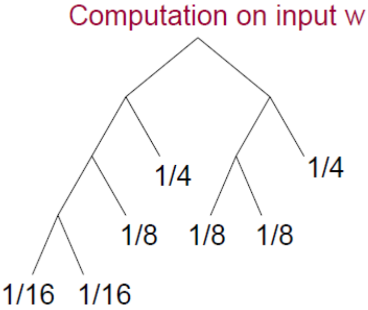
Theory of Computation
Probabilistic Complexity Classes

Probabilistic Polynomial-Time TM

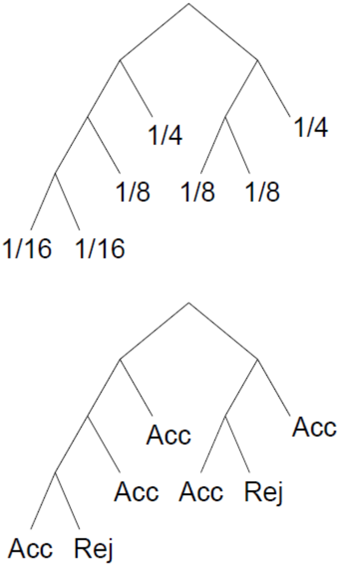
- New kind of NTM, in which each nondeterministic step is a coin flip: has exactly 2 next moves, to each of which we assign probability $\frac{1}{2}$
- To each branch of length k, we assign probability $(\frac{1}{2})^k$
- Now we can talk about probability of acceptance or rejection, on input w.



Probabilistic Polynomial-Time TM (Cont'd)

- Probability of acceptance = $\sum_{accepting\ path\ \sigma} Prob(\sigma)$
- Probability of rejection = $\sum_{rejecting\ path\ \sigma} Prob(\sigma)$
- Example:
  - Prob. Acceptance = $\frac{1}{16} + \frac{1}{8} + \frac{1}{4} + \frac{1}{8} + \frac{1}{4} = \frac{13}{16}$
  - Prob. Rejection = $\frac{1}{16} + \frac{1}{8} = \frac{3}{16}$
- We consider TMs that halt (either accept or reject) on every branch - deciders.
- So the two probabilities total 1.

Computation on input w

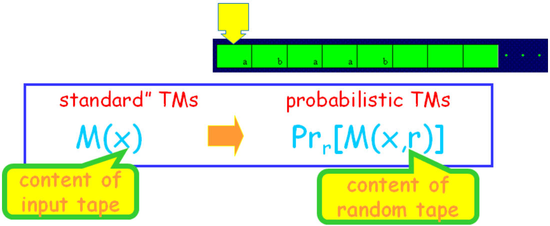


Probabilistic TM

Definition 1

A probabilistic TM (PTM) is a TM with distinguished states called coin-tossing states. For each coin-tossing state, the finite state control specifies two possible next states. The computation of a PTM is deterministic except that in coin-tossing states the machine tosses an unbiased coin to decide between the two possible next states.

Another way to view PTM



Error Probability

Definition 2

Given a PTM M and an input x, $x \in L(M)$ iff Prob$(M$ accepts $x) > \frac{1}{2}$.

Definition 3

The error probability of a PTM M is a function $e_M(x)$=Prob$\{M$ gives the wrong answer on $x\}$

Definition 4

A PTM M is with bounded error prob. if $\exists \epsilon < \frac{1}{2}, e_M(x) \leq \epsilon$, for all x.

We write $M(x) = 1$ (resp., =0) for M accepts (resp., rejects) x.

Probabilistic TMs Accepting r.e. Sets

Theorem 5

Every r.e. set is accepted by some PTM with finite average running time.

Proof.

Let W be an r.e. set and let M be a DTM accepting W. Construct the following PTM M'

1. repeat
2. simulate one step of $M(x)$
3. if $M(x)$ accepted at last step then accept
4. until cointoss()="heads"
5. if cointoss()="heads" the accept else reject

Clearly if $x \notin W$, M' terminates only at line 5. In this case, the prob= $\frac{1}{2}$, so $x \notin L(M')$. If $x \in W$, ... □

Definition 6

A language $L \in$ RP (Randomized Polynomial Time), iff a probabilistic Polynomial-time TM M exists, such that

- $x \in L \Rightarrow \text{Prob}(M(x) = 1) \geq \frac{1}{2}$
- $x \notin L \Rightarrow \text{Prob}(M(x) = 1) = 0$

Definition 7

A language $L \in$ co-RP, iff a probabilistic Polynomial-time TM M exists, such that

- $x \in L \Rightarrow \text{Prob}(M(x) = 1) = 1$
- $x \notin L \Rightarrow \text{Prob}(M(x) = 0) \geq \frac{1}{2}$

These two classes complement each other, i.e., coRP = $\{\bar{L} \mid L \in \ RP\}$.

