P vs NP

VSTUPNÍ ABECEDA $\{0,1\}$

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

TS T rozhoduje L pokud $T(x)$ vrátí 1 $\forall x \in L$ a vrátí 0 pokud $x \notin L$

$DTIME(n^c) = \{ L$ jazyk t.ž. $\exists T_L$ rozhodující L, a $T_L(x)$ vrátí hodnotu v čase $|x|^c \}$

$P = \bigcup_{c \geq 1} DTIME(n^c)$ "efektivní"

Př: Je G souvislý?
Je x dělitelné 3?

\# Komponent G → \# komponent ≤ 1 NE
≤ 2 ~~NE~~
≤ 3 ANO

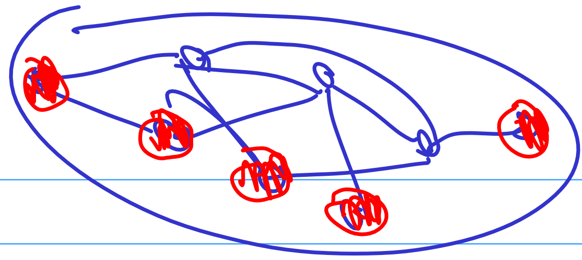
Ověřovací Turingův stroj pro jazyk L
(verifier)

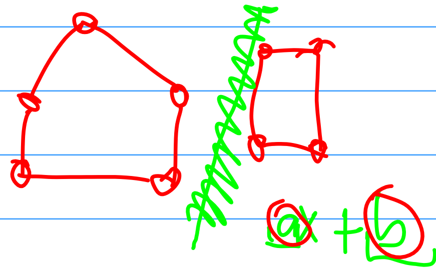
$a := \underbrace{87354473}_{= \underbrace{7879 * 11087}_{\text{CERTIFIKÁT}}}$

for $i := 2$ to $\lfloor \sqrt{n} \rfloor$
$a \bmod i = 0$?

$P \equiv$ efektivně rozhodnout $x \in L$

$NP \equiv$ efektivně ověřit $x \in L$





$TS(I,H) \rightsquigarrow 1$ / $\emptyset$

$$NTIME(n^c) = \{ L : \exists d>0\ \exists T_L,\ \exists p \text{ polynom}$$

1) $\forall x \in L\ \exists h \in \{0,1\}^*, |h| \leq d \cdot n^c$

2) $T_L(x,h)$ vrátí 1 v čase $d \cdot n^c$ $\forall x \in L$

3) $\forall x \notin L\ \forall h \in \{0,1\}^*$ $T_L(x,h)$ vrátí $\emptyset$ $\}$

$$NP = \bigcup_c NTIME(n^c)$$

$$DTIME(n^c) \subseteq NTIME(n^c)$$

---

nedeterministický rozhodovací TS

Σ abeceda

Q množina stavů $q_{YES}, q_{NO} \in Q$

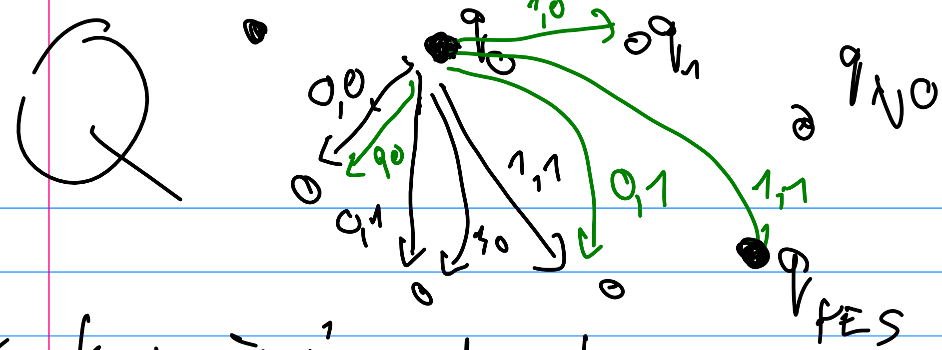
vstupní páska, k pracovních

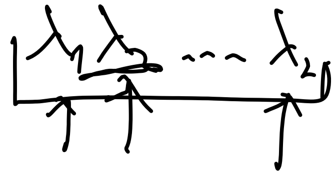
δ_0, δ_1 přechodové funkce

$$\underbrace{Q \times \Sigma^{1+k}} \rightarrow Q \times \Sigma^k \times \{L,R,S\}^{k+1}$$

