Strukturální složitost -2017

Thursday, March 2, 2017 9:11 PM

2/0 zk

zkoušel se z probrané látky

Věty o hierarchii

více prostředků (čas, prostor, ...) dovolují spočítat více

$DTIME(t(n))$ ... problémy řešitelné v čase $O(t(n))$

$M_1, M_2, M_3 \ldots$ výčet všech Turingových strojů (TS)

- **univerzální TS** (jednopáskový)

na vstupu x, i, T, kde i a T jsou binárně zakódovaná

číslo, simuluje M_i na x po $\geq c_i \cdot T$ krocích, $+\infty$.

simulace běží v čase $\leq T$.

c_i je snadno spočitatelná konstanta závisející na i.

na své pásce simuluje všech k_i pásek stroje M_i.

pozice hlav na páskách označuje "*".

pro odsimulování jednoho kroku M_i projde pásku,

posbírá informace o symbolech pod simulovanými

hlavami a upraví patřičně simulované pásky.

ℓ-tý simulovaný krok trvá $\leq O(\ell)$.

Fakt:

- na dvoupáskovém univerzálním TS lze t kroků

simulace v čase $U(t \log t)$.

Věta: pro časově konstruovatelné fce $t(n), T(n) \geq n$,
$T(n) \in \omega(t^2(n))$, $DTIME(t(n)) \subsetneq DTIME(T(n))$.

Dk: zkonstruujeme $L \subseteq DTIME(T(n))$ t.ž. $L \notin DTIME(t(n))$.

diagonalizace

algoritmus pro L:

na vstupu x délky n
nechť binární zápis n je $1 * * * \dots * 1 \underbrace{00\dots0}_{i}$

simuluj M_i na vstupu x po $T(n)$ kroků.
Pokud M_i přijme x $\rightarrow$ odmítni x
Jinak přijmi x.

end.

zjevně $L \in DTIME(T(n))$

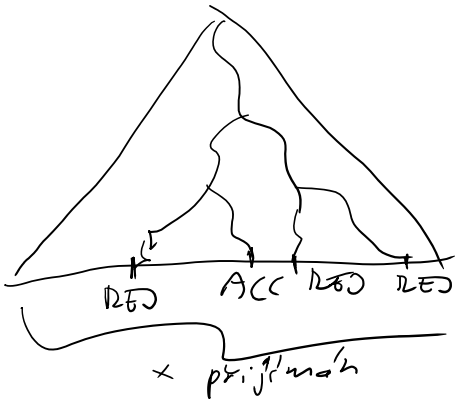
$L \notin DTIME(t(n))$: sporem. Předpokládejme, že L je rozpoznávání TS M_i v čase $t(n)$.
Pro dostatečně velké n, $t(n)$ kroků M_i lze simulovat během $T(n)$ kroků našeho alg.
a na vstupech x takové dostatečné délky n, kde 2^i je nejvyšší mocnina 2 dělící n, se alg. pro L chová jinak než M_i. spor

Nedeterministická hierarchie

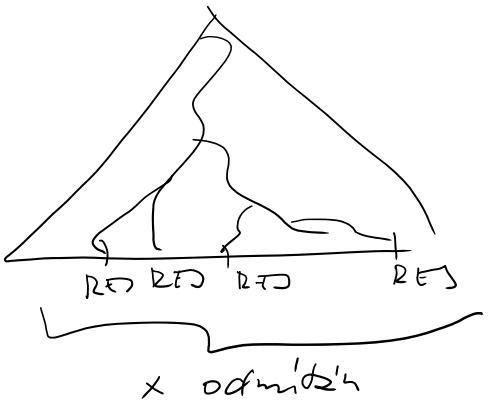
nedeterministický výpočet

nedeterministický výpočet

– hází si nedeterministickou korunou.
vstup x je přijímán, pokud pro nějakou posloupnost hodů vypoví přijme.
Jinak je odmítán



x přijímán



x odmítán

strom možných výpočtů na x

$NTIME(t(n))$ ... jazyky přijímané nedet. TS pracujícími v čase $O(t(n))$.