Comparing RP with NP

- Let R_L be the relation defining the witness/guess for L for a certain TM.
- NP:
  - $x \in L \Rightarrow \exists y, (x, y) \in R_L$
  - $x \notin L \Rightarrow \forall y, (x, y) \notin R_L$
- RP:
  - $x \in L \Rightarrow Prob((x, r) \in R_L) \geq \frac{1}{2}$
  - $x \notin L \Rightarrow \forall r, (x, r) \notin R_L$
- Obviously, $RP \subseteq NP$

Amplification

- The constant $\frac{1}{2}$ in the definition of RP is arbitrary.
- If we have a probabilistic TM that accepts $x \in L$ with probability $p < \frac{1}{2}$, we can run this TM several times to "amplify" the probability.
- If $x \notin L$, all runs will return 0.
- If $x \in L$, and we run it n times than the probability that none of these accepts is
  $\mathrm{Prob}(M_n(x) = 1)$ = 1-$\mathrm{Prob}(M_n(x) \neq 1)$ = 1-$\mathrm{Prob}(M(x) \neq 1)^n$ = 1-(1-$\mathrm{Prob}(M(x) = 1))^n$ = $1 - (1 - p)^n$

Alternative Definitions for RP

Definition 8

$L \in RP_1$ iff $\exists$ probabilistic Poly-time TM M and a polynomial $p(.)$, s.t.

- $x \in L \Rightarrow \text{Prob}(M(x) = 1) \geq \frac{1}{p(|x|)}$
- $x \notin L \Rightarrow \text{Prob}(M(x) = 1) = 0$

Definition 9

$L \in RP_2$ iff $\exists$ probabilistic Poly-time TM M and a polynomial $p(.)$, s.t.

- $x \in L \Rightarrow \text{Prob}(M(x) = 1) \geq 1 - 2^{-p(|x|)}$
- $x \notin L \Rightarrow \text{Prob}(M(x) = 1) = 0$

Claim: $RP_1 = RP_2$

The class PP

Definition 10

$L \in PP$ (Polynomial Probabilistic Time) iff there exists a polynomial-time probabilistic TM M, such that $\forall x \in L$:

- if $x \in L$, $\text{Prob}(M(x) = 1) > \frac{1}{2}$, and
- if $x \notin L$, $\text{Prob}(M(x) = 1) \leq \frac{1}{2}$.

The class BPP

Definition 11

$L \in BPP$ (Bounded-Error Polynomial Probabilistic Time) iff there exists a polynomial-time probabilistic TM M, such that $\forall x \in L$:
$\mathrm{Prob}(M(x) = \chi_L(x)) \geq \frac{2}{3}$, where

- $\chi_L(x) = 1$ if $x \in L$, and
- $\chi_L(x) = 0$ if $x \notin L$.

Note: The BPP machine success probability is bounded away from failure probability.

Theorem 12

If $L \in BPP$, then there exists a probabilistic polynomial TM M', and a polynomial $p(n)$ s.t. $\forall x$, $Prob_{r \in \{0,1\}^{p(n)}}(M'(x, r) \neq \chi_L(x)) < \frac{1}{3p(n)}$

The class ZPP

Definition 13

$L \in ZPP$ (Zero-Error Polynomial Probabilistic Time) iff there exists a polynomial-time probabilistic TM M, such that $\forall x \in L$:
$M(x) = \{0, 1, \perp\}$,

- $\text{Prob}(M(x) = \perp) < \frac{1}{2}$, and
- $\text{Prob}(M(x) = \chi_L(x) \vee M(x) = \perp) = 1$

- $\text{Prob}(M(x) = \chi_L(x)) > \frac{1}{2}$
- The symbol $\perp$ is "I don't know".
- The value $\frac{1}{2}$ is arbitrary and can be replaced by $2^{-p(|x|)}$ or $1 - \frac{1}{p(|x|)}$.

