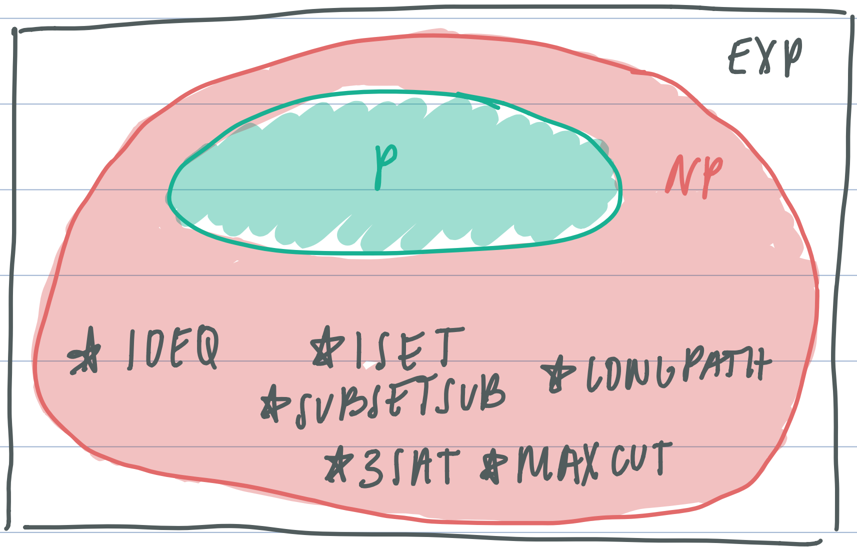
CS121 Lecture 17: Cook Levin Theorem

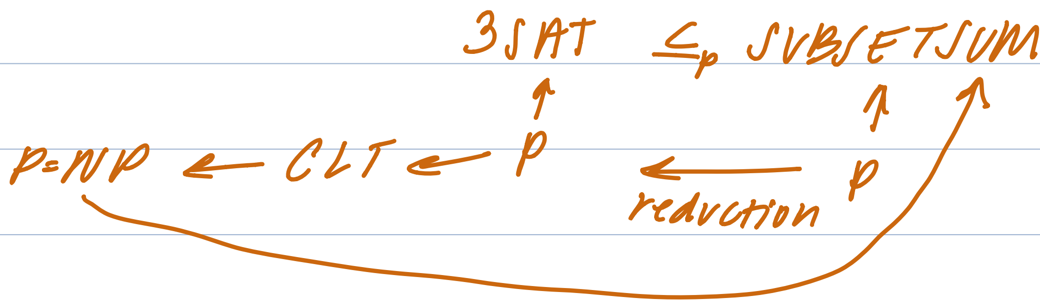
October 29, 2019



NP : class s.t. $P \subseteq NP \subseteq EXP$ containing all above problems

Cook Levin Theorem:
If $3SAT \in P$, then $P = NP$

Prove: if $SUBSETSUM \in P$, then $P = NP$



NP-Complete : Problems such as 3SAT, SUBSETSUM, satisfying if $F \in P$, then $P = NP$.

Def (informal): NP is the set of problems for which a solution can be efficiently verified.

Slightly more formal: NP is set of instructions $F: \{0,1\}^* \to \{0,1\}$ s.t. for every $x \in \{0,1\}^*$, $F(x) = 1$

iff there is some polynomial-size "proof" demonstrating this.

Def. Let $F:\{0,1\}^* \to \{0,1\}$. Then $F \in NP$ if there is a poly-time V and poly-time $q: \mathbb{N} \to \mathbb{N}$ s.t. for every $x \in \{0,1\}^*$

to ensure length of certification is bounded

$$F(x) = 1 \leftrightarrow \exists_{w \in \{0,1\}^*} \ |w| \le q(|x|) \text{ and } V(x,w) = 1$$

verification proof

Q1. Prove that $ISET \in NP$.

input: G, k

output: 1 iff $\exists S \subseteq U(G)$ $|V| \ge k$ $\forall (u,v) \in E(G)$ either $u \notin S$ or $v \notin S$

pf. $x = (G, k)$

w = description of $S \in \{0,1\}^n$ $\quad n = |V(G)|$

Q2. Prove that $P \subseteq NP$

pf. $F: \{0,1\}^* \to \{0,1\}$ $\quad F \in P$

know $\to$ poly M $\quad M(x) = F(x) \ \forall x$

$V(x, w)$: return $M(x)$

Q3. Prove that $NP \subseteq EXP$

pf. Let $F \in NP$, then $\exists V, q(n)$ such that $\forall x$, $F(x) = 1$ iff $\exists w \in \{0,1\}^n$, $|w| \le q(n)$ and $V(x,w) = 1$

- Given input size, enumerate all inputs ($q(n) \cdot 2^{s(n)}$) and check them (V is poly(n)) $\rightarrow$ exponential time.
- By time heirarchy theorem, X is subset of n.

Cook-Levin Theorem Proof

$\forall F \in NP,\ F \leq_p$ 3SAT $\leftarrow$ 3SAT is NP-hard.

