第 4-11 讲: 随机算法

姓名：朱宇博　　**学号：**191220186

评分：_____　　**评阅：**_____

2021 年 5 月 26 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)
$[2, n^c]$ 中质数近似有 $\frac{n^c}{\ln n^c}$ 个，因此 $c\log_2 n$ 个 bit 足够去实现该随机选择。
因为 $s \le p \le n^c$，故 $|s| \le c\log_2 n$
综上，the communication complexity of this protocol is $2c\log_2 n$
(ii)
在 $x \le y$ 时，被判定为相等的概率

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

故 Prob ((Rr, Rn) accepts (x, y)) $\ge 1 - \frac{lnn^c}{n^{c-1}}$

题目 2 (JH 5.2.2.8)

解答：
(i)
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 $u, v \in \{0,1\}^n$，$u \ne v$，使得 $\overline{(}C_1(u)) = \overline{(}C_1(v))$。
所以 $\overline{(}C_2(\overline{(}C_1(u)), u)) = \overline{(}C_2(\overline{(}C_1(v)), u))$。
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)

Random Inequality ($R_{\mathrm{I}}, R_{\mathrm{II}}$)

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 $s = Number(x) \bmod p$ 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 $q = Number(y) \bmod p$.
If $q \neq s$, then R_{II} outputs 1 ("~~accept~~").reject
If $q = s$, then R_{II} outputs 0 ("~~reject~~").accept

采用该算法即可。根据书中的证明，可得:
(1) 在 $x \equiv y$ 时，$Prob((R_I, R_n)accepted(x, y)) = 1$.
(2) 在 $x \not\equiv y$ 时, $Prob((R_I, R_n)accepts(x, y)) \leq \frac{\ln n^2}{n}$
故 $Prob(A(x) = F(x)) \geq 1 - \frac{\ln n^2}{n} \geq \frac{1}{2} + \epsilon$，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 $u, v \in \{0,1\}^n$，$u \not\equiv v$，使得 $\overline{(}C_1(u)) = \overline{(}C_1(v))$。
所以 $\overline{(}C_2(\overline{(}C_1(u)), u)) = \overline{(}C_2(\overline{(}C_1(v)), u))$。
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。

4 反馈