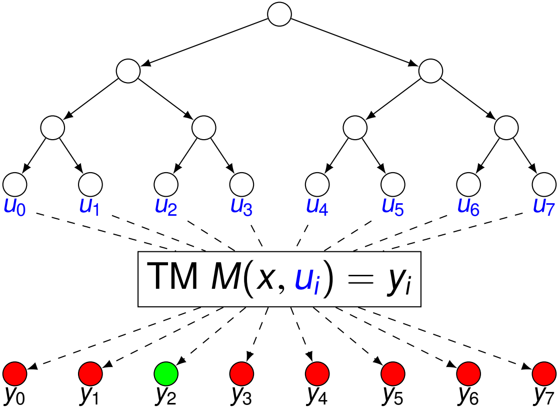
ZPP = RP ∩ coRP

- Let $L \in ZPP$, M be the PTM that recognizes L.
- Define $M'(x) =$
  - let $b = M(x)$
  - $b = \perp$ then return 0, else return b
- If $x \notin L$, $M'(x)$ will never return 1.
- If $x \in L$, $\text{Prob}(M'(x) = 1) > \frac{1}{2}$, as required.
- ZPP ⊆ RP
- The same way, ZPP ⊆ coRP.

ZPP = RP ∩ coRP

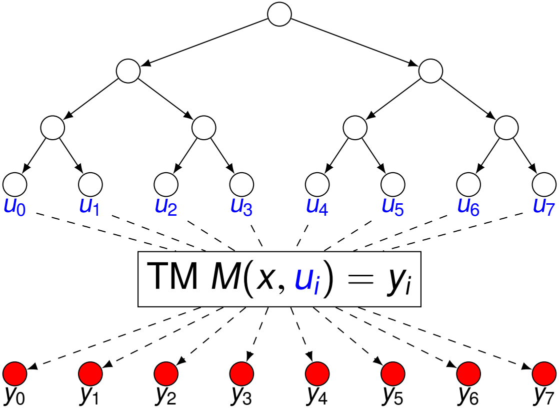
- Let $L \in RP \cap coRP$, M_{RP} and M_{coRP} be the PTMs that recognize L according to RP and $coRP$.
- Define: $M'(x) =$
  - if $M_{RP} = YES$, return 1
  - if $M_{coRP} = NO$, then return 0, else return $\perp$
- $M_{RP}(x)$ never returns YES if $x \notin L$, and $M_{coRP}(x)$ never returns NO if $x \in L$. Therefore, $M'(x)$ never returns the opposite of $\chi_L(x)$.
- The probability that M_{RP} and M_{coRP} are both wrong $< \frac{1}{2} \Rightarrow$ $\text{Prob}(M'(x) = \perp) < \frac{1}{2}$.
- RP ∩ coRP ⊆ ZPP

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



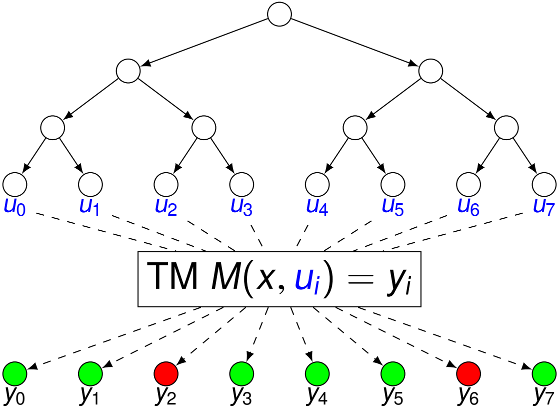
- $L \in$ **NP**:
  - if $x \in L$: at least one ●
  - if $x \notin L$: all ●

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



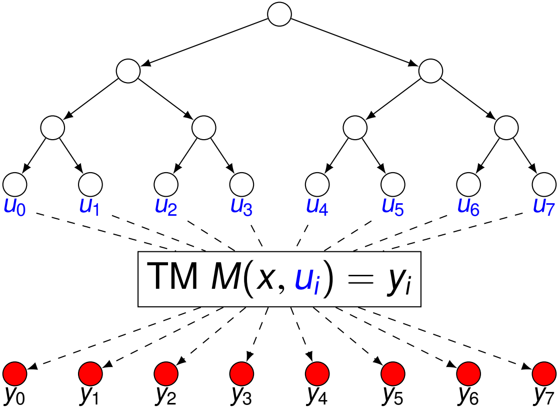
- $L \in$ **NP**:
  - if $x \in L$: at least one ●
  - if $x \notin L$: all ●

