# HW1 Advanced Proof systems

name : Guy Levy
id : 206865362

1.1:

$X$ non-negative RV.
$\mu = E[X]$.
$\alpha < 1$.

show $P(X > \alpha\mu) < \frac{1}{\alpha}$

assume $P(X > \alpha\mu) \geq \frac{1}{\alpha}$ for the sake of contradiction.

$E[X] = \Sigma_{x \geq 0} x Pr[X = x]$
$= \Sigma_{0 \leq x \leq \alpha\mu} x Pr[X = x] + \Sigma_{x > \alpha\mu} x Pr[X = x]$
$\geq 0 + \Sigma_{x > \alpha\mu} x Pr[X = x]$
$> \alpha\mu \cdot \frac{1}{\alpha} = E[X]$

which is a contradiction.

1.2:

show: $\forall \epsilon \in (0, p] : Pr[|X - p| > \epsilon] < 2^{-\omega(\epsilon^2 n)}$

will bound: $Pr[X - p > \epsilon]$ other side is similar.
$= Pr[\bar{X} > \epsilon]$
$= Pr[e^{\lambda \bar{X}} > e^{\lambda\epsilon}]$ (for any positive lambda)
$= Pr[e^{\lambda \bar{X}} > \frac{E[e^{\lambda \bar{X}}]}{E[e^{\lambda \bar{X}}]} e^{\lambda\epsilon}]$
$< \frac{E[e^{\lambda \bar{X}}]}{e^{\lambda\epsilon}}$ (from Markov's inequality choosing as $\alpha$: $\frac{e^{\lambda\epsilon}}{E[e^{\lambda \bar{X}}]}$)
$\leq \frac{e^{\frac{\lambda^2}{n} p(1-p)}}{e^{\lambda\epsilon}}$ (from lemma $(*)$ which we show later)
$= e^{-\frac{\epsilon^2}{4p(1-p)} n}$ (setting lambda as $\frac{n\epsilon}{2p(1-p)}$)
$= 2^{-\Omega(\epsilon^2 n)}$

$(*)$ lemma: $E[e^{\lambda\bar{X}}] \leq e^{\frac{\lambda^2}{n}p(1-p)}$ :

$E[e^{\lambda\bar{X}}]$
$= E[e^{\frac{\lambda}{n}\sum_i^n \bar{X}_i}]$
$= \Pi_i^n E[e^{\frac{\lambda}{n}\bar{X}_i}]$ (from the fact that $\bar{X}_i$ are independent)
$= \Pi_i^n (p \cdot e^{\frac{\lambda}{n}(1-p)} + (1-p) \cdot e^{\frac{\lambda}{n}(-p)})$
$\leq (p \cdot (1 + \frac{\lambda}{n}(1-p) + \frac{\lambda^2}{n^2}(1-p)^2) + (1-p) \cdot (1 + \frac{\lambda}{n}p + \frac{\lambda^2}{n^2}p^2))^n$
$= (1 + \frac{\lambda^2}{n^2}p(1-p))^n$
$= (1 + \frac{\frac{\lambda^2}{n}p(1-p)}{n})^n \to e^{\frac{\lambda^2}{n}p(1-p)}$
so for high enough $n$ we get what we need.

1.4:

$\Pi = (P, V)$
if $x \in L : Pr[(P,V)(x) = 1] \geq \frac{2}{3}$
if $x \notin L : \forall P^* \;\; Pr[(P^*, V)(x) = 1] \leq \frac{1}{3}$

denote $\Pi^t = (P^t, V^t)$ as we used this notation in class where
the interaction is repeated sequentially t times and V decides by majority.

