Computational problem

Decisional problem.

Instances

$(7, 9)$ $\qquad S = \{(7,9), (2,5), \ldots\} \subseteq \mathbb{Z} \times \mathbb{Z}$

$\downarrow$

$(0111, 1001)$ $\qquad \mathcal{L} = \{(0111, 1001), (0010, 0101), \ldots\}$

$\downarrow$

Language. $\qquad \mathcal{L} \subseteq \{0, 1\}^*$

$$\mathcal{L} = \{ (a,b) \in \{0,1\}^* \times \{0,1\}^* : g\underline{cd(a,b) = 1} \}$$

$$(x,y) \in \{0,1\}^* \times \{0,1\}^*$$

I want to check whether $(x,y) \in \mathcal{L}$ <u>or not</u> ?

"decide" whether $(x,y) \in \mathcal{L}$ or not

$$(x,y) \rightarrow \boxed{A}$$

P-class:

A language L is in P-class if $\exists$ a deterministic poly time decider for L.

Decider for a language L:

Let M be a TM. We call M is a decider for L if

$M(x) = 1$ iff $x \in L$.

We call M to be a "poly-time" decider if $\exists$ a positive poly $p()$ such

$\forall x \in \{0,1\}^*$, $M(x)$ runs for at most $p(|x|)$ steps where $|x|$ denotes the size of the i/p string x.

We call the TM M to be "deterministic" if at any point of time, there is at most one move of the turing machine M.

A language $L \in P$ if $\exists$ a det. poly time TM M such that $M(x)=1$ iff $x \in L$. M is a "poly-time decider" for L.

$\wedge \mid$

- **Boolean Satisfiability problem.**

Suppose $\phi(x_1, x_2, \ldots, x_n)$ is a boolean expression over n variables.

We call that $\phi(x_1, x_2, \ldots, x_n)$ has a "satisfying assignment" if $\phi(v_1, v_2, \ldots, v_n) = 1$, when $x_i = v_i$ for all $i = 1(1)n$, where $v_i \in \{0,1\}$

$$\underset{\overset{\parallel}{0}}{x_1} \wedge \underset{\overset{\parallel}{0}}{x_2} \vee \neg \underset{\overset{\parallel}{0}}{x_3} = 1$$

$\mathcal{L} = \{\phi(x_1, x_2, \ldots, x_n) : \phi \text{ has a satisfying assignment}\}$

$\psi \overset{?}{\in} \mathcal{L}$

$\langle \underbrace{\psi, w}_{} \rangle$

certificate

$|y| = 5|x|^3$

<u>NP-class:</u> $\mathcal{L} = \{x \in \{0,1\}^* : Q(x) = 1\}$.

A language $\mathcal{L}$ is in NP-class if $\exists$ a two-input det. poly-time TM M, and $\exists$ a polynomial $p()$, such that $\forall x \in \mathcal{L}, \exists$ $y \in \{0,1\}^*$, $|y| \le p(|x|)$ and $M(x, y) = 1$.

Suppose $\mathcal{L}$ be a language. Let $R_{\mathcal{L}} \subseteq \{0,1\}^* \times \{0,1\}^*$ be a reln.

We say that R_L is poly-time "decidable" if $\exists$ a two input det. poly-time TM M such that

