Lecture 6

$$P = \bigcup_{c \in \mathbb{N}} \mathrm{DTIME}(n^c)$$

polynomial

A language $A \leq_p B$

poly-time reducible

if $\exists$ poly-time computable f s.t.

$\forall x \in \{0,1\}^*$

$$x \in A \longleftrightarrow \underline{f(x)} \in B$$

- Give me ANY x

↳ I can transform it into

<u>some</u> $f(x)$

s.t.

if $x \in A$, then $f(x) \in B$

and if $f(x) \in B$ then $x \in A$

$3SAT \leq_p INDSET_k$

- Give me <u>any</u> ~~string~~ Boolean Formula x

↳ I can turn it into <u>some</u> graph G

Check this

* $INDSET_k \leq_p 3SAT$

↳ Give me any graph G

↳ I can construct a particular 3CNF ϕ_G s.t.

$G \in IND_k \longleftrightarrow \phi_G \in 3SAT$

$G = (V, E)$

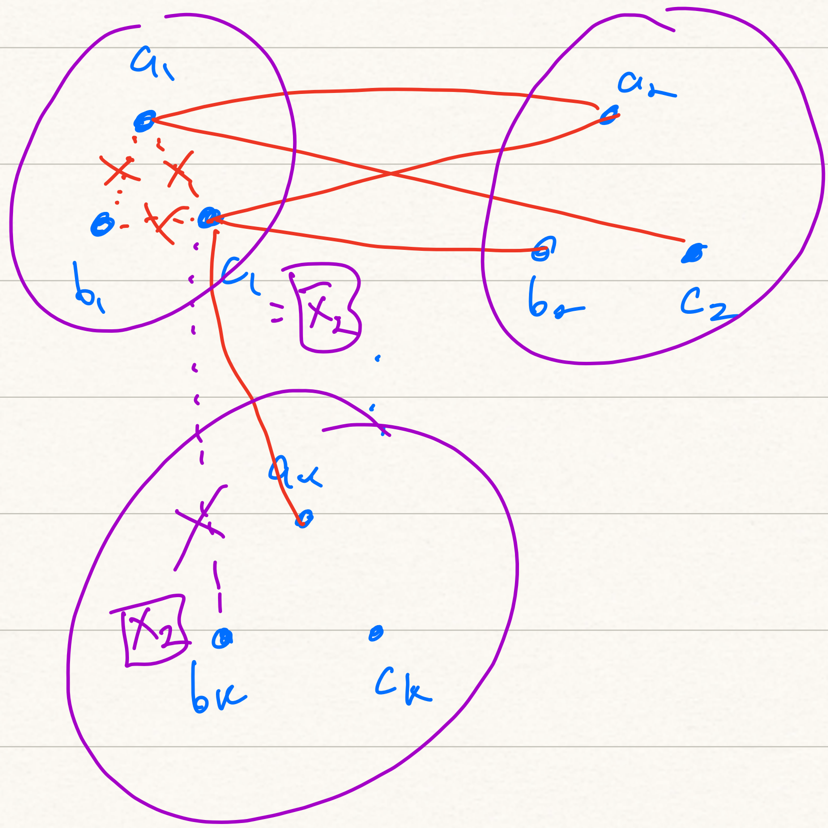
$|V| = n$

K-clique is NP-complete

- $G = (V, E)$
- A k-clique of G is $S \subseteq V$ s.t. $|S| = k$ and $\forall\, u, v \in S,\ (u, v) \in E$

