

发布日期：2023 年 12 月 4 日

截止日期：2023 年 12 月 15 日

计算复杂性理论 — 第四次作业

姓名： XXX

学号： nnnnnnnnnnnnnnnn

问题 1 设多项式时间概率图灵机 \mathbb{P} 以零误差判定 L , 即 $\Pr[\mathbb{P}(x) = L(x)] = 1$ 。证明 $L \in \mathbf{P}$ 。

解答 TODO

问题 2 证明 $\mathbf{RP} \subseteq \mathbf{NP}$ 。

解答 TODO

问题 3 \mathbf{RP} 中的问题的单侧误差随机算法的出错概率可以是 $1 - \frac{1}{\text{poly}(n)}$ 。证明: \mathbf{NP} 中的问题有出错概率是 $1 - \frac{1}{2^{\text{poly}(n)}}$ 的单侧误差随机算法。

解答 TODO

问题 4 设拉斯维加斯算法 \mathbb{A} 的期望运行时间为 $T(n)$, 运行时间超过 $99T(n)$ 的概率是 $\frac{1}{e(n)}$, 这里 $e(n)$ 为多项式。说明如何构造满足如下条件的斯维加斯算法 \mathbb{A}' : (i) 算法 \mathbb{A}' 和算法 \mathbb{A} 判定同样的问题; (ii) 算法 \mathbb{A}' 运行时间超过 $99T(n)$ 的概率不超过 $\frac{1}{2^{e(n)}}$ 。

解答 TODO

问题 5 在定理 2.3 的证明之后的一段, 我们解释了如何从 SAT 的判定算法找出一个可满足公式的一个可满足真值指派。用此算法思想证明 $\mathbf{NP} \subseteq \mathbf{BPP}$ 蕴含 $\mathbf{NP} \subseteq \mathbf{RP}$ 。结合练习 2, 后者等价于 $\mathbf{NP} = \mathbf{RP}$ 。

解答 TODO

问题 6 由定理 4.7 知 $\mathbf{BPP}^{\mathbf{BPP}} = \mathbf{BPP}$ 。证明 $\mathbf{ZPP}^{\mathbf{ZPP}} = \mathbf{ZPP}$ 。若 $\mathbf{RP}^{\mathbf{RP}} = \mathbf{RP}$, 你能推出什么结果?。

解答 TODO

问题 7 $L \in \mathbf{BPL}$ 当且仅当存在对数空间概率图灵机 \mathbb{P} 满足 $\Pr[\mathbb{P}(x) = L(x)] \geq \frac{2}{3}$ 。证明 $\mathbf{BPL} \subseteq \mathbf{P}$ 。

解答 TODO

问题 8 证明: 若 $\mathbf{NP} \neq \mathbf{P}$, 则 $\#\text{CYCLE}$ 就没有常数近似比的近似算法。

解答 TODO

问题 9 证明引理 4.8。

解答 TODO □

问题 10 证明：定义在有限域 \mathbf{F}_2 上的方阵的积和式和行列式值相等，并以此说明 $\oplus\text{Matching} \in \mathbf{P}$ 。

解答 TODO □

问题 11 构造满足 (4.7.2) 和 (4.7.3) 的公式 $\varphi(x) \cdot \psi(y)$ 和 $\varphi(x) + \psi(y)$ 。

解答 TODO □

问题 12 证明 $\oplus\mathbf{P} \subseteq \mathbf{P}^{\#\mathbf{P}}$ 。

解答 TODO □

问题 13 证明 $\oplus\mathbf{P}$ 在补运算下是封闭的。

解答 TODO □

问题 14 语言 L 在 \mathbf{UP} 中当且仅当有一个非确定时间图灵机 N 接受 L ，并且对任意输入 x ， $N(x)$ 最多有一条接受路径。也可用确定图灵机定义 \mathbf{UP} 。不难看出， $\mathbf{P} \subseteq \mathbf{UP} \subseteq \mathbf{NP}$ 。一个合取范式在语言 $\mathbf{USAT} \subseteq \mathbf{SAT}$ 中当且仅当它只有一个可满足真值指派。证明 \mathbf{USAT} 为 \mathbf{UP} -完全的。

解答 TODO □

问题 15 证明：若 $\mathbf{USAT} \in \mathbf{RP}$ ，则 $\mathbf{NP} = \mathbf{RP}$ 。

解答 TODO □

问题 16 证明定理 4.12。

解答 TODO □

问题 17 设 $k < n$ ，从 m -独立哈希函数族 $\mathcal{H}_{n,n}$ 构造 m -独立哈希函数族 $\mathcal{H}_{n,k}$ 和 $\mathcal{H}_{k,n}$ ，并证明其正确性。

解答 TODO □

问题 18 证明 $\mathbf{NP} \subseteq \mathbf{RP}^{\oplus\mathbf{P}}$ 。定理 4.14 可改成 $\Sigma_i^p \subseteq \mathbf{RP}^{\oplus\mathbf{P}}$ 吗？

解答 TODO □

问题 19 证明 $\text{Reachability} \in \mathbf{RL}$ 。

解答 TODO □

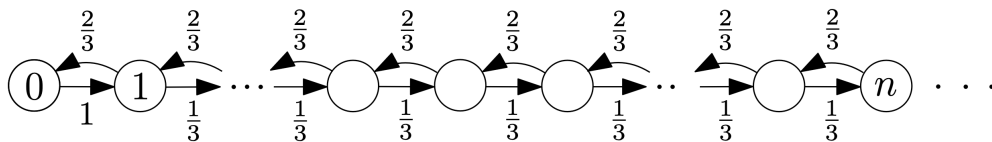
问题 20 证明：若将条件 (4.9.1) 改成 $\Pr[|A(x) - f(x)| \leq \epsilon f(x)] \geq 2/3$ ，并要求算法的时间函数是 $|x|$ 和

$\frac{1}{c}$ 的多项式, 得到的是一个等价的定义。

解答 TODO

□

问题 21 下图是一无限状态马尔科夫链。证明其为时间可逆的。



解答 TODO

□

问题 22 设 \mathbf{x} 为 \hat{G} 上的分布。证明 $\langle (\hat{G}_{\mathbf{x}^{\parallel}})^{\parallel}, (\hat{G}_{\mathbf{x}^{\perp}})^{\parallel} \rangle = -\langle (\hat{G}_{\mathbf{x}^{\parallel}})^{\perp}, (\hat{G}_{\mathbf{x}^{\perp}})^{\perp} \rangle$ 。

解答 TODO

□

问题 23 借鉴引理 4.43 的证明, 推出 $\lambda_{G \otimes H} \leq \sqrt{\lambda_G^2 + \lambda_H^2 + \lambda_G \lambda_H + \lambda_H^4}$ 。

解答 TODO

□

问题 24 在强显式扩张图构造中, 重新定义 $\{G_k\}_{k \in \omega}$ 如下:

$$G_0 = H^2$$

$$G_{k+1} = (G_k \otimes G_k)^3 \otimes H$$

用推论 4.4 之前的那一段中所描述的方法将 $\{G_k\}_{k \in \omega}$ 扩展到扩张图族, 会遇到什么困难?

解答 TODO

□

问题 25 莱因戈尔德算法 (见第 231 页) 中, 如果我们用一个 $(D^8, D, 1/4)$ -扩张图 H , 并归纳定义 $G_{k+1} = (G_k \otimes H)^4$, 证明会遇到哪些困难? 如果在设计莱因戈尔德算法时我们使用的是置换积而非之字积, 是否会遇到同样的困难?

解答 TODO

□