

LECTURE 11

Note Title

3/14/2007

TODAY : • AMPLIFICATION OF BPP

- $BPP \subseteq PH$

- $BPP \subseteq \sum_2^P \cap \Pi_2^P$

———— x ————

Weak & Strong definitions of BPP

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

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

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

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

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

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

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

AMPLIFICATION THEOREM:

Strong BPP = Weak BPP

Proof: (of " \geq ")

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

Consider M' which does the following

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

- let $Z_i = M(x, y_i)$

$$\triangle \bar{Z} = \frac{\sum Z_i}{t}$$

- if $\bar{Z} \geq S(n) + \frac{1}{2 \cdot p(n)}$ accept x_i
else reject

To analyse need to know

What is the probability that if

t i.i.d. (independent identically dist)
random variables Z_1, \dots, Z_t $Z_i \in [0, 1]$

with expectation μ take on average
value $\in [\mu \pm \epsilon]$

Chernoff Bound:

if z_1, \dots, z_t i.i.d. in $[0, 1]$ &

$$E[z_i] = \mu \quad \text{then} \quad \Pr \left[\left| \frac{\sum z_i}{t} - \mu \right| \geq \epsilon \right] \leq e^{-\epsilon t}$$

————— x —————

Applying to our case:

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

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

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

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

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



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

• 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 ;

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

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

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

Implications:

$[100:1]$ $NP \subseteq BPP$ (very unlikely)

\uparrow
my odds
 $\Rightarrow NP \subseteq P/poly$

$\Rightarrow P_{IT}$ collapses

$\Rightarrow \neg IHA$ (unlikely)

$[10:1]$

\uparrow my odds

$$\underline{BPP \subseteq \sum_2^P \cap \Pi_2^P} \quad [\text{Sipser-Lautemann}]$$

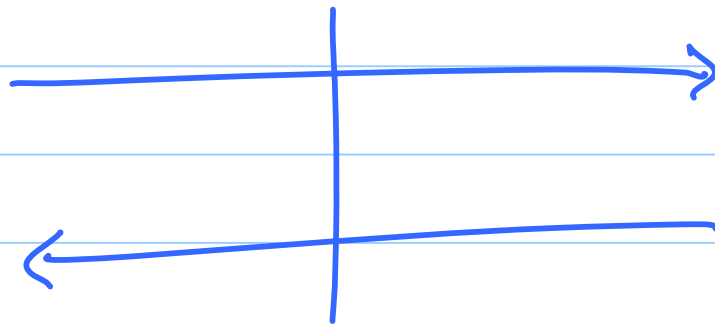
Recall \sum_2^P

Prosecution: "x ∈ 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 $\exists y$ st. $M(x, y)$ 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 $y_1 \dots y_k$: k possible variations
(first)
- Defense picks y .

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

$\Sigma_2^P = \{x \in L \mid \text{BPP-decided by } M\}$


Prosecution

Defense

$y_1 \dots y_k$



y



Jury: Accept if $\exists i$ st.

$M(x, y \oplus y_i)$ 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

$$\bullet \Pr_{y_i} [y_i \text{ wrong for } y] \leq \frac{1}{2^{2^m}} \leq \frac{1}{2}$$

$$\bullet \Pr_{y_1, \dots, y_k} [y_1, \dots, y_k \text{ all wrong for } y] \leq \frac{1}{2^k} \text{ [independent]}$$

$$\bullet \Pr_{y_1, \dots, y_k} [\exists y \text{ s.t.}] \leq \frac{\#y}{2^k}$$

Pick $k \geq |y| + 1$ & we are ok. \square

↓ Now we're with the defense.

Soundness: $x \notin L \Rightarrow \forall y_1 \dots y_k \exists y$ 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.

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

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

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

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

above is < 1 .



Implications

• Quantifiers do capture uncertainty

• Randomized hierarchy

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

s.t. $\exists M$

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

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

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

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

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

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

- $\text{promise BPP} \subseteq \text{promise-BPP}$

- [EXERCISE]:

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

- [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" \Rightarrow easy ?

[Valiant-Vazirani]:

Defn: Unique SAT = (Π_Y, Π_N)

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

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

[W]: $\text{SAT} \leq_R \text{Unique-SAT}$

\leq_R : Randomized reduction!

————— x —————

$A \leq_R B$ 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 # $\in \{2^{m-1} \dots 2^m\}$

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

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

- Map $\phi(x) \rightarrow \phi'(x) =$
" $\phi(x)$ and
 $h(x) = (0 \dots 0)$ ".

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

$$\left. \begin{array}{l} 2. \exists x \text{ s.t. } \phi'(x) = 1 \\ 3. x \text{ above is unique} \end{array} \right\} \text{w.p. } > 0.$$

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

Then (2):

$$\begin{aligned} \Pr[\exists x \text{ s.t. } h(x) = \bar{0}] \\ \geq 1 - \left(1 - \frac{1}{2^{m+c}}\right)^{2^{m-1}} \\ = \Omega\left(\frac{1}{2^c}\right) \end{aligned}$$

(3):

$$\begin{aligned} \Pr[\exists x, y \text{ s.t. } h(x) = h(y) = \bar{0}] \\ \leq \frac{1}{2^{m+c}} \cdot \frac{1}{2^{m+c}} \cdot 2^m \cdot 2^m \\ = O\left(\frac{1}{2^{2c}}\right) \dots \end{aligned}$$

Next Lecture:

- Using Pairwise Independent h .
- Formal analysis.