Probabilistic TM (PTM)

- **Defn:** • We call M a PTM if it has two transition fns. δ_0, δ_1 and in each transition step M randomly follows δ_i with prob. $= 1/2$.

  • We say M decides L if $x \in L$ iff $\Pr_{\text{steps}}[M \text{ accepts } x] \geq 2/3$.

- Naturally, we can now talk about "efficient" PTMs.

Defn: • For a $T: \mathbb{N} \to \mathbb{N}$ a PTM M decides L in $T(n)$ time if M halts on every $x \in \{0,1\}^*$ in $\leq T(|x|)$ steps, regardless of its random choices, and decides $x \in ? L$.

- $\underline{\mathrm{BPtime}(T(n))} := \{L \subseteq \{0,1\}^* \mid$ a PTM M decides L in time $O(T(n))\}$.

- $\underline{\mathrm{BPP}} := \bigcup_{c \in \mathbb{N}} \mathrm{BPtime}(n^c)$.

(bounded prob. poly-time)
(unlike, prob. poly-time PP!)

Proposition: (i) $P \subseteq BPP \subseteq PP \subseteq Pspace \subseteq EXP$.

(ii) Alternatively, $L \in \underline{BPP}$ if $\exists$ det. poly-time TM M & $c > 0$ s.t. $\forall x \in \{0,1\}^*$, $x \in L$ iff $\Pr_{r \in \{0,1\}^{|x|^c}}[M(x,r) = 1] \geq \frac{2}{3}$.

- This is closer to our notion of a "randomized poly-time" algorithm M solving a problem L.

Examples of PTMs

- **Primality**: Given an $n \in \mathbb{N}$. Check whether it is prime.
  - Solovay-Strassen (1970s) gave the first rand. poly-time algorithm.
  - It was the first formal PTM!

Algo: (1) Pick a random $a \in (\mathbb{Z}/n\mathbb{Z})^*$.
(2) Output Yes if $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$.

Jacobi symbol

Exercise: Prove the correctness & the $\tilde{O}(\lg^2 n)$ time-complexity.

Polynomial Identity testing: Given a polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]$ in some "compact" way. Check whether $f =? 0$.

arithmetic circuit

Exercise: Prove that a random evaluation works.

- Egs. $\sqrt{\cdot} \bmod p$ & undirected connectivity in $\mathbb{L}$.

Open: (1) $P = BPP$?

(theoretical evidence for "yes"!)

(2) $BPP \neq NP$?

(later we will show a PH collapse!)

- BPP captures prob. algo, with two-sided error, i.e. if a PTM M decides L then it may make an error on x regardless of $x \in L$ or $x \notin L$.

One-sided error : RP & coRP

- Defn: • $L \in$ Rtime$(T(n))$ if $\exists$ PTM running in time $O(T(n))$ s.t.

$x \in L \Rightarrow \Pr[M \text{ accepts } x] \geq 2/3$

$x \notin L \Rightarrow \quad " \quad = 0$.

• $RP := \bigcup_{c \in \mathbb{N}} \text{Rtime}(n^c)$

(randomized poly-time)

Proposition: (i) Primes $\in$ coRP. & Primes $\in$ RP required different ideas.

(ii) PIT $\in$ coRP.

(iii) $RP \cup coRP \subseteq BPP$.

(iv) $RP \subseteq NP$ & $coRP \subseteq coNP$.

Zero-sided error probabilistic: ZPP (Las Vegas algo.)

- **Defn**:
  - Consider a PTM M and the random variable $time_M(x)$, on any input x. We say that M has an expected running-time $T(n)$ if $\forall x$, $Exp[time_M(x)] \leq T(|x|)$.
  - $L \in Ztime(T(n))$ if $\exists$PTM that correctly decides L in expected time $O(T(n))$.
  - $ZPP := \bigcup_{c \in \mathbb{N}} Ztime(n^c)$.

Las Vegas — Monte Carlo (BPP)

Proposition: (i) $ZPP \subseteq RP \cap coRP$.

(ii) $RP \cap coRP \subseteq ZPP$.

