CPTH 3

Saswata Mukherjee (BMC201945)
Somnath Bhattacharjee (BMC201954)

April 23, 2021

Question 1.

Let for a fixed TM M, $T_{M,x}$ be the r.v. for the time taken by M to conclude on the input x
Let $L \in ZPP$ with the TM M
$\therefore E(T_{M,x}) \leq p(|x|)$ for some polynomial p

Now we will design a PTM M' for L:
on input x , M' will run x on M for $3p(|x|)$ and answer accordingly. If the computation is not done yet, it will simply reject x.

So clearly if $x \notin L$ then anyway M' will reject it
So $P[M'(x) = 0] = 1$

if $x \in L$ then if it halts within $3p(|x|)$ steps then surely $M'(x) = M(x) = 1$ or $P[M'(x) = 1] = 1$
otherwise

$$\begin{aligned} P[M'(x) = 0] &= P[T_{M,x} > 3p(|x|)] \\ &\leq \frac{E(T_{M,x})}{3p(|x|)} && \text{(marcov's inequality)} \\ &\leq \frac{p(|x|)}{3p(|x|)} = \frac{1}{3} \end{aligned}$$

Hence $L \in RP$
Hence $ZPP \subseteq RP$
Hence co-ZPP$\subseteq$ co-RP
Now it is quite obvious that ZPP =co-ZPP as we can simply swap the accept and reject state
Hence ZPP $\subseteq$ RP $\cap$ co-RP

Now let $L \in$ RP $\cap$ co-RP
So we have M_1 to recognise L for RP and M_2 to recognise L for co-RP
We will design a new TM M which on input x runs x on M_1 and M_2 both. If $M_1(x) = 1$ then $M(x) = 1$ and if $M_2(x) = 0$ then $M(x) = 0$

(Note $M_1(x) = 1$ and $M_2(x) = 0$ both cannot happen simultaneously)
if any of these does not happen then it will repeat this step again and again.

Clearly M will never err.
say, $N_{M,x}$ is the random variable for number of iterations needed for $M(x)$
and A_i is the event that, $M(x)$ reaches ith iteration.
so, $Pr(A_{i+1}|A_i) \leq \frac{1}{3}$ for all $i \geq 1$ (from definition of RP, co-RP)
so, $Pr(A_{i+1}) = Pr(A_{i+1} \cap A_i)$ (as, $A_{i+1} \subset A_i$)
$= Pr(A_{i+1}|A_i)Pr(A_i) \leq \frac{1}{3}Pr(A_i) = \cdots \leq \frac{1}{3^{i-1}}$ (by induction)
say, B_i is the event that $M(x)$ halts after ith iteration then, $B_i \subset A_i$
$\implies Pr(B_i) \leq Pr(A_i)$
so, $Pr(N_{M,x} = i) \leq \frac{1}{3^{i-1}}$ for all $i \geq 1$
so, $E[N_{M,x}] = \sum_{i\geq 1} iPr(N_{m,x} = i) \leq \sum_{i\geq 1} \frac{i}{3^{i-1}} < k$
(for some $k > 0$, as the series converges)
Now, each iteration takes $p(|x|)$ time where $p(n)$ is a polynomial.
$\implies E[T_{M,x}] \leq kp(|x|)$ ($T_{M,x}$ is the random variable for time taken by $M(x)$)
so, expected time is polynomial in $|x| \implies$ RP $\cap$ coRP $\subseteq$ ZPP
$\implies$ ZPP = RP $\cap$ coRP.

Question 2.

We will prove it just like BPP $\subseteq$ P/poly
With the similar work like error reduction we will have a equivalent definition for randomisation reduction : $A \leq_r B$ iff there exists a polytime PTM M

$$(1)x \in A \implies P(B(M(x) = 1) \geq 1 - \frac{1}{2^{|x|+1}}$$

$$(2)x \notin A \implies P(B(M(x) = 1) \geq \frac{1}{2^{|x|+1}}$$

Hence from the calculation we done in the last assignment we can say there will be some random bits $r \in \{0,1\}^{p(n)}$ which is 'good' for any input x

Now using that machine M and random bits r we can construct a circuit which will end up giving the corresponding circuit of 3-SAT which is in NP/poly
And clearly the size will be atmost quadratic of running time of M which is polynomial on $|x|$

Claim. 3-SAT is in NP/poly

For CNF $\varphi(x_1, \ldots, x_n)$, we will basically construct a circuit which has branches of φ all possible assignment for $(x_1, \ldots, x_n)$. Now if $\varphi \in$ 3-SAT then we have a certified assignment for φ, hence we will consider that specific branch corresponds to that

satisfying assignment and vice versa
Hence our claim is true

Question 3.

