Věta (Cook-Levin): SAT je NP-úplný
NP-těžký

SAT ≡ formule φ v CNF-tvaru
(konjunktivní normální forma)

$x_1, \dots, x_n \in \{0,1\}$ proměnné

$$\varphi := \bigwedge_{i=1}^{m} C_i$$

$C_i \equiv$ klauzule, $\bigvee_{j=1}^{n_i} l_j$

$l_j \in \{x_k, \neg x_k\}$

$\exists$ přiřazení 0/1 proměnným x_i t.ž. $\varphi(x_1 \dots x_n) = \text{TRUE}$

3-SAT, neboli SAT kde $k_i \geq 3$ $\forall i \in [m]$, je také těžký jako SAT
(neboli, z COOK-LEVIN je 3SAT NP-úplný)

Poznámka: 2-SAT je P (lze řešit párováním v grafech)

Věta: Velikost nezávislé množiny je NP-úplná Indset
INPUT: G, a číslo $x \rightsquigarrow \exists I \subseteq V(G)$ nezávislá, $|I| = x$

nezávislá množina ≡ $G[I]$ nemá hran

všechny dvojice z I, $\left|\binom{I}{2}\right| = \binom{|I|}{2}$ $\equiv E(G) \cap \binom{I}{2} = \emptyset$

Dk: 1) Indset $\in$ NP
VSTUP $= (G, x)$

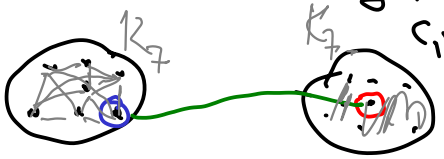
hint ≡ seznam x vrcholů
$x \cdot \log n = \text{poly}(\text{VSTUP})$

$O(k \log n)$ { for $i = 1$ to x, for $j = 1$ to $i-1$:
vrchol hint[i] ~ vrchol hint[j] : RETURN FALSE
RETURN TRUE

2) Indset je NP-těžký, ukážeme $3SAT \leq_p$ Indset

φ je 3-SAT formule s m klauzulemi

G_φ s $7m$ vrcholy, $\forall C_i = l_1^i \vee l_2^i \vee l_3^i$ { 7 splňujících částečné přiřazení proměnným
1. nesplňující



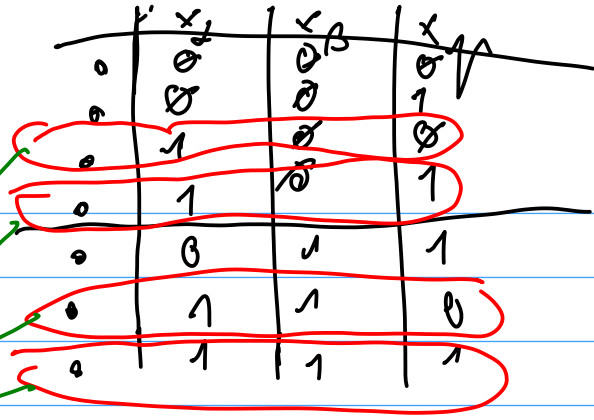
$\forall C_{i_1}, C_{i_2}$ klauzule

pokud • přiřazení proměnným je nekompatibilní s • přiřazením

$c_{i_1} = x_\alpha \vee \neg x_\beta \vee x_\gamma$

$c_{i_2} = x_\gamma \vee x_\varepsilon \vee \neg x_\alpha$

	x_γ	x_ε	x_α
•	0	0	0



Ψ splnitelná $\iff$ G_Ψ má nezávislou množinu velikosti m

Ψ splnitelná: $\exists x_1 \dots x_n : \forall c_i$ je splnitelná $\rightsquigarrow$ $c_i = l_1^{(i)} \vee l_2^{(i)} \vee l_3^{(i)}$

pro $l_{1,2,3}^{(i)} = \pm x_{1,2,3}^{(i)}$

$\left(x_1^{(i)}, x_2^{(i)}, x_3^{(i)}\right) \rightsquigarrow$ • vrchol v G_Ψ $v_i(x)$

$\{v_i(x) \; i \in [m]\}$ je nezávislá množina

---

mějme m-vrcholovou nezávislou I v G_Ψ

$\forall i \in [m]$ ≤ 1 vrchol z c_i v I, ale m vrcholů v I

$\Rightarrow$ právě jeden vrchol z c_i v I

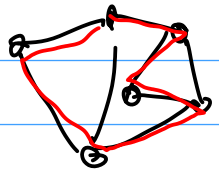
přiřaďme x_j podle $x_j^{(i)}$ pro c_i obsahující x_j pokud existuje; pokud ne, nastav x_j libovolně

