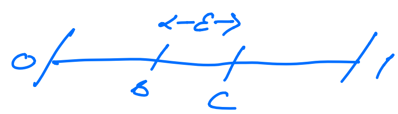
Today

- BPP error reduction (Chernoff Bound)
- BPP vs P/poly
- BPP vs PH
- Randomized Space

CSS.203.1 Computational Complexity
- Lecture #15 (7 Apr '21)

Instructor: Prahladh Harsha

$0 < s < c < 1$



$BPP_{c,s}$: $L \in BPP_{c,s}$ if

$\exists$ a TM M and a poly $p(\cdot)$ st

$x \in L \Rightarrow \Pr_r[M(x,r) = \text{accept}] \geq c$

$x \notin L \Rightarrow \Pr_r[M(x,r) = \text{accept}] \leq s.$

& furthermore M runs on the input pair (x,r) in time at most $p(|x|)$.

Last time: $BPP = BPP_{2/3,\, 1/3}$.

Today $BPP = BPP_{2/3,\, 1/3}$

$= BPP_{c,s}$ for all $0 < s < c < 1$ as long as $|c - s| \geq \frac{1}{poly(n)}$

$= BPP_{1 - 1/2^{n^d},\, 1/2^{n^d}}$, for all constants d.

BPP - machine : Semantic Definition.

Machine M - 2 inputs : x - real input

r - random input

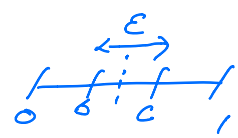
$$ACC_M(x) = \{ r \in \{0,1\}^m \mid M(x,r) = acc \}$$

$$REJ_M(x) = \{ r \in \{0,1\}^m \mid M(x,r) = acc \}$$

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^m} [r \in ACC(x)] \geq c$$

$$x \notin L \Rightarrow \Pr_{r \in \{0,1\}^m} [r \in ACC(x)] \leq s.$$

M - BPP m/c for $L \in BPP_{c,s}$



BPP error reduction ($t \in \mathbb{Z}_{>0}$)

M_t: On input x

- random input $(r_1 \ldots r_t) \in (\{0,1\}^m)^t$

- (1) Run $M(x, r_i)$, for $i \in [t]$

(2) Accept if

$$\#\{ i \mid M(x, r_i) = acc \} \geq \left(\frac{c+s}{2} \right) t$$

- reject otherwise.

Lemma $x \in L \Rightarrow \Pr_{r_1 \ldots r_t} [(r_1 \ldots r_t) \in ACC_{M_t}(x)] \geq 1 - \exp(-C\varepsilon^2 t)$

$$x \notin L \Rightarrow \Pr_{r_1 \ldots r_t} [(r_1 \ldots r_t) \in ACC_{M_t}(x)] \leq \exp(-C\varepsilon^2 t)$$

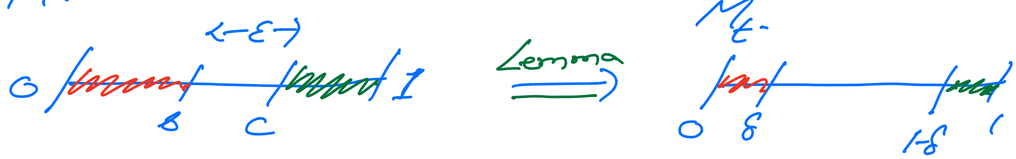
Remarks: (1). Choose $t = \frac{1}{C\varepsilon^2}\log\left(\frac{1}{\delta}\right)$

error of M_t can be made to be less than δ

(2) δ can be made as small as $\frac{1}{2^{n^d}}$ for any constant d & still keep t polynomial

(3) ε needs to be at least $\frac{1}{n^c}$ for some constant c.

