Hamiltonian cycle in $G=(V,E)$ is a cycle which covers all vertices in G, that is a permutation π of V

$v_{\pi_1} v_{\pi_2} \cdots v_{\pi_n}$ $n=|V|$ s.t.

(*) $v_{\pi_i} - v_{\pi_{i+1}}$ is an edge for $i=1,2,\ldots,n$ where $\pi_{n+1}=\pi_1$

To show that G has a hamiltonian cycle, we just need to give a permutation certifying this.

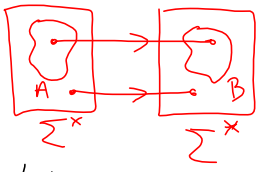
Conversely, if G does not have a ham. cycle then no permutation π which satisfies (*)

Def A Polynomial reduction for A to B

(A, B languages over alphabet Σ

is a function $f: \Sigma^* \to \Sigma^*$ s.t

1. $x \in A \iff f(x) \in B$



2. f can be calculated in pol time
so $\exists k \in \mathbb{Z}_+$ s.t $f(x)$ is computed in time $O(|x|^k)$

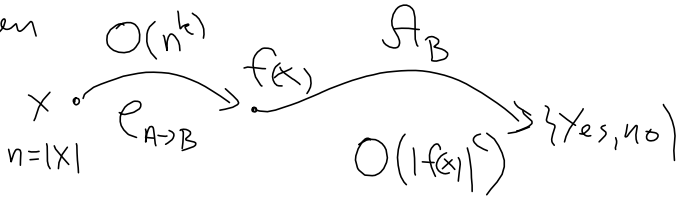
If such an f exist then we writ $A \leq_p B$

Lemma 1 If $A \leq_p B$ and $B \in P$ then $A \in P$

P: suppose A_B solves B in time $O(n^c)$

and that $C_{A\to B}$ computes f s.t $x \in B \iff f(x) \in B$ in time $O(n^k)$

then



time to produce answer {yes, no}

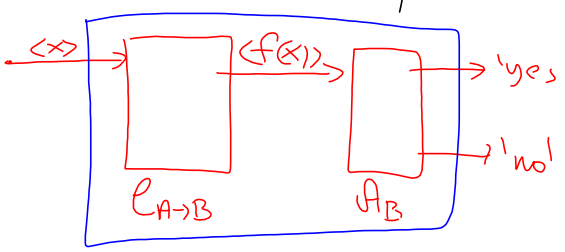
is $O((n^k)^c) = O(n^{kc})$

and A_B accepts (says 'yes') $f(x)$

$\Downarrow$

$x \in A$

so we have $A \in P$

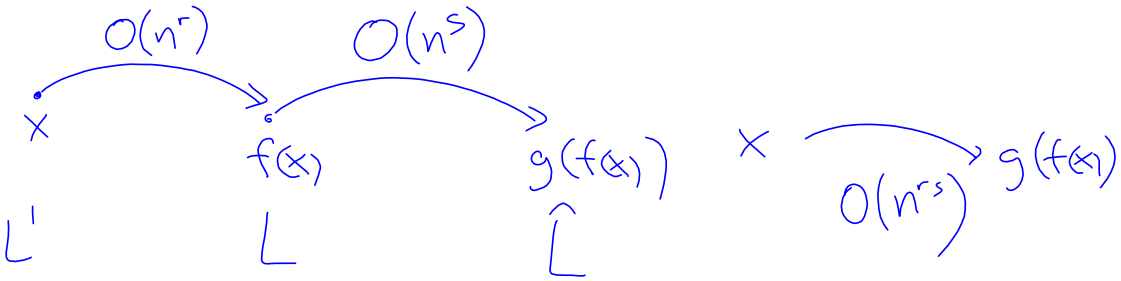


Def 7.34 L is called NP-complete (written $L \in NPC$) if

1. $L \in NP$
2. $\forall L' \in NP : L' \leq_p L$

On April 18 we will see that there are such problems.

Theorem If L is NPC ($L \in NPC$) and $L \leq_p \hat{L}$, $\hat{L} \in NP$ then $\hat{L} \in NPC$



SATISFIABILITY (SAT)

Given $x_1, x_2, \ldots, x_n$ Boolean variables

and $C_1, C_2 \ldots C_m$ clauses over

$x_1 \ldots x_n, \bar{x}_1, \ldots, \bar{x}_n$ ($\bar{x}_i = \begin{cases} \text{True if } x_i = \text{false} \\ \text{false} -\!\!\!-\!\!\!- \text{true} \end{cases}$)

e.g. $C_i = (x_{i_1} \vee \bar{x}_{i_2} \vee x_{i_3} \vee \bar{x}_{i_4})$ ← literals

Question Given $f = C_1 \wedge C_2 \wedge \ldots \wedge C_m$

does then exist $\varphi : \{x_1, x_2, \ldots, x_n\} \to \{T, F\}^n$

s.t f is true

SAT $\in$ NP

Certificate is just a φ above s.t all clauses are satisfied (evaluate to true)

Thm Cook-Levin (April 18)

SAT $\in$ NPC

3-SAT : SAT restricted to
each clause has exactly 3 literals

Thm 3-SAT is NPC

P: 3-SAT $\in$ NP clear (show good φ)

show SAT $\leq_p$ 3-SAT

Let $f = C_1 \wedge C_2 \wedge \cdots \wedge C_m$ be SAT formula
over variables $x_1, x_2, \ldots x_n$.
make 3-SAT instance f' s.t f 'yes' instance of SAT
$\Leftrightarrow$ f' ------- 3-SAT