Simulace nedet. TS univerzálním nedet. TS

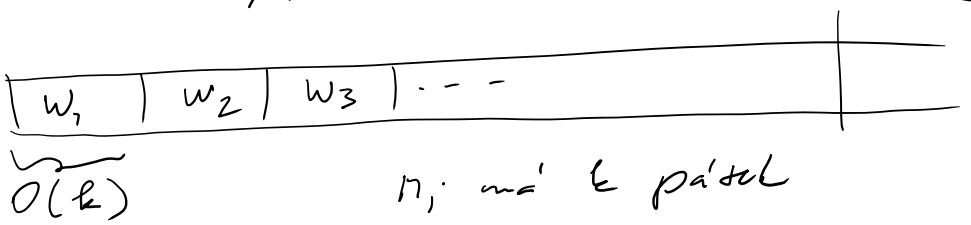
Existuje univerzální NTS, který na vstupu x, i, T, kde i, T jsou binárně zapsaná čísla, v čase T odsimuluje $\geq c_i \cdot T$ kroků nedeterministického výpočtu NTS M_i na vstupu x.
Tento univerzální stroj přijme x, i, T, pokud některý ze simulovaných výpočtů M_i na x přijme během $c_i \cdot T$ kroků.

c_i je konstanta snadno spočitatelná z c.

⟶ efektivnější simulace než dřív.

Dk: (idea)

uhodni historii výpočtu M_i na x, tedy posloupnost "obsahů" výpočtu, kdy každé okno udává: obsah pásek pod jednotlivými hlavami, stav TS M_i, co která hlava zapíše, kam se pohne a co bude nový stav M_i.



pro každou z k pásek M_i ověř její konzistenci "přechrátlým" operací nad ní na druhé pásce našeho univerzálního NTS. □

Věta o nedeterministické časové hierarchii:

Pro časově konstruovatelné fce $t(n), T(n) \geq n$,

$T(n) \in \omega(t(n+1))$, $NTIME(t(n)) \subsetneq NTIME(T(n))$

Dk: opožděná diagonalizace

$n_0 = 1 \qquad n_k = 2^{t^2(n_{k-1}+1)}$

nechť 2^{i_k} je nejmenší mocnina 2 dělící k.

Nechť 2^{i_k} je nejmenší mocnina 2 dělící k.
Na vstupech délky $n_{k-1}+1, \dots n_k$
diagonalizujeme NTS M_{i_k}.

alg.:
na vstupu O^n
urči: k, t.ž. $n_{k-1} < n \leq n_k$.
pokud $n < n_k$, pak simulujeme M_{i_k} na O^{n+1}
pomocí univerzálního NTS po $T(n)$ kroků
simulace. Přijmi pokud M_{i_k} přijme. — deterministicky
pokud $n = n_k$: proztloukáním všech možností
výpočtu M_{i_k} na $O^{n_{k-1}+1}$ zjisti, zda
M_{i_k} přijímá $O^{n_{k-1}+1}$. Pokud ano, odmítni,
jinak přijmi.
→ trvá $\leq 2^{t(n_{k-1}+1)} \cdot t^3(n_{k-1}+1)$ kroků $\leq n_k \leq T(n_k)$

M_{i_k} nerozpoznává náš jazyk L v čase $O(t(n))$:
pokud M_{i_k} přijímá O^n pro $n_{k-1} < n \leq n_k$,
pak $O^{n_k} \notin L$.
pokud M_{i_k} odmítá O^n pro — " —
pak $O^{n_k} \in L$.
pokud M_{i_k} přijímá O^n a odmítá O^{n+1}
pro nějaké $n_{k-1} < n < n_k$

pak $0^n \notin L$

pokud M_k odmítě 0^n a přijímá 0^{n+1}

pro nějaké $n_{k-1} < n < n_k$

pak $0^n \in L$

Koucky v 3/16/2017 9:03 PM

$$P = \bigcup_k DTIME(n^k + k) \qquad NP = \bigcup_k NTIME(n^k + k)$$

$$E = \bigcup_k DTIME(2^{kn}) \qquad NE = \bigcup_k NTIME(2^{kn})$$

$$EXP = \bigcup_k DTIME(2^{n^k}) \qquad NEXP = \bigcup_k NTIME(2^{n^k})$$

$$EEXP = \bigcup_k DTIME(2^{2^{n^k}}) \qquad NEEXP = \bigcup_k NTIME(2^{2^{n^k}})$$