a v každém kroku rozhodne, zda použít δ_0 nebo δ_1

ned. TS přijímá x v čase T pokud $\exists$ běh TS posloupnost T výběrů 0/1 tj. vstup = x, a TS udělá T kroků s δ_0/δ_1 dle výběru tak skončí v q_{YES}





det. konečný automat $\qquad \Sigma = \{0,1\}^2$

nedet. konečný automat

NTS $T \rightsquigarrow h := \{0,1\}^{T_x}$ a ověř. TS $T'(x,h)$

$x \in L$

NTS(x) za T_x kroků

MÁME: ověř TS T_0 $\forall x \in L \; \exists h_x \in \{0,1\}^* \; |h_x| \leq T_x$

a T ověří že $x \in L$ za T_x kroků, $T_x = O(|x|^c)$

CHCEME NTS T_N co v čase $O(|x|^c)$ rozhodne L

$x \in L$ vrátí YES v čase $O(|x|^c)$

1) v prvních $d \cdot n^c$ krocích vygenerovat (nedeterministicky) posloupnost $\{0/1\}^{d \cdot n^c}$

$\delta_0 : q_{INIT H} \to q_{GO}, 0, R$

$\delta_1 : \quad = q_{GO}\; 1, R$

2) $T_0(x, \text{WORK})$

$q_{GO} \quad \delta_0 : q_{INIT H}$

$\delta_1 : q_{T_0}$

$\exists$ běh T_R že

$\leq 3 \cdot T_x$ krocích přijme $x \in L$

Je-li L rozhodovaný NTS v čase $O(n^c)$ tak $\exists$ DTS rozhodující L v čase $O(2^{n^c})$

$\forall$ posloupnosti $q \in \{0,1\}^{n^c}$ odsimuluj NTS s výběrem δ_0/δ_1 dle q

Polynomiální redukce

L je polynomiálně redukovatelný na L'

$$L \leq_p L' \text{ pokud } \exists f : \{0,1\}^* \to \{0,1\}^*$$

co je spočitatelná v p-čase $f(x)$ spočte v $p(|x|)$

t.ž. $\forall x \in \{0,1\}^* \quad x \in L \iff f(x) \in L'$

Def.: L^* je NP-těžký / NP-hard pokud $\forall L \in NP \quad L \leq_p L^*$

$L_{TS} = \{x \in \text{Inputs} : TS(x) = 1\}$

Def.: NP-úplný / NP-complete L: $L \in NP$ & L je NP-těžký

$L \le_p L'$ & $L' \le_p L'' \Rightarrow L \le_p L''$

Kdyby $\exists L$: L je NP-těžký & $L \in P \Rightarrow P = NP$

-úplný & $L \in P \Leftrightarrow P = NP$

existuje NP-úplný jazyk L?

$\mathrm{TMSAT} = \{ (\alpha, x, 1^n, 1^t) ; \exists H_x^\alpha \in \{0,1\}^n$ t.ž. OTS $T_\alpha(x, H_x^\alpha) = 1$ za t kroků $\}$

1) $\boxed{\mathrm{TMSAT} \in NP}$ $\quad y = (\alpha, x, 1^n, 1^t)$

pokud $\exists$ OTS T_y t.ž. $\forall y \in \exists \tilde{H}_y \in \{0,1\}^{p(|y|)}$ a T_y rozhodne o $y \in \mathrm{TMSAT}$ v čase $O(p(|y|))$.