- $3SAT \le_p k\text{-clique}$

$$\phi = (a_1 \vee b_1 \vee c_1) \wedge \cdots \wedge (a_k \vee b_k \vee c_k)$$

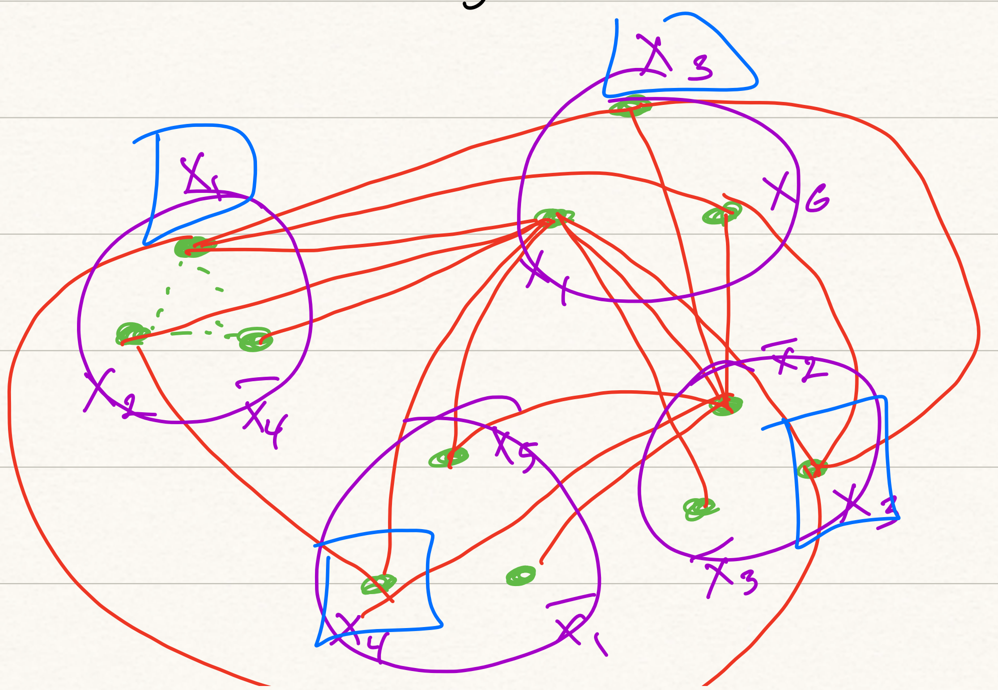


$$\phi \xrightarrow{f} G_\phi$$

- ϕ is 3SAT iff G_ϕ has k-clique

- ϕ is SAT $\longrightarrow$
  at least one literal per clause
  ϕ_i is $= 1$ (satisfied)

- Look at the triples of vertices in G_ϕ
  - Pick any one satisfied literal from ϕ's SAT assignment



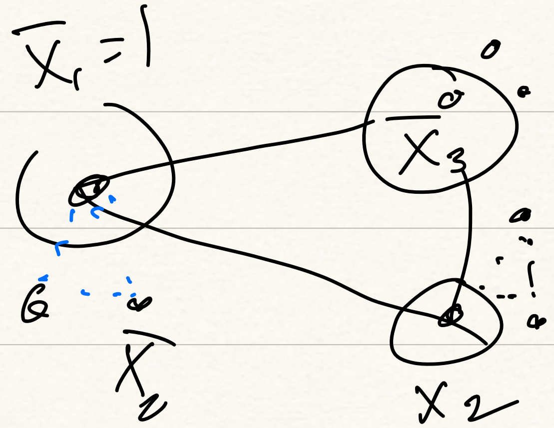
- This must be a k-clique
  - If you pick x_i, you won't pick $\overline{x_i}$
    - no edge here anyways

  - Things in clauses are not connected
  - Every x_i must be connected to the others you picked in the k-1 other clauses

k-clique $\Rightarrow \phi$ is SAT

- Have a k-clique
- __Know__:
  - clusters aren't self connected
  - x_i and $\overline{x_i}$ are not connected

$\Rightarrow$ the k-clique has exactly one node per triple



Search vs. Decision

- If $P \neq NP$, we can't efficiently search in NP.

- If $P = NP \rightarrow$ you can solve efficiently.

Thm: Suppose $P = NP$. Then $\forall\, L \in NP$ w/ verifier M_L, $\exists$ a poly-time

$\hat{M}_L$ s.t. $\forall x \in L$

$\hat{M}_L(x) = w$ s.t.