completeness:
let $x \in L$
$Pr[(P^t, V^t)(x) = 1]$
$= Pr[V \text{ accepts } \frac{t}{2} \text{ of runs or more}]$
$= Pr[\frac{1}{t}\sum_i^t E_i \geq \frac{1}{2}]$ (where $E_i$ denotes indicator for the event that V accepted in the i'th round)
$\geq Pr[|\frac{1}{t}\sum_i^t E_i - \frac{2}{3}| \leq \frac{1}{6}]$
$= 1 - Pr[|\frac{1}{t}\sum_i^t E_i - \frac{2}{3}| > \frac{1}{6}]$
$> 1 - e^{-\frac{\frac{1}{6}^2}{4\frac{2}{3}(1-\frac{2}{3})}t}$ (from Chernoff proof in 1.2)
$> 1 - e^{-\frac{t}{32}}$
$= 1 - 2^{-\Omega(t)}$

soundness:
let $x \notin L$
$Pr[(P^t, V^t)(x) = 1]$
$= Pr[\frac{1}{t}\sum_i^t E'_i \geq \frac{1}{2}]$ ($E'_i$ : V accepts in the i'th run now that $x \notin L$)
$\leq Pr[|\frac{1}{t}\sum_i^t E'_i - \frac{1}{3}| > \frac{1}{6}]$ ($A \to B \Rightarrow Pr(A) \leq Pr(B)$)
$\leq 1 - e^{-\frac{\frac{1}{6}^2}{4\frac{2}{3}(1-\frac{2}{3})}t}$ (Chernoff)
$= 2^{-\Omega(t)}$

2.

show $IP^{ps} = NP$

$(I) \;\; NP \subseteq IP^{ps}$
Let $L \in NP$
exists polytime $V$ and polynomial $l$ such that
$\forall x \in L \; \exists m \in \{0,1\}^{l(|x|)} : V(x,m) = 1$
$\forall x \notin L \; \forall m^* \in \{0,1\}^{l(|x|)} : V(x, m*) = 0$

protocol:
$(P_1, V_1)$ where given $x$, $P_1$ searches for $m \in \{0,1\}^{l(|x|)}$ such that $V(x,m) = 1$
if $P_1$ finds such $m$ it sends is to $V_1$ which accepts if and only if $V(x,m) = 1$.

completeness:
let $x \in L$
$Pr[(P_1, V_1)(x) = 1]$
$= Pr[P_1 \text{ finds } m \text{ such that } V(x,m) = 1] = 1$ ($P_1$ is unbounded so finds such $m$ iff exists)
$\geq \frac{2}{3}$

perfect soundness:
let $x \notin L$
$Pr[(P_1, V_1)(x) = 1]$
$= Pr[P_1 \text{ finds } m \text{ such that } V(x,m) = 1] = 0$ (such $m$ does not exist)

$(II) \;\; IP^{ps} \subseteq NP$
Let $L \in IP^{ps}$
exists protocol $(P, V)$ ($V$ PPT, $P$ unbounded) such that:
if $x \in L : Pr[(P,V)(x) = 1] \geq \frac{2}{3}$
if $x \notin L \; \forall P^* : Pr[(P^*, V)(x) = 1] = 0$

can think of $V$ as deterministic poly machine that takes randomness string $\alpha$ as input.

let $x \in L$ , $Pr[(P,V)(x) = 1] \geq \frac{2}{3}$
$\Rightarrow \;\; \exists \alpha$ such that $(P, V_\alpha)(x) = 1$
the interaction is polynomial in $|x|$ ($V_\alpha$ is poly time)
and so we denote the interaction as $m$, then $V_\alpha(x,m) = 1$ (point 1)

let $x \notin L$, with the same $\alpha$ as before $\forall P^*$
$(P, V_\alpha)(x) = 0$ (because $\forall P^* \; Pr_\alpha[(P^*, V)(x) = 1] = 0$)
so no $m$ of polynomial length could be sent to $V_\alpha$ to make it accept on $x$

$\Rightarrow \ \forall m^* \ V_\alpha(x, m^*) = 0$ (point 2)

from point 1 and 2 we conclude $L \in NP$

3.