- $P \subsetneq EXP \subsetneq EEXP \ldots$
- $NP \subseteq EXP \subsetneq EEXP \subseteq NEEXP$

  $\Rightarrow NP \subsetneq NEEXP$

Tvrzení: $NP = NEXP \Rightarrow NEXP = NEEXP \Rightarrow NP = NEEXP$

Důsledek: $NP \subsetneq NEXP$

Dk: "padding argument"

$L \in NEEXP$ ... machine M in time $2^{2^{n^k}}$

$L' = \{ x \# 0^{2^{|x|^k}} ; x \in L \}$

$L' \in NEXP$: 1) ověř, že počet 0 je správný vůči $|x|$ (deterministicky v poj-čase vůči délce vstupu $x \# 0^m$.)

2) spusť stroj M na x.

jelikož M běží v čase $2^{2^{n^k}}$, celkový čas 2^{n^k}

bitu M vůči délce vstupu $x\#0^2$ je
pouze exponenciální (dokonce $L \in NE$).

$\Rightarrow L' \in NEXP \Rightarrow L' \in NP$

$\Rightarrow L \in NEXP$: "na vstupu x, vyhodnoť slovo
$x\#0^{2^{n^k}}$ a spusť NP-stroj
pro L'."

$\Rightarrow L \in NTIME\left(\left(2^{n^k}\right)^{k'}\right)$ ☒

- $BPTIME(t(n))$ ... jazyky rozpoznávané pravděpodobnostními s chybou $\leq \frac{1}{3}$ v čase $t(n)$
- $PPTIME(t(n))$ — " — s chybou $< \frac{1}{2}$ v čase $t(n)$.

$BPP = \bigcup_k BPTIME(n^k + k)$ $\quad PP = \bigcup_k PPTIME(n^k)$

- $NP \subseteq PP$ (uvidíme Todovu větu $PH \subseteq P^{PP}$)

pst $\frac{1}{2} - 2^{-t(n)\cdot 1}$ pro ACC

$\Rightarrow$ stačí jeden přijímající výpočet
NP-stroje pracujícího v čase $t(n)$,
aby se pst. přijetí přehoupla
přes $> \frac{1}{2}$.

☒

$BPP \subseteq EXP \subsetneq EEXP \subseteq BPEEXP$

$\Rightarrow BPP \subsetneq BPEEXP$

$\Rightarrow BPP \subsetneq BPEXP$

padding argument

a) testování prvočíselnosti s jedním použitím $\in BPP$.

lepší hierarchie? Neznáme. viz níže

- výpočty s nápovědou

$M \dots TS \qquad g: \mathbb{N} \to \{0,1\}^*$

nápovědní fce

$x, g(|x|)$ vstup pro stroj M.

různá nápověda $\Rightarrow$ různý jazyk

$BPTIME(t(n))/f(n)$ ... jazyky rozpoznávané pravděpodobnostními TS v pol-čase chybou $\leq \frac{1}{3}$ a nápovědou pro vstupy délky n dlouhou $f(n)$.

$BPTIME(t(n))/1$ ... obsahují nerekurzivní jazyky např. založené na Halting problému.

pro důkaz viz o hierarchii potřebujeme vyčíst všech TS typu BPP. Ten ale neznáme a nemůžeme vytvořit.

Otázka: Úplný jazyk pro BPP?

Otevřená: Úplný jazyk pro BPP?

Věta: $\forall$ konst. $a, k \geq 1$, existuje $L \in BPTIME(n^{4^{ak}})$ //
t.ž. $L \notin BPTIME(n^k)/a$.

Dk: "opožděná diagonalizace"
- diagonalizace proti všem možným strojům a napovídám délky a.
- být nápověd bude vadit, zda mnou vybraný bezpečně simulovat stroj M_i s nápovědí z.

→ Různé nápovědy pro stroj M_i budeme diagonalizovat na různých délkách vstupu:

na vstupu délky $n'+j$ simulují stroj M_i s j-tou nápovědí na vstupu délky $n'' \approx (n')^2$
bid naší nápovědy vzdá, zda to je bezpečné.