$M_L(x, w) = 1$

- we show for SAT
  - Let A be an algorith which decides $\phi \in$ SAT
    - A runs in poly-time because P = NP

- Build new algorithm B as follows

will find sat. assignment for ϕ.

$B(\phi)$ has n literals $x_1, \ldots, x_n$

1. Run $A(\phi) \to b$
2. If $b = 0$
   ↳ reject
3. Else find the assignment

3.1 Write

$$\phi|_{x_1=0} \quad \phi|_{x_1=1}$$

$$(x_1 \vee x_2)$$
$$\downarrow$$
$$(0 \vee x_2) \to x_2$$

3.2 Test $A(\phi|_{x_1=0})$

$A(\phi|_{x_1=1})$ ✗

|

↳ at least one must be satisfying

(3.3) Pick one of them

$\phi' = \phi|_{x_1=0}$ assigned

(3.4) Try $\phi'_{x_2=0}$ $\phi'_{x_2=1}$

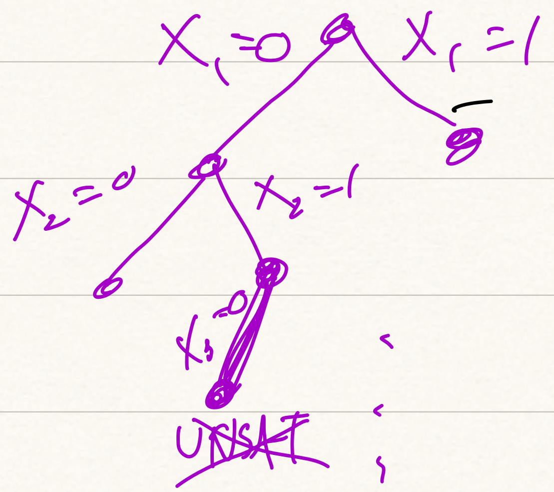
⋮

Output the assignment of

$x_1, \dots, x_n$

$|\phi|$ poly in this

$\# \vee + \# \wedge$



X =0

$\wedge 1$

$x_2 = 1$

$x_3 = 0$

coNP

- $coNP = \{ L \mid \overline{L} \in NP \}$

$L \subseteq \{0,1\}^*$

$\overline{L} = \{0,1\}^* \setminus L$

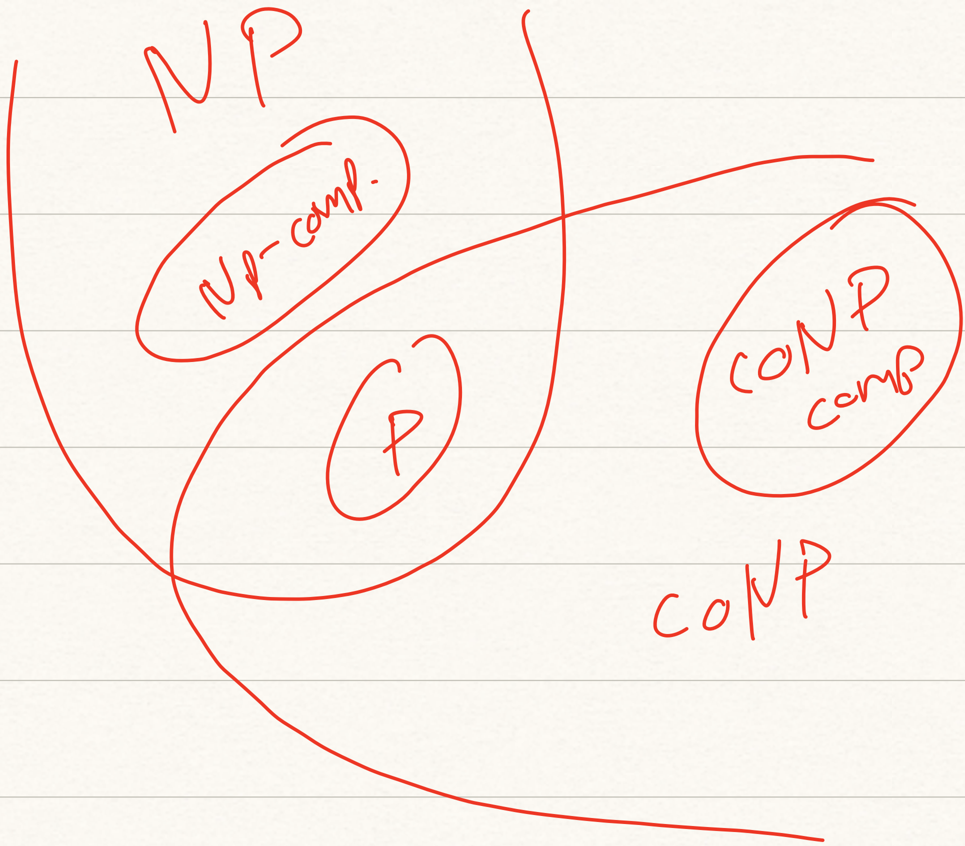
everything in $\{0,1\}^*$ but not in L.

