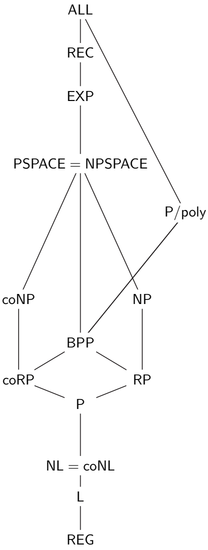
Základy zložitosti (opakovanie)

kuko

17.2.2021

Pokročilá teória zložitosti


ALL
REC
EXP
PSPACE = NPSPACE
P/poly
coNP
NP
BPP
coRP
RP
P
NL = coNL
L
REG

Základné triedy

- DTIME($f(n)$) – problémy riešiteľné v čase $O(f(n))$
- DSPACE($f(n)$) – problémy riešiteľné v pamäti $O(f(n))$
- $\mathrm{L} = \mathrm{DSPACE}(\log n)$ – logaritmický priestor,
- $\mathrm{P} = \bigcup_k \mathrm{DTIME}(n^k)$ – polynomiálny čas,
- $\mathrm{PSPACE} = \bigcup_k \mathrm{DSPACE}(n^k)$ – polynomiálny priestor,
- $\mathrm{EXP} = \bigcup_k \mathrm{DTIME}(2^{n^k})$ – exponenciálny čas.

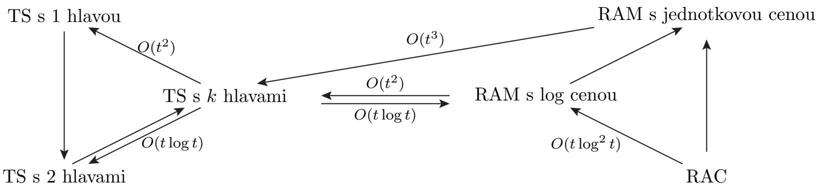
Základné triedy

- DTIME($f(n)$) – problémy riešiteľné v čase $O(f(n))$
- DSPACE($f(n)$) – problémy riešiteľné v pamäti $O(f(n))$
- $\mathrm{L} = \mathrm{DSPACE}(\log n)$ – logaritmický priestor,
- $\mathrm{P} = \bigcup_k \mathrm{DTIME}(n^k)$ – polynomiálny čas,
- $\mathrm{PSPACE} = \bigcup_k \mathrm{DSPACE}(n^k)$ – polynomiálny priestor,
- $\mathrm{EXP} = \bigcup_k \mathrm{DTIME}(2^{n^k})$ – exponenciálny čas.

Základné triedy

$$\mathsf{L} \subseteq \mathsf{P} \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP}$$

Sekvenčné modely



Nedeterminizmus

- NTIME($f(n)$) – problémy riešiteľné nedeterministicky v čase $O(f(n))$
- NSPACE($f(n)$) – problémy riešiteľné nedeterministicky v pamäti $O(f(n))$
- NL $=$ NSPACE($\log n$) – logaritmický priestor,
- NP $= \bigcup_k$ NTIME(n^k) – polynomiálny čas,
- NEXP $= \bigcup_k$ NTIME(2^{n^k}) – exponenciálny čas.

Nedeterminizmus

- NTIME($f(n)$) – problémy riešiteľné nedeterministicky v čase $O(f(n))$
- NSPACE($f(n)$) – problémy riešiteľné nedeterministicky v pamäti $O(f(n))$
- $\mathrm{NL} = \mathrm{NSPACE}(\log n)$ – logaritmický priestor,
- $\mathrm{NP} = \bigcup_k \mathrm{NTIME}(n^k)$ – polynomiálny čas,
- $\mathrm{NEXP} = \bigcup_k \mathrm{NTIME}(2^{n^k})$ – exponenciálny čas.