M:



/ $\varepsilon \geq \frac{1}{n^c}$

$\delta = \frac{1}{2^{n^d}}$

$BPP_{c,s}$

$BPP_{1-\delta,\delta}$

Abstracting:

$Z_1, \dots, Z_t$

$Z_i = \mathbb{1}[r_i \in ACC(x)]$ Indicator r.v telling if the i^{th} random string causes m/c to acc

$$\begin{cases} x \notin L & \mathbb{E}[Z_i] = \Pr[Z_i = 1] \leq s. \\ \mathrm{Error}_{M_t}(x) = \Pr\left[\sum Z_i > \left(\frac{c+s}{2}\right)t\right] = \Pr\left[\sum Z_i > \left(s+\frac{\varepsilon}{2}\right)t\right] \end{cases}$$

$$\begin{cases} x \in L. & \mathbb{E}[Z_i] = \Pr[Z_i = 1] \geq c. \\ \mathrm{Error}_{M_t}(x) = \Pr\left[\sum Z_i < \left(\frac{c+s}{2}\right)t\right] = \Pr\left[\sum Z_i < \left(c-\frac{\varepsilon}{2}\right)t\right] \end{cases}$$

Thm: [Chernoff Bound]

$Z_1 \ldots Z_t$ – independent 0/1-valued random variables

$$\mathbb{E}[Z_i] = p$$

$$\Pr\left[\sum_{i=1}^{t} Z_i > (p+\varepsilon)t\right] \leq e^{-KL(p+\varepsilon \| p)\cdot t}$$

$$\Pr\left[\sum_{i=1}^{t} Z_i < (p-\varepsilon)t\right] \leq e^{-KL(p-\varepsilon \| p)\cdot t}$$

$KL(p+\varepsilon \| p)$: $\quad p, q \in (0,1)$

$$KL(p\|q) = p \ln \frac{p}{q} + (1-p)\ln\frac{(1-p)}{(1-q)}$$

$$KL(p+\varepsilon\|p),\ KL(p-\varepsilon\|p) = O(\varepsilon^2)$$

(Chernoff Bound $\Rightarrow$ Lemma)

Pf: (of Chernoff Bound)

(proof due to Kabanets-Impagliazzo)

Idea: Reduce to the RP-error reduction case.

$\forall S \subseteq [t]$

$$\Pr\left[\bigwedge_{i} (Z_i = 1)\right] = p^{|S|} \quad \ldots \quad (\star)$$

(independence of Z_i's)

Pick the set S randomly

For each $i \in [t]$, independently

$$\begin{cases} i \in S & - \text{ w/ prob } \lambda \\ i \notin S & - \text{ w/ prob } 1-\lambda \end{cases}$$

$$\Pr_{\substack{Z_1 \ldots Z_t \\ S}}\left[\bigwedge_{i \in S} (Z_i = 1)\right] \quad \ldots \quad (\star)$$

$$(\star) = \sum_{A \subseteq [t]} \Pr[S = A] \cdot \Pr\left[\bigwedge_{i \in S} (Z_i = 1) \,\middle|\, S = A\right]$$

$$= \sum_{A \subseteq [t]} \lambda^{|A|} (1-\lambda)^{t-|A|} \cdot p^{|A|}$$

$$= \sum_{k=0}^{t} \binom{t}{k} \lambda^k (1-\lambda)^{t-k} p^k$$

$$= (p\lambda + 1-\lambda)^t \quad \ldots \quad (1)$$

$$(*) \geq \underbrace{\Pr_{Z_1..Z_t}\left[\sum Z_i > (p+\varepsilon)t\right]}_{} \cdot \Pr\left[\bigwedge_{i\in S}(Z_i=1) \,/\, \sum Z_i > (p+\varepsilon)t\right]$$

$$\triangleq \mu \cdot \Pr_{S, Z_1..Z_t}\left[\bigwedge_{i\in S}(Z_i=1) \,\Big/\, \sum Z_i > (p+\varepsilon)t\right]$$

$$\geq \mu \cdot (1-\lambda)^{(1-p-\varepsilon)t} \quad \ldots \quad (2)$$

$$\mu \leq \left(\frac{p\lambda + 1-\lambda}{(1-\lambda)^{1-p-\varepsilon}}\right)^t = (f(\lambda))^t$$

