Lecture 14

Randomized Computations

- Deterministic TMs
  - ↳ not random

- Non-det. TMs
  - ↳ Non-det $\neq$ random

- We will have fair random bits

$$b \xleftarrow{\$} \{0,1\}$$

$$\Pr[b=1] = \Pr[b=0] = 1/2$$

Def. A probabilistic Turing machine (PTM) is a TM w/ 2 transition functions (δ_0, δ_1).

For all x, PTM M on input x does the following

- For each step of computation, sample $\underbrace{b \xleftarrow{\$} \{0,1\}}$ uniformly at random
- Execute δ_b

- For PTM M, M(x) denotes the random variable corresponding to M's output on input x given random choices.
- We say M runs in time T if $\forall x$, M(x) halts in $O(T(|x|))$ steps

for <u>all</u> random choices.

- PTM vs. NTM: accepting string x
  - For NTM N

    $N(x)=1 \iff$ there is at least one accepting comp. path.

  - PTM: need to count # of accepting paths
    - want this #/fraction to be large

<u>Def.</u> Let L be a language, $T:\mathbb{N}\to\mathbb{N}$ be a function. We say PTM

M <u>decides</u> L in time T
if $\forall x$, $M(x)$ halts in
$O(T(|x|))$ steps and

$$\underbrace{\Pr}_{\text{over random choices } M \text{ makes}}[M(x) = L(x)] \geq 2/3$$

two-sided error

$$L(x) = \begin{cases} 1 & x \in L \\ 0 & x \notin L \end{cases}$$

<u>Def</u>. BPTIME(T) is all L
s.t. $\exists$ time T PTM that decides
L.

- $BPP = \bigcup_{c \in \mathbb{N}} BPTIME(n^c)$

* BPP still a worst-case class

Fact:
- $P \subseteq BPP$
- $BPP \subseteq EXP$
- Unknown:
  1. $BPP \not\subseteq NEXP$
  2. $P = BPP$

     complexity theorists believe this is true

Alt Def: $L \in BPP$ if there exists poly-time DTM D and polynomial p s.t. $\forall x$

$$\Pr_{r \leftarrow \{0,1\}^{p(|x|)}} \left[M(x,r) = L(x) \right] \geq \frac{2}{3}$$

$p(|x|)$

$BPP \subseteq EXP$

If D is as

Construct M s.t.

$M(x)$

- enumerate over all $r \in \{0,1\}^{p(|x|)}$
- Run $D(x,r)$
- Check that $D(x,r)=1$ for at least $2/3$ of all r.

$\to \# r \geq \frac{2^{p(|x|)} \cdot 2}{3}$

$\to \in EXP$

3 BPP Algorithm examples

① Finding the Median

- Given $\underbrace{S = \{a_1, \dots, a_n\}}_{\text{set of } n \text{ numbers}}$,

$$\text{median}(S) = x \quad \text{s.t.}$$

$$x \geq s \quad \text{for } \lfloor \tfrac{n}{2} \rfloor \ s \in S$$

$$x \leq t \quad \text{for } \lfloor \tfrac{n}{2} \rfloor \ t \in S$$

- Easy det. alg

① Sort $S = (s_1, \dots, s_n)$

② If n is even, set

$$x = \frac{s_{n/2} + s_{1+n/2}}{2} \qquad \left(x \in [s_{n/2}, s_{1+n/2}]\right)$$

If n is odd, set

$$x = s_{\lceil \frac{n}{2} \rceil}$$

③ $O(n\log(n))$ time

- Give rand alg running in time $O(n)$ for finding kth-smallest element.

FindKthElement(k, S): $S = \{a_1, \dots, a_n\}$ not necessarily sorted

① Pick $i \xleftarrow{\$} [n]$. Set $x = a_i$.

② Scan S, count # of elements $c \in S$ s.t. $c \le x$. Let m be this number.

③ If $m = k$, output x.

④ If $m > k$:

- Let $S' = \{c \in S \mid c \le x\}$
- Run FindKthElement(k, S')

5. If $m < k$
   - Let $T = \{c \in S \mid c \geq x\}$
   - Run FindKthElement$(k-m, T)$

Intuition for $O(n)$ time

1. non-random parts are linear time
2. Expected sizes of S', T are $\leq \frac{9n}{10}$

$\Rightarrow$ If $T(n)$ is the runtime then

$$T(n) = O(n) + T\left(\tfrac{9n}{10}\right) = O(n)$$

- Polynomial Identity Testing

- Let $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$
- $\deg p = \sum \deg(x_i)$
  $:= d$

  ↳ largest degree d_i in any monomial

Ex: $p(x_1, x_2, x_3) = x_1^{100} + x_2^2 x_3^{50} + x_1^3 x_2^5 x_3^7$

$d_1 = 100, \quad d_2 = 5, \quad d_3 = 50$

$d = 155$

Q: Is $p \equiv 0$?

