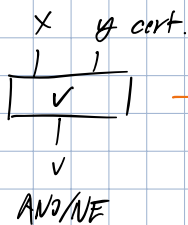


$P \subseteq NP$

Verifikátor:

- musí být polyn.



$\rightarrow$ to jsou všechny mož. důkazy

$\rightarrow$ omezení důkazy cert.

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

$L(x) = 1 \Leftrightarrow \exists y \in \{0,1\}^*$ certifikát $\rightarrow$ může být např.: model formule 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 $\equiv \forall L \in NP: L \rightarrow U$

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

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

Důk:

Nechť $L \in NP$. Pak $L \rightarrow U$. Pak ale: $L \in P$, jelikož

převod $L \rightarrow U$ je polyn. a U trvá, tudíž je to celé polynomiální.

Věta: Cookova: SAT je NP-úplný.

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

Důk: Nechť $X \in NP$. Pak $X \rightarrow U \rightarrow L$. Tedy $X \rightarrow L$.

Tedy: L je NP-úplný.

NP-úplné problémy

logické

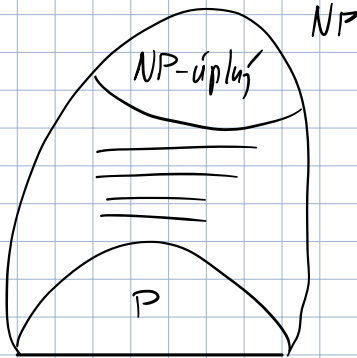
SAT
2-SAT
3,3-SAT
obvodový SAT

grafové

Ulihn
NěMun
3D-průsečí
barvení
Hamilton prst/cykle
Steinerův strom

číslové

Součet podmnožin
Dm lapěčnicki
Butoh
 $Ax=b, x \in \{0,1\}^m$



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

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

s n vstupy a 1 výstupem

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

"Ok:"

Nechť G je alg. řešící L v čase $\leq p(x)$.

Nějme délku vstupů n , $T := p(n)$

STP "přechází" pro G vel. T

- tedy polynomiální problém lze vyřešit pomocí polynomiální hodnoty sítě.

T logů pro každý krok

Věta: Obvodový SAT je NP-úplný (Shon Cookova věta)

Chceme $L \rightarrow O-SAT$

Ok: Nechť $L \in NP$, V jeho verifikátor, q polynom omezení délky důkazu.

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

V

|
ANO/NE

Podle lemma o obvodu vygeneruji obvod pro V na vstupu délky $n+q(n)$.

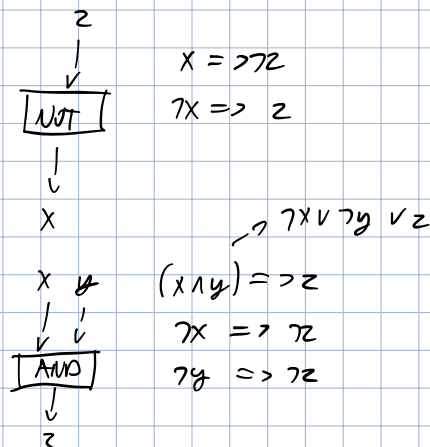
To V mi vrátí už délku vstup pro $O-SAT$

Věta: $0\text{-SAT} \rightarrow \text{SAT}$

Ok: BÚN: Obsahuje pouze NOT, AND (max. konstante se mi to zdá)

Pro výstup každého hradla zavedeme novou proměnnou.

To mi generuje formule SATu,
čímž dostáváme převoditelnost.



Jak řešit NP-úplné problémy?

- 1) malý vstup, vyčerpání programu
- 2) speciální vlastnosti (např.: bipartita otd)
- 3) omezení číselných vstupů
- 4) aproximční algoritmy
- 5) heuristiky