Claim. $\exists$ $AM[O(1)]$ protocol for proving set lower bound so that error probability is exponentially small.

we have a $AM[O(1)]$ protocol for S so that,
if $|S| \geq K \implies Pr_r[\exists y : V(S,y,r) = 1] \geq \frac{2}{3}$
and, $|S| \leq \frac{K}{2} \implies Pr_r[\forall y,\ V(S,y,r) = 1] \leq \frac{1}{3}$
($S \subseteq \{0,1\}^m$ and for any $X \in S$ in S has a short membership proof)

Now, in our new protocol:
$V \rightarrow$ randomly picks n pairs (h_i, y_i) independently, where $h_i \in \mathcal{H}_{m,k}$, $y_i \in \{0,1\}^k$ and sends to P.
$P \rightarrow$ finds (if possible) $x_i \in S$ so that $h_i(x_i) = y_i$ and sends to V.
$V \rightarrow$ accepts iff $\exists$ more than $\frac{n}{2}$ functions in $\{h_i\}_{i=1}^n$ so that $h_i(x_i) = y_i$ for some $x_i \in S$.

Analysis: define $\{X_i\}_{i=1}^n$ be a random variables and

$$X_i = \begin{cases} 1 & \text{if } h_i(x_i) = y_i \text{ for some } x_i \in S \\ 0 & \text{otherwise} \end{cases}$$

and, $X = \frac{1}{n}\sum_{i=1}^n X_i$

if $|S| \geq K \implies \mu = E[X] \geq \frac{2}{3}$
so, $Pr[X \leq \frac{1}{2}] = Pr[X - \frac{2}{3} \leq -\frac{1}{6}] \leq Pr[|X - \mu| \geq \frac{1}{6}] \leq e^{-\frac{n}{c}}$
(for some constant c)
$\implies Pr[X > \frac{1}{2}] \geq 1 - e^{-\frac{n}{c}}$

again, if $|S| \leq \frac{K}{2} \implies \mu = E[X] \leq \frac{1}{3}$
so, $Pr[X > \frac{1}{2}] \leq Pr[X > \frac{1}{3} + \frac{1}{12}] \leq Pr[|X - \mu| > \frac{1}{12}] \leq e^{-\frac{n}{k}}$
for some constant k.
Hence, the error probability of our protocol becomes exponentially small.

here we define a perfectly complete $AM[O(1)]$ protocol for proving set lower bound:-

On input a set S,
I.V and P act as the protocol defined for exponentially small error.
II. V sends the description of S_x to P, P computes S_x and sends to V.
where $r \in S_x$ iff $\exists y$ so that $V(S,r,y) = 1$
and sends to V
and clearly for any $r \in S_x$, P can convince V with a small membership proof.

(say $n_1 = \frac{l}{n} + 1$, $|S_x| \geq (1 - \frac{1}{n_1 2^n})2^l$ if $x \in L$, and $|S_x| \leq \frac{1}{n_1 2^n} 2^l$ if $x \notin L$)
III. P produces $u_1, \dots u_{n_1} \in \{0,1\}^l$ and sends to V
IV. V picks randomly $r_0 \in \{0,1\}^l$ and sends to P
V. P proves if $r_0 \in \bigcup_{i=1}^{n_1}(S_x + u_i)$
if it can prove to V that, for some i, $r_0 + u_i \in S_x$ then, V accepts otherwise reject.

we know that, if $x \in L \implies |S_x| \geq (1 - \frac{1}{n_1 2^n})2^l$
$\implies \exists u_1, \dots u_{n_1}$ so that $\bigcup_{i=1}^{n_1}(S_x + u_i) = \{0,1\}^l \implies V$ accepts with probability 1.
$x \notin L \implies |S_x| \leq \frac{2^l}{n_1 2^n} \implies Pr[V \text{ accepts }] = Pr_{r \in \{0,1\}^l}[r_0 \in \bigcup_{i=1}^{n_1}(S_x + u_i)] \leq \frac{1}{2^n}$

Question 4.