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



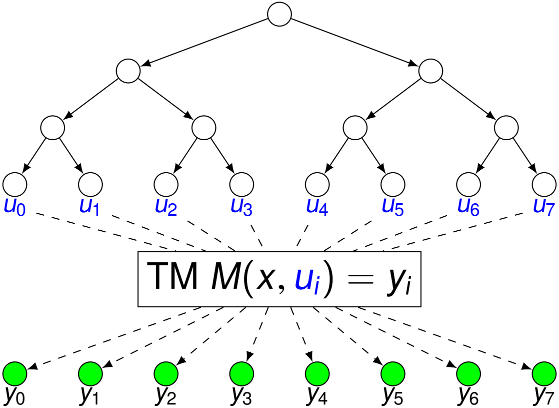
- $L \in$ **RP**:
  - if $x \in L$: at least 75% 🟢
  - if $x \notin L$: all 🔴

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



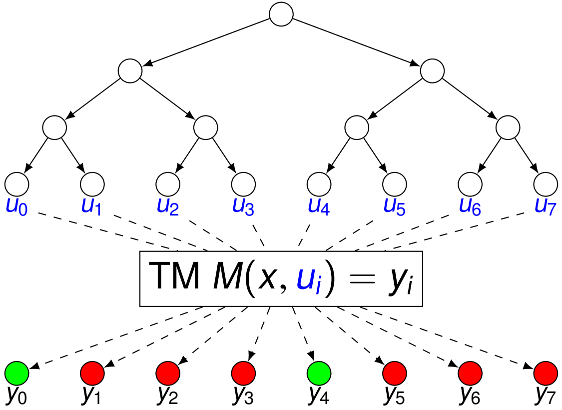
- $L \in$ **RP**:
  - if $x \in L$: at least 75% ●
  - if $x \notin L$: all ●

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



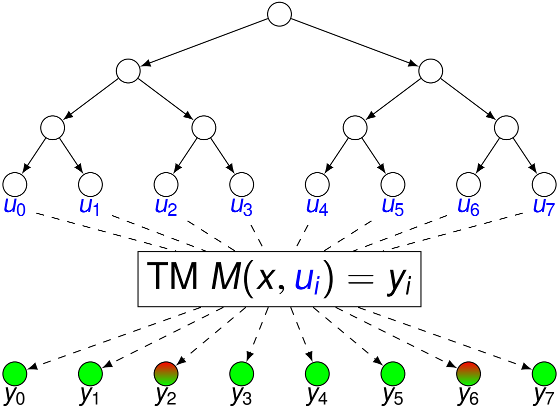
- $L \in$ **coRP**:
  - if $x \in L$: all ●
  - if $x \notin L$: at least 75% ●

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



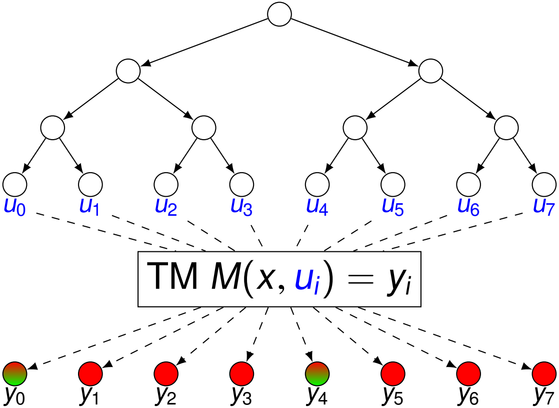
- $L \in$ **coRP**:
  - if $x \in L$: all 🟢
  - if $x \notin L$: at least 75% 🔴

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



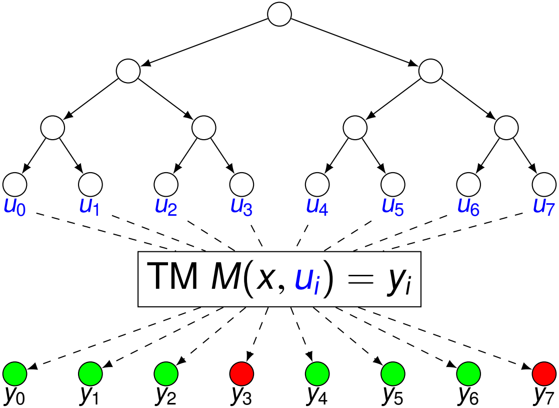
- $L \in$ **ZPP**:
  - if $x \in L$: no 🔴
  - if $x \notin L$: no 🟢