Nedeterminizmus

$$\mathsf{L} \subseteq \mathsf{NL} \subseteq \mathsf{P} \subseteq \mathsf{NP} \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP} \subseteq \mathsf{NEXP} \subseteq \mathsf{EXPSPACE}$$

Nedeterminizmus

- $L \in \mathrm{NP} \iff$ dá sa deterministicky overiť v poly čase
- $\exists L' \in \mathrm{P} : (x \in L \iff \exists y \in \{0,1\}^{\mathrm{poly}(|x|)} : x\#y \in L')$

Nedeterminizmus

- $L \in \mathrm{NP} \iff$ dá sa deterministicky overiť v poly čase
- $\exists L' \in \mathrm{P} : (x \in L \iff \exists y \in \{0,1\}^{\mathrm{poly}(|x|)} : x\#y \in L')$

Veta (Savitch)

Nech $\log n \leq s(n)$ *je páskovo konštruovateľná, potom*

$$\mathrm{NSPACE}(s(n)) \subseteq \mathrm{DSPACE}(s(n)^2).$$

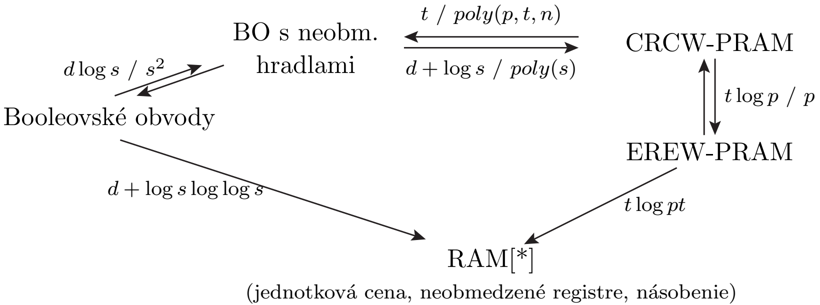
Takže napríklad $\mathrm{PSPACE} = \mathrm{NPSPACE} = \mathrm{coNPSPACE}$.

Veta (Immerman-Szelepcsenyi)

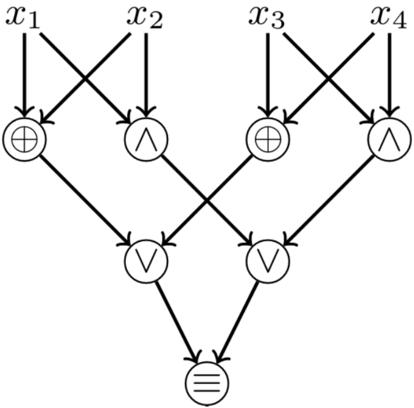
Nedeterministický priestor je uzavretý na komplement: $\mathrm{NSPACE}(s(n)) = \mathrm{coNSPACE}(s(n))$ *pre* $s(n) \geq \log n$. *Špeciálne* $\mathrm{NL} = \mathrm{coNL}$ *a kontextové jazyky sú uzavreté na komplement.*

Paralelizmus

Paralelné modely

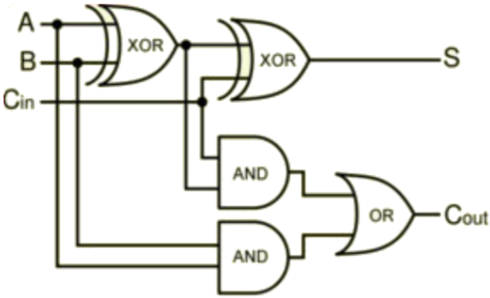


Obvody

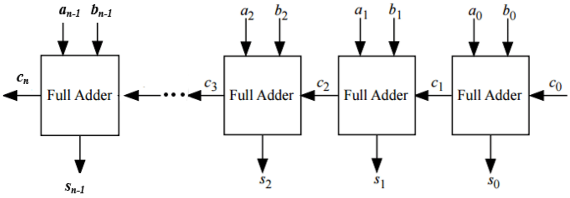


Testuje deliteľnosť tromi (či $x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod 3$).
Najmenší možný, ak povolíme $\oplus$ a $\equiv$.