· λ_* - λ minimizes $f(\lambda)$

$$\lambda_* = \frac{\varepsilon}{(p+\varepsilon)(1-p)}$$

(Check that $\lambda_* \leq 1 \iff p+\varepsilon \leq 1$)

$$f(\lambda_*) = \left(\frac{p}{p+\varepsilon}\right)^{p+\varepsilon}\left(\frac{1-p}{1-p-\varepsilon}\right)^{1-p-\varepsilon}$$

$$= e^{-KL(p+\varepsilon \| p)}$$

where $KL(p+\varepsilon \| p) = (p+\varepsilon)\ln\frac{p+\varepsilon}{p} + (1-p-\varepsilon)\ln\left(\frac{1-p-\varepsilon}{1-p}\right)$

$$\mu \le e^{-KL(p+\varepsilon \| p)\cdot t} \qquad \boxtimes$$

BPP's relationship w/ other complexity classes

- Last time

$$P \subseteq BPP \subseteq PSPACE$$

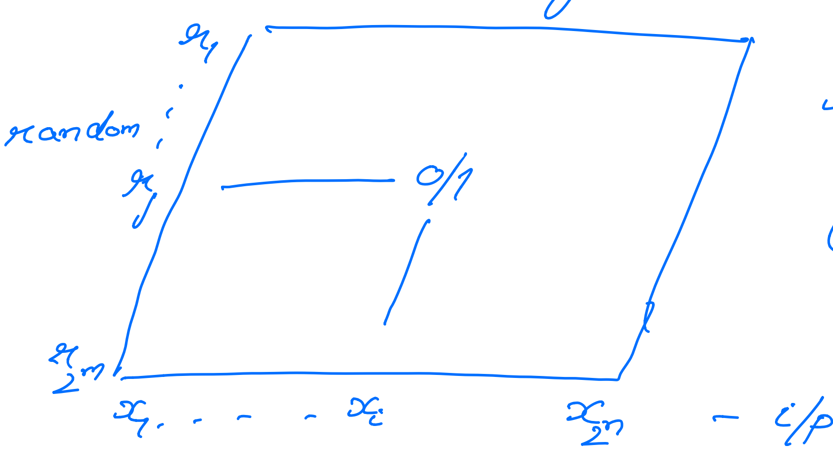
BPP vs P/poly

Theorem [Adleman] $BPP \subseteq P/poly$

$L \in BPP$

$L \in BPP_{1-\delta,\,\delta}$

Fix n - input length



For each input x, at least $(1-\delta)$ of random strings are correct

Suppose no random string is correct on all inputs.

fraction of error $\geq \frac{1}{2^n}$

$$\delta \geq \frac{1}{2^n}$$

Drive the error of BPP alg down to $\frac{1}{2^{n+1}}$

then $\delta < \frac{1}{2^n}$

Hence, there exists a random string that is correct $\forall$ inputs of length n.

Alternatively

If, $\Pr_r[\exists x \in \{0,1\}^n, r \in ERR_M(x)] < 1$

then $\exists$ random string r that is correct for all inputs $x \in \{0,1\}^n$

$$\Pr_r[\exists x, r \in ERR_M(x)]$$

$$\leq \sum_{x \in \{0,1\}^n} \Pr[r \in ERR_M(x)]$$

$$\leq 2^n \cdot \delta < 1 \quad \left(\text{if } \delta = \frac{1}{2^{n+1}}\right)$$

Hence, $L \in P/poly$

BPP vs PH

Theorem [Gacs–Sipser] $BPP \subseteq \Sigma_2^p \cap \Pi_2^p$

Pf: Suffices to show $BPP \subseteq \Sigma_2^p$

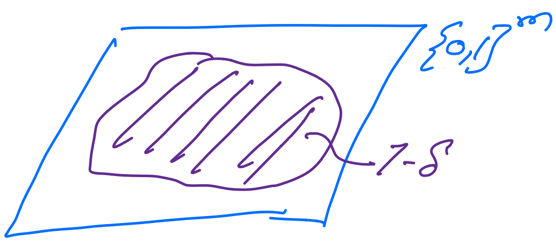
$L \in BPP$

Assume error $\leq \delta$.