1) přiřazení je dobře definované
2) každá klauzule je splněná $\rightsquigarrow$ Ψ je splněná

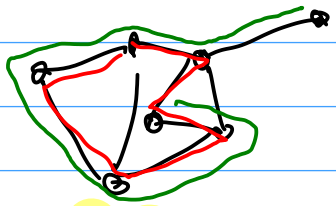
∎

Věta: Hamiltonovská kružnice HC
cesta HP

$G=(V,E)$ HC ≡ cyklus v G obsahující všechny $v \in V$

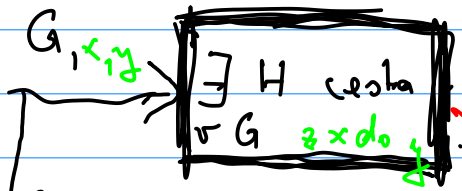


HP ≡ cesta v G obsahující všechny v

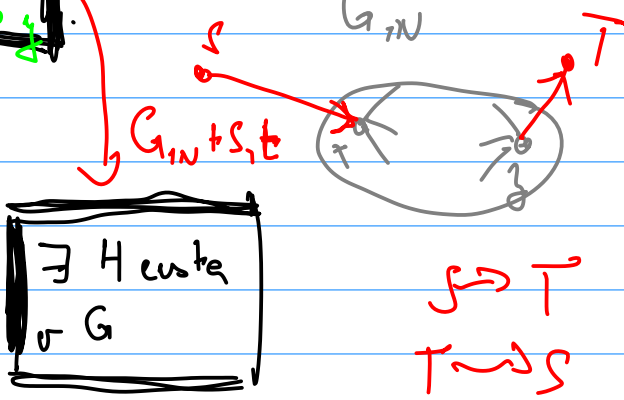


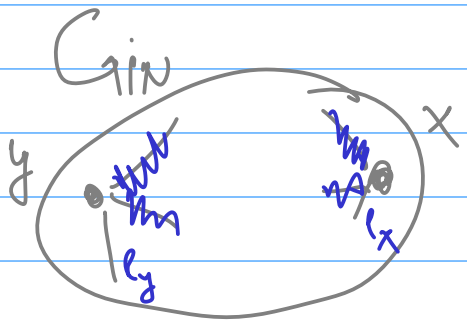
a) H kružnice $\leq_p$ H cesta
b) H cesta $\leq_p$ H kružnice

G_{IN} ∃ H kružn.o?