- jelikož $n'' \approx (n')^2$, po $\log n$ opakováních je vstup dostatečně dlouhý pro opožděnou diagonalizaci

def: $n_0^* = 1$

$n_i = n_{i-1}^* + 1$ $\quad$ $n_i^* = n_i^{d^{m_i}}$

$m_i = \lg n_i$ $\quad$ $d = 2^{(a+1)k}$

všimni si: $n_i^* \geq \left(2^{(n_i^{a+1})^k}\right)^c$

takže na vstupu délky n_i^* je dost času na deterministickou prohledávání chování M_i na vstupu délky $\leq n_i + (2^a)^{n_i} = n_i^a + n_i$

def.: $n_{i,j} = n_i^{d^j}$ $\quad j = 0, \dots \lfloor \log n_i \rfloor$

pro $w \in \{0,1\}^{a(n_i - j - 1)}$ & $z \in \{0,1\}^a$

$n_{i,j,wz} = n_{i,j} + \overline{wz}$ ... číslo reprezentované řetězcem wz

pro řetězec y délky $n_{i,j,wz}$ definujeme:

$$f(y) = y z 1 0^{n_{i,j+1,w} - n_{i,j,wz} - a - 1}$$

$$\Rightarrow |f(y)| = n_{i,j+1,w}$$

alg: M na vstupu x délky n s nápovědou $b \in \{0,1\}$

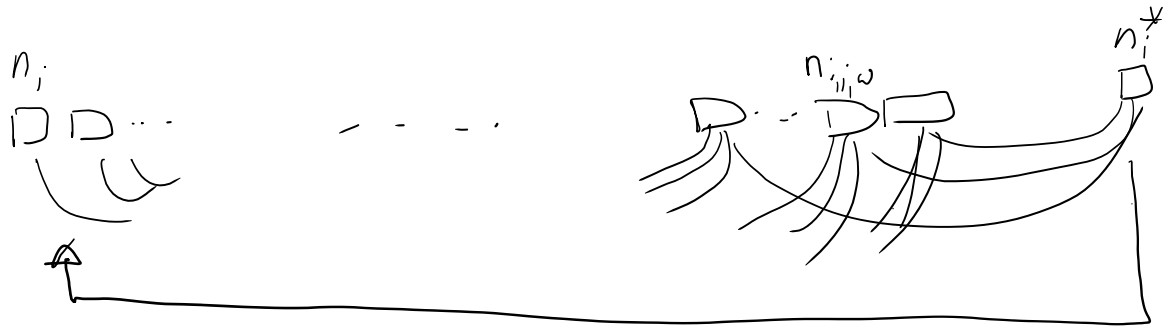
1. If $b = 0$ → REJECT
2. If $n = n_{i,j,wz}$ pro nějaké w & z patřičné délky simuluj M_i na $f(x)$ s nápovědou z.
3. If $n_i = n_i^*$, zkontroluj chování M_i na vstupu y t.ž. $\underbrace{f(f(f \dots (f(y)) \dots)}_{m_i \text{-krát}} = x$

a pokud platí a bitů z y jako nápověda pro M_i.

→ udělej opak než M_i na y s nápovědou

· dá se snadno zkontrolovat, že M má dost času

na pravděpodobnostní chodník stojí n_i pracujících v čase n^k.



diagonalizace

Koucky v 3/30/2017 9:24 PM

- Polynomial Identity Testing

Schwarz-Zippel lema: Let $p \neq 0$ be a polynomial in n vars of total degree d over a field F. Let $S \subseteq F$. The # of roots in S^n is at most $d \cdot |S|^{n-1}$.

Corollary: If $|S| \geq 2d$ then a random point in $|S|^n$ will be root w.p. $\leq \frac{1}{2}$.

Pf: Induction on n:

- For $n=1$ this is a standard fact about # of roots.
- Induction step:

$$p(x_1 \dots x_n) = \sum_{i=0}^{d_1} p_i(x_1 \dots x_{n-1}) \cdot x_n^i$$

Let d' be the largest d' s.t. $p_{d'} \neq 0$.

