Today: Amplification of BPP

- \text{BPP} \subseteq \text{PH}
- \text{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p

Weak & Strong definitions of BPP

L \in \text{Strong BPP} \iff \nexists \text{ poly } q(n) \exists \text{ det. } \text{ poly-time } M(*,*) \text{ s.t. } \forall x \in \{0,1\}^n

\text{if } x \in L \implies \Pr[M(x,y) \text{ accepts}] \geq 1 - 2^{-2^{\Omega(n)}}

\text{if } x \notin L \implies \Pr[M(x,y) \text{ accepts}] \leq 2^{-2^{\Omega(n)}}
$L \in \text{Weak BPP}$ if \( \exists \) nice \( S(n) \) & poly \( p(n) \) and det. polytime \( M(\cdot, \cdot) \) s.t. \( \forall x \in \{0,1\}^n \):

\[
\begin{align*}
    x \in L & \implies \Pr \left[ M(x, y) \text{ accepts} \right] \geq S(n) + \frac{1}{p(n)} \\
    x \notin L & \implies \Pr \left[ M(x, y) \text{ accepts} \right] \leq S(n)
\end{align*}
\]

**Amplification Theorem:**

**Strong BPP = Weak BPP**

**Proof:** (of “\( \geq \)“)

Say \( L \in \text{Weak BPP} \) with m/c \( M, S(n), p(n) \)

Consider \( M' \) which does the following
\[ M'(x; y_1, \ldots, y_t) \]

- 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 \( x_i \);
  else reject

To analyze need to know

What is the probability that if \( t \) i.i.d. (independent identically dist)
random variables \( Z_1, \ldots, Z_t \), \( Z_i \in [0, 1] \)
with expectation \( \mu \) take on average value \( \mu \pm \epsilon \)
Chernoff Bound:

if $Z_1 \ldots Z_t$ i.i.d. in $[0,1]$ &
$E[Z_i] = \mu$ then $P_r \left[ \left| \frac{\sum Z_i}{t} - \mu \right| \geq \epsilon \right] \leq e^{-\frac{\epsilon^2 t}{2}}$

Applying to our case:

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

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

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

$\leq \exp \left( - \frac{t}{\rho(n)^2} \right)$.

Picking $t \geq q(n) \cdot \rho(n)^2$ works.

(Similarly when $x \notin L$)
$\text{BPP} \leq \text{P}^\text{poly}$  \hspace{1cm} [\text{Adleman}]

- Sufﬁce to prove Strong BPP $\leq \text{P}^\text{poly}$.
- Say $L \in \text{Strong BPP}$.
  - Set $q(n) = 2^n$ and say $M$ runs $L$ in strong BPP.
- Say $y$ wrong for $x$ if
  \[ M(x, y) \neq L(x) \]
- Fix $x$;
  \[ \Pr[y \text{ wrong for } x] \leq \frac{1}{2^{2n}} \]
- \[ \Pr[y \text{ s.t. } y \text{ wrong for } x] \leq \frac{2^n}{2^{2n}} = \frac{1}{2^n} \]
\[ \Rightarrow \exists y \text{ s.t. } y \text{ not wrong for any } a. \]

- Use \( M \) as advice \( TM \) with advice \( y \). Always Right! \( \square \)

---

**Implications:**

\[ \frac{100}{1} \]

\[ \frac{10}{1} \]

\[ \frac{my \ odds}{my \ odds} \]

\[ NP \subseteq BPP \text{ (very unlikely)} \]

\[ \Rightarrow NP \subseteq \mathbb{P}^{1 \text{/poly}} \]

\[ \Rightarrow \text{PH collapses} \]

\[ \Rightarrow \exists IHA \text{ (unlikely)} \]
\[ \text{BPP} \leq \Sigma^p_2 \cap \Pi^p_2 \quad \text{[Sipser-Lautemann]} \]

Recall \( \Sigma^p_2 \)

Prosecution: "\( x \in L \)"

\[ = \Pr \left[ m(x, y) \text{ accepts} \right] \]

\( \quad \text{huge} \quad \text{tiny} \)

Defense: "What? me?"

\[ \text{Jury decides.} \]
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 $Y_1 \ldots Y_k$: $k$ possible variations
- Defense picks $y$.
Idea 3 may work, but depends on $M$; Idea 4 cleaner

$$\Sigma_2^p \ni x \in L \quad (\text{BPP-decided by } M)$$

**Prosecution**

$$Y_1, \ldots, Y_k$$

**Defense**

$$y$$

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

$$M(x, y \oplus y_i) \text{ accepts}$$
Completeness: \( x \in L \Rightarrow \exists y_1, \ldots, y_k \text{ s.t.} \)

\[ \forall y \]

\[ \exists i \text{ s.t.} \]

\[ M(x, y \oplus y_i) \text{ accepts.} \]

[Sort of like Adleman].

