Lecture 25: Probabilistic Complexity Classes

Date: November 28, 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

$A(x) = \begin{cases} \text{accept} & \text{if } x \in A \\ \text{reject} & \text{if } x \notin A \end{cases}$

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

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

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

Proposition 1. *The following relations hold.*

- $\mathrm{P} \subseteq \mathrm{RP} \subseteq \mathrm{NP}$. $\rightarrow$ Follow from defn. $\underline{\mathrm{P} \subseteq \mathrm{RP} \subseteq \mathrm{BPP}}$
- *If* $A \in \mathrm{BPP}$ *then* $\overline{A} \in \mathrm{BPP}$.

Open : $\mathrm{BPP} \subseteq \mathrm{NP}$? $\underbrace{\mathrm{NP} \subseteq \mathrm{BPP}}_{\text{Unlikely}}$?

$\mathrm{coBPP} = \{A \mid \overline{A} \in \mathrm{BPP}\} = \mathrm{BPP}$

$A \in \mathrm{BPP}$. M is a BPP algo for A.

BPP algo for $\overline{A}$: Input x

Run M on x & Flip answer.

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

$\Pr_y(M(x,y) \neq A(x)) \leq \frac{1}{2^{n^d}}$.

$A \in$ ~~BPP~~ RP. Let N be an RP algo for A.

M: Input x
    For $i = 1$ to k
        Run N on x
        Return accept if N accepts
    Return reject.

If $x \notin A$, then
$\Pr_y(M(x,y)$ accepts$) = 0$
If $x \in A$ then
$\Pr_y(M(x,y)$ reject$) \leq \left(\frac{1}{4}\right)^k$
$= \frac{1}{2^{n^d}}$ when $k = n^d/2$

$A \in$ BPP. Let N is a BPP algo for A

M: Input x
    accept $= 0$
    For $i = 1$ to k
        ~~[illegible]~~ Run N on x
            if N accepts accept++
    If (accept $> k/2$)
        return accept
    else return reject

$\Pr_y(M(x,y) \neq A(x))$

$= \sum_{j=0}^{k/2} \Pr_y(j$ runs of N are correct$)$

$= \sum_{j=0}^{k/2} \left(\frac{3}{4}\right)^j \left(\frac{1}{4}\right)^{k-j} \binom{k}{j}$

$\leq \left(\frac{1}{4}\right)^k 3^{k/2} \underbrace{\sum_{j=0}^{k/2} \binom{k}{j}}_{= 2^{k-1}}$

$\leq \left(\frac{1}{4}\right)^k \cdot 3^{k/2} \cdot 2^k$

$= \left(\frac{3}{4}\right)^{k/2}$

$= \left(\frac{3^3}{4^3}\right)^{k/6} < \left(\frac{1}{2}\right)^{k/6}$

$= \frac{1}{2^{n^d}}$ when $k = 6n^d$.

$\sum_{j=0}^{k} \binom{k}{j} = (1+1)^k = 2^k$.

$\binom{k}{j} = \binom{k}{k-j}$

$\sum_{j=0}^{k/2} \binom{k}{j} \sim 2^k/2$.

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.

$|\langle C, a\rangle| \leq n$, $a(P_i) \leq 2^n$, # lines in $C \leq n$

$val(C^a) \sim (2^n)^{2^n}$

$P_1 = ?$
$P_2 = P_1 * P_1$
$\vdots$
$P_i = P_{i-1} * P_{i-1}$
$\vdots$
$P_n = P_{n-1} * P_{n-1} = P_1^{2^n}$

Randomized Algo: Pick m at random $[2, N]$
Compute answers line by line modulo m.
If the last line is 0 then answer 0
else answer non-zero.

If $val(C^a) = 0$ then algo answers 0 always.

Case 1: m is a prime number. We make an error when $val(C^a) \neq 0$ and m is a prime divisor of $val(C^a)$.

distinct prime divisor of $b \leq \log b$.
Prime Number Theorem: # primes $< N$ is $\sim \frac{N}{\ln N}$.

$Pr(\text{error}) \leq Pr(\text{picking } m \text{ composite}) + Pr(\text{picking } m \text{ prime divisor of } C^a)$

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*

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

$$\leq \frac{N - \frac{N}{\ln N} + n 2^n}{N}$$

$$= 1 - \frac{1}{\ln N} + \frac{n 2^n}{N}$$

Take $N = cn^2 \cdot 2^n$.

$$= 1 - \frac{1}{dn\log n} + \frac{1}{cn} < \frac{1}{4}.$$