BPP and relationship with other classes

(Theorems about BPP)

[Adleman 79] $BPP \subsetneq P/poly$

Hardcoding the randomness

Choices of r

2^m

$m = |r|$

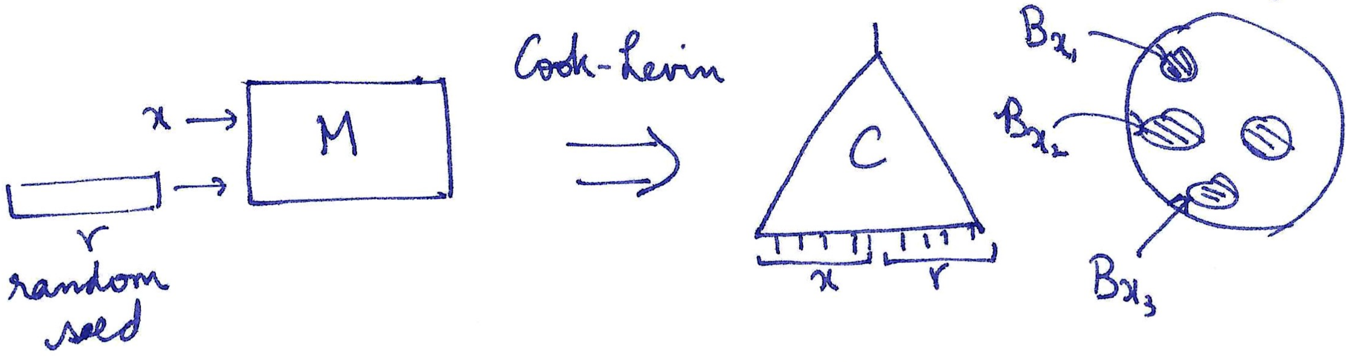
$m = p(n)$

Proof: Consider $\mathcal{L} \in BPP$

$\exists$ prob. poly time TM s.t.

$$\forall x \quad \Pr_r \left[M(x,r) \neq \mathcal{L}(x) \right] < 1/2^n$$

Let $\mathcal{L}_n$ be strings in $\mathcal{L}$ of length n. We need to construct circuit C_n that decides $\mathcal{L}_n$.



For x of length n, define $B_x = \{ r \mid |r| = p(n) \text{ s.t. } M(x,r) \neq \mathcal{L}(x) \}$

I want to find string r, $|r| = p(n)$

s.t. $\forall x$ of length n, $x \notin B_x$

$$\equiv \boxed{r \notin \bigcup_{x \in \{0,1\}^n} B_x}$$

$$\Pr_r\Big[r \notin \bigcup_{x\in\{0,1\}^n} B_x\Big] = 1 - \Pr_r\Big[r \in \bigcup_{x\in\{0,1\}^n} B_x\Big] > 0$$

$$\Pr_r\Big[r \in \bigcup_x B_x\Big] \leq \sum_{x\in\{0,1\}^n} \Pr_r\big[r \in B_x\big]$$ Union Bound

$$< \sum_x 1/2^n < 1$$

→ There exists $r_n \notin \bigcup_x B_x$

This r_n is a "universal" good random seed for all inputs of length n.

Consider running $M(x, r_n)$ where $x \in \{0,1\}^n$

Output $M(x, r_n) = L(x)\ \forall x \in \{0,1\}^n$

There is a circuit of polynomial size that "implements" $M(x, \boxed{r_n})$ $C_n(x)$ ∎

↳ fixed.

Thm [Sipser - Gács 82, 83] $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$.

(Note that $BPP = \text{co-}BPP$.

It suffices to prove $BPP \subseteq \Sigma_2^P$.

$BPP = \text{co-}BPP \subseteq \text{co-}\Sigma_2^P = \Pi_2^P$)

Proof of Clm 2: $\left|\bigcup_{i=1}^{k}(u \oplus S)\right| \leqslant \sum_{i=1}^{k} |u \oplus S| = k|S|$

$$\leqslant k \times \frac{2^m}{2^n} < 2^m$$

$\frac{2m}{n}$

$m = poly(n)$

Proof of Clm 1: Pick shifts $u_1, \ldots, u_k$ uniformly at random

To show

$$\Pr_{u_1, \ldots, u_k}\left[\bigcup_{i=1}^{k}(u_i \oplus S) = \{0,1\}^m\right] > 0$$

$$\Longleftrightarrow \Pr_{u_1, \ldots u_k}\Big[\exists\, y \in \{0,1\}^m \text{ s.t. } \underbrace{y \notin \bigcup_{i=1}^{k}(u_i \oplus S)}_{\text{Call this event } B_y}\Big] < 1$$

$$\Pr_{u_1 \ldots u_k}\left[\bigcup_{y \in \{0,1\}^m} B_y\right]$$

$$\leqslant \sum_{y} \Pr_{u_1 \ldots u_k}[B_y] < 2^m \times 2^{-m} = 1$$

Clm: $\Pr_{u_1 - u_k}[B_y] < 2^{-m}$

Proof: $\Pr_{u_1 - u_k}[B_y] = \Pr_{u_1 -- u_k}\left[y \notin \bigcup_{i=1}^{k}(u_i \oplus S)\right]$

$$= \Pr_{u_1 -- u_k}\Big[\bigcap_{i=1}^{k}\underbrace{(y \notin (u_i \oplus S))}_{y \text{ is not covered by } i^{th} \text{ shift}}\Big]$$

$$= \prod_{i=1}^{k} \Pr_{u_i}[y \notin (u_i \oplus S)]$$

$y \notin u_i \oplus S$

$u_i \oplus y \notin S$

$k = \frac{2m}{n}$

$u_i \notin S \oplus y$

$$= \prod_{i=1}^{k} \Pr_{u_i}[u_i \notin S \oplus y] < (2^{-n})^k = 2^{-n\left(\frac{2m}{n}\right)} < 2^{-m}$$

