

理论计算机科学基础

期末整理

郭嘉睿

ntguojiarui@pku.edu.cn

2022 年 1 月 16 日

7 时间复杂度

定理 7.1. 设 $t(n) \geq n$, 则每个 $t(n)$ 时间多带 TM 都与某个 $O(t^2(n))$ 时间单带 TM 等价.

定理 7.2. 设 $t(n) \geq n$, 则每个 $t(n)$ 时间单带 NTM 均与某个 $2^{O(t(n))}$ 时间 DTM 等价.

定义 7.3 (NP). NP 的两个等价定义:

$$\text{NP} = \{L \mid L \text{ 有多项式时间验证机} \} = \{L \mid \text{某个多项式时间 NTM 判定 } L \}.$$

定理 7.4 (Cook 定理). 任何 NP 语言均可在多项式时间内归约到 cnf-SAT.

一些 NPC 问题及它们的归约:

1. 3SAT, SAT: 通过 cnf-SAT 归约;
2. CLIQUE, VC, HAMPATH, SUBSET-SUM: 通过 3SAT 归约;

8 空间复杂度

定理 8.1 (Savitch 定理). 设 $f(n) \geq \log n$, 则 $\text{NSPACE}(f(n)) \subseteq \text{SPACE}(f^2(n))$.

推论: $\text{PSPACE} = \text{NPSPACE}$.

定理 8.2. 全带量词布尔公式问题 TQBF 是 PSPACE 完全的.

一些 PSPACE 完全问题: 公式博弈 FORMULA-GAME, 广义地理学游戏 GG.

定义 8.3 (亚线性空间). 亚线性空间 TM 是指将 TM 的带分为一条输入带 (只读), 一条工作带 (读写) 和一条单向输出带 (只写, 禁止回头或修改), 且工作带的大小是亚线性的.

定理 8.4. PATH 是 NL 完全的.

定理 8.5. $\text{NL} = \text{coNL}$.

9 空间难解性

定理 9.1 (空间层次定理). 对于任意空间可构造函数 $f: \mathbb{N} \rightarrow \mathbb{N}$, 存在语言 A , 在空间 $O(f(n))$ 内判定但不在空间 $o(f(n))$ 内判定.

定理 9.2 (时间层次定理). 对于任意时间可构造函数 $t: \mathbf{N} \rightarrow \mathbf{N}$, 存在语言 A , 在时间 $O(t(n))$ 内判定但不在时间 $o\left(\frac{t(n)}{\log t(n)}\right)$ 内判定.

定理 9.3. $\text{EQ}_{\text{REX}\uparrow}$ 是 EXPSPACE 完全的.

定理 9.4. $\text{NONMIN-FORMULA} \in \text{NP}^{\text{SAT}}$.

定理 9.5 (对角化的局限性). 存在语言 A, B , 使得 $P^A \subset \text{NP}^A, P^B = \text{NP}^B$.

定义 9.6 (ATM). 交错式 $\text{TM}(\text{ATM})$ 是一种 NTM , 其计算树中的非确定性分支点包括全称和存在两类, 一个全称分支点接受当且仅当它所有儿子接受, 一个存在分支点接受当且仅当它至少一个儿子接受, 根接受则整个计算接受.

ATM 复杂性的结论: $P = \text{AL}, \text{PSPACE} = \text{AP}, \text{EXP} = \text{APSPACE}$.

定义 9.7 (电路族). 一个电路族 C 是无穷个电路 $C = (C_0, C_1, \dots)$, 其中 C_n 有 n 个输入变量. 若对每个字符串 $w, w \in A \Leftrightarrow C_n(w) = 1$, 其中 $|w| = n$, 则称 C 在 $\{0, 1\}$ 上判定 A .

电路族的规模复杂性是 C 中的规模, 深度复杂性是 C 中从输入到输出的最长路径长度. $\text{P/poly} = \bigcup_k \text{SIZE}(n^k)$.

定理 9.8. $\text{TIME}(t(n)) \subseteq \text{SIZE}(O(t^2(n)))$. 进一步, $P \subseteq \text{PSIZE}$.

定理 9.9. 电路可满足性问题 CIRCUIT-SAT 是 NP 完全的.

定理 9.10 (Karp-Lipton 定理). $\text{NP} \subseteq \text{P/poly} \Leftrightarrow \text{PH} = \Sigma_2\text{P}$.

定义 9.11 (对数空间一致性). 一个布尔电路族 (C_1, \dots) 是对数空间一致的, 当且仅当存在一个对数空间 $\text{TM}: T$, 当输入 1^n 时, T 输出 $\langle C_n \rangle$.

定义 9.12 (NC 类). NC 类是指多项式规模, 对数多项式规模深度的电路. 更一般的, NC^k 类是指多项式规模, $O(\log^k n)$ 深度的电路.

定理 9.13. $\text{CIRCUIT-VALUE}(\text{CVP})$ 是 P 完全的.

10 复杂性高级专题

定义 10.1 (PP). PP 指错误概率 $\varepsilon = 0.5$, 在多项式时间内运行的概率算法.

定义 10.2 (BPP). BPP 指错误概率 $\varepsilon = 0.5 - \delta$ (其中 δ 是任意常数), 在多项式时间内运行的概率算法.

定义 10.3 (RP). RP 指错误概率 $\varepsilon = 0.5 - \delta$ (其中 δ 是任意常数), 在多项式时间内运行且只出现弃真型错误的概率算法.

定义 10.4 (coRP). coRP 指错误概率 $\varepsilon = 0.5 - \delta$ (其中 δ 是任意常数), 在多项式时间内运行且只出现取伪型错误的概率算法.

定义 10.5 (ZPP). ZPP 指错误概率 $\varepsilon = 0$, 期望运行时间为多项式时间的概率算法 (或: 在多项式时间内运行, 但允许 3 种输出 0, 1, ? 的概率算法).

它们之间的关系:

1. $\text{ZPP} \subseteq \text{RP} \cap \text{coRP} \subseteq \text{RP} \cup \text{coRP} \subseteq \text{BPP} \subseteq \text{PP}$.
2. $\text{BPP} \subseteq \text{PSIZE}$ (利用加强引理证明).
3. $\text{BPP} \subseteq \Sigma_2\text{P} \cap \Pi_2\text{P}$.
4. $\text{PH} \subseteq \text{P}^{\text{PP}}$.

11 一些没什么用的东西

一些语言的接受性/空性/满性/等价性的复杂度:

	A	E	ALL	EQ
DFA	L	NL 完全	P	PSPACE
NFA	NL 完全	NL 完全	PSPACE 完全	
PDA	至少 NL 完全		不可判定	不可判定
LBA	PSPACE 完全	不可判定	不可判定	不可判定
TM	不可判定	不可判定	不可判定	不可判定

运算封闭性 (Y 表示封闭, 表格中的条件表示在该操作下封闭当且仅当这一条件为真):

	P	NP	coNP	EXP
\cap	Y	Y	Y	Y
\cup	Y	Y	Y	Y
\sim	Y	P=NP	P=NP	Y
\cdot	Y	Y	Y	Y
$*$	Y	Y	Y	Y
同态	P=NP	Y		
$L_{\frac{1}{2}-}$	P=NP	Y		Y
RC	Y	Y	Y	Y
CUT	Y	Y	Y	Y