- $p(x_1, \ldots, x_n)$:

$\mathbb{Z}^n \mapsto \mathbb{Z}$

$\Rightarrow$ could have $O(2^n)$ monomials

Ex: $p(\vec{x}) = \prod_{i=\phi}^{n} (c_i - x_i)$

ZeroCheck(p):

1. Sample $k \xleftarrow{\$} [2^{2n}]$
2. Sample unif. random $\alpha_1, \dots, \alpha_n \xleftarrow{\$} [10 \cdot 2^n]$
3. Check if $p(\alpha_1, \dots, \alpha_n) \bmod k = 0$

   ↳ output True if yes, False if no.

Observations: let $y = p(\alpha_1, \dots, \alpha_n)$

1. If $y = 0$ then $y \bmod k = 0$ ✓

② Suppose $y \neq 0$.

- What is $\Pr_{y \neq 0}[x \bmod k = 0]$

$\Rightarrow \Pr_k[\,k \text{ divides } y\,]$

$\rightarrow$ if prime factors of y are $p_1, \ldots, p_\ell$

$\rightarrow$ enough to say k is not one of these $p_1, \ldots, p_\ell$

$\rightarrow$ By the Prime # Theorem

# of primes in $[2^{2n}]$ is at least $\frac{2^{2n}}{2n}$ ...

$\rightarrow \log(y) \leq 5n2^n = o\left(\frac{2^{2n}}{2n}\right)$

$\Rightarrow$ # of k not $= p_1, \ldots, p_\ell$

is at least $\frac{2^{2n}}{4n}$

$\Rightarrow$ w.p. at least $\delta = \frac{1}{4n}$

k will <u>not</u> be in this

set.

$$\Rightarrow \Pr\left[\begin{array}{l} y \bmod k_1 = 0 \\ \vdots \\ y \bmod k_m = 0 \end{array} \middle|\, y \neq 0\right] \leq \left(1 - \frac{1}{4n}\right)^m$$

③ Suppose $y = 0$ but $p \not\equiv 0$.

$$\Pr_{\alpha_1, \ldots, \alpha_n}\left[y = 0 \mid p \not\equiv 0\right] \leq \frac{d}{\underline{|[0, 2^n]|}}$$

Schwartz-Zippel

- **Verifying Matrix Mults**
  - Let $A, B \in \mathbb{Z}_p^{n \times n}$ p is prime
  - Want to check if

$$C = A \cdot B \quad , C \in \mathbb{Z}_p^{n \times n}$$

- Fastest matrix-mult alg:

$$O(n^{2.37286})$$

  $\rightarrow$ cannot run on real computer

- Also $O(n^3)$ time trivial way
- **Rand alg: $O(n^2)$ time.**

  1. $r \xleftarrow{\$} \mathbb{Z}_p$
  2. Write $x = (1, r, r^2, \ldots, r^{n-1})^T$
  3. Check $\underbrace{Cx}_{O(n^2)} = A \underbrace{(Bx)}_{(n \times n) \cdot n = O(n^2)}$

$O(n)$

$$\underbrace{(n \times n) \cdot n}_{O(n^2)}$$

- If $C = AB$, then
  $$Cx = A(Bx) \quad \forall x$$

- What if $C \neq AB$?

$$Cx = \begin{pmatrix} \langle c_1, x \rangle \\ \langle c_2, x \rangle \\ \vdots \\ \langle c_n, x \rangle \end{pmatrix}$$

$$= \begin{pmatrix} \langle c_1, (1, r, r^2, \ldots, r^{n-1}) \rangle \\ \vdots \\ \langle c_n, \ldots \rangle \end{pmatrix}$$

$$c_i(x) = c_{i,1} + c_{i,2}\, x + \cdots + c_{i,n}\, x^{n-1}$$

$$\langle c_i, (1, r, \ldots, r^{n-1}) \rangle = c_i(r)$$

$$\Pr_r[Cx = A(Bx) \mid C \neq AB] \leq \frac{n-1}{p}$$

$$\Pr_r[Cx \neq A(Bx) \mid C \neq AB] \geq 1 - \frac{n-1}{p}$$

One-Sided Error

- Class RP

Def. RTIME(T) is the set of all languages L s.t. $\exists$ PTM M running in time T s.t. $\forall x$

$$x \in L \Rightarrow \Pr[M(x)=1] \geq 2/3$$
$$x \notin L \Rightarrow \Pr[M(x)=0] = 1$$

$- RP = \bigcup_c RTIME(n^c)$

$coRP = \{ L : \bar{L} \in RP \}$

or equivalently

$L \in coRP$ if $\exists$ PTM M running in polynomial time s.t.

$\forall x$

$x \in L \Rightarrow Pr[M(x) = 1] = 1$

$x \notin L \Rightarrow Pr[M(x) = 1] \leq \frac{1}{3}$

$Pr[M(x) = 0] \geq 2/3$