$|S \oplus y| = |S| > (1 - 2^{-n}) \times 2^m$

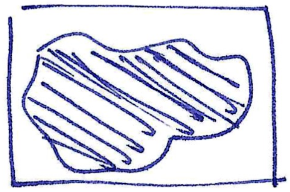
$\Pr_{u_i}[u_i \notin S \oplus y] < 2^{-n}$

$\blacksquare$

Clm 1 (Covering when $x \in L$) $S \subseteq \{0,1\}^m$ $\left(k = \frac{2m}{n}\right)$

If ~~$|A_x| \geq$~~ $|S| \geq \left(1 - \frac{1}{2^n}\right) 2^m$ then

$\exists\ u_1, u_2, \ldots, u_k \in \{0,1\}^m$ s.t.



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

Clm 2 (Inability to cover when $x \notin L$) : $S \subseteq \{0,1\}^m$

If $|S| < \frac{2^m}{2^n}$ then $\forall\ u_1, \ldots, u_k \in \{0,1\}^m$

$$\bigcup_{i=1}^{k} (u \oplus S) \subsetneq \{0,1\}^m$$

If $x \in L$, $|A_x| > \left(1 - \frac{1}{2^n}\right) 2^m$. If $x \notin L$, $|A_x| < \frac{2^m}{2^n}$

Combining with Clms 1 & 2,

$$x \in L \iff \exists\ u_1, \ldots, u_k \in \{0,1\}^m \text{ s.t. } \bigcup_{i=1}^{k} (u \oplus A_x) = \{0,1\}^m$$

$$\iff \exists\ u_1, \ldots, u_k\ \forall\ y \in \{0,1\}^m\ [\exists\ i \leq k \text{ s.t. } y \in u_i \oplus A_x]$$

$$\iff \exists\ u_1 \ldots u_k\ \forall\ y\ [\exists\ i \leq k \text{ s.t. } u_i \oplus y \in A_x]$$

$$\iff \exists\ u_1 \ldots u_k\ \forall\ y\ [\underbrace{\exists\ i \leq k \text{ s.t. } M(x, u_i \oplus y) \text{ accepts}}_{\text{Poly. time computation}}]$$

Hence $L \in \Sigma_2^P$.

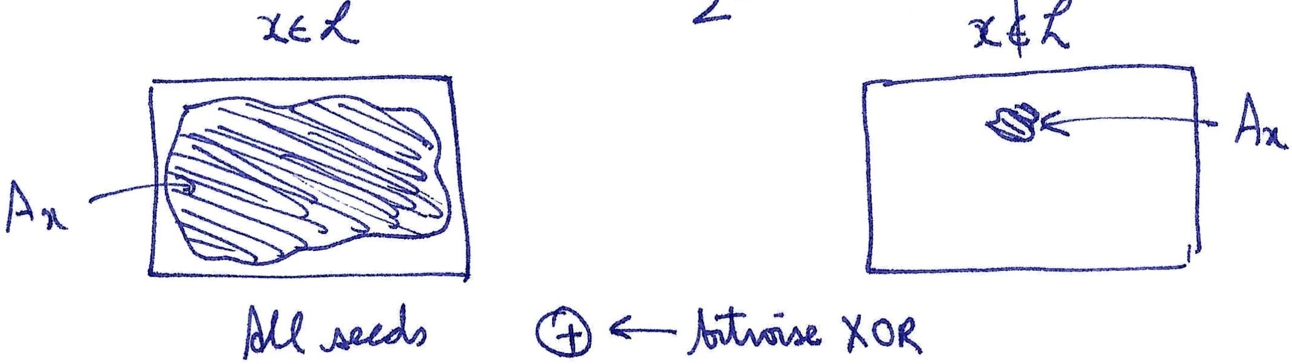
Proof: $L \in BPP$. There exists a poly. time prob TM M and a size bound $m = p(n)$ s.t.

$$\forall x: \quad \Pr_{r \in \{0,1\}^{\underbrace{p(n)}_{m}}} \left[M(x,r) \neq L(x) \right] < 1/2^n$$

For x, $A_x = \{ r \in \{0,1\}^m \mid M(x,r) \text{ accepts} \}$

If $x \in L$: $\quad |A_x| > (1 - 1/2^n) \underbrace{2^m}_{\text{all seeds/choices of randomness}}$

If $x \notin L$, $\quad |A_x| < \dfrac{2^m}{2^n}$



$\oplus$ ← bitwise XOR

$$x \oplus y$$

Consider $u \in \{0,1\}^m$

$u \oplus A_x = \{ u \oplus v \mid v \in A_x \}$ "Shifting A_x by u"

$|u \oplus A_x| = |A_x|$

$k = 2m/n = \text{poly}(n)$