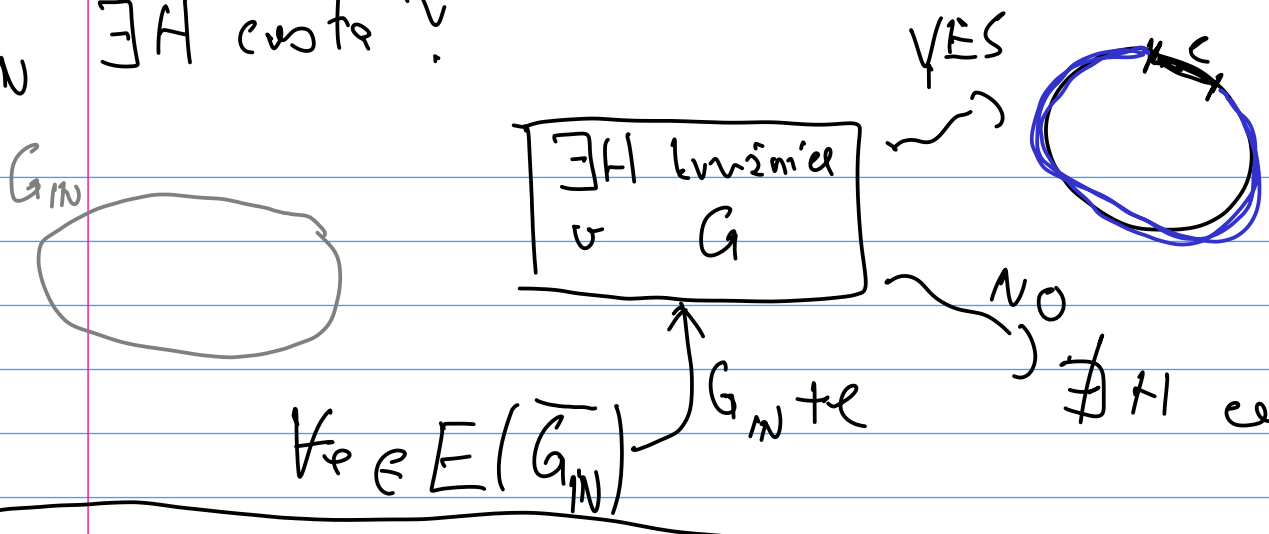
$\forall (x,y) \in E(G_{in})$

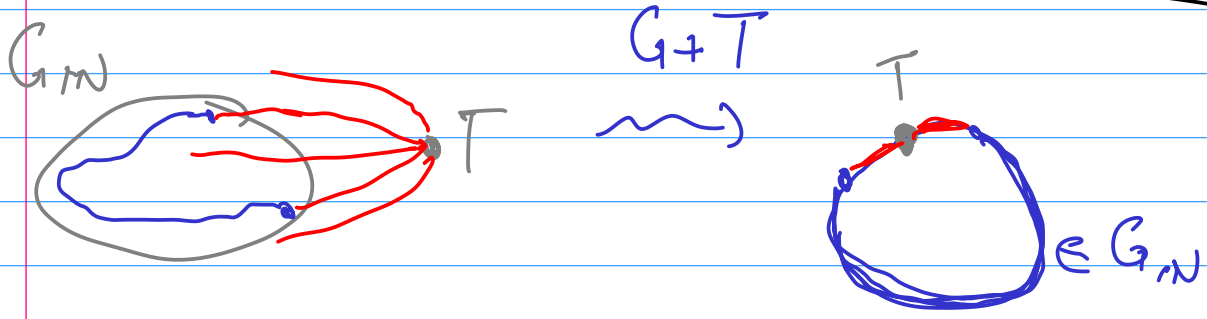




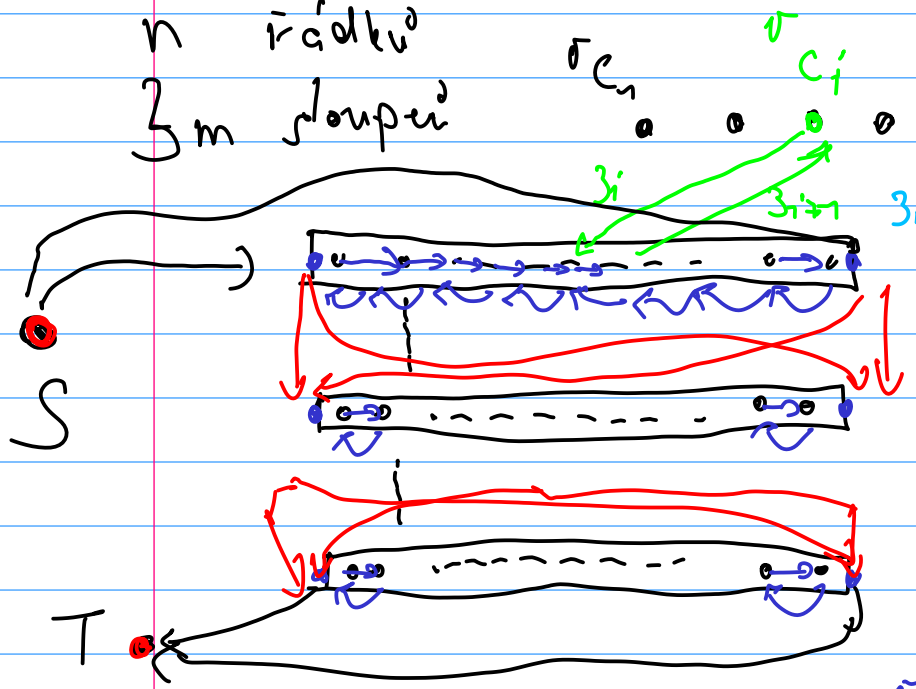
$\forall l_x$ $\forall l_y$ hrana incidentní s x s y

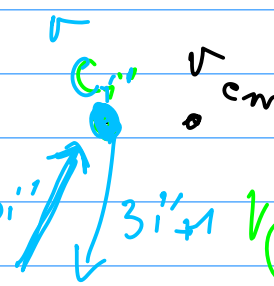
G_N $\exists H$ cesta ?





SAT $\leq_p$ Gar. H cesta $\varphi = \bigwedge C_i$ s proměnnými $\{x_1, \ldots, x_n\}$





$V(C_i \to 3_{i,j}$
$3_{i+1,j} \to C_i)$

pokud x_j má negativní pozitivní výskyt v C_i

$x_j \equiv$ TRUE

řádek j zleva → doprava

$x_j \equiv$ FALSE

zprava ← doleva

Def: oblivious Turingův stroj OTS $m+1$

TS $\quad Q \times \underbrace{\Sigma}^{m+1} \longrightarrow Q \times \Sigma^{m} \times \{L,R,S\}$

výpočet $TS(x)$ podívejme se na těch $m+1$ pásků L/R/S dělky #kroků TS na x

move	$\sigma(x)$	R S
move	$\tau(x)$	S R
	⋮	
move	$m(x)$	S S

TS je oblivious pokud $\forall i \in \{0,1,\dots m\}$ move$_i$ závisí jen na $|x|$

