GPS 10 due Mon Nov 16
HW 10 due Tue Nov 17

Given undirected $G = (V, E)$ & integer $k \geq 0$:

- Independent Set (IS): Is there $S \subseteq V$, $|S| = k$ & no two $u, v \in S$ share an edge?
- Clique: Is there $S \subseteq V$, $|S| = k$, s.t. for all $u, v \in S$ $(u \neq v)$ there is $uv \in E$?
- Vertex Cover (VC): Is there $S \subseteq V$, $|S| = k$, s.t. for all $uv \in E$, $u \in S$ or $v \in S$ (or both).

Last time: $IS \leq_p$ Clique

Theorem: $IS \leq_p VC$

Proof: Given input to IS $G = (V, E)$ & k.

Make input to VC $G' = (V', E')$ & k'.

$G' := G$

$k' := |V| - k$

Yes, poly time.

Suppose S is an <u>ind. set</u> in G with $|S| = k$.

For all $uv \in E$, $u \notin S$ or $v \notin S$.

Let $S' = V \setminus S$. S' is a vertex cover, &

$$|S'| = |V| - |S| = |V| - k = k'.$$

Suppose $S' \subseteq V'$ is a vertex cover of $G' = G$. &

$|S'| = |V| - k$.

For all $uv \in E$, $u \in S'$ or $v \in S'$.

So $u \notin (V \setminus S')$ or $v \notin (V \setminus S')$.

Let $S = V \setminus S'$ is independent &

$$|S| = |V| - |S'| = |V| - k' = k$$

Same proof shows $VC \leq_p IS$.

So $VC \leq_p Clique$ & $Clique \leq_p VC$.

Complexity classes:

P: Decision problems (or languages) with Polynomial time algorithms.

Ex: Given directed $G=(V,E)$ & $s,t \in V$, & $k \geq 0$, is $dist(s,t) \leq k$?

Not (?) an Ex: Independent Set.

NP: decision problems where a Yes instance has a poly size proof that can be verified in polynomial time.

$A \in P$ iff $\exists$ a function $Q_A : \{0,1\}^* \to \{False, True\}$

$\{False, True\}$

where $Q_A(x)$ takes $poly(|x|)$ time &
$Q_A(x)$ returns whether x is a Yes instance for A $(x \in L_A)$

$A \in NP$ iff $\exists\ R_A : \{0,1\}^* \times \{0,1\}^* \to \{False, True\}$

where $R_A(x, y)$ takes $poly(|x|, |y|)$ time &

($x \in L_A$ (x is a Yes) iff $\exists$ a certificate $y \in \{0,1\}^*$ s.t.

verifier

$|y| \leq poly(|x|)$ &

$R(x, y) = True$

Ex: Independent Set: Given $G=(V,E)$ & k s.t. there is an ind. set $S \subseteq V$ with $|S|=k$, the certificate is a description of S.

Ex: Vertex Cover: Given $G=(V,E)$ & k. If there is a vertex cover $S \subseteq V$ with $|S|=k$, certificate is S.

Ex: Shortest Path: Given $G=(V,E)$ & $s,t \in V$, & k, if $dist(s,t) \leq k$, certificate is ... ϵ.
Just run Dijkstra & ignore certificate.