Method modify clauses whose length is $\neq 3$

$C = (\lambda_1 \vee \lambda_2 \vee \cdots \vee \lambda_k)$, $k \geq 4$ λ_i literal

$\downarrow$

$(\lambda_1 \vee \lambda_2 \vee y_1) \wedge (\bar{y}_1 \vee \lambda_3 \vee y_2) \wedge (\bar{y}_2 \vee \lambda_4 \vee y_3) \wedge \cdots \wedge (\bar{y}_{k-4} \vee \lambda_{k-2} \vee y_{k-3}) \wedge (\bar{y}_{k-3} \vee \lambda_{k-1} \vee \lambda_k)$

$y_1 \cdots y_{k-3}$ new variables private to C

$C = (\lambda_1 \vee \lambda_2) \rightarrow (\lambda_1 \vee \lambda_2 \vee z) \wedge (\lambda_1 \vee \lambda_2 \vee \bar{z})$

$C = (\lambda_1) \rightarrow (\lambda_1 \vee w \vee y) \wedge (\lambda_1 \vee w \vee \bar{y}) \wedge (\lambda_1 \vee \bar{w} \vee y) \wedge (\lambda_1 \vee \bar{w} \vee \bar{y})$

each C is satisfied by truth assignment to $x_1, x_2 \cdots x_n$
if and only if new formula f' is satisfied
by the same assignment to $x_1 \cdots x_n$ and arbitrary to new var's

Conversely if φ' satisfies f' then $\varphi'_{|x_1 \cdots x_n}$ satisfies f

Clique: Given $G=(V,E)$ and $k \in \mathbb{Z}_+$

Does G have a complete subgraph on k vertices?

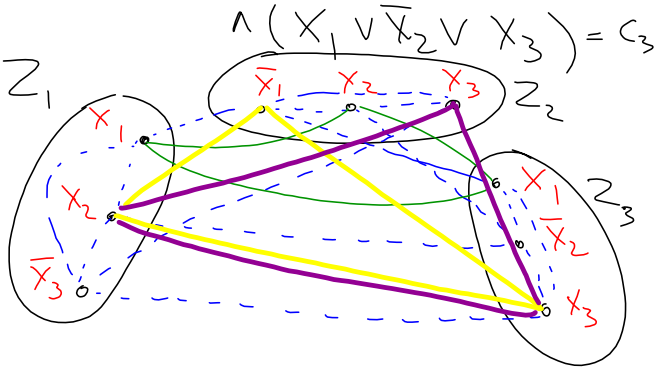
Clique $\in$ NP

Thm 3-SAT $\leq_p$ Clique

P: 'by example' to show idea

Given $f = (x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \bar{x}_2 \vee x_3)$

(C_1, C_2, C_3)



yellow, green and purple are different φ's.

#clauses

$k = m \ (=3)$

---- = no edge

all other edges present

Claim G has a k-clique $\Leftrightarrow$ f is satisfiable

$\Rightarrow$ Let H be a k-clique in G.

then $|H \cap Z_i| = 1 \quad \forall i \in \{1,2,\dots,m\}$

and if a vertex labelled x_i is in H then H has no vertex labelled $\bar{x}_i$.

put x_i = true if H has a copy of x_i

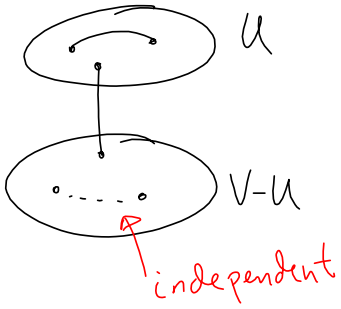
x_i = false if no copy of x_i in H

$\Leftarrow$ Suppose $\varphi : \{x_1, x_2, \dots, x_n\} \to \{T, F\}^n$

pick, for each C_j one literal such that this is true under φ and put corresponding vertex in H. Then these vertices form a clique in H.

Vertex cover (VC)

Given $G=(V,E)$ and $p \in \mathbb{Z}_+$
Does then exist $U \subseteq V$ s.t $|U|=p$
and every edge touches U?



VC ∈ NP ✓

new problem

INDEPENDENT SET (IndS)
Given $G=(V,E)$ and $q \in \mathbb{Z}_+$
does $\exists W \subseteq V$ s.t $|W|=q$
and no edge inside W?

IndS ∈ NP ✓

U is a vertex cover
$\Leftrightarrow$ $V-U$ independent

Theorem Independent set is NPC

Clique $\leq$ Independent set

U is a clique in G
$\Leftrightarrow$
U is an independent **set** in $\bar{G}$

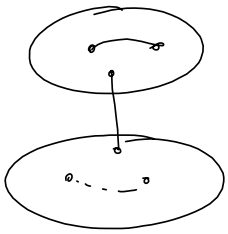
so $G,k \longrightarrow \bar{G},k$
is yes for Clique $\Leftrightarrow$ $\bar{G},k$ yes for ind set

Given $G=(V,E)$
complement $\bar{G}$ is
$\bar{G}=(V,E')$
$uv \in E' \Leftrightarrow uv \notin E$

clique Ind set VC

$(G, k) \longrightarrow (\bar{G}, k) \longrightarrow (\bar{G}, n-k)$

$|V(G)| = n$



G has a clique of size k

$\Updownarrow$

$\bar{G}$ has an independent set of size k

$\Updownarrow$

$\bar{G}$ has a vertex cover of size $n-k$