(iii) $ZPP = RP \cap coRP \subseteq NP \cap coNP$.

Proof:

(i) Let $L \in ZPP$ be decided by a PTM M with expected running-time $T(n)$.

- On an input x:
  1) Run $M(x)$ for $3 \cdot T(|x|)$ steps.
  2) If x is not accepted, output <u>NO</u>.

- If $x \notin L$, we made no error.
- If $x \in L$, we err with prob.

$$\leq \frac{T(|x|)}{3 \cdot T(|x|)} = \frac{1}{3}.$$

Markov's inequality

$\Rightarrow$ $L \in RP$. ($\because L \in ZPP$)

- Similarly, we can prove $L \in coRP$. (Instead of NO, output Yes.)

$\Rightarrow$ $L \in RP \cap coRP$. $\square$

(ii) Let $L \in RP \cap coRP$ be decidable by PTMs M_1 resp. M_2 in time $\le n^c$, for a constant $c > 0$.

- On input x:
  1) Pick a <u>random</u> r.
  2) Run $M_1(x,r)$ & $M_2(x,r)$.
  3) If $M_1(x,r) = M_2(x,r)$ then output the <u>common</u> decision.

  else repeat (1).

- Suppose $x \in L$. Thus, $M_2(x,r) = Yes$.

  $\Pr_r[M_1(x,r) \ne Yes] \le 1/3$.

$\Rightarrow \Pr_{r_1,..,r_t}[\forall i \in [t], M_1(x,r_i) \ne Yes] \le 3^{-t}$.

$\Rightarrow Exp[\#\text{iterations}] \le \sum_{t=1}^{\infty} (t+1) \cdot \frac{1}{3^t} = O(1)$.

$\Rightarrow$ Expected time complexity $= O(n^c)$.

- The case of $x \notin L$ is similar.

$\Rightarrow L \in ZPP$. $\square$

Why 2/3? Prob. amplification

- The (2/3)-rd in the defn. of prob. classes is arbitrary. In fact, we can use any fraction that is inverse-polynomial away from 1/2.

Theorem: Let a PTM M be deciding L s.t. $\forall x$, $x \in L$ iff $\Pr[M \text{ accepts } x] \geq \left(\frac{1}{2} + |x|^{-c}\right)$.

Then, $\forall d$, $\exists$ PTM M' s.t. $\forall x$, $x \in L$ iff $\Pr[M' \text{ accepts } x] \geq \left(1 - 2^{-|x|^d}\right)$.

Pf sketch:

- Idea: Run M k times on x, and output the majority value. Apply the Chernoff bound on error prob.

- The PTM M' is: (Fix $k = 8.|x|^{d+2c}$)
  On input x, run $M(x)$ k times.
  Let the outputs be $y_1, \ldots, y_k \in \{0,1\}$.
  Output Majority$(y_1, \ldots, y_k)$.

- For $i \in [k]$, let $\underline{X_i}$ be the random variable $\begin{cases} 0, & \text{if } y_i \text{ is } \underline{\text{wrong}} \\ 1, & \text{otherwise.} \end{cases}$

<u>Chernoff's bound</u>: Let $X_1, \ldots, X_k$ be independent identically distributed (<u>i.i.d.</u>) boolean random variables. Let $\Pr[X_i = 1] =: p$ for $i \in [k]$ & $\delta \in (0,1)$. Then,

$$\Pr\left[\left|\frac{\sum_{i\in[k]} X_i}{k} - p\right| > \delta\right] < e^{-\delta^2 pk/4}.$$

$$\Rightarrow \Pr[M' \text{ is wrong}] = \Pr\left[\sum_{i=1}^{k} X_i < k/2\right]$$

$p := \Pr[M(x) \text{ is correct}]$

$$= \Pr\left[p - \frac{\sum X_i}{k} > p - \frac{1}{2}\right] = \Pr\left[\left|p - \frac{\sum X_i}{k}\right| > n^{-c}\right]$$

$$< \exp\left(-\frac{1}{4} \cdot n^{-2c} \cdot \left(\frac{1}{2}+n^{-c}\right) \cdot 8n^{d+2c}\right)$$

$$= \exp\left(-n^{d} \cdot (1+2n^{-c})\right)$$

$$< e^{-n^d} < 2^{-n^d}. \qquad \square$$

<u>Exercise:</u> The Chernoff bound has a neat proof using $\text{Exp}[e^{t \cdot \sum_i X_i}]$ & the Markov's bound.

