

第 4-11 讲: 随机算法

姓名: _ 学号: _

评分: _____ 评阅: _____

2023 年 6 月 7 日

请独立完成作业, 不得抄袭。
若得到他人帮助, 请致谢。
若参考了其它资料, 请给出引用。
鼓励讨论, 但需独立书写解题过程。

1 作业 (必做部分)

题目 1 (JH 5.2.2.7)

解答:

(i)

在 $[2, n^c]$ 中, 质数的近似数量为 $\frac{n^c}{\ln n^c}$, 因此 $c \log_2 n$ 个比特足以实现随机选择。

由于 $s \leq p \leq n^c$, 所以 $|s| \leq c \log_2 n$ 。

因此, 该协议的通信复杂度为 $2c \log_2 n$ 。

(ii)

当 $x \leq y$ 时, 被判定为相等的概率为

$$\frac{n-1}{n^c / \ln n^c} \leq \frac{\ln n^c}{n^{c-1}}$$

因此 $\text{Prob}((Rr, Rn) \text{ accepts } (x, y)) \geq 1 - \frac{\ln n^c}{n^{c-1}}$ 。

题目 2 (JH 5.2.2.8)

解答:

反证法。假设存在一种确定性算法, 使得 the communication complexity 小于 n 。

由假设可推得, 必然存在 $u, v \in \{0, 1\}^n$, $u \neq v$, 使得 $\bar{C}_1(u) = \bar{C}_1(v)$ 。

所以 $\bar{C}_2(\bar{C}_1(u), u) = \bar{C}_2(\bar{C}_1(v), u)$ 。

显然 $u \equiv u$, 可得 $u \equiv v$, 这与假设矛盾。

故 for every $n \in \mathbb{N}^+$, that every deterministic one-way protocol computing $Equality_n$ has a communication complexity of at least n .

(ii)

采用该算法即可。根据书中的证明, 可得:

(1) 在 $x \equiv y$ 时, $\text{Prob}((R_I, R_n) \text{ accepted}(x, y)) = 1$ 。

Random Inequality (R_I, R_{II})

Input: $x, y \in \{0, 1\}^n$
 Step 1: R_I chooses uniformly a prime p from the interval $[2, n^2]$ at random.
 {Note that there are approximately $n^2 / \ln n^2$ primes in this interval and so $2\lceil \log_2 n \rceil$ random bits are enough to realize this random choice.}
 Step 2: R_I computes $s = \text{Number}(x) \bmod p$ and sends p and s to R_{II} .
 {The length of the message is $4\lceil \log_2 n \rceil$ ($2\lceil \log_2 n \rceil$ bits for each of p and s). This is possible because $s \leq p \leq n^2$.}
 Step 3: R_{II} computes $q = \text{Number}(y) \bmod p$.
 If $q \neq s$, then R_{II} outputs 1 ("accept").reject
 If $q = s$, then R_{II} outputs 0 ("reject").accept

(2) 在 $x \neq y$ 时, $\text{Prob}((R_I, R_n)\text{accepts}(x, y)) \leq \frac{\ln n^2}{n}$

故 $\text{Prob}(A(x) = F(x)) \geq 1 - \frac{\ln n^2}{n} \geq \frac{1}{2} + \epsilon$, 满足题目要求。

(iii)

反证法。假设存在一种 one-sided-error, 使得 the communication complexity 小于 n 。

由假设可推得, 必然存在 $u, v \in \{0, 1\}^n$, $u \neq v$, 使得 $\bar{C}_1(u) = \bar{C}_1(v)$ 。

所以 $\bar{C}_2(\bar{C}_1(u), u) = \bar{C}_2(\bar{C}_1(v), u)$ 。

显然 $u \equiv u$, 可得 $u \equiv v$, 这与假设中的 one-sided-error 矛盾。

故 one-sided-error 的 communication complexity 至少为 n 。

2 作业 (选做部分)

3 Open Topics

Open Topics 1 (例题 5.2.2.5)

请讲解例题 5.2.2.5, 并说明, 为什么这个随机算法代价好于“任何”确定性算法。

Open Topics 2 (Karger's Algorithm)

参考资料:

- [Wikipedia\[Karger's algorithm\]](#)

4 反馈