Obvody



- Úplná 1-bitová sčítačka
- $S = A + B + C_{in} \pmod 2 = A \oplus B \oplus C_{in}$
- $C_{out} \equiv (A + B + C_{in} \geq 2) \equiv C_{in} \wedge (A \oplus B) \vee (A \wedge B)$ je prenos do vyššieho rádu



a_{n-1} b_{n-1}
a_2 b_2
a_1 b_1
a_0 b_0
c_n
Full Adder
c_3
Full Adder
c_2
Full Adder
c_1
Full Adder
c_0
s_{n-1}
s_2
s_1
s_0

Definícia (BO)

Booleovský obvod C je acyklický orientovaný graf.

- *Vrcholy, do ktorých nejde hrana voláme vstupné,*
- *ostatné vrcholy sú hradlá označené $\wedge$, $\vee$, alebo $\neg$,*
- *niektoré vrcholy sú označené ako výstupné.*

Tradične budeme vyžadovať, že hradlá $\wedge$ a $\vee$ majú dva vstupy, hradlo $\neg$ jeden. V booleovských obvodoch s neobmedzeným stupňom môžu mať hradlá $\wedge$ a $\vee$ ľubovoľne veľa vstupov.
Postupnosť $C_0, C_1, C_2, C_3, \ldots$

- PRAM s poly #procesorov v poly čase = P
- *uniformné* obvody polynomiálnej veľkosti = P

- PRAM s poly #procesorov v poly čase $=$ P
- *uniformné* obvody polynomiálnej veľkosti $=$ P

Neuniformnosť

- SIZE($f(n)$) – problémy riešiteľné obvodom veľkosti $f(n)$
- SIZE($O(n2^n)$) $=$ ALL

- SIZE($f(n)$) – problémy riešiteľné obvodom veľkosti $f(n)$
- SIZE($O(n2^n)$) $=$ ALL

Neuniformnosť

x	y	z	f(x,y,z)
F	F	F	**F**
F	F	T	**T**
F	T	F	**F**
F	T	T	**T**
T	F	F	**T**
T	F	T	**T**
T	T	F	**T**
T	T	T	**F**

$$C_n(x) \equiv \bigvee_{|z|=n, z\in L} \left(\bigwedge_{i:z_i=1} x_i \wedge \bigwedge_{i:z_i=0} \neg x_i \right)$$

Neuniformnosť

x	y	z	f(x,y,z)
F	F	F	**F**
F	F	T	**T**
F	T	F	**F**
F	T	T	**T**
T	F	F	**T**
T	F	T	**T**
T	T	F	**T**
T	T	T	**F**

$$C_n(x) \equiv \bigvee_{|z|=n, z \in L} \left(\bigwedge_{i:z_i=1} x_i \wedge \bigwedge_{i:z_i=0} \neg x_i \right)$$

Neuniformnosť

Definícia (P/poly)

P/poly $= \bigcup_k \text{SIZE}(n^k)$ *je trieda jazykov rozhodovaných neuniformnými obvodmi polynomiálnej veľkosti.*

- P $\subseteq$ P/poly
- nepredpokladá sa, že by SAT $\in$ P/poly
- TS s polynomiálnou radou

Neuniformnosť

Definícia (P/poly)

$\mathsf{P/poly} = \bigcup_k \mathsf{SIZE}(n^k)$ *je trieda jazykov rozhodovaných neuniformnými obvodmi polynomiálnej veľkosti.*

- $\mathsf{P} \subseteq \mathsf{P/poly}$
- nepredpokladá sa, že by $\textsc{Sat} \in \mathsf{P/poly}$
- TS s polynomiálnou radou

Náhodnosť

Náhodnosť

- pravdepodobnostné TS

Definícia (BPP)

BPP *je trieda jazykov L, pre ktoré existuje PTS M bežiaci v polynomiálnom čase,*

- *ak* $x \in L \Rightarrow \Pr_r[M(x) = 1] \geq 2/3$,
- *ak* $x \notin L \Rightarrow \Pr_r[M(x) = 1] \leq 1/3$.

