Homework 3

5130309059 李佳骏

taringlee@sjtu.edu.cn

2015.10.19

Exercise 3.15

Thanks for my roommate's help to tell me how to simulate **Hoeffding's inequality** to solve this exercise and like hints above that "The case of zero error protocols is slightly different:", the proof will imitate the proof of **Theorem 3.14**.

PROOF: It is sufficient to prove that any public coin protocol $\mathcal{P}$, using any number of random bits, can be transformed into another public coin protocol, $\mathcal{P}'$, with the same communication complexity that uses $O(\log n)$ random bits without error. The proof then follows because Alice can simply flip that many random coins by herself, send the random coin flips to Bob, and the two players proceed as in $\mathcal{P}'$.

Let $Z(x, y, r)$ be a random variable that gets communication length that $\mathcal{P}$ gives on input (x, y) and random string r. Because Alice can send x to Bob directly, $Z_{r\in\Pi}(x, y, r) \leq n$, for all (x, y). We will build a new protocol, which uses fewer random bits, using the probabilistic method. Let t and δ be a parameter(to be fixed) and $r_1, ..., r_t$ be t strings. For such strings, define a protocol $\mathcal{P}_{r_1,...,r_t}$ as follows: Alice and Bob choose $1 \leq i \leq t$ uniformly at random and then proceed as in $\mathcal{P}$ with r_i as their common random string. We now show that there exist strings $r_1, ..., r_t$ such that $E_i[Z(x, y, r_i)] \leq R_0^{pub}(f) + \delta$, for all (x, y). For this choice of strings the protocol $\mathcal{P}_{r_1,...,r_t}$ is the desired protocol. To do so, we choose the t values $r_1, ..., r_t$ at random(according to the probability distribution Π). Consider a particular input pair (x, y) and compute the probability that $E_i[Z(x, y, r_i)] > R_0^{pub}(f) + \delta$. By the **Hoeffding's inequality**, since $E_r[Z(x, y, r) \leq R_0 pub(f)]$, we get

$$\Pr_{r_1,...,r_t}[(E_i[Z(x, y, r_i)] - R_0^{pub}(f)) > \delta] \leq e^{\frac{-2t\delta^2}{n^2}}$$

By choosing $t = O(n^3)$ and $\delta = \log n$, this is smaller than 2^{-2n}. Thus, for a random choice of $r_1, ..., r_t$ the probability that for *some* input (x, y), $E_i[Z(x, y, r_i)] > R_0^{pub}(f) + \delta$ is smaller than $2^{-2n}2^{2n} = 1$. This implies that there exists a choice of $r_1, ..., r_t$ where for *every* (x, y) the communication length of protocol $\mathcal{P}_{r_1,...,r_t}$ is at most $R_0^{pub}(f)+\delta$. Finally note that the number of random bits used by the protocol $\mathcal{P}_{r_1,...,r_t}$ is $\log t = O(\log n)$ and that the communication complexity is bounded by $R_0^{pub}(f)+\delta+\mathcal{P}_{r_1,...,r_t} = R_0^{pub}(f)+\log n+\log_t = O(R_0^{pub}(f)+\log n)$.

Exercise 3.31

It's difficult for me to solo this exercise. Fortunately, we found a paper, *UNBIASED BITS FROM SOURCES OF WEAK RANDOMNESS AND PROBABILISTIC COMMUNICATION COMPLEXITY*, to help us to settle it. However, this paper show tons of strange definitions and I could not comprehend them completely. Hence, I finished this problem 3 days later.

We called function f is δ-robust on a rectangle R if f satisfied that

$$\mid Pr[f(x, y) = 1|(x, y) \in R] - Pr[f(x, y) = 0|(x, y)] \mid \in [\frac{1-\delta}{2}, \frac{1+\delta}{2}]$$

And We prove **Theorem 1**, there are at least $1 - 2^{-2^n}$ fraction of function which δ-robust on every rectangle R ($\mid R \mid \geq t$) satisfied $\log t - n - 5 \geq 2\log \delta^{-1}$.

To prove this theorem, we use **Chernoff Bound** firstly.

$$Pr[\frac{1}{|R|}\sum_{(x,y)\in R} f(x,y) - \frac{1}{2} \geq \frac{\delta}{2}] \leq 2^{1-\frac{\delta^2}{8}t}$$

And like we did in 3.15. We use **Union Bound** to detect the probability of function rectangle out of δ-robust. It means $2^{2^n}2^{2^n}2^{1-\frac{\delta^2}{8}t} \leq 2^{-2^n}$. So, we know that **Theorem 1**is legal with high probability.

Hence we prove **Theorem 2**, Suppose that for every $\log t \geq 2n - k - 1 + \log\delta$, the Boolean function f which is δ-robust on every rectangle $R(\mid R \mid \geq t)$. Then $D^{\text{uniform}}_{\frac{1}{2}-\delta}(f) > k$.

For every $\gamma \in 0,1^k$, denote by $C(\gamma)$ the set of (x,y) pairs on which the communication of Alice and Bob is γ. Let $G(\gamma) = (x,y) \in C(\gamma) : P(x,y) = f(x,y)$. Since the protocol has at least $\frac{1+\delta}{2}$ accuracy, we sum them, and find

$$\sum_{\gamma\in 0,1^k} |G(\gamma)| \geq (\frac{1}{2} + \delta)2^{2n}$$

Thus we say that $C(\gamma)$ is SMALL if $|C(\gamma)| < 2^{2n-k-1}\delta$. Since there are at most 2^k rectangles $C(\gamma)$ and the number of points in all small rectangles is at most $2^{2n-1}\delta$. Thus we have:

$$\sum_{\gamma\geq \text{SMALL}} |G\gamma| \geq (\frac{1+\delta}{2})2^{2n}$$

This implies that $\exists\gamma \in 0,1^k$ s.t. $|C(\gamma)| \geq 2^{2n-k-1}\delta$ and $|G(\gamma)| \geq \frac{1+\delta}{2}|C(\gamma)|$. We find a contradiction that $\log_2 |C\gamma| \geq 2n - k - 1 + log_2\delta$ without δ-robust happened.

Finally, by setting $k = n - 1 - 2\log\delta^{-1}$, and $\epsilon = \frac{\delta}{2}$, there are at least $1 - 2^{-2^n}$ fraction of all functions and we get $D^{\text{uniform}}_{\frac{1}{2}-\epsilon}(f) = n - 1 - 2\log\delta^{-1} = n - O(\log\epsilon^{-1})$