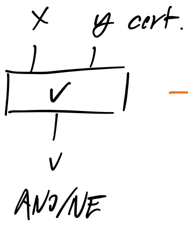
$P \subseteq NP$ Verifikátor: —> chceme ho polynomiální

- musí být polyn.



—> to jsou vlastně mat. důkazy

—> omezení délky cert.

Df: $L \in NP \equiv \exists V \in P$ verifikátor t.ž. $\exists g$ polynom $\forall x \in \{0,1\}^*$ vstup

$$L(x) = 1 \iff \exists y \in \{0,1\}^*$$ certifikát —> může být např. model teorie SATu

$$|y| \leq g(|x|)$$ verifikace

$$V(x,y) = 1$$ verifikace

$P \subseteq NP$

L je převoditelný na U

Df: NP-těžkost: Problém U je NP-těžký $\equiv \forall L \in NP : L \to U$

Df: NP-úplný $\equiv$ navíc $U \in NP$

Lemma: Pokud $U \in P$ a U je NP-úplný $\Rightarrow P = NP$.

Dk: Nechť $L \in NP$. Pak $L \to U$. Pak ale: $L \in P$, jelikož převod $L \to U$ je polyn. a U taky, tudíž je to celé polynomiální.

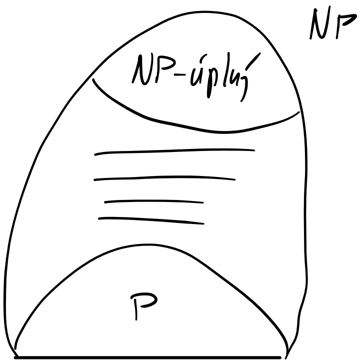
Věta: Cookova: SAT je NP-úplný.

Lemma: Nechť $U, L \in NP$. $U \to L$ a U je NP-úplný $\to$ L je NP-úplný.

Dk: Nechť $X \in NP$. Pak $X \to U \to L$. Tedy $X \to L$.
Tedy: L je NP-úplný.

NP-úplné problémy

logické	grafové	číselné
SAT	Klika	Součet podmnožin
3-SAT	NzMnn	Dva loupežníci
3,3-SAT	3D-párování	Batoh
obvodový SAT	barvení	$Ax=b$, $x \in \{0,1\}^m$
	Hamilton path/cycle	
	Steinerův strom	



Lemma: Pro $\forall L \in P$, $\exists A$ algoritmus a $\exists f$ polynom:

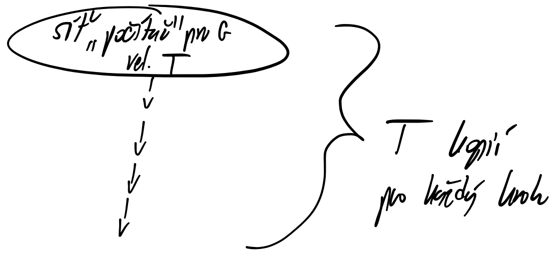
$\forall n \in \mathbb{N}$ $A(n)$ doběhne do $f(n)$ kroků a spočítá hradlovou síť B_n

s n vstupy a 1 výstupem

t.ž. $\forall x \in \{0,1\}^n$: $B_n(x) = L(x)$.

„Dk:" Nechť G je alg. řešící L v čase $\leq p(x)$. polynom

Mějme délku vstupu n, $T := p(n)$

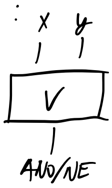


- tedy polynomiální problém lze vypočítat pomocí polynomiální hradlové sítě.

Věta: Obvodový SAT je NP-úplný (Skoro Cookova věta) Chceme $L \to$ O-SAT

Dk: Nechť $L \in NP$, V jeho verifikátor, g polynom omezující délku důkazu.

Pro vstup x délky n: $|x| = n$, $|y| = g(n)$



Podle lemmatu o obvodech vygeneruji obvod pro V na vstupech délky $n+g(n)$.

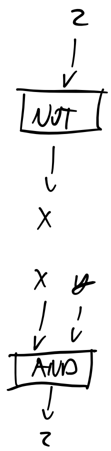
To V mi vrací už dělá vstup pro O-SAT

Věta: O-SAT $\to$ SAT

Dk: BÚNO: Obsahuje pouze NOT, AND (max. konstantně se mi to zvětší)

Pro výstup každého hradla zavedeme novou proměnnou.

To mi generuje formule SATu, čímž dostávám převeditelnost.



$x \Rightarrow \neg z$

$\neg x \Rightarrow z$

$(x \wedge y) \Rightarrow z \quad \to \neg x \vee \neg y \vee z$

$\neg x \Rightarrow \neg z$

$\neg y \Rightarrow \neg z$

Jak řešit NP-úplné problémy?

1) malý vstup, vylepšování programu
2) speciální vlastnosti (např.: bipartita atd)
3) omezení číselných vstupů
4) aproximační algoritmy
5) heuristiky