⚠ $coNP \neq \overline{NP}$

$coNP \cap NP \neq \emptyset$

$P \subset coNP \cap NP$

if $L \in P$
then $\bar{L} \in P$



$\overline{SAT} = \{ \phi : \phi$ does not have a SAT assignment $\}$

$\overline{SAT} \in coNP$

- A language $L \in coNP$ if $\exists$ polynomial p and poly-time TM M_L such that

NP $\exists w$

$x \in L \longleftrightarrow \underline{\forall w \in \{0,1\}^{p(|x|)}}$ $M_L(x,w) = 1$

$x \notin L \longleftrightarrow \forall w \in \{0,1\}^{p(|x|)}$ $M_L(x,w) = 1$

(neg. both

ψ sides

$x \cancel{\in} L \longleftrightarrow \exists w \in$ s.t.

$M_L(x, w) = 0$

$x \in \bar{L} \longleftrightarrow \exists w \in$ ..

$M_L(x, w) = 0$

$x \in \bar{L} \longleftrightarrow \exists w \in$ ..

$M_{\bar{L}}(x, w) = 1$

$\neg(\forall x) = \exists \neg x$

$\neg(\exists x) = \forall \neg x$

- If $P = NP$ then $NP = coNP$.

if $L \in P$ then $\bar{L} \in P$

$$\mathrm{NP} \overset{?}{=} \mathrm{coNP}$$

- coNP $\neq$ NP then $P \neq NP$

coNP completeness

- L is coNP-complete if
  - $L \in$ coNP and
  - $\forall L' \in$ coNP
    $L' \leq_p L$

- coNP: Tautology

TAUT: $\{ \phi$ is a tautology$\}$

↳ true for every assignment

- TAUT $\in$ coNP
- $L \leq_p$ TAUT for any $L \in$ coNP.
- Consider $\overline{L} \in NP$

↳ $\overline{L} \leq_p SAT$

- Let ϕ_x be the SAT such that

$$x \in \overline{L} \longleftrightarrow \phi_x \in SAT$$

$$\rightarrow x \notin \overline{L} \longleftrightarrow \phi_x \notin SAT$$

$$x \in L \longleftrightarrow \phi_x \notin SAT$$

$$x \in L \longleftrightarrow \neg\phi_x \in TAUT \ \square$$

Recall

$$\text{EXP} = \bigcup_{c \in \mathbb{N}} \text{DTIME}(2^{n^c})$$

EXPTIME

$$\text{NEXP} = \bigcup_{c \in \mathbb{N}} \text{NTIME}(2^{n^c})$$

$$P \subseteq NP \subseteq \text{EXP} \subseteq \text{NEXP}$$

Thm: If $P = NP$ then

$$\text{EXP} = \text{NEXP}$$

↳ $\text{NEXP} \neq \text{EXP} \Rightarrow$

$$P \neq NP$$