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.

<u>Open:</u> (1) $P = BPP$?

(theoretical evidence for "yes"!)

(2) $BPP = NP$?

(later we will show a PH collapse!)

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

<u>One-sided error</u> : RP & coRP

- <u>Defn:</u> • $L \in$ <u>$\mathrm{Rtime}(T(n))$</u> if $\exists$ PTM running in time $O(T(n))$ s.t.

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

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

• <u>RP</u> $:= \bigcup_{c \in \mathbb{N}} \mathrm{Rtime}(n^c)$

(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

- 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 $O(T(n))$.

• $ZPP := \bigcup_{c\in\mathbb{N}} Ztime(n^c)$.

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

$\Rightarrow L \in RP$.

- 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 $\leq n^c$, 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, $M_2(x,r) = Yes$.
  $\Pr_r[M_1(x,r) \neq Yes] \leq 1/3$.

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

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

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