We knwo there is a bijection $f : \{0,1\}^n \to \mathbb{F}_{2^n}$
Hence we can extend the bijection to an isomorphism and hence extend the set $\{0,1\}^n$ to a field of cardinality 2^n by defining the addition and the multiplication in this way:

$$a + b = f^{-1}(f(a) + f(b))$$
$$a.b = f^{-1}(f(a).f(b))$$

Now we will define $\mathcal{H}_{n,n}$ first
To define $\mathcal{H}_{n,k}$ for $k < n$ we can use the collection $\mathcal{H}_{n,n}$ and truncate the last $n - k$ bits of the output. It will be obvious from our procedure that removing last $n - k$ digits will not change the probability

Define
$$\mathcal{H}_{n,n} = \left\{h_{a,b} \middle| h_{a,b}(x) = ax + b, \forall a, b \in \{0,1\}^n\right\}$$
Now let for some $x_1 \neq x_2, y_1, y_2 \in \{0,1\}^n$ and $h_{a,b} \in \mathcal{H}_{n,n}$

$$\begin{aligned}
&\begin{cases} h_{a,b}(x_1) = y_1 \\ h_{a,b}(x_2) = y_2 \end{cases} \\
\implies &\begin{cases} ax_1 + b = y_1 \\ ax_2 + b = y_2 \end{cases} \\
\implies &\begin{bmatrix} x_1 & 1 \\ x_2 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \\
\implies &\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} x_1 & 1 \\ x_2 & 1 \end{bmatrix}^{-1} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \qquad \text{(the matrix is invertible as } x_1 \neq x_2\text{)}
\end{aligned}$$

So, $Pr_{h \in \mathcal{H}_{n,n}}[h(x_1) = y_1 \wedge h(x_2) = y_2]$
$= Pr_{a,b \in \mathbb{F}_{2^n}}[ax_1 + b = y_1 \wedge ax_2 + b = y_2]$

$= Pr_{a,b \in \mathbb{F}_{2^n}} [\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} x_1 & 1 \\ x_2 & 1 \end{bmatrix}^{-1} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}] = 2^{-2n}$

if $k < n$ then, by our construction,

$$\begin{aligned} & \begin{cases} h_{a,b}(x_1) = y_1 \\ h_{a,b}(x_2) = y_2 \end{cases} \\ \implies & \begin{cases} ax_1 + b = y_1' \\ ax_2 + b = y_2' \end{cases} \end{aligned}$$

where $y_1' = y_1 y_1''$ and $y_2' = y_2 y_2''$
y_1'' and y_2'' are $n-k$ length bit string and such y_1'', y_2'' will exist.
Hence, $Pr_{h \in \mathcal{H}_{n,k}}[h(x_1) = y_1 \wedge h(x_2) = y_2] = \dfrac{1}{2^{2n}}$

Question 5.

Let $\varphi = c_1 \wedge c_2 \wedge \cdots \wedge c_m$ be a 3-CNF formula on $x_1, \ldots, x_n$ variables
Now let $c_i = l_1 \vee l_2 \vee l_3$
Define $l_j' = x_k$ if $l_j = x_k$ for some x_k
if $l_j = \neg x_k$ for some x_k then $l_j' = 1 - x_k \; \forall j = 1, 2, 3$
Note $l_j' \equiv l_j$ *i.e.* if $l_j = 1$ then $l_j' = 1$ and if $l_j = 0$ then $l_j' = 0$
Define a new variable y_i which takes values from $\mathbb{F}_2$

$$\begin{aligned} & y_i = l_1 \vee l_2 \\ \implies & (1 - l_1')(1 - l_2') = 1 - y_i \\ \implies & y_i + l_1' + l_2' + l_1' l_2' = 0 \end{aligned}$$

Now say $p_{i1}(x_1, \ldots, x_n, y_1, \ldots, y_m) = y_i + l_1' + l_2' + l_1' l_2'$
Clearly $p_{i1} \equiv y_i \equiv l_1 \vee l_2$

Now $p_{i2}(x_1, \ldots, x_n, y_1, \ldots, y_m) = y_i + l_3' + y_i l_3' - 1$
Clearly $p_{i2} + 1 \equiv y_i \vee l_3$

clearly $p_{i1}, p_{i2} \in \mathbb{F}_2[x_1, \ldots, x_n, y_1, \ldots, m]$ and degree of each monomial in it is at-most 2
also $p_{i1} = 0 \iff y_i = l_1 \wedge l_2$ and $p_{i2} = 0 \iff y_i \wedge l_3$
Hence $p_{i1} = 0$ and $p_{i2} = 0 \iff$ for some assignment $c_i = 1$
(we can put the same values for x_i for both cases)
Hence $\{p_{i1}, p_{i2} | \forall i = 1(1)n\}$ has a solution iff φ has a satisfiable assignment.
(we can put the same values for x_i for both cases)

Clearly the reduction is in polynomial time. Hence 3-SAT $\leq_p$ QUADEQ
Hence QUADEQ is NP-Hard

Now $\{p_i(x_1, \ldots, x_n)\} \in$ QUADEQ
$\iff \exists$ some assignment for $(x_1, \ldots, x_n)$ s.t. $p_i(x_1, \ldots, x_n) = 0$

$\Longrightarrow$ it is in NP

Hence QUADEQ is NP-complete