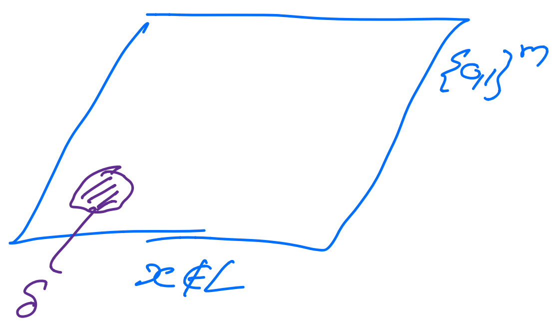
To show $L \in \Sigma_2^p$, we need to show

$$x \in L \iff \exists z\ \forall y,\ \varphi(x,y,z)$$

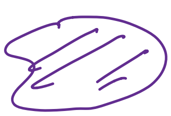
Lautemann's proof



$x \in L$



$x \notin L$

 — $ACC(x)$

$S \subseteq \{0,1\}^m$, $u \in \{0,1\}^m$

$S \oplus u = \{x \oplus u \mid x \in S\}$

$(x \oplus u)_i = x_i \oplus u_i$

Idea:

$x \in L$: $|ACC(x)| \geq (1-\delta) \cdot 2^m$

$\exists$ few translates $u_1 \dots u_k$

$$\bigcup_{i=1}^{k} (ACC(x) \oplus u_i) = \{0,1\}^m$$

$\Rightarrow \exists\, u_1 \dots u_k\ \forall r \in \{0,1\}^m,\ \exists i \in [k]$

$r \in ACC(x) \oplus u_i$.

$\Rightarrow \exists\, u_1 \dots u_k\ \forall r \in \{0,1\}^m\ \bigvee_{i=1}^{k} (M(x, r+u_i) = 1)$

Similarly,

$x \notin L \Rightarrow |ACC(x)| \leq \delta \cdot 2^m$

$\forall$ few translates $u_1 \dots u_k$ $\bigcup_{i=1}^{k} (ACC(x) \oplus u_i)$

$\neq \{0,1\}^m$

$\Downarrow$

$\forall\, u_1 \dots u_k\ \exists r \in \{0,1\}^m\ \bigwedge_{i=1}^{k} (M(x, r+u_i) = 0)$

Claim: If δ, k satisfy $\delta k < 1$

$x \notin L \Rightarrow \forall u_1 \dots u_k$ $\bigcup (ACC(x) \oplus u_i)$

$\neq \{0,1\}^m$

Pf: $|\bigcup ACC(x) \oplus u_i| \leq k \cdot |ACC(x)|$

$\leq k \cdot \delta\, 2^m < 2^m$ $\boxtimes$

Claim: If δ, k satisfy $2^m \cdot \delta^k < 1$
$\exists\, u_1 .. u_k,\ \bigcup (ACC(x) + u_i) = \{0,1\}^m$

Pf: Probabilistic method
Choose $u_1 .. u_k$ randomly

$$\Pr_{u_1..u_k}\left[\bigcup (ACC(x) \oplus u_i) = \{0,1\}^m\right]$$

$$= 1 - \Pr_{u_1..u_k}\left[\exists r \in \{0,1\}^m,\ r \notin \bigcup (ACC(x) \oplus u_i)\right]$$

$$> 1 - \sum_{r \in \{0,1\}^n} \Pr_{u_1..u_k}\left[r \notin \bigcup (ACC(x) \oplus u_i)\right]$$

$$= 1 - \sum_{r \in \{0,1\}^n} \Pr_{u_1..u_k}\left[\forall i \in [k],\ r \notin ACC(x) \oplus u_i\right]$$

$$= 1 - \sum_{r} \left(\Pr\left[r \notin ACC(x) \oplus u\right]\right)^k$$

$$\geq 1 - \sum_{r} \delta^k = 1 - 2^m \cdot \delta^k$$

If $2^m \cdot \delta^k < 1$, then $\exists\, u_1 .. u_k ..$

$\boxtimes$

Two conditions

$$\left.\begin{array}{l} \delta k < 1 \\ 2^m \cdot \delta^k < 1 \end{array}\right\} \Leftarrow \left\{ \frac{m}{\log(\frac{1}{\delta})} < k < \frac{1}{\delta} \right.$$

Choose $\delta = \frac{1}{2^n}$ & $k = m$.

satisfies above.

$BPP \subseteq \Sigma_2^P$ $\boxtimes$