Def. P = set of polynomial time predicates

Input $x \in \{0,1\}^n$, $|x| = n$

Runtime $p(n)$

Def. FP = set of polynomial time functions.

Def. NP = <u>nondeterministic</u> polynomial time

- Some configurations have 2 successors

language $L \in NP \iff \exists$ poly time TM $M(x)$

s.t. $\forall x \, (x \in L \iff M(x)$ has <u>an</u> accepting computation$)$

Def A language $L \subset \{0,1\}^*$

And WLOG, polynomial time Turing Machines (TM) have a "clock" attached which make it explicitly poly time!

An alternate **Def**. A language $L \in NP \iff \exists$ poly time predicate $R(x,y)$,

$\exists\, p(n)$ polynomial, $\forall x \, \big(x \in L \iff (\exists\, y, |y| \le p(|x|))\, R(x,y)\big)$

<u>Notation</u>

$NP = \Sigma_1^P$

$coNP = \Pi_1^P = \{L \mid \bar{L} \in NP\}$, $\bar{L} = \{0,1\}^* \setminus L$

(and $x \in \bar{L} \iff (\forall y \; |y| \le p(|x|))\, \neg R(x,y)$)

- we can generalize Σ_i^P, Π_i^P, $i \ge 1$ polynomial time hierarchy

$$PH = \bigcup_i \Sigma_i^P = \bigcup_i \Pi_i^P$$

$L \in \Sigma_i^P \iff \exists$ formula

$$\exists\, y_1, |y_1| \le p_1(|x|) \;\; \forall y_2, |y_2| \le p_2(|x|) \; \cdots \; Q y_i, |y_i| \le p_i(|x|) \; R(x, \vec{y})$$

poly time

where p_j's are poly's

$$\boxed{\forall x \, (x \in L \iff \varphi(x) \text{ is true})}$$

$L \in P \iff \bar{L} \in P$

<u>Open</u>: $NP = coNP$?

<u>Def</u>. Probabilistic TM (PTM)

- some configurations have 2 successors
- choice on successor is made at random

<u>Def</u> Bounded Probabilistic Poly Time (BPP)

$L \in BPP \iff \exists$ poly time PTM, $M(x)$, s.t.

$\forall x \left(x \in L \iff Pr(M(x) \text{ accepts}) \geq \frac{2}{3} \right)$

and $\forall x \left(x \notin L \iff Pr(M(x) \text{ accepts}) \leq \frac{1}{3} \right)$

Alternately,

$L \in BPP \iff \exists$ ~~Deterministic TM (DTM)~~ poly time predicate $R(x,y)$, $\exists$ poly $p(n)$

s.t. $\forall x \left(x \in L \iff (\#y \in \{0,1\}^{p(n)}) R(x,y) \geq \frac{2}{3} \cdot 2^{p(n)} \right)$

and $\forall x \left(x \notin L \iff (\#y \in \{0,1\}^{p(n)}) R(x,y) \leq \frac{1}{3} \cdot 2^{p(n)} \right)$

- BPP is unchanged if we replace $1/3, 1/2$ by $2^{-n}, 1-2^{-n}$ or

$\frac{1}{2} - \frac{1}{n}, \frac{1}{2} + \frac{1}{n}$

$2^{-r(n)}, 2^{r(n)}$

$\frac{1}{2} - \frac{1}{r(n)}, \frac{1}{2} + \frac{1}{r(n)}$ for any poly $r(n)$

Def. $\#P$ class of functions

$$f \in \#P \iff f : \{0,1\}^* \longrightarrow \mathbb{N} \overset{\text{iso}}{\simeq} \{0,1\}^*$$

$f \in \#P \iff \exists$ poly time predicate $R(x,y)$, $\exists$ poly $p(n)$ s.t.

$$\forall x \left(f(x) = \left(\#y \in \{0,1\}^{p(|x|)} \right) R(x,y) \right)$$

Equivalently, $\exists$ poly time NTM $M(x)$ s.t.

$$\forall x \left(f(x) = (\# \text{ accepting computations of } M(x)) \right)$$

- $\#P \subseteq PSPACE$

  <u>Open</u> $P = PSPACE$?

Def. $P^{\#P}$ (or more generally P^X where $X \subseteq \{0,1\}^*$), where $\#P$ (or X) is an <u>oracle</u>.
Poly time TM that is allowed to "query" $f \in \#P$ (or X).

for $\#P$, query is some $z \in \{0,1\}^*$ and answer is $f(z)$

<u>Easy THM's</u> $NP \subseteq P^{\#P}$

$coNP \subseteq P^{\#P}$

$BPP \subseteq P^{\#P}$

<u>Toda's THM</u>. Polynomial Hierarchy ($\bigcup$ all classes) $PH \subseteq P^{\#P}$

Overall Picture:

$$P \left. \begin{array}{l} \subseteq NP \\ \subseteq coNP \\ \subseteq BPP \end{array} \right\} \subseteq \Sigma_2^P \subseteq PH \subseteq P^{\#P} \subseteq PSPACE$$