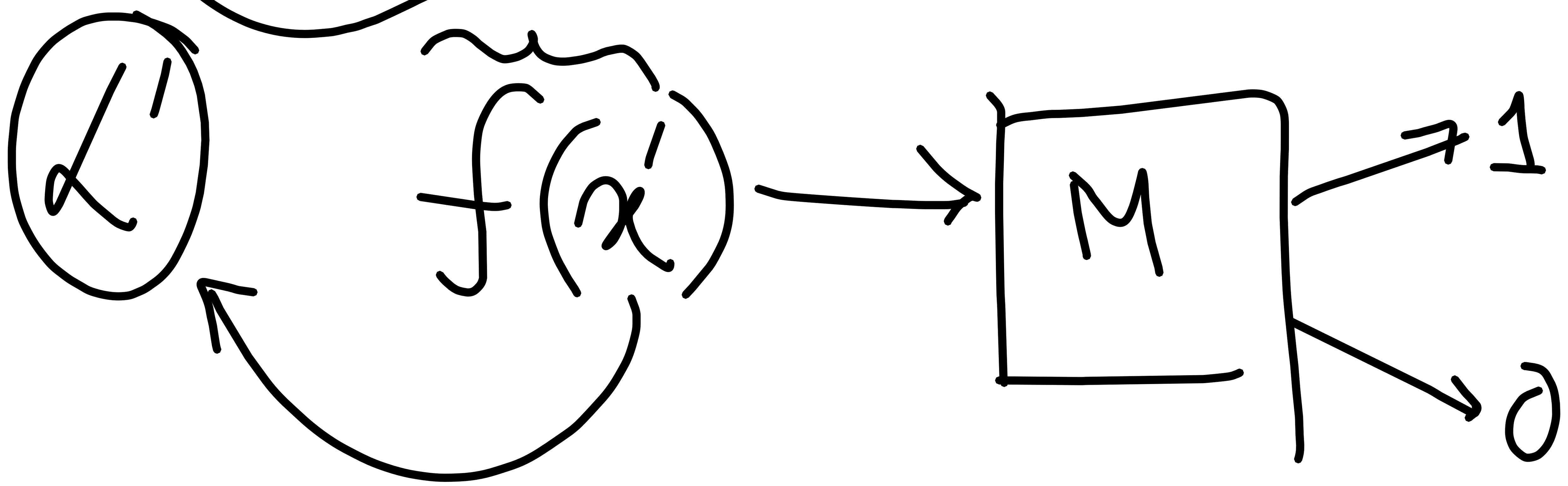
$M(x,y) = 1$ iff $(x,y) \in R_L$.

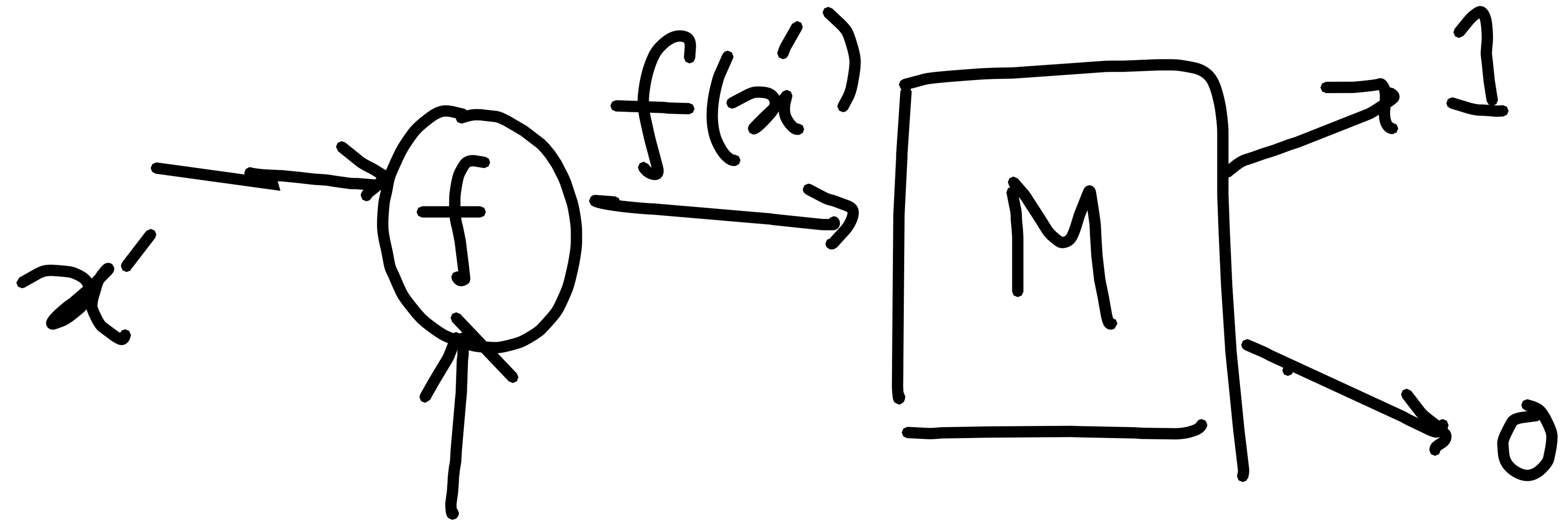
A language $\mathcal{L}$ is in NP, if $\exists$ a poly-time decidable reln R_L such that $\forall x \in \mathcal{L}, \exists\, y : |y| \leq p(|x|), (x,y) \in R_L$

