Lecture 11

Note Title

Today:
- Amplification of BPP
- $BPP \subseteq PH$
- $BPP \subseteq \Sigma_2^p \cap \Pi_2^p$

Weak & Strong definitions of BPP

$L \in$ Strong BPP if $\forall$ poly $q(n)$

$\exists$ det. polytime $M(\cdot,\cdot)$ s.t. $\forall x \in \{0,1\}^n$

$x \in L \Rightarrow \Pr[M(x,y) \text{ accepts}] \geq 1 - 2^{-q(n)}$

$x \notin L \Rightarrow \Pr[M(x,y) \text{ accepts}] \leq 2^{-q(n)}$

$L \in$ Weak BPP if $\exists$ nice $S(n)$ & poly $p(n)$ and det. polytime $M(\cdot,\cdot)$ s.t. $\forall x \in \{0,1\}^n$

$$x \in L \Rightarrow \Pr[M(x,y) \text{ accepts}] \geq S(n) + \frac{1}{p(n)}$$

$$x \notin L \Rightarrow \Pr[M(x,y) \text{ accepts}] \leq S(n)$$

AMPLIFICATION THEOREM:

Strong BPP = Weak BPP

Proof: (of "$\supseteq$")

Say $L \in$ Weak BPP with m/c M, $S(n)$, $P(n)$

Consider M' which does the following

$M'(x; y_1 \dots y_t)$

- Let $z_i = M(x, y_i)$

  & $\bar{z} = \frac{\sum z_i}{t}$

- if $\bar{z} \geq s(n) + \frac{1}{2 \cdot p(n)}$ accept x;

  else reject.

To analyse need to know

What is the probability that if

t i.i.d. (independent indentically dist)

random variables $z_1 \dots z_t$ $z_i \in [0,1]$

with expectation μ take on average

value $\notin [\mu \pm \epsilon]$

Chernoff Bound:

if $Z_1 \ldots Z_t$ i.i.d. in $[0,1]$ &

$E[Z_i] = \mu$ then $P_r\left[\left|\frac{\sum Z_i}{t} - \mu\right| \geq \epsilon\right] \leq e^{-\epsilon^2 t}$

Applying to our case:

Say $x \in L$; then $E[Z_i] = s(n) + \frac{1}{p(n)}$

$$P_r\left[\frac{\sum Z_i}{t} \leq \left(s(n) + \frac{1}{2 \cdot p(n)}\right)\right]$$

$$\leq P_r\left[\left|\frac{\sum Z_i}{t} - s(n)\right| \leq \frac{1}{2 \cdot p(n)}\right]$$

$$\leq \exp\left(-t/p(n)^2\right).$$

Picking $t \geq q(n) \cdot p(n)^2$ works.
(Similarly when $x \notin L$) $\boxtimes$

$BPP \subseteq P/_{poly}$ [Adleman]

- Suffices to prove Strong $BPP \subseteq P/_{poly}$!
- Say $L \in$ Strong BPP.
  - Set $q(n) = 2n$ & say M places L in strong BPP
  - Say y wrong for x if

    $$M(x,y) \neq L(x)$$

  - Fix x;

    $$\Pr_y [y \text{ wrong for } x] \leq \frac{1}{2^{2n}}$$

  - $$\Pr_y \left[\exists x \text{ s.t. } y \text{ wrong for } x \right] \leq \frac{2^n}{2^{2n}} \leq \frac{1}{2^n}$$

- $\Rightarrow \exists y$ s.t. y not wrong for any x.
- Use M as advice TM with advice y. Always Right! $\boxtimes$

Implications:

[100 : 1] ↑ my odds

NP $\subseteq$ BPP (very unlikely)

$\Rightarrow$ NP $\subseteq$ P/poly

$\Rightarrow$ PH Collapses

$\Rightarrow$ $\neg$ IHA (unlikely)

[10 : 1] ↑ my odds

$BPP \subseteq \Sigma_2^P \cap \Pi_2^P$ [Sipser-Lautemann]

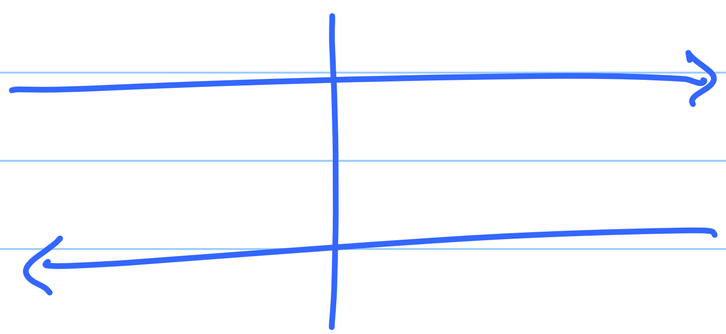
Recall Σ_2^P

Prosecution: "$x \in L$"

$= \Pr[m(x,y) \text{ accepts}]$ huge

Defense: "What? me?"

tiny



Jury decides.

Idea 1:

Let Defense pick y ... but this is no good -- since $\exists y$ s.t. $M(x, y)$ rejects.

Idea 2:

Let Prosecution pick y .... but this is no good either ....

Idea 3: (almost works)

- Let Defense pick most bits of y
- Prosecution picks remaining few.

Idea 4: (cleaner implementation)

- Prosecution specifies $y_1 \dots y_k$ (first) : k possible variations
- Defense picks y.

