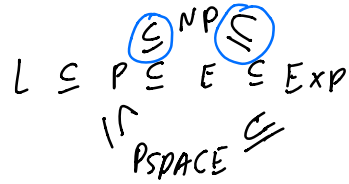


Nondeterministic Polynomial Time



Independent set:

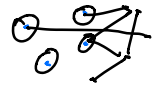
$$ISet(G, k) = \begin{cases} 1 & \text{if } G \text{ has an independent set of size } k \\ 0 & \text{o.w.} \end{cases}$$

\swarrow graph \searrow number

a set of vertices with no induced edges.

Subset sum:

$$Subsum(a_1, \dots, a_n, t) = \begin{cases} 1 & \text{if } \exists S \text{ s.t. } \sum_{i \in S} a_i = t \\ 0 & \text{o.w.} \end{cases}$$



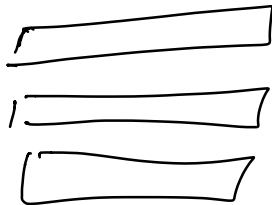
Composit num:

$$Comp(N) = \begin{cases} 1 & \text{if } N = A \cdot B, A, B \neq 1 \\ 0 & \text{o.w.} \end{cases}$$

Def: $f: \{0,1\}^* \rightarrow \{0,1\}$ is in NP if \exists poly p and a polytime machine V s.t. $\forall x \in \{0,1\}^*$, $f(x) = 1 \Leftrightarrow \exists w \in \{0,1\}^{p(|x|)}, V(x,w) = 1$.

OPEN: $P \stackrel{?}{=} NP$.

Original Definition



Program

1. read x_i, y_i ... goto $\begin{cases} \rightarrow \text{line 5} \\ \rightarrow \text{line 7} \end{cases}$
- 2.
- ⋮

$NTIME(t(n))$

$$NP = \bigcup_{c \geq 1} NTIME(n^c)$$

Thm: If r, t are time constructible functions
with $r(n+1) \leq O(t(n))$ then

$$NTIME(r(n)) \neq NTIME(t(n)).$$

X _____ X

Polytime Reductions

Def: f is polytime reducible to g if \exists poly time computable h
s.t. $f(x) = g(h(x))$. $\boxed{f \leq_p g}$.

Def: f is NP-hard if $g \leq_p f$ for every $g \in NP$.

Def: f is NP-complete if f is NP-hard and $f \in NP$.

Circuit-SAT

$$\text{Circuit-SAT}(C) = \begin{cases} 1 & \text{if } \exists w \text{ s.t. } C(w) = 1 \\ 0 & \text{o.w.} \end{cases}$$

a boolean circuit

Thm: Circuit-SAT is NP-hard.

Pf: Suppose $f \in NP$. WANT: $f \leq_p \text{Circuit-SAT}$

$$\Leftrightarrow \exists h \text{ s.t. } f(x) = \text{Circuit-SAT}(h(x)).$$

We know $\exists V$ s.t.

$$f(x) = 1 \Leftrightarrow \exists w \text{ s.t. } V(x, w) = 1 \Leftrightarrow \exists w \text{ s.t. } C_x(w) = 1$$

$$h(x) : \text{output } C_x(w) \text{ s.t. } C_x(w) = V(x, w).$$



$$f \leq_p \text{Circuit-SAT} \leq_p 3\text{-SAT} \leq_p \text{Isat}$$

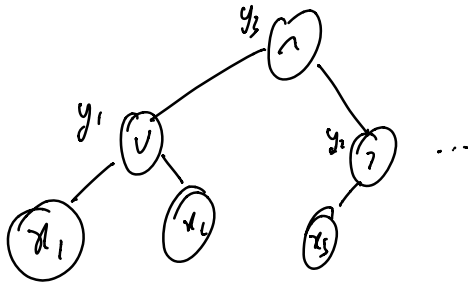
\leq_p Subset Sum

3-SAT

$$\phi = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_5 \vee x_2 \vee \bar{x}_1) \wedge \dots$$

$$3\text{-SAT}(\phi) = \begin{cases} 1 & \text{if } \exists x \text{ s.t. } \phi(x) = 1 \\ 0 & \text{o.w.} \end{cases}$$

Thm: Circuit-SAT \leq_p 3-SAT



$$\begin{aligned} y_1 &= x_1 \vee x_2 \\ y_2 &= \neg x_3 \\ y_3 &= y_1 \wedge y_2 \\ &\vdots \end{aligned}$$