$$(\langle G_1, G_2 \rangle, \phi)$$

$$\langle G_1, G_2 \rangle \in \mathcal{L} \Rightarrow \exists \phi$$

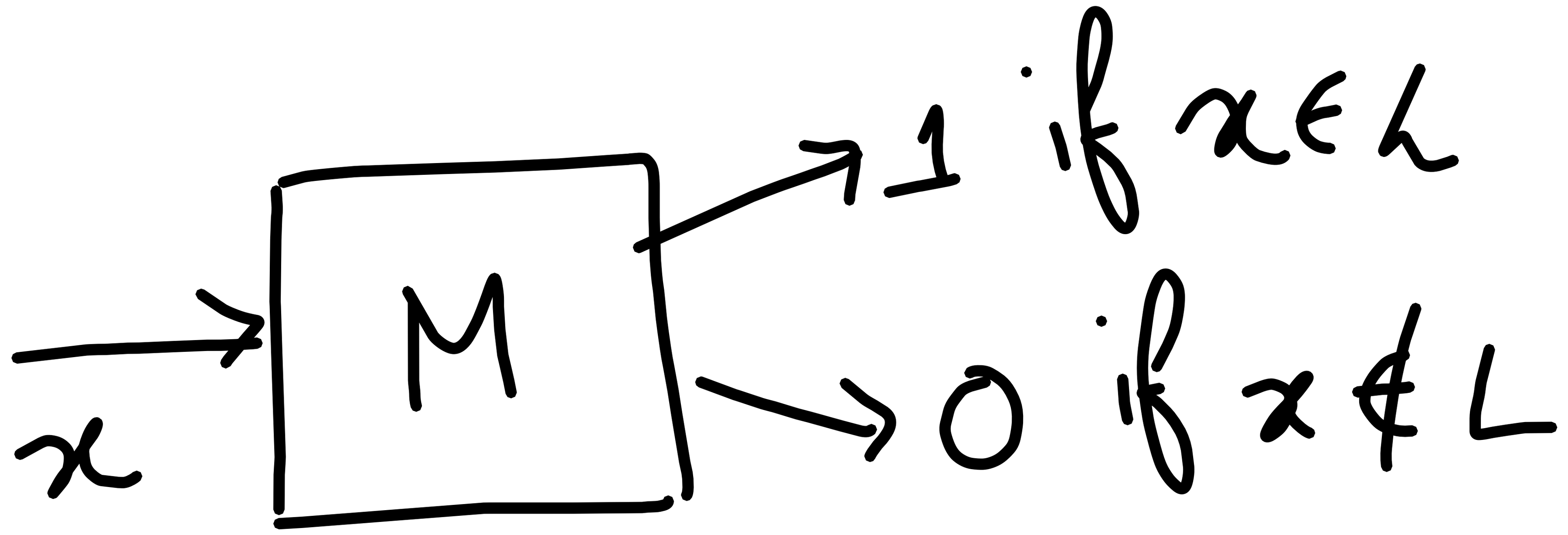
$\mathcal{L}$ and $\mathcal{L}$ is "decidable" by some poly-time TM M.





Let $\mathcal{L}$ and $\mathcal{L}'$ be two languages. We call that $\mathcal{L}'$ is poly. time reducible to $\mathcal{L}$, denoted as $\mathcal{L}' \leq_p \mathcal{L}$ if $\exists$ a poly-time computable fn.

$f : \{0,1\}^* \to \{0,1\}^*$ such that $x' \in \mathcal{L}' \iff f(x') \in \mathcal{L}$



A fn. f is poly-time computable fn. if $\exists$ a det. poly. time TM M_f such that $\forall x \in Dom(f)$

$$f(x) = M_f(x)$$

Let $\mathcal{L}$ be a language. We say that $\mathcal{L}$ is "NP-Hard" if for every $\mathcal{L}' \in NP$, we have

$$\mathcal{L}' \leq_p \mathcal{L}$$

*$\mathcal{L}$ is NP-complete if $\mathcal{L} \in NP$.

