NP Completeness, SAT, Reductions

* **NP**

$L \subseteq \{0,1\}^* \in NP$ if $\exists p: \mathbb{N} \to \mathbb{N}$, polynomial time TM M s.t. $\forall x \in \{0,1\}^*$ $x \in L$ iff $\exists u \in \{0,1\}^{p(|x|)}$ s.t. $M(x, u) = 1$

$u \rightarrow$ certificate of x wrt L and M

Examples - Traveling salesman, INDSET, IPROG

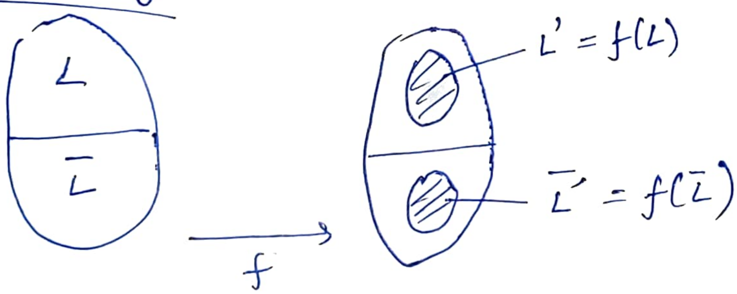
- $P \subseteq NP \subseteq EXP$

  $\hookrightarrow \bigcup_{c>1}$

* **NDTM, NTIME**

For every $T: \mathbb{N} \to \mathbb{N}$, $L \subseteq \{0,1\}^*$, $L \in NTIME(T(n))$ if $\exists$ $c>0$ and a $c \cdot T(n)$-time NDTM s.t. $\forall x \in \{0,1\}^*$ $x \in L \Leftrightarrow M(x) = 1$

* **Reducibility**



$L \subseteq \{0,1\}^*$ is polynomial time Karp reducible to $L' \subseteq \{0,1\}^*$, if $\exists f: \{0,1\}^* \to \{0,1\}^*$ s.t. $\forall x \in \{0,1\}^*$ $x \in L \Leftrightarrow f(x) \in L'$

$L \leq_p L'$

L' is NP-hard if $L \leq_p L'$ $\forall L \in NP$

L' is NP-complete if $L' \in NP$ and L' is NP-hard

Hamiltonian Path & Cycles

A directed / undirected path that visits each vertex of a graph exactly once.

If this path is a cycle $\Rightarrow$ Hamiltonian Cycle,

Let L be a language denoting all graphs with a hamitonian cycle, L' denoting all graphs with a hamiltonian path.

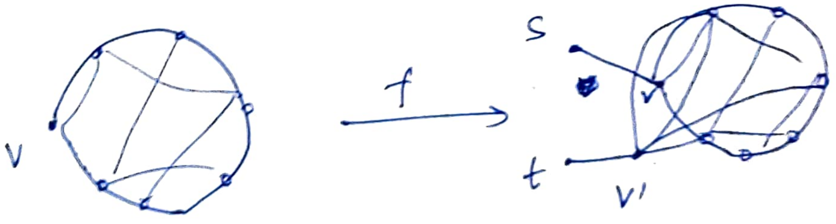
To show: $L \leq_p L'$

Define $f: \mathcal{G} \to \mathcal{G}$

$\mathcal{G}$: set of all graphs in binary strings

Consider $G \in \mathcal{G}$, $G = (V, E)$, $G \in L$

Let a vertex $v \in V$ (occurs in HC)



$G \in L$ $\qquad\qquad$ $G' \in L'$

Add v' in G' s.t. v' is a copy of v (same edges)

Add degree one vertices s, t connected to v, v' respectively.

1. $G \in L \Rightarrow f(G) \in L'$

Represent HC by $(v, v_1)(v_1, v_2) \cdots (v_n, v)$

In $f(G)$ consider the path $(s, v)(v, v_1) \cdots (v_n, v')(v', t)$

Clearly HP

2. $f(G) \in L' \Rightarrow G \in L$

Any HP has two endpoints s, t

$HP \equiv (s, v)(v, v_1) \cdots (v_n, v')(v', t)$

$(v_n, v') \in E$ and $(v_n, v) \in E$

$\therefore (v, v_1)(v_1, v_2) \cdots (v_n, v)$ is a HC

* $L \leq_p L'$ and $L' \leq_p L'' \Rightarrow L \leq_p L''$

$x \to f_1(x)$ $\quad f_1(x) \to f_2(f_1(x))$

$f_2 \circ f_1$ is still a polynomial time computable fn

* L is NP-hard, $L \in P \Rightarrow P = NP$

all NP L' reduce to L but $L \in P \Rightarrow P = NP$

* L is NP-complete, $L \in P \Leftrightarrow P = NP$

$\Rightarrow$ by def. $\quad \Leftarrow$ by def.