So $P \subseteq NP$. $(R_A(x,y) = Q_A(x))$

Non-deterministic Polynomial time

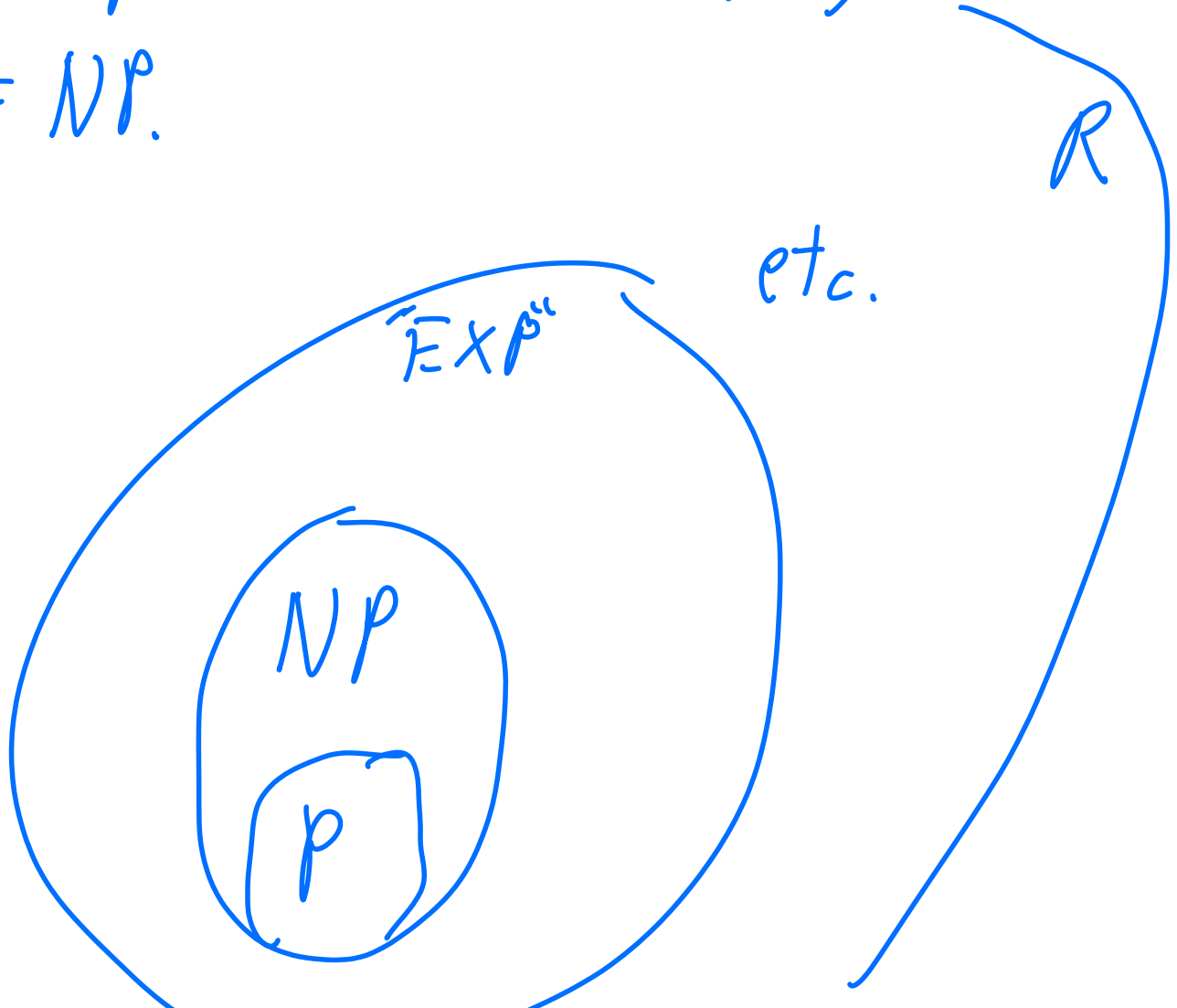
Problem B is NP-hard if for all problem $A \in NP$, $A \leq_p B$.

$\Rightarrow$ poly time alg for B leads to poly time algs for all $A \in NP$

Most people believe $P \neq NP$, so B probably has no poly time alg.

B is NP-complete if B is NP-hard &
$B \in NP$.

NP-complete problems have poly time algs iff $P = NP$.



Ex: (CNF) SAT:

A Boolean formula $\phi(x_1, x_2, \ldots, x_n)$

has variables x_i

literals x_i & $\overline{x}_i$.

ϕ is in conjunctive normal form (CNF)

if it is the conjunction (AND) of

several clauses & each clause

is the disjunction (OR) of

one or more literals.

$$\phi = (x_1 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_2 \vee x_4) \wedge$$
$$(x_2 \vee x_3 \vee \bar{x}_4) \wedge \cdot (\bar{x}_1 \vee \bar{x}_3 \vee \bar{x}_4)$$

SAT: Given CNF Boolean formula ϕ, can we set the variables to make ϕ True?

Yes! $x_1 = x_2 = x_3 = \text{True}$

$x_4 = \text{False}$

Thm: SAT $\in$ NP-complete

SAT $\in$ NP: How to set variables

To prove B is NP-hard, reduce

any NP-hard problem A to B.

(show $A \leq_p B$)

(all of NP) $\leq_p A \leq_p B$

Ex: 3SAT: SAT but with exactly 3 literals per clause.

Thm: 3SAT is NP-complete

Proof: Show $SAT \leq_p 3SAT$.

Given CNF formula ϕ, need to make a 3CNF formula ϕ'.

Repeatedly take a long (≥ 4 literal) clause of ϕ, replace with two shorter clauses with a brand new variable.

$$(x_1 \vee x_2 \vee x_3 \vee x_4 \vee x_5)$$

$$\Rightarrow (x_1 \vee x_2 \vee z_1) \wedge (x_3 \vee x_4 \vee x_5 \vee \overline{z_1})$$

After, add some extras to clauses that are too short:

$$(x_1 \vee x_2) \Longrightarrow (x_1 \vee x_2 \vee z) \wedge (x_1 \vee x_2 \vee \overline{z})$$