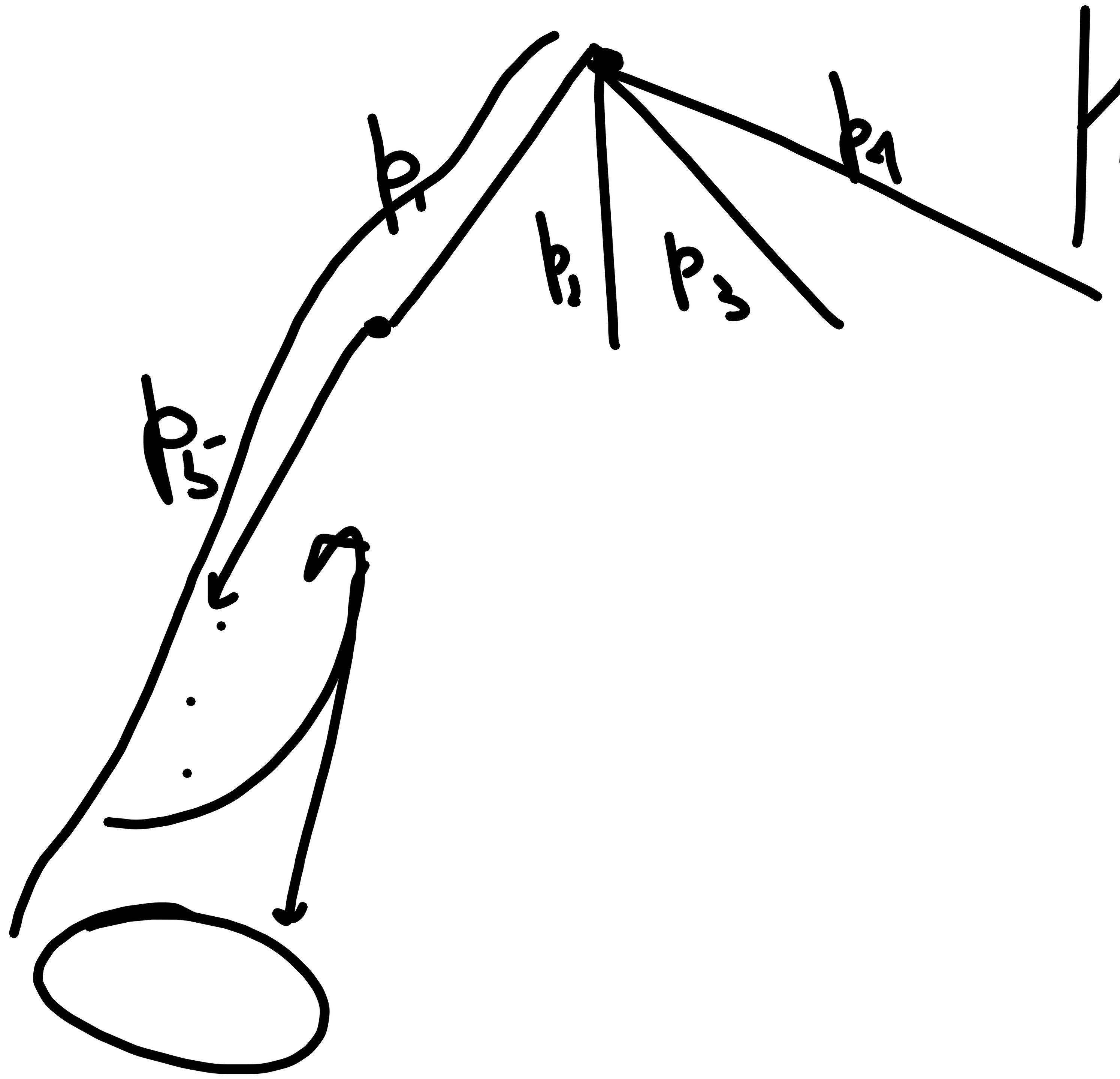
$\mathcal{L}' \leq_p \mathcal{L}$ and $\mathcal{L}$ is poly-time decidable $\Rightarrow \mathcal{L}'$ is poly-time decidable.

"worst case hardness measure!"

$$\frac{\mathcal{L} \in NPC \qquad \mathcal{L}' \in NP}{\forall \mathcal{L}'' \leq_p \mathcal{L} \qquad \mathcal{L} \leq_p \mathcal{L}'}$$

BPP-class:

Probabilistic TM:



$$\Pr_r\left[M(x)=1\right]=\frac{\#\{r:\ M(r,x)=1\}}{|R|}$$

$\in$

M runs for some polynomial $p(\,)$

$\{0,1\}^{p(|x|)}$

A language $\mathcal{L}$ is in BPP class if $\exists$ a prob. poly time Turing Machine M such that the following two holds:

$P \subseteq BPP$

(i) $\forall x \in \mathcal{L} \quad \Pr[M(x)=1] \geq \frac{2}{3}$ $\quad P \subseteq NP$

(ii) $\forall x \notin \mathcal{L} \quad \Pr[M(x)=1] \leq \frac{1}{3}$.