Náhodnosť

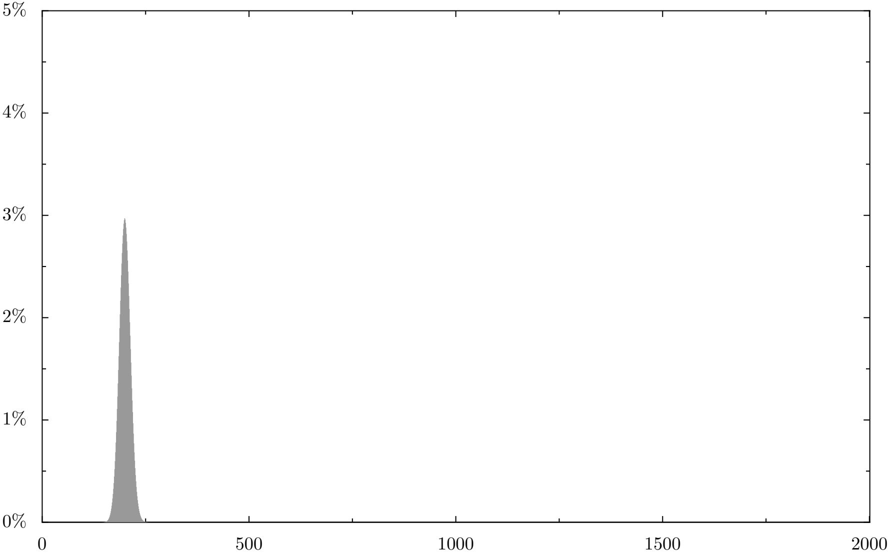
- pravdepodobnostné TS

Definícia (BPP)

BPP *je trieda jazykov* L*, pre ktoré existuje PTS* M *bežiaci v polynomiálnom čase,*

- *ak* $x \in L \Rightarrow \Pr_r[M(x) = 1] \geq 2/3$,
- *ak* $x \notin L \Rightarrow \Pr_r[M(x) = 1] \leq 1/3$.

Náhodnosť



- pravdepodobnostné TS

Definícia (BPP)

BPP *je trieda jazykov L, pre ktoré existuje PTS M bežiaci v polynomiálnom čase,*

- *ak* $x \in L \Rightarrow \Pr_r[M(x) = 1] \geq 1/2 + 1/n^c$,
- *ak* $x \notin L \Rightarrow \Pr_r[M(x) = 1] \leq 1/2 - 1/n^c$.

Náhodnosť

- pravdepodobnostné TS

Definícia (BPP)

BPP *je trieda jazykov L, pre ktoré existuje PTS M bežiaci v polynomiálnom čase,*

- $ak\ x \in L \Rightarrow \Pr_r[M(x) = 1] \geq 1 - 1/2^{n^k}$,
- $ak\ x \notin L \Rightarrow \Pr_r[M(x) = 1] \leq 1/2^{n^k}$.

Veta (Adleman)

$BPP \subseteq P/poly$.

Dôkaz.

- BPP stroj M, na n-bitovom vstupe sa pomýli s pp. $\leq 1/2^{(n+1)}$.
- $Pr_r[M \text{ sa mýli na } x] \leq 1/2^{(n+1)}$
- $Pr_r[M \text{ sa mýli na } \textit{nejakom} \text{ vstupe}] \leq 2^n \times (1/2^{(n+1)}) \leq 1/2$
- pre polovicu r sa M nepomýli na žiadnom vstupe
- $\Rightarrow$ existuje také r; môžeme ho použiť ako radu pre M

$\square$

- príklad aplikácie: testovanie prvočísel

Veta (Adleman)

BPP $\subseteq$ P/poly.

■ **Dôkaz.**

- BPP stroj M, na n-bitovom vstupe sa pomýli s pp. $\leq 1/2^{(n+1)}$.
- $\Pr_r[M \text{ sa mýli na } x] \leq 1/2^{(n+1)}$
- $\Pr_r[M \text{ sa mýli na } \textit{nejakom} \text{ vstupe}] \leq 2^n \times (1/2^{(n+1)}) \leq 1/2$
- pre polovicu r sa M nepomýli na žiadnom vstupe
- $\Rightarrow$ existuje také r; môžeme ho použiť ako radu pre M

□

- príklad aplikácie: testovanie prvočísel

Veta (Adleman)

BPP $\subseteq