Claim / DCV: $\forall$ TS $\exists$ existuje OTS o t.ž. $TS(x) = OTS(x)$ a pokud $TS \in DTIME(f)$ tak $OTS \in DTIME(f^2)$

$\forall$ Boolean function $f: \{0,1\}^l \to \{0,1\}$ $\exists$ Ψ SAT formule s l proměnnými a 2^l klauzelmi velikosti l

t.ž. $f(x_1 \dots x_n) = \Psi(x_1 \dots x_l)$

DL: fix f. $\forall v \in \{0,1\}^l \rightsquigarrow C_v$ t.ž.

$C_v(v)$ FALSE

$C_v(u)$ TRUE $\forall u \neq v$

$$C_v = x_1 \vee x_2 \vee \dots \vee \neg x_j \vee \dots x_l \qquad v_j = 1$$

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

Dk (Cook-Levin): $L \in NP$, i.e., $\exists T$ Turing stroj

$\forall x \in \{0,1\}^*$ $\quad x \in L \iff T(x,h)=1$ pro nějaký $h \in \{0,1\}^{p(|x|)}$

$\forall$ čase $p(|x|)$ $\quad$ polynom p

$\forall$ poly čase umíme pro $x \in \{0,1\}^*$ najít Ψ_x

t.ž. Ψ_x je TRUE $\iff x \in L$

IDEA NAIVNÍ: $f_x(h): \{0,1\}^{p(x)} \to T(x,h)$

$\rightsquigarrow \Psi_{f_x}$ MOC VELKÁ

BÚNO, T má 1 pracovní pásku a je oblivious

speciálně znamená, že $\forall h$: move$_0$$((x,h))$ move$_1$$((x,h))$

$=$ move$_0$$((x,0^{p(|x|)}))$ move$_1$$((x,0^{p(|x|)}))$

$y := (x,h)$

když známe pohyb hlavy, $Q \times \Sigma \times \Sigma \to Q \times \Sigma$

otisk v čase $t \equiv (q,a,b) \in Q \times \Sigma \times \Sigma$

$c := \lceil \log_2 |Q \times \Sigma \times \Sigma| \rceil$

posloupnost otisků $\underbrace{o_1, o_2 \ldots o_{T(|y|)}}$ odpovídají $T(y)$?

jak ověřit o_i, když už známe $o_{<i}$? SIMULACÍ POSLEDNÍHO KROKU

stačí ověřit z $(\underbrace{o_{i-1}}_{(2c+1)\text{-bitů}}, \underbrace{y_{\text{INPUTPOS}(i)}}, \underbrace{o_{\text{PREV}(i)}})$

INPUTPOS(i) ≡ pozici čtecí hlavy v i-tém kroku

PREV(i) ≡ číslo kroku $<i$, kdy naposledy byla prac. hlava na stejné buňce jako v i

pokud ex. $|y|$ jinak $\emptyset$

$(*)$ jednoznačně určuje i-tý krok TS

$$F: \{0,1\}^{2c+1} \to \{0,1\}^c$$

$F(*) = TRUE \Leftrightarrow$ validní krok

$\forall i: \quad O_i = F(O_{i-1}, y_{INPUTPOS(i)}, O_{PREV(i)})$?

$\Vert$ otisky $O_1 \dots O_{T(|y|)}$ odpovídají běhu $TT(y)$

⊗ proměnné formule $\equiv$ bity y, binární kod otisků $O_1 - O_{T(|y|)}$

$n + p(|x|)$ $\qquad$ $c \cdot T(|y|)$

poly mnoho proměnných v $|x|$

1) $y_1 \dots y_{|x|} = x$ $\qquad$ $2|x|$ klauzulí, $(x_i \vee \overline{y_i})(\overline{x_i} \vee y_i)$

2) $O_1 = (\vdash, START, x_1, \dots, \square)$ $\qquad$ c.t. podformule

3) $O_{T(|y|)} = (q_{HALT}, y_{INPUTPOS(T(|y|))}, \dots, \square)$ $\qquad$ c.t. podformule

4) $\forall i: \quad O_{i+1} = (O_i, y_{INPUTPOS(i+1)}, O_{PREV(i+1)})$

$T(|y|) \times (c^2+1)$-bit podformulí

Redukce $(x) \xrightarrow{Poly(|x|)} \psi_x$ $\begin{cases} TRUE & x \in L \\ FALSE & x \notin L \end{cases}$

$\Vert$ OTS

$L \le_P SAT$ $\qquad$ QED