CNF : Conjunction of clauses

$\downarrow$

disjunction of literals

$\bigwedge_i \left(\bigvee_j v_j \right) = F$

SAT $= \{ F \mid \exists u \text{ s.t } u \models F \}$ set of all satisfiable formulas

3SAT $=$ all satisfiable 3CNF

max 3 literals / clause

Cook - Levin Theorem

1. SAT is NP complete
2. 3SAT is NP complete

Sketch: SAT $\in$ NP (u is the certificate)

1 → Prove SAT is NP-hard

2 → SAT $\leq_p$ 3SAT $\Rightarrow$ 3SAT is NP hard

1 → reduce every $L \in NP$ to SAT

construct polynomial type $f: \{0,1\}^* \to$ SAT

- for every boolean $f: \{0,1\}^l \to \{0,1\}$ $\exists$ l-variable CNF of $\underbrace{\text{size}}_{\text{no. of } \vee, \wedge}$ $l2^l$ s.t. $\varphi(u) = f(u)$ $\forall u \in \{0,1\}^l$

Pf: for any $v \in \{0,1\}^l$ $\exists$ a clause C_v s.t. $C_v(v) = 0$, $C_v(u \neq v) = 1$ (Just negate all 1's)

$$\varphi = \bigwedge_{v: f(v) = 0} C_v$$

- use boolean function $\{0,1\}^{p(|x|)} \to M(x,u)$ for $L \in NP$. This gives CNF Ψ_x s.t. $\Psi_x(u) = M(x,u)$. Thus u exists iff $\Psi_x \in$ SAT

Size of Ψ_x is exponential $P(|x|)\, 2^{p(|x|)}$

Use the fact that M is a polynomial time TM

Two tape oblivious TM $\Rightarrow$ form $O(p(|x|))$ size CNF

$2 \Rightarrow$ SAT $\le_p$ 3SAT

$u_1 \vee u_2 \cdots \vee u_{n-3} \vee u_{n-2} \vee u_{n-1} \vee u_n \rightarrow$ clause

$= (u_1 \vee u_2 \cdots \vee u_{n-2} \vee z) \wedge (u_{n-1} \vee u_n \vee \bar{z})$

INDSET is NP complete

~~Note~~ ind set of size k

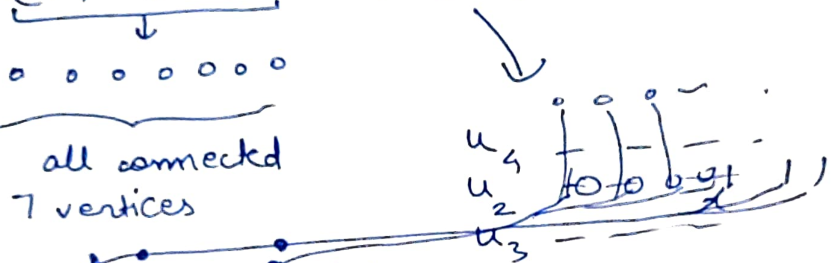
INDSET $= \{(G, k) : k$ ind. vertices in $G\}$

- 3SAT $\le_p$ INDSET

Define f s.t. 3CNF formula $\rightarrow$ graph G

~~Pick~~ For 3 literal clause $\Rightarrow$ 7 partial assigments

$\underbrace{(\bar{u}_1 \vee \bar{u}_2 \vee \bar{u}_3) \wedge (u_4 \vee u_2 \vee u_3) \wedge \cdots (u_x \vee u_y \vee u_z)}_{k \text{ clauses}}$



u_1	0	0	0	0	1	1	1
u_2	0	0	1	1	0	0	1
u_3	0	1	0	1	0	1	0

connect all conflicts

$\{1, 1, 1\} \rightarrow \bar{u}_1 \vee \bar{u}_2 \vee \bar{u}_3 = 0$

$\varphi \in$ 3SAT is satifiable iff $f(\varphi) = G$ has ind set of size k

$\Rightarrow$ take the certificate

$\Leftarrow$ assign values to u_i

* $P \stackrel{?}{=} NP$ $\rightarrow$ proofs
$\rightarrow$ crypto ?