AMIT YADAV

Assignment : 7

H7.1

Let $L \in ZPP = RP \cap Co\text{-}RP$.

$\Rightarrow \exists$ PTM A such that if $x \in L$, $P[A(x) = 1] \geq \frac{1}{2}$

if $x \notin L$, $P[A(x) = 1] = 0$

Also,

$\exists$ PTM B s.t. if $x \in L$, $P[B(x) = 1] = 1$

if $x \notin L$, $P[B(x) = 1] \leq \frac{1}{2}$

Now, construct M (a PTM) such that on input x:

1. Run A on x.
2. Run B on x.
3. Accept or reject according to following table:

A	B	output
Yes	No	Not possible
No	Yes	Don't know (?)
Yes	Yes	Yes (accept)
No	No	No (reject)

If output is don't know, then repeat steps 1, 2, 3 one more time.

(Only 2-times, in total)

Now,

if $x \in L$, then B will always out-put 'yes' on x.

$\therefore$ M's output can be either ? or Yes.

$\therefore$ if $x \in L$, then $P[M(x)=0] = 0$.

if $x \notin L$, then A will always say 'no' on x.

$\therefore$ if $x \in L$, then $P[M(x)=1] = 0$.

$P[M(x) = ?]$

This is possible only when A and B output 'No' and 'yes' respectively, both the times.

if $x \in L$,

$\therefore$ $P[M(x)=?] \leq \frac{1}{2} \times 1 \times \frac{1}{2} \times 1 \leq \frac{1}{4}$

if $x \notin L$

$P[M(x)=?] \leq 1 \times \frac{1}{2} \times 1 \times \frac{1}{2} \leq \frac{1}{4}$

$\therefore$ $P[M(x)=?] \leq \frac{1}{4} \leq \frac{1}{3}$

(b) Given : $L \in ZPP$.

Let A and B be PTM as defined in part (a).

Design M' s.t. on input x :

① Run A on x.

② Run B on x.

③ If A accepts, then accept.
If B rejects, then reject.
Else repeat above steps again.

We know that Probability of A and B rejecting and accepting any given input respectively is $\leq \frac{1}{2}$.
By repeating steps ① and ②, we decrease the probility of confusion (i.e. No and Yes output.

Now, let runtime for steps ① and ② combined $= P(n)$.
Then, $E[\text{total runtime}] = \frac{1}{2}P(n) + \frac{1}{2} \times \frac{1}{2} P(n) + \cdots\cdots$

$\therefore$ $E[\text{runtime}]$ is Polynomial.

Also, since construction of M' is similar to M, therefore if M' halts on x, then $M'(x) = 1$ iff $x \in L$.

H7.2

Given: $L \subseteq \{0,1\}^*$

$\exists c, \exists$ PTM M s.t $\forall x \in \{0,1\}^*$,

if $x \in L$ then $P[M(x)=1] \geq \frac{1}{|x|^c}$

if $x \notin L$, then $P[M(x)=1] = 0$.

Sol: we construct M' such that on input x:

① Run PTM M k-times.

② If output of M is 'yes' at any iteration, then accept. Else reject.

Now, if $x \notin L$, then M will always output No.

$\therefore$ $P[M'(x)=1] = 0$ if $x \notin L$.

If $x \in L$, then

$$P[M'(x)=1] = 1 - P[M'(x)=0] \geq 1 - \left(1 - \frac{1}{|x|^c}\right)^k$$

If we look at term $\left(1-\frac{1}{n^c}\right)^k$ $(n = |x|)$

$$\left(1-\frac{1}{n^c}\right)^k \leq \frac{1}{2^{n^d}} \quad \text{for} \quad k \geq \frac{n^d}{\log\left(\frac{1}{1-\frac{1}{n^c}}\right)} \approx \frac{n^d}{\frac{1}{n^c}} = n^{d+c}$$

$\therefore$ For a given c and d, choose $k = n^{d+c}$.

Analysis of m':

Runtime of m' $=$ $K \times$ Runtime of m.

$=$ polynomial (since m is PTM).

Hence, $\forall d > 0$, m' exists.

H 7.3 To prove $SAT \in P/Poly \Rightarrow \Sigma_2^P = \Pi_2^P$.

Sol: Let L be any language in Π_2^P, (like $\overline{QSAT_2}$ which is Π_2^P complete).

Then $\exists R \in P$ s.t.

$x \in L \Leftrightarrow \forall y \; \exists z$ s.t. $R(x, y, z) = 1$.

The problem $\exists z$ s.t. $R(x, y, z) = 1$ is in $\Pi_1^P \equiv NP$.

Since, SAT is NP-complete, we can reduce it to SAT

i.e $\exists z$ s.t. $R(x, y, z) = 1 \Leftrightarrow \phi_{x,y} \in SAT$.

$\therefore$ We can re-write L as

$x \in L \Leftrightarrow \forall y \; (\phi_{x,y} \in SAT)$. —— (1)

Now, since $SAT \in P/Poly$, $\exists$ a circuit of polyn. size for every input.

$\therefore$ We can write our original problem as

$x \in L \iff \exists c \; \forall y \; c(\phi_{xy}) = 1$

circuit

Since, circuit is polynomial size w.r.t. size of ϕ_{xy} and $c(\phi_{xy}) \in P$. &

$\therefore$ The above problem is in Σ_2^P.

$\therefore \quad \Pi_2^P \subseteq \Sigma_2^P \Rightarrow PH = \Sigma_2^P = \Pi_2^P$