NP-hard + in NP = NP-complete

Define NANDSAT

Input: NAND-CIRC program P (aka circuit w/ NAND gates)

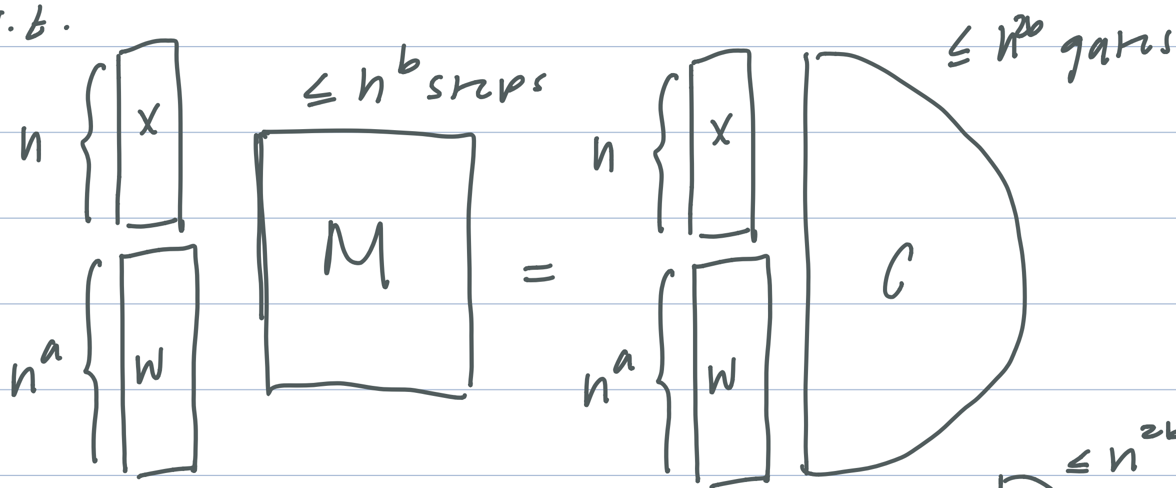
Output: 1 iff there is $x \in \{0,1\}^n$ s.t. $P(x) = 1$

every funct in NP can be reduced to NANDSAT

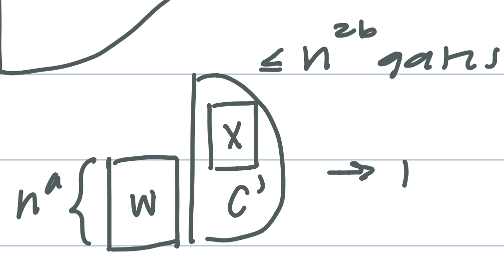
Lemma 1: $\forall F \in NP,\ F \leq_p$ NANDSAT

If $F \in NP$ we know $\exists$ poly-time TM M s.t. $\forall x \in \{0,1\}^n$

By proof of $P \subseteq P_{/poly}$ can find n^{2b} sized circuit C s.t.



$F(x) = 1 \longleftrightarrow \exists w \in \{0,1\}^{n^a}$



Define 3NAND

Input: φ is AND of constraints of form $z_i = NAND(z_j, z_k)$

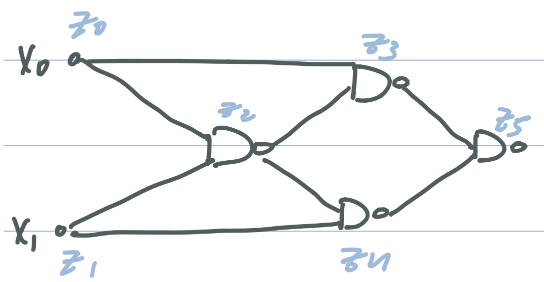
Output: 1 iff there is assignment $z \in \{0,1\}^n$ satisfying φ

Q. If $\varphi = (z_0 = NAND(z_2, z_3)) \wedge (z_3 = NAND(z_2, z_1)) \wedge (z_1 = NAND(z_2, z_3))$, what is $3NAND(\varphi)$?

$(z_0, z_1, z_2, z_3) = (1, 1, 0, 1)$

Lemma 2: NANDSAT $\leq_p$ 3NAND

Proof by example.



$\rightarrow$

$$\left.\begin{array}{l} z_2 = NAND(z_0, z_1) \\ z_3 = NAND(z_0, z_2) \\ \quad\vdots \\ z_5 = 1 \quad \left\{ \begin{array}{l} z_6 = NAND(z_0, z_0) \\ z_5 = NAND(z_0, z_6) \end{array} \right. \end{array}\right\} \text{7-var assignment}$$

Lemma 3: 3NAND $\leq_p$ 3SAT

For every $a, b, c \in \{0,1\}$

$$\left.c = NAND(a,b) \longleftrightarrow \begin{array}{l} \bar{a} \vee \bar{b} \vee \bar{c} \\ \wedge \quad c \vee a \\ \wedge \quad c \vee b \end{array}\right\} \text{key claim}$$

Key claim $\rightarrow$ lemma. Every 3NAND formula $\rightarrow$ 3SAT constraints.