LECTURE 26: BPP AND THE POLYNOMIAL TIME HIERARCHY

Date: November 30, 2023.

A Probabilistic Turing Machine M is an ordinary (deterministic) Turing machine with a special read-only, "random-bits" tape — M moves its tape head right in each step, and never overwrites it. For M that runs in time $T(n)$ time, we assume that the random-bits tape contains a binary string of length $T(n)$. The result of the computation of M (i.e., accept/reject) on input x with y on random-bits tape will be denoted by $M(x, y)$.

$$\mathsf{Pr}_y(M(x,y) \text{ accepts}) = \frac{|\{y \in \{0,1\}^{T(|x|)} \mid M(x,y) \text{ accepts}\}|}{2^{T(|x|)}}$$

Randomized Time: A language $A \in \mathrm{RTIME}(T(n))$ is there is a probabilistic TM M running in time $T(n)$ such that

- if $x \in A$ then $\mathsf{Pr}_y(M(x,y) \text{ accepts}) \geq \frac{3}{4}$, and
- if $x \notin A$ then $\mathsf{Pr}_y(M(x,y) \text{ accepts}) = 0$.

$$\mathrm{RP} = \cup_c \mathrm{RTIME}(n^c)$$
$$\text{co-RP} = \{A \mid \overline{A} \in \mathrm{RP}\}$$

Bounded Probabilistic Time: A language $A \in \mathrm{BPTIME}(T(n))$ is there is a probabilistic TM M running in time $T(n)$ such that

- if $x \in A$ then $\mathsf{Pr}_y(M(x,y) \text{ accepts}) \geq \frac{3}{4}$, and
- if $x \notin A$ then $\mathsf{Pr}_y(M(x,y) \text{ accepts}) \leq \frac{1}{4}$.

$\Big\}\ \mathsf{Pr}_y(M(x,y) \neq A(x)) \leq \frac{1}{4}$.

$$\mathrm{BPP} = \cup_c \mathrm{BPTIME}(n^c)$$

Proposition 1. *The following relations hold.*

- $\mathrm{P} \subseteq \mathrm{RP} \subseteq \mathrm{NP}$. and $P \subseteq RP \subseteq BPP$. Follow defns.
- *If* $A \in \mathrm{BPP}$ *then* $\overline{A} \in \mathrm{BPP}$.

Lemma 2 (Amplification Lemma). *If $A \in \mathrm{RP}$ then for any polynomial n^d there is a probabilistic polynomial-time bounded TM M such that for any input x of length n,*

- *if $x \in A$ then $\mathsf{Pr}_y(M(x,y)$ accepts$) \geq 1 - 2^{-n^d}$, and*
- *if $x \notin A$ then $\mathsf{Pr}_y(M(x,y)$ accepts$) = 0$.*

If $A \in \mathrm{BPP}$ then for any polynomial n^d there is a probabilistic polynomial-time bounded TM M such that for any input x of length n,

- *if $x \in A$ then $\mathsf{Pr}_y(M(x,y)$ accepts$) \geq 1 - 2^{-n^d}$, and*
- *if $x \notin A$ then $\mathsf{Pr}_y(M(x,y)$ accepts$) \leq 2^{-n^d}$.*

$\Big\}$ Error can be reduced

An Arithmetic Circuit C (with unspecified inputs) is a sequence of assignments $A_1, A_2, \ldots A_n$, where each A_i is of one of the following forms.

$$
\begin{aligned}
&P_i = i, \ \ i \text{ is an integer} \\
&P_i = ? \\
&P_i = P_j * P_k, \ \ j, k < i \\
&P_i = P_j + P_k, \ \ j, k < i
\end{aligned}
$$

where each P_i is a variable that appears on the left-hand side in only A_i. For an assignment a that maps unspecified inputs to an integer, let C^a be the circuit that results from replacing the line $P_i = ?$ by $P_i = a(P_i)$, and its value is the value assigned to variable P_n in the last line.

Proposition 3. *The arithmetic circuit value problem is given an arithmetic circuit C and an assignment a, determine if the value of C^a is 0. The arithmetic circuit value problem is in* RP.

Pick a random modulus
Compute the value of each line modulo the number we pick

Proposition 4. *The* **polynomial identity testing** *problem is given an arithmetic circuit C, determine if for every assignment a, the value of C^a is 0. The polynomial identity testing problem is in* RP.

Lemma 5 (Schwartz-Zippel). *Let $p(x_1, x_2, \ldots x_m)$ be a polynomial of degree $\leq d$ and S be any finite set of integers. Then*

$$|\{(a_1, a_2, \ldots a_m) \in S^m \mid p(a_1, a_2, \ldots a_m) = 0\}| \leq d|S|^{m-1}$$

$$\Pr_{(a_1, \ldots a_m) \in S^m} \left(p(a_1, \ldots a_m) = 0 \right) \leq \frac{d}{|S|}$$

Pick a random assignment $a \in S^m$
Evaluate C^a.

S is finite.

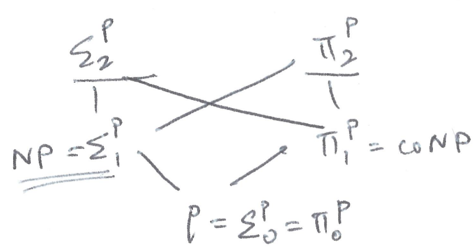
Compute each modulo a random modulus

Sources of error: (a) Random assignment is root.
(b) Error due modular arithmetic.

Bipartite Graphs: An undirected graph $G = (V, E)$ is **bipartite** if there is a partition (U_1, U_2) of V such that $E \subseteq (U_1 \times U_2)$.