BPP & the PH

- $BPP \overset{?}{\subseteq} NP$ is not known, but $BPP \subseteq \Sigma_2 \cap \Pi_2$ is!

<u>Theorem</u> (Sipser-Gács 1983): $BPP \subseteq \Sigma_2 \cap \Pi_2$.

<u>Pf:</u>

- It suffices to show $BPP \subseteq \Sigma_2$.

- Let $L \in BPP$, and M be a poly-time TM $(m := n^c)$ s.t. $\forall x \in \{0,1\}^n$,

$$x \in L \Rightarrow \Pr_{r \in \{0,1\}^m}[M(x,r)=1] \geq (1-2^{-n})$$

$$x \notin L \Rightarrow \Pr_{r}[M(x,r)=1] \leq 2^{-n}.$$

- Denote $S := \{r \in \{0,1\}^m \mid M(x,r)=1\}$. Then, as before,

$$|S| \geq (1-2^{-n})\, 2^m \quad \text{if } x \in L,$$
$$|S| \leq 2^{m-n} \quad \text{if } x \notin L.$$

- The idea is to check the "largeness" of this S in Σ_2. (Use "expansion" in a graph.)

- For $U = \{u_1, \ldots, u_k\} \subseteq \{0,1\}^m$, define an undirected graph $\underline{G_U}$ with:

  $\{0,1\}^m$ as <u>vertices</u>, and

  <u>edges</u> (s,s'), where $s \oplus s' = u_i$ for some i.

- Note that G_U is <u>regular</u> with $\deg = k$.

- Fix $k := \lfloor \frac{m}{n} \rfloor + 1$.

- For any $S \subseteq \{0,1\}^m$, define $\underline{\Gamma_U(S)}$ to be the neighbours of S in G_U.

<u>Claim 1:</u> $|S| \leq 2^{m-n} \Rightarrow \forall U, |U|=k, |\Gamma_U(S)| < 2^m$.

<u>Pf:</u>

- $|\Gamma_U(S)| \leq k \cdot |S| \leq \frac{k}{2^n} \cdot 2^m < 2^m$. $\square$

<u>Claim 2:</u> $|S| \geq (1-2^{-n}) 2^m \Rightarrow \exists U, |U|=k, \Gamma_U(S) = \{0,1\}^m$.

<u>Pf:</u>

- We construct a U <u>probabilistically</u>!
- Choose $u_1, \ldots, u_k \in \{0,1\}^m$ randomly.

- Let $\underline{E_r}$ be the event that $r \notin \Gamma_U(S)$
& $\underline{E_{r,i}}$ " " " " $r \notin S \oplus u_i$.

- Clearly,

$$\Pr_u [E_{r,i}] = 1 - \frac{|r \oplus S|}{2^m} \leq 2^{-n}.$$

- So,

$$\Pr_u [E_r] \leq \prod_{i=1}^{k} \Pr_u [E_{r,i}] \leq 2^{-nk} < 2^{-m}.$$

$$\Rightarrow \Pr_u [\exists r, E_r] < 1.$$

$$\Rightarrow \Pr_u [\forall r, \neg E_r] > 0.$$

$$\Rightarrow \exists u, \ T_u(S) = \{0,1\}^m. \qquad \square$$

- Claims 1 & 2 imply: $\forall x \in \{0,1\}^n$,

$$x \in L \text{ iff } \exists u_1, \ldots, u_k, \forall r, \bigvee_{i \in [k]} M(x, r \oplus u_i) = 1.$$

$\in \{0,1\}^m$

$$\Rightarrow L \in \Sigma_2. \qquad \square$$