For $a_1, \dots a_n \in S^{n-1}$ be a root of $p(x_1, \dots x_n)$

either $p_d'(a_1, \dots a_{n-1})$ is zero

(which happens at most $(d-d')\cdot |S|^{n-2}$ times by IH for $a_1, \dots a_{n-1}$)

or a_n is a root of $\sum_{i=0}^{d'} p_i(a_1, \dots a_{n-1})\, x^i$

which for each $a_1, \dots a_{n-1}$ happens at most d' times. Thus in total we have

$$(d-d')\cdot |S|^{n-1} + d' \cdot |S|^{n-1} \le d\,|S|^{n-1}$$

choice of a_n

roots of p. ∎

Time-space Trade-off for SAT

Věta 1: $NTIME(n) \not\subseteq DTISP(n^c, n^d)$ pro $c = 1.4$, $d = 0.02$.

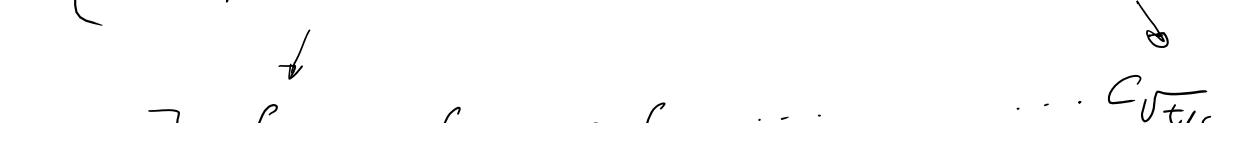
- technika jak zpět ke Kannanovi 1983 - 1989.

(Lipton + Viglas 1999)

Věta (Nepomjaščij): $DTISP(t, s) \subseteq \Sigma_2 TIME(\sqrt{t \cdot s})$

Dk:
- nedeterministicky uhodni konfigurace M $c_1, \dots c_{\sqrt{t/s}}$
- univerzálně ověř pro $i \in \{1, \dots \sqrt{t/s} - 1\}$, že c_i dá po $\sqrt{ts}$ krocích c_{i+1}.

(c_1 počáteční konf. M a $c_{\sqrt{t/s}}$ přijímající konf. M)



$\exists \quad C_1 \ldots C_2 \ldots C_3 \ldots \qquad \ldots C_{\sqrt{t/s}}$

$\forall i \qquad C_i \xrightarrow{\sqrt{ts}} C_{i+1}$ determ. výpočet

oba kroky trvají $O(\sqrt{ts})$ kroků $\Rightarrow \Sigma_2^t TIME(\sqrt{ts})$ ∎

<u>Lema:</u> Pokud $NTIME(n) \subseteq DTIME(n^c)$ $\quad c > 1$

pak pro $\forall \tau(n) \geq n$

$$\Sigma_2^t TIME(\tau) \subseteq NTIME(\tau^c).$$

<u>Pf:</u> $\Sigma_2^t TIME(\tau) = \exists y_1 \in \{0,1\}^\tau \ \forall y_2 \in \{0,1\}^\tau \ R(x, y_1, y_2)$

kde $R(x, y_1, y_2)$ je počitatelný v lineárním čase vůči $|x| + |y_1| + |y_2|$

Podle předpokladu $\forall y_2 \in \{0,1\}^\tau R(x, y_1, y_2)$ lze nahradit $DTIME(\tau^c)$ výpočtem na vstupu x, y_1. Dostaneme tedy

$$\exists y_1 \in \{0,1\}^\tau \underbrace{R'(x, y_1)}_{DTIME(\tau^c)}$$

$$= NTME(\tau^c)$$ ∎

<u>Dk Věty 7:</u> uvažme $\tau(n) \geq n^2$

$DTIME(\tau, \tau^{d/c}) \underset{\text{(Nepomjašt.)}}{\subseteq} \Sigma_2^t TIME(\tau^{1/2 + d/2c})$

$\underset{\text{(Lema)}}{\subseteq} NTIME(\tau^{c/2 + d/2})$

paddingem $\qquad (\tau^{c/2 + dc/2})$

$DTIME(\tau^c, \tau^d) \subseteq NTIME(\tau^{c^2/2 + dc/2})$

$\cap$ ← předpoklad

$NTIME(\tau)$

$\Rightarrow NTIME(\tau) \subseteq NTIME(\tau^{c^2/2 + dc/2})$

pro τ polynomiální & $\frac{c^2}{2} + \frac{dc}{2} < 1$

$c = 1.4$
$c^2 = 1.96$
$d = 0.02$

je tato spor s větou o nedeterministické hierarchii. ∎

Limit této techniky $c \leq 1.81\ldots$ [Williams '13]