 **NP** 完全的?

第 4 题

证明：$\mathtt{SAT} \leqslant_K \mathtt{IP}$。

IP = Integer Programming

第 5 题

证明 $\{\psi 01^{|\psi|^c} \mid \psi \in \mathsf{SAT}\} \in \mathrm{NPC}$，并且 $\left\{\psi 01^{2^{|\psi|}} \mid \psi \in \mathsf{SAT}\right\} \in \mathrm{P}$。

第 6 题

在定理 2.3 的证明[a]中，我们假定 TMNP 的验证器 $\mathbb{M}$ 是健忘的。如果不做此假定，我们应该如何构造从 TMNP 到 SAT 的归约？

[a]即 Cook-Levin 定理。

- 记录读写头的位置

第 7 题

设 TMEXP 为语言 $\{\langle \alpha, x, 1^n \rangle \mid \mathbb{M}_\alpha(x)在2^n步内输出1\}$。证明 TMEXP 是 EXP-完全的。这种构造时间复杂性类完全问题的一般方法是否适用于空间复杂性类，比如 PSPACE?

- 对于空间复杂性类，如何确保停机?

第 8 题

在命题 7 的证明中，我们用到了 SAT 的稠密性。证明此性质。

- 稠密性 = 语言中长度不超过 n 的串有 $2^{\mathrm{poly}(n)}$ 个。

第 9 题

指出下面“证明”的错误：假定 $\mathrm{NP} = \mathrm{P}$，那么 $\mathrm{NP}^{\mathrm{O}} = \mathrm{P}^{\mathrm{O}}$ 对任意神谕 O 成立。根据定理 2.6，存在神谕 B 使得 $\mathrm{NP}^{\mathrm{B}} \neq \mathrm{P}^{\mathrm{B}}$。矛盾。因此 $\mathrm{NP} \neq \mathrm{P}$。

第 10 题

设 f 是可计算函数，g 是处处有定义的可计算函数。定义神谕是函数 g 的类型 P^g，并定义 $f \leqslant_C g$。

第 11 题

在库克归约的定义中，子程序调用是适应性的，即神谕图灵问的第 $i+1$ 个问题可能依赖于神谕前面问过的 i 个问题的答案。定义非适应性库克归约 $\leqslant_C^{na}$。

第 12 题

在量化布尔公式的定义中，见第 33 页 (1.10.3) [a]，要求 $\varphi(x^1, \ldots, x^n)$ 是合取范式。证明：

1. 若要求 $\varphi(x^1, \ldots, x^n)$ 是析取范式，QBF 依然是 PSPACE-完全的；
2. 若只要求 $\varphi(x^1, \ldots, x^n)$ 不含量词，QBF 依然是 PSPACE-完全的。

[a]公式 (1.10.3) 为 $Q_1 x^1 Q_2 x^2 \cdots Q_n x^n . \varphi(x^1, \cdots, x^n)$。

- PSPACE 对补运算封闭

第 13 题

证明：$\Sigma_i^p = \Sigma_{i+1}^p$ 蕴含 $\Sigma_i^p = \mathrm{PH}$。

$$\Sigma_{i+1}^p = \mathsf{NP}^{\Sigma_i^p}$$

第 14 题

上海交通大學 SHANGHAI JIAO TONG UNIVERSITY

定义一个神谕 A，使得 $\mathbf{PH}^A = \mathbf{P}^A$ 成立。

- 什么是神谕?
- 什么是 $\mathbf{PH}^A$?

第 16 题

证明：若 $A, B \in \Sigma_i^p$，必有 $A \cup B, A \cap B \in \Sigma_i^p$。

典型错误

设 A 和 B 分别由图灵机 $\mathbb{M}_1$ 和 $\mathbb{M}_2$ 计算。对于 $A \cup B$，分别调用 $\mathbb{M}_1$ 和 $\mathbb{M}_2$，输出结果的析取；对于 $A \cap B$，输出结果的合取。