3.1
Find $k$ such that $V = V^k_{\text{naive}}$ satisfies:
if $|S| \geq t: \quad Pr[V() = 1] \geq 0.99$
if $|S| \leq \frac{t}{100}: \quad Pr[V() = 1] \leq 0.01$

Precalculations:
$Pr[V() = 1] = Pr[|\{i|u_i \in S\}| \geq \frac{kt}{2|U|}]$
(denote $E_i$ the indicator that $u_i \in S$)
$= Pr[\sum_i^k E_i \geq \frac{kt}{2|U|}]$
$= \frac{1}{k} Pr[\sum_i^k E_i \geq \frac{t}{2|U|}]$
$= Pr[\bar{E} \geq \frac{t-2|S|}{2|U|}]$ (using the notation convention from question 1)

Soundness:
$Pr[V() = 1] = Pr[\bar{E} \geq \frac{t-2|S|}{2|U|}]$
$\leq Pr[\bar{E} \geq \frac{0.98t}{2|U|}]$ (using $|S| \leq \frac{t}{100}$)
$\leq e^{-\frac{(0.49\frac{t}{|U|})^2}{4\frac{|S|}{|U|}(1-\frac{|S|}{|U|})}k} = 0.01$
$\Rightarrow \ k = -log(0.01) \cdot \frac{4}{(0.49)^2} \cdot \frac{|S|(|U|-|S|)}{t^2}$

Completeness:
$Pr[V() = 1] = Pr[\bar{E} \geq \frac{t-2|S|}{2|U|}]$
$\geq Pr[\bar{E} \geq \frac{-t}{2|U|}]$ (using $|S| \geq t$)
$= 1 - Pr[\bar{E} < \frac{-t}{2|U|}]$
$= 1 - Pr[|\bar{E}| > \frac{t}{2|U|}]$
$\geq 1 - e^{-\frac{(\frac{t}{2|U|})^2}{4\frac{|S|}{|U|}(1-\frac{|S|}{|U|})}k} = 0.99$
$\Rightarrow e^{-\frac{t^2k}{16|S|(|U|-|S|)}} = 0.01$
$\Rightarrow \ k = -16 \cdot log(0.01) \cdot \frac{|S|(|U|-|S|)}{t^2}$

So to acheive both completeness and soundness we take the higher $k$:
$k = -log(0.01) \cdot \frac{4}{(0.49)^2} \cdot \frac{|S|(|U|-|S|)}{t^2}$

3.2
We cannot replace the interactive protocol because the $k$ we found is needed to reach 0.01 error is often exponential
(as $|U| - |S|$ is often exponential) and so no lonely PPT verifier could get a good error in poly time using this protocol.
(for example in the protocol for showing $GNI \in AM$ we saw in class $|U| - |S|$ is exponential in $n$ the graph size).

4.

4.1
$C = A \cdot B$
algorithm:
for $i \in [n]$:
    for $j \in [n]$:
        $C_{i,j} = \sum_{k=1}^{n} A_{ik}B_{kj}$

4.2

$x \neq \vec{0}$ so $x_k \neq 0$ for some $k \in [n]$.
$y_k$ is random so $x_k y_k$ is random.
So $(\sum_{i \neq k, i \in [n]} x_i y_i) + (x_k y_k)$ is random.
i.e $\langle x, y \rangle$ is a uniformly random number sampled from $\mathbb{F}$ so:

$Pr_{y \in \mathbb{F}^n}[\langle x, y \rangle = 0] = \frac{1}{|\mathbb{F}|}$

4.3

describe PPT verifier $V(A, B, C)$:
sample $r \leftarrow \mathbb{F}^n$ ($O(n)$)
$r_B = B \cdot r$ ($O(n^2)$)
$r_{AB} = A \cdot r_B$ ($O(n^2)$)
$r_C = C \cdot r$ ($O(n^2)$)
if $r_{AB} = r_C$ accept ($O(n)$)

otherwise reject

$V$ runs in $O(n^2)$

completeness:
$AB = C \Rightarrow A(Br) = Cr \Rightarrow V(A, B, C) = 1 \Rightarrow Pr[V(A, B, C) = 1] = 1$

soundness:
$AB \neq C \Rightarrow AB - C \neq 0$
$Pr[V(A, B, C) = 1] = Pr[ABr = Cr] = Pr[(AB - C)r = 0]$
$= Pr[\forall i \in [n] : \langle row_i(AB - C), r\rangle = 0]$
( $AB - C \neq 0$ so there exists some $k \in [n]$ for which $row_k(AB - C) \neq \vec{0}$ )
$\leq Pr[\langle row_k(AB - C), r\rangle = 0]$
$= \frac{1}{|\mathbb{F}|}$ (from 4.2)
$\leq \frac{1}{2}$ (a field consists of at least 2 distinct elements)