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



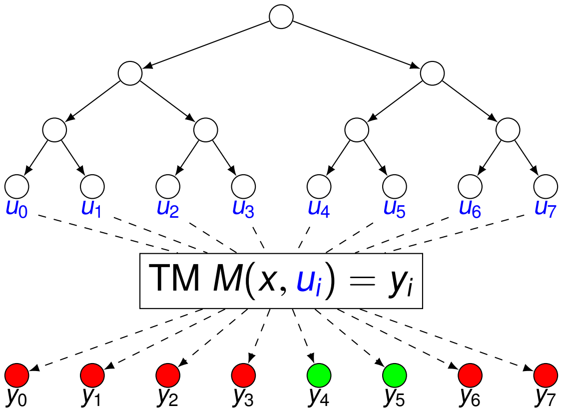
- $L \in$ **ZPP**:
  - if $x \in L$: no 🔴
  - if $x \notin L$: no 🟢

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



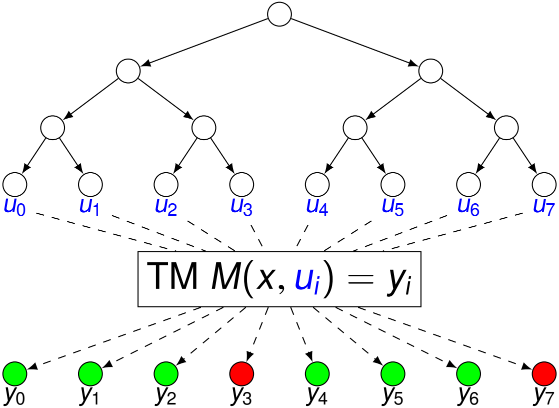
- $L \in$ **BPP**:
  - if $x \in L$: at least 75% 🟢
  - if $x \notin L$: at least 75% 🔴

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



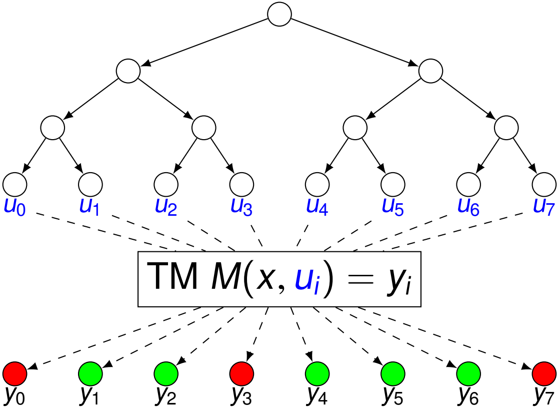
- $L \in$ **BPP**:
  - if $x \in L$: at least 75% 🟢
  - if $x \notin L$: at least 75% 🔴

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



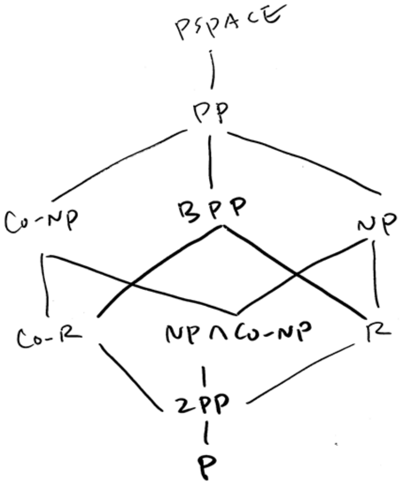
- $L \in$ **PP**:
  - if $x \in L$: at least 75% ●
  - if $x \notin L$: less than 75% ●

NP vs. RP vs. coRP vs. ZPP vs. BPP vs. PP



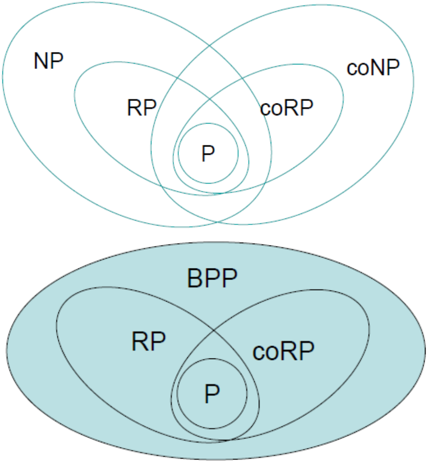
- $L \in$ **PP**:
  - if $x \in L$: at least 75% ●
  - if $x \notin L$: less than 75% ●

Relationship among Probabilistic Classes



Relationships between Prob. classes

Relationship among Probabilistic Classes



Where does BPP fit in?

Some Notes

- Probabilistic classes with ones-sided error - RP and coRP - are common.
- ZPP defines random computations with zero-sided error, but probabilistic runtime.
- Many BPP algorithms have been de-randomised successfully
- Many experts believe that (Conjecture)

$$P = ZPP = RP = RP = BPP \subset PP$$

- BPP = P is equivalent to the existence of strong pseudo-random number generators, which many experts consider likely