$T_y(y, H_y) = 1$ v čase $O(p(|y|))$

$H_y := H_x^\alpha$ délky $n = O(\mathrm{poly}(|y|))$

o) SIMULUJ $T_\alpha(x, H_y)$ v čase $O(t^2)$

2) TMSAT je NP-těžký

$\forall L \in NP \quad L \leq_p TMSAT$

mějme nějaké $L \in NP$

$\rightsquigarrow \exists$ OTS T_L v čase poly(|x|)

$\alpha :=$ index T_L

REDUKCI PRO L

x pro T_L tak $(\alpha, x, \underbrace{1 \dots 1}, \underbrace{1 \dots 1}^{p(x)})$

$f(x) = y$ v čase poly(x)

CHCEME $x \in L \iff y \in TMSAT$ $\square$

SAT (satisfiability)

$x_1 \dots x_n$ n proměnných 0/1 (FALSE/TRUE)

$c_1 \dots c_m$ m klauzulí v proměnných $\equiv (x_1 \vee x_3 \vee \neg x_7)$

||| disjunkce literálů, literál $\equiv x_i \,/\, \neg x_i$

$\bigwedge_{i=1}^{m} c_i$ je splnitelná

$\exists \{0,1\}^n$ tak že $\forall c_i$ je TRUE

VĚTA (COOK-LEVIN): SAT je NP-~~úplný~~ těžký

"⊙" $SAT \in NP$ ✓

$\ell_i < \begin{matrix} x_i \\ \neg x_i \end{matrix}$

redukce "De Morganny" nemí polynomiální

$$\bigwedge \left(\bigvee \ell_i\right) = \boxed{\bigvee \left(\bigwedge \ell_i'\right)}$$

$$\underbrace{(x_1 \wedge x_2 \wedge \neg x_3)}\vee (x_4 \wedge x_{30} \wedge \neg x_{38})$$

$$(x_1 \wedge \neg x_1 \wedge \ldots)$$

c je klauzule, $|c|$ počet literálů

3-SAT: $\bigwedge c_i$ $\quad$ c_i klauzule

$\forall i \in [m]: |c_i| = 3$

Lemma: $SAT \le_p 3\text{-}SAT$

DK: $\varphi \quad \varphi$ přidej c_i do φ

$c_i \in \varphi$ $\quad |c_i| = 3 \rightsquigarrow$

$|c_i| = 1 \rightsquigarrow$ nastav $\quad c_i = x_j \rightsquigarrow x_j := T$

$c_i = \neg x_j \rightsquigarrow x_j := F$

$|c_i| = 2$ přidej pomocnou proměnnou y_i

a klauzule $(c_i \vee y_i) =: c_i^{(1)}$

do ψ $(c_i \vee \neg y_i) =: c_i^{(2)}$

$m_i := |c_i| \geq 4$ $\underbrace{\ell_1 \vee \ell_2 \dots \vee \ell_{m_i}}$

$\leadsto$

3 $c_i^{(1)} := (\ell_1 \vee \ell_2 \vee \underbrace{y_i})$

$m_i - 1$ $c_i^{(2)} := (\ell_3 \vee \ell_4 \dots \vee \ell_m \vee \neg y_i)$

$\wedge$

3 $m-2$

$\wedge$

3 $m-3$

$\wedge$

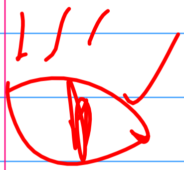
3 3

$c_i \to c_i^{(1)}, c_i^{(2)}, \dots, c_i^{(m_i-2)}$

$+$ $m-2$ pomocných proměnných

$\leadsto$ φ měla délku $\sum_{i=1}^{m} m_i$ $\quad$ ψ má délku $\leq 3 \cdot \sum m_i$

ψ má $x_1, \dots, x_n$ $+ \leq 3 \cdot \sum m_i$ proměnných velikost polí v $(\sum m_i)$

 $\exists$ splnitelné $x_1 \dots x_n$ pro φ

$\Updownarrow$

$\exists$ splnitelné $x_1, \dots, x_n, y_1 \dots y_z$ pro ψ

Dk: indukcí podle délky φ