A perfect matching in an undirected graph $G = (V, E)$ is a subset $M \subseteq E$ such that (a) no two edges in M share a vertex, and (b) every vertex is the endpoint of some edge in M.

Theorem 6 (Lovász). *Given a bipartite graph G, determining if G has a perfect matching is in* RP.



Theorem 7 (Gacs-Sipser). BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$.

Need to show: $\underline{BPP \subseteq \Sigma_2^P}$ and $BPP \subseteq \Pi_2^P$.

If $BPP \subseteq \Sigma_2^P$ then $BPP = co\,BPP \subseteq co\,\Sigma_2^P = \Pi_2^P$

Let $A \in BPP$. There is probabilistic TM M that runs in poly time

- $x \in A$ then $Pr_y(M(x,y) \text{ accepts}) \geq 1 - \frac{1}{2^{|x|}}$
- $x \notin A$ then $Pr_y(M(x,y) \text{ accepts}) \leq \frac{1}{2^{|x|}}$

Let $|x| = n$. Let assume M takes time $m = n^c$ on input x.

$A_x = \{y \in \{0,1\}^m \mid M(x,y) \text{ accept}\}$

$R_x = \{y \in \{0,1\}^m \mid M(x,y) \text{ reject}\}$. $\quad A_x \cup R_x = \{0,1\}^m$.

If $x \in A$, then $|A_x| \geq 2^m - 2^{m-n}$ $\quad (|R_x| \leq 2^{m-n})$

If $x \notin A$, then $|A_x| \leq 2^{m-n}$ $\quad (|R_x| \geq 2^m - 2^{m-n})$

$x \oplus y$ – bitwise XOR

$101 \oplus 011 = 110$

$x \oplus B = \{x \oplus y \mid y \in B\}$

$y \in x \oplus B$ iff $y \oplus x \in B$.

<u>Claim</u>: $\underline{x \in A}$ iff $\exists z_1 \exists z_2 \ldots \exists z_m \bigcup_{i=1}^{m} A_x \oplus z_i = \{0,1\}^m$

$B \in \Sigma_2^P$ iff $\exists R$ s.t. $B = \{x \mid \exists y_1 \forall y_2 \, R(x, y_1, y_2)$ and R is poly time computable$\}$.

$A = \{x \mid \exists z_1 \exists z_2 \ldots \exists z_m \forall y \; y \in \bigcup_{i=1}^{m} A_x \oplus z_i\}$

$= \{x \mid \exists z_1 \exists z_2 \ldots \exists z_m \forall y \bigvee_{i=1}^{m} \underline{y \oplus z_i \in A_x}\}$ $\longrightarrow M(x, y \oplus z_i)$ accepts.

$= \{x \mid \exists z_1 \exists z_2 \ldots \exists z_m \forall y. \; M(x, y \oplus z_i) \text{ accepts for some } i\}$.

$x \notin A$: $|A_x| \le 2^{m-n}$. For any z, $|A_x \oplus z| = |A_x| \le 2^{m-n}$.

For any $z_1, z_2 \dots z_m$.

$$\left|\bigcup_{i=1}^{m} A_x \oplus z_i\right| \le m\, 2^{m-n} < 2^m$$

$x \in A$: $|A_x| \ge 2^m - 2^{m-n}$ and $|R_x| \le 2^{m-n}$.

If $z_1, z_2 \dots z_m$ is "bad", then $\underbrace{\exists w.\ \text{s.t}\ \forall i.\ w \oplus z_i \notin A_x}$.

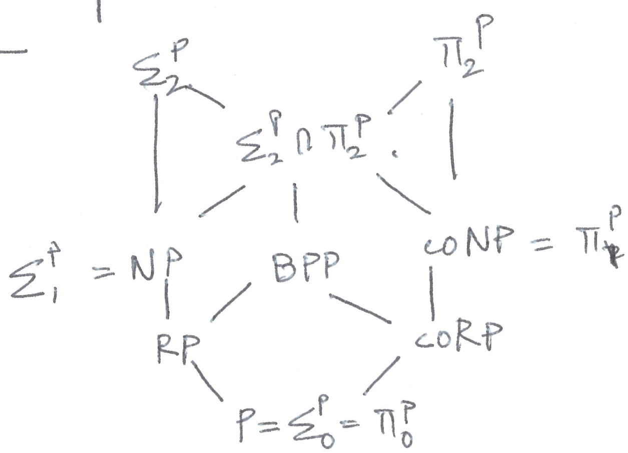
$\exists w.\ \{w \oplus z_1, w \oplus z_2 \dots w \oplus z_m\} \subseteq R_x$.

$z_1, z_2 \dots z_m$ is bad $\longleftrightarrow$ $w, \{\underbrace{w \oplus z_1 \dots w \oplus z_m}_{m \text{ strings}}\} \subseteq R_x$.

$\# w, \{w \oplus z_1 \dots w \oplus z_m\} \le 2^m \left(2^{m-n}\right)^m = 2^{m^2 - m(n-1)}$

$\# z_1, z_2 \dots z_m = \left(2^m\right)^m = 2^{m^2} >$

$\exists$ is a good tuple.



Evidence why $NP \not\subseteq BPP$:

P/poly = All problems that can be solved using poly sized circuits

Karp-Miller Thm: If SAT $\in$ P/poly then $PH = \Sigma_2^p$.

Adelman Thm : $BPP \subsetneq P/poly$.

Corollary : $NP \subseteq BPP$ then $PH = \Sigma_2^p$.