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

- \( \Pr_{y_i} \left[ y_i \text{ wrong for } y \right] \leq \frac{1}{2^{en}} \leq \frac{1}{2} \)

- \( \Pr_{y_1, \ldots, y_k} \left[ y_1, \ldots, y_k \text{ all wrong for } y \right] \)

\[ \left( \frac{1}{2^{en}} \right)^k \leq \frac{1}{2^k} \text{ [independent]} \]

- \( \Pr_{y_1, \ldots, y_k} \left[ \exists y \text{ s.t.} \right] \leq \frac{\#y}{2^k} \)

Pick \( k \geq |y| + 1 \) we are ok.
\[ \text{Now we're with the defense.} \]

**Soundness:** \( x \in L \Rightarrow \forall y \ldots y_k \exists y_i \text{ s.t.} \]

\( \forall i \) \( m(x, y \oplus y_i) \) reject.

**Proof:**

- \( y \) wrong for \( y_i \) if

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

- \( \Pr_y [y \text{ wrong for } y_i] \leq 2^{-2^n} \)

- \( \Pr_y [\exists i \in [1 \ldots k] \text{ s.t. } y \text{ wrong for } y_i] \leq k \cdot 2^{-2^n} \)

\[ = 2|y| \cdot 2^{-2^n} \leq 1 \?

Set \( q(n) = n \); then \( |y| = n^c \) for some \( c \); for large enough \( n \)

above is \( < 1 \).
Implications

- Quantifiers do capture uncertainty

Randomized hierarchy

\[ \text{promise } \text{RP} \supseteq (\Pi_y, \Pi_N) \]

\[ \exists M \ni \forall x \in \Pi_y \Rightarrow R_y \left[ M(x, y) \text{ accept} \right] \geq \frac{2}{3} \]

\[ \exists x \in \Pi_N \Rightarrow \quad 0 \]

\[ \text{promise } \text{BPP} \supseteq (\Pi_y, \Pi_N) \quad \forall \]

\[ \forall x \in \Pi_y \Rightarrow \quad \geq \frac{2}{3} \]

\[ \forall x \in \Pi_N \Rightarrow \quad \leq \frac{1}{3} \]
• $\text{promise RP} \leq \text{promise- BPP}$

• $\text{promise BPP} \leq \text{promise- BPP}$

• [Exercice]:
  
  $\text{promise- BPP} \leq \text{promise RP}$

• [Continued]:

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

Unique SAT;
Parity SAT; \# SAT;

\{ Counting \# solutions….

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

"Hard to invert functions in crypto" have unique inverse; but maybe "uniqueness" = easy?
Vahid-Vazirani:

**Def**: Unique SAT = $(\Pi_Y, \Pi_N)$

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

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

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

$\leq_R$: Randomized reduction!

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

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

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

[Warning: Doesn't amplify].
Idea: Guess # solutions to \( \phi \)

approximately. Say \( # \in [2^{m-1} + 1 \cdots 2^m] \)

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

\[ h : \{0,1\}^n \rightarrow \{0,1\}^{m+c} \]

- Map \( \phi(x) \rightarrow \phi'(x) = \phi(x) \) and \( h(x) = (0\cdots0) \).

Claim: 1. \( \phi' \) can be computed in polytime from \( \phi \).

2. \( \exists x \) s.t. \( \phi'(x) = 1 \) \( \wp > 0 \).

3. \( x \) above is unique.
Ignoring (1) for now; can pick $h$ totally at random.

Then (2):

$$\Pr\left[ \exists x \in \mathcal{X} : h(x) = \overline{0} \right]$$

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

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

(3):

$$\Pr\left[ \exists x, y \in \mathcal{X} : h(x) = h(y) = \overline{0} \right]$$

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

$$= \mathcal{O}\left( \frac{1}{2^{2c}} \right) \ldots$$
Next Lecture:

- Using Pairwise Independent $h$.
- Formal analysis.