- efficient computation ~ poly-time comput.

- The search version $R \subseteq \{0,1\}^* \times \{0,1\}^*$
  - poly-bounded $\stackrel{\text{def}}{=} \exists$ poly p s.t. $(x,y) \in R \Rightarrow |y| \leq p(|x|)$
  - Notation: $R(x) \stackrel{\text{def}}{=} \{y : (x,y) \in R\}$, $S_R \stackrel{\text{def}}{=} \{x : R(x) \neq \emptyset\}$

[illegible]

- PolyFind $\stackrel{\text{def}}{=} \left\{ R : \begin{array}{l} \exists \text{ poly-time alg } A \text{ s.t.} \\ \forall x \in S_R \;\; A(x) \in R(x) \\ \forall x \notin S_R \;\; A(x) = \bot \end{array} \right\}$ $\xleftarrow{}$ p.b.

- PolyCheck $\stackrel{\text{def}}{=} \left\{ R \underset{\text{bound}}{\text{poly}} : \begin{array}{l} \exists \text{ poly-time alg } A \text{ s.t.} \\ A(x,y) = 1 \text{ iff } (x,y) \in R \end{array} \right\}$

בעית חיפוש סבירה צריכה להיות ← PC

(זה המשמעות של חיפוש פתרון שאז ניתן לבדוק נכונותו...)

- The P-vs-NP Question as $PC \overset{?}{\subseteq} PF$

האם לכל $R \in PC$ מתקיים $R \in PF$?

משערים $PC \not\subseteq PF$ לפני נסכם

⇐ אובדן המשמעות של מושג "הפתרון"

ו/וו "חיפוש" "פתרון"

$PF \not\subseteq PC$: $R \stackrel{\text{def}}{=} \{(x,x) : x \in \{0,1\}^*\} \cup \{(x, \sigma^{t}) : \ldots \}$

$\sigma = \text{Halt}(x)$

The decision version

$P \stackrel{\text{def}}{=} \{S : \exists \text{ poly-time } A \text{ s.t. } A(x) = 1 \text{ iff } x \in S\}$

$NP \stackrel{\text{def}}{=} \{S : \exists \text{ poly } p \; \exists \text{ eff. verifiable proofs of length } \leq p$

$\Rightarrow \exists p \; \exists \text{ poly-time verification procedure } V$

Witness (complete) $\forall x \in S \; \exists w \in \{0,1\}^{\leq p(|x|)}$ s.t. $V(x,w) = 1$

(sound) $\forall x \notin S \; \forall w \;\; V(x,w) = 0$

[illegible] : V רץ בזמן פולינומיאלי

באורך של הקלט (x)

המשמעות של $P = NP$ ⇐ אובדן משמעות

מושג "ההוכחה"