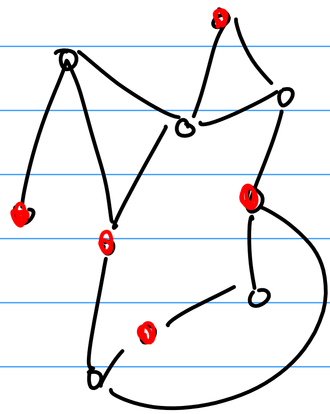
CS500 3/27

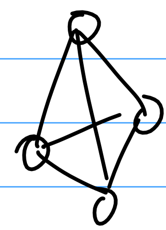
HW #1 is out.

SAT $\leq$ X for all $X \in \{$ Ind Set ... ... Partition $\}$



$k=4$ Yes Easy to check

no ind set ≥ 6 No ?



SAT: φ (CNF) is satisfiable!

Give $x_1=1, x_2=0, x_3=1 \dots$

Answer to I_X is No

$\iff \forall t \;\; |t| \leq p(|I_X|) \quad C(I_X, t) = NO$

P = class of problems solvable in poly-time

2SAT, BIPARTITEMATCHING, SHORTESTPATH $\in$ P

NP = class of problems that have poly-time certifier

3SAT $\in$ NP $\qquad \varphi$

$t = 0110111$ binary string of length n

3SAT Certifier $C(\varphi, t)$

φ: formula, instance of 3SAT

t: truth assignment $01101011 0 \ldots 1$, certificate

3COLORING $C(G, t)$

G: graph, instance of 3COLORING

t: certificate $\underbrace{RGBRRGB \ldots R}_{n = \#\text{vertices}}$

NP DOES NOT MEAN ~~non-polynomial-time~~

NONDETERMINISTIC POLYNOMIAL TIME

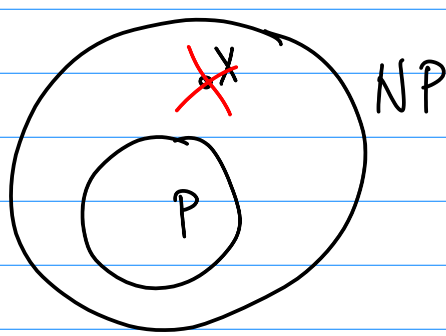
co-NP No-Answer can be certified

__Theorem:__ $P \subseteq NP$

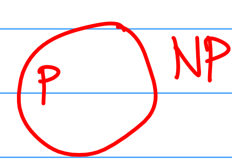
Proof: Let $X \in P$. Need to show $X \in NP$.

Need alg. $C(I_X, t)$ running in $p(|I_X| + |t|)$

$$C(I_X, t) = A_X(I_X) \qquad \square$$



$X \in NP \setminus P$



$P \subseteq NP \subseteq EXP$

EXP = solvable in time $O(2^{p(n)})$

p polynomial

$n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot n \leq n^n = 2^{n \log n}$

Proof: $X \in NP$ Need to find alg A_X running in $O(2^{p(|I_X|)})$ time

$C(I_X, t)$ where $|t| \leq q(|I_X|)$

$A_X(I_X)$: for all t of length $|t| \leq q(|I_X|)$: $2^{q(|I_X|)}$

run $C(I_X, t)$

if yes, return YES

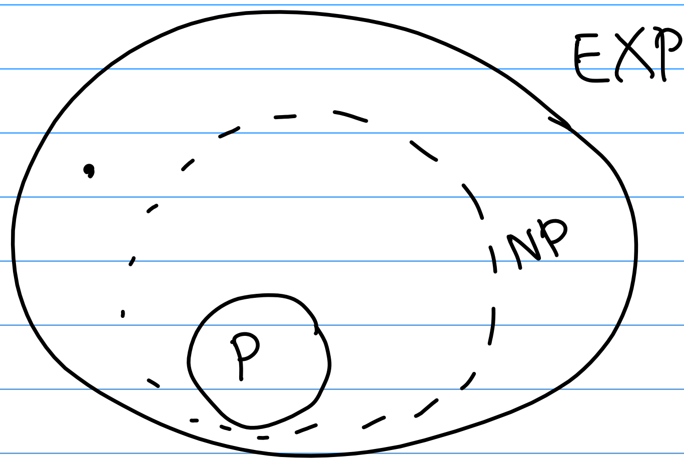
$O(r(|I_X| + |t|))$

$\leq O(r(|I_X| + p(|I_X|)))$

return NO

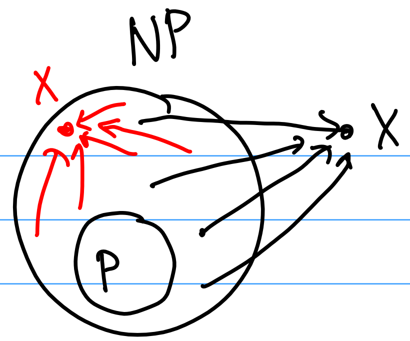
running time is $O(2^{q(|I_X|)} \cdot r(|I_X| + p(|I_X|)))$

$= O(2^{q(|I_X|) + \log r(\dots)})$



$P \subseteq NP \cap co\text{-}NP$

$\stackrel{?}{=}$



1973 Stephen Cook
Levin

Cook-Levin: $\forall\ Y \in NP \quad Y \leq SAT$

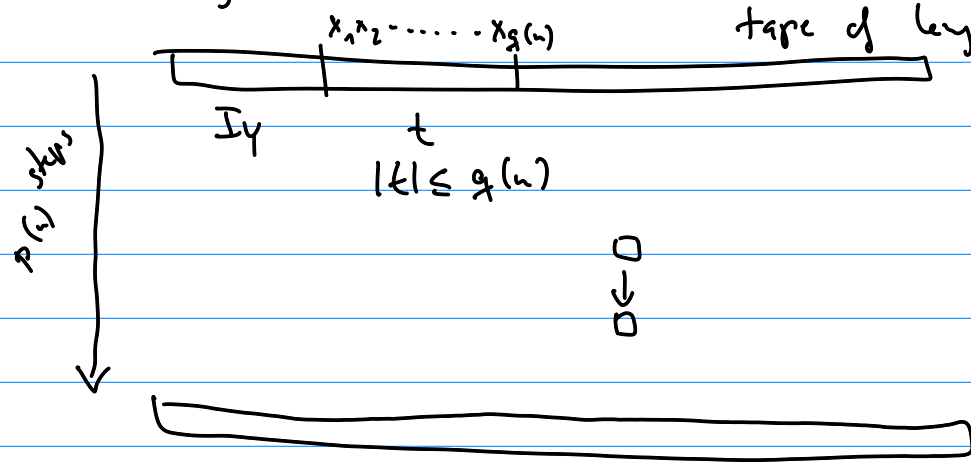
"Proof" $\quad C(I_Y, t)$ runs in poly-time

$I_Y \longrightarrow \varphi$ in CNF

$\exists t\ \underbrace{C(I_Y, t)}_{\text{Turing machine TM}} \qquad \varphi$ is satisfiable

$n = |I_Y|$

tape of length $p(n)$



Claim: Vertex Cover is NP-complete

① $VC \in NP$ certificate is the VC

② $\forall Y \in NP \quad Y \leq \text{VERTEX COVER}$

SAT is NPC $\Rightarrow \forall Y \in NP \quad Y \leq \text{SAT} \leq \text{VERTEX COVER}$

$\Rightarrow Y \leq \text{VERTEX COVER}$

$P \subseteq NP \qquad \underbrace{NP \subseteq P} \qquad \Rightarrow \qquad P = NP$