Problem Solving Homework (Week 12)

161180162 Xu Zhiming

May 28, 2018

JH Chapter 5

5.2.2.7

(i) First, in order to achieve realize the random choice of prime p, $c\lceil\log_2 n\rceil$ bits are needed. Besides $s = \textsc{Number}(x) \mod p$ requires another $c\lceil\log_2 n\rceil$ bits. Both p and s are sent, therefore, the communication complexity is $2c\lceil\log_2 n\rceil$.

(ii) Suppose $x \neq y$ while

$$\textsc{Number}(x) \mod p = \textsc{Number}(y) \mod p$$

$$\therefore \left(h = \left|\textsc{Number}(x) - \textsc{Number}(y)\right|\right) \equiv 0 \mod p$$

Since $x, y \in 0, 1^n$, h is less than 2^n, i.e., h has fewer than n different prime divisors, which means that at most $n-1$ primes $l_i \in \{2, 3, \ldots, n^c\}$ have the property

$$\textsc{Number}(x) \mod l_i = \textsc{Number}(y) \mod l_i$$

Therefore, the probability that R_1 randomly chooses a prime with the property mentioned above for the given input (x, y) is at most

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

$$\therefore \mathit{Prob}\left((R_1, R_2) \text{ accept } (x, y)\right) \geq 1 - \frac{c \ln n}{n^{c-1}}$$

5.2.2.8

(i) *Proof.* Suppose we use deterministic algorithm to compute $\mathit{Equality}_n$, then we need to compare each pair $\{x_i, y_i\}, i = 1, 2, \ldots, n$. This process needs at least n communication complexity since at least n bits from either x or y should be transmitted to another computer for comparison. □

(ii) Suppose C_1 and C_2 share enough random $0-1$ strings, say, $O(n)$ ones. Then C_1 randomly picks one string, and sends its index (the length of which is $O(\log_2 n)$) to C_2. This is a two-sided-error algorithm and

$$P(\mathit{Equality}_n(x, y) = 1) \geq \frac{2}{3}, \text{ if } x = y$$

$$P(\mathit{Equality}_n(x, y) = 0) \geq \frac{2}{3}, \text{ if } x \neq y$$

(iii) *Proof.* Since one-sided-error algorithm accepts every input (x, y) only if $x = y$. Then to make this happens, we need to verify every single bit pair (x_i, y_i) for $i = 1, 2, \ldots, n$. Otherwise, leave out some bit pairs unchecked will cause our algorithm accept (x, y) while $x \neq y$. In order to do this, alike what's mentioned in (i), at least n bits should be transmitted. Therefore, the lower bound of communication complexity for one-sided-error algorithm with regard to $\mathit{Equality}_n$ is n. □