[Idea 3 may work, but depends on M;
Idea 4 cleaner]

Σ_2^P : $x \in L$ (BPP-decided by M)

Prosecution $\qquad\qquad\qquad\qquad$ Defense

$$\xrightarrow{\quad y_1 \dots y_k \quad}$$

$$\xleftarrow{\quad y \quad}$$

Jury: Accept if $\exists i$ s.t.

$M(x, y \oplus y_i)$ accepts

Completeness: $x \in L \Rightarrow \exists\, y_1 \dots y_k$ s.t.

$\forall\, y$

$\exists\, i$ s.t.

$M(x, y \oplus y_i)$ accepts.

[Sort of like Adleman].

Proof: y_i wrong for y if $M(x, y \oplus y_i)$ rejects

- $\Pr_{y_i}[\,y_i \text{ wrong for } y\,] \le \frac{1}{2^{\ell(m)}} \le \frac{1}{2}$
- $\Pr_{y_1 \dots y_k}[\,y_1 \dots y_k \text{ all wrong for } y\,] \le \frac{1}{2^k}$ [independent]
- $\Pr_{y_1 \dots y_k}[\,\exists\, y \text{ s.t. } \sim\,] \le \frac{\# y}{2^k}$

Pick $k \ge |y| + 1$ & we are o.k. ⊠

↓ Now we're with the defense.

Soundness: $x \notin L \Rightarrow \forall y_1 \ldots y_k \ \exists y$ s.t.

$\forall i \quad M(x, y \oplus y_i)$ rejects.

Proof:
- y wrong for y_i if $M(x, y \oplus y_i)$ accepts.
- $\Pr_y [y \text{ wrong for } y_i] \leq 2^{-q(n)}$
- $\Pr_y [\exists i \in [1 \ldots k] \text{ s.t. } y \text{ wrong for } y_i] \leq k \cdot 2^{-q(n)}$

$$= 2|y| \cdot 2^{-q(n)} < 1 \,?$$

Set $q(n) = n$; then $|y| = n^c$ for some c; for large enough n above is < 1. $\boxtimes$

Implications

- Quantifiers do capture uncertainty
- Randomized hierarchy

$\boxed{\text{promise } RP} \ni (\Pi_Y, \Pi_N)$

s.t. $\exists M$

$x \in \Pi_Y \Rightarrow \Pr_y [M(x,y) \text{ accepts}] \geq \frac{2}{3}$

$x \in \Pi_N \Rightarrow \qquad = 0$

---

promise BPP $\ni (\Pi_Y, \Pi_N)$ s.t. ....

$x \in \Pi_Y \Rightarrow \ldots \qquad \geq \frac{2}{3}$

$x \in \Pi_N \Rightarrow \ldots \qquad \leq \frac{1}{3}$

- $\text{promise RP}^{\text{promise RP}} \subseteq \text{promise-BPP}$
- $\text{promise BPP}^{\text{promise BPP}} \subseteq \text{promise-BPP}$
- [EXERCISE]:

  $\text{Promise-BPP} \subseteq \text{promise RP}^{\text{promise RP}}$

- [Continued]

  $P = \text{Promise-RP} \Rightarrow P = \text{Promise-BPP}.$

  $\boxtimes$

Next two lectures

$$\left.\begin{array}{l}\text{Unique SAT ;}\\ \text{Parity SAT ;}\\ \text{\# SAT ;}\end{array}\right\}$$ Counting # solutions....

- Unique-SAT : Motivated by Crypto & one-way permutations.

"Hard to invert functions in crypto" have unique inverse ; but maybe "uniqueness" ⇒ easy ?

[Valiant-Vazirani]:

Defn: Unique SAT $= (\Pi_Y, \Pi_N)$

$$\Pi_Y = \{ \phi \mid \exists !\, x \text{ s.t. } \phi(x) = 1 \}$$

$$\Pi_N = \{ \phi \mid \forall x \quad \phi(x) = 0 \}$$

[W]: SAT $\leq_R$ Unique-SAT

$\leq_R$: Randomized reduction!

$A \leq_R B$ if $\exists$ prob. alg. R, poly p s.t.

$x \in A_Y \Rightarrow R(x) \in B_Y$ w.p. $\geq \frac{1}{p(n)}$

$x \in A_N \Rightarrow R(x) \in B_N$ w.p. 1.

[Warning: Doesn't amplify].

[VV] Idea: • Guess # solutions to ϕ approximately. Say $\# \in \{2^{m-1}+1 \ldots 2^m\}$

• Pick "random" hash function (How? Later!)

$$h : \{0,1\}^n \to \{0,1\}^{m+c}$$

• Map $\phi(x) \longrightarrow \phi'(x) =$

"$\phi(x)$ and

$h(x) = (0 \ldots 0)$".

• Claims: 1. ϕ' can be computed in polytime from ϕ.

2. $\exists\, x$ s.t. $\phi'(x) = 1$

3. x above is unique

$\Big\}$ w.p. > 0.

Ignoring (1) for now; can pick h totally at random.

Then (2):

$$\Pr[\exists x \text{ s.t. } h(x) = \bar{0}]$$

$$\geq 1 - \left(1 - \frac{1}{2^{m+c}}\right)^{2^{m-1}}$$

$$= \Omega\left(\frac{1}{2^c}\right)$$

(3):

$$\Pr[\exists x, y \text{ s.t. } h(x) = h(y) = \bar{0}]$$

$$\leq \frac{1}{2^{m+c}} \cdot \frac{1}{2^{m+c}} \cdot 2^m \cdot 2^m$$

$$= O\left(\frac{1}{2^{2c}}\right) \quad \ldots$$

Next Lecture:

- Using Pairwise Independent h.
- Formal analysis.