Quiz 11

(1) Consider the class PP defined as follows:

$L \in PP$ if there is a randomised poly-time TM M s.t.

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^{T(|x|)}}[M(x,r) = 1] > 1/2$$

$$x \notin L \Rightarrow \Pr_{r \in \{0,1\}^{T(|x|)}}[M(x,r) = 1] < 1/2.$$

i) Show that $NP \subseteq PP$.

ii) Show that $coNP \subseteq PP$.

iii) Why does the proof of (i) not show that $NP \subseteq BPP$?

[4+2+4]

Hint: Accepting branch → Accept

Rejecting branch → Reject with prob $\frac{1}{2} + \frac{1}{2^{T(|x|)}+1}$

Accept with prob. $\frac{1}{2} - \frac{1}{2^{T(|x|)}+1}$

Made with Goodnotes

(2) Let $BPP_{0.8,0.7}$ be defined as follows:

$L \in BPP_{0.8,0.7}$ if there is a randomised poly-time TM M s.t.

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^{T(|x|)}}[M(x,r) = 1] \geq 0.8$$

$$x \notin L \Rightarrow \Pr_{r \in \{0,1\}^{T(|x|)}}[M(x,r) = 1] \leq 0.7$$

Show that $BPP_{0.8,0.7} = BPP$. [10]

Theorem 18.12 — Chernoff/Hoeffding bound. If $X_0, \ldots, X_{n-1}$ are i.i.d random variables such that $X_i \in [0,1]$ and $\mathbb{E}[X_i] = p$ for every i, then for every $\epsilon > 0$

$$\Pr\left[\left|\sum_{i=0}^{n-1} X_i - pn\right| > \epsilon n\right] \leq 2 \cdot e^{-2\epsilon^2 n}. \tag{18.2}$$

Made with Goodnotes

Solution

(1) i) Let $L \in NP$. Then there is a non-deterministic TM M s.t.

$x \in L \Rightarrow$ there is a computation branch of M that is accepting

$x \notin L \Rightarrow$ every computation branch of M is rejecting.

WLOG we can assume that all the vertices of the computation tree of M has degree ≤ 2

↳ Check. Why?

Also, let $T(n)$ be the time complexity of M.

Consider the following probabilistic TM M'

On input x

1. for $i = 1$ to $T(|x|)$
2. If it is not a halting configuration
3. If there is no branching
4. Execute the next step.
5. else randomly choose $b \in \{0,1\}$
6. if $b = 0$

Made with Goodnotes

7. execute the next step in the left branch.
8. else execute the next step in the right branch.
9. else
10. if it is an accepting state, accept
11. else
12. accept with probability $\frac{1}{2} - \frac{1}{2^{(T(|x|)+1)}}$ & reject with probability $\frac{1}{2} + \frac{1}{2^{T(|x|)+1}}$

$$\Pr_{r \in_{u.a.r} \{0,1\}^{T(|x|)}} [M'(x) = 1]$$

$$= \Pr_{r \in_{u.a.r} \{0,1\}^{T(|x|)}} [M' \text{ went down an accepting path}] +$$

$$\left(\frac{1}{2} - \frac{1}{2^{(T(|x|)+1)}}\right) \Pr_{r \in_{u.a.r} \{0,1\}^{T(|x|)}} [M' \text{ went down a rejecting path}]$$

When $x \in L$, there is at least one accepting path

Let the no. of accepting paths be w

(assume that the computation tree is a full binary tree → Why can this be assumed WLOG?)

$$\Rightarrow \Pr_{r \in_{u.a.r} \{0,1\}^{T(|x|)}} [M' \text{ went down an accepting path}] = \frac{w}{2^{T(|x|)}}$$

Made with Goodnotes

$$\Rightarrow \Pr_{r \in_{u.a.r} \{0,1\}^{T(|x|)}}\left[M'(x)=1\right] \geq$$

$$\frac{w}{2^{T(|x|)}} + \left(1 - \frac{w}{2^{T(|x|)}}\right)\left(\frac{1}{2} - \frac{1}{2^{T(|x|)+1}}\right)$$

$$= \frac{w}{2^{T(|x|)}} + \frac{1}{2} - \frac{1}{2^{T(|x|)+1}} - \frac{w}{2^{T(|x|)+1}} + \frac{w}{2^{2T(|x|)}}$$

$$= \frac{1}{2} + \frac{2w - 1 - w}{2^{T(|x|)+1}} + \frac{w}{2^{2T(|x|)}}$$

$$= \frac{1}{2} + \underbrace{\frac{w-1}{2^{T(|x|)+1}}}_{\geq 0 \text{ since } w \geq 1} + \frac{w}{2^{2T(|x|)}} > \frac{1}{2}$$

When $x \notin L$, there is no accepting path

$$\Rightarrow \Pr_{r \in_{u.a.r} \{0,1\}^{T(|x|)}}\left[M'(x)=1\right] = \frac{1}{2} - \frac{1}{2^{T(|x|)+1}} < \frac{1}{2}.$$

Thus $L \in PP$.

(1) iii) If generalise the proof on error reduction, it is easy to see that if $\Pr[M(x) = L(x)] \geq \frac{1}{2} + \varepsilon$ and we wanted M' to be such that

$$\Pr[M(x) = L(x)] \geq 1 - \delta,$$

then the number of iterations reqd.

Made with Goodnotes

is $O\left(\frac{1}{\varepsilon^2}\log(1/\delta)\right)$. → Phase check !!

In this case, if the proof were to work for showing NP ⊆ BPP, then we have that ε can be as low as $\frac{1}{2^{2T(|x|)}}$ and $\delta = 1/3$

Thus, the no. of iterations reqd. would become exponential. Thus, the algorithm would not be efficient anymore.

---

(2) Consider the following machine:

M': On input x

1. Run M on x k (to be fixed later) times and let $y_1, \ldots, y_k$ be the outputs
2. if $\sum_{i=1}^{k} y_i \geq 0.75\,k$
3. L output 1.
4. else output 0

We now analyse the probability that M' outputs incorrectly. (i.e. $P_r[M'(x) \neq L(x)]$)

Note that $M'(x) = \begin{cases} 1 & \text{if } \sum y_i \geq 3k/4 \\ 0 & \text{o.w.} \end{cases}$

Made with Goodnotes

Case I: $L(x) = 0$

Then,

Define $Y = \sum_{i=1}^{k} y_i$.

$$\Pr\left[M'(x) \neq L(x)\right] = \Pr\left[M'(x) = 1\right]$$

$$= \Pr\left[\sum_{i=1}^{k} y_i \geq 3k/4\right] = \Pr\left[Y \geq 3k/4\right]$$

Also, $\mathbb{E}[y_i] \leq 0.7$

> **Theorem 18.12 — Chernoff/Hoeffding bound.** If $X_0, \ldots, X_{n-1}$ are i.i.d random variables such that $X_i \in [0,1]$ and $\mathbb{E}[X_i] = p$ for every i, then for every $\epsilon > 0$
>
> $$\Pr\left[\left|\sum_{i=0}^{n-1} X_i - pn\right| > \epsilon n\right] \leq 2 \cdot e^{-2\epsilon^2 n}. \qquad (18.2)$$

$$\Rightarrow \Pr\left[Y \geq 3k/4\right] \leq \Pr\left[|Y - 0.7k| \geq 0.05k\right]$$

$$\leq \frac{2}{e^{2(0.05)^2 k}}$$

Case II: $L(x) = 1$.

Then, $\Pr\left[M'(x) \neq L(x)\right] = \Pr\left[M'(x) = 0\right]$

$$= \Pr\left[\sum_{i=1}^{k} y_i < 3k/4\right] = \Pr\left[Y < 3k/4\right]$$

Since $\mathbb{E}[y_i] \geq 0.8$, $\Pr\left[Y < 3k/4\right]$

$$\leq \Pr\left[|0.8k - Y| \geq 0.05k\right] \leq \frac{2}{e^{2(0.05)^2 k}}.$$

Made with Goodnotes

So in either case,

$$\Pr\left[M'(x) \neq L(x)\right] \leq \frac{2}{e^{2(0.05)^2 k}}.$$

We want

$$\frac{2}{e^{2(0.05)^2 k}} \leq \frac{1}{3}$$

$$\Leftrightarrow e^{2(0.05)^2 k} \geq 6$$

$$\Leftrightarrow k \geq \frac{\ln 6}{2(0.05)^2}$$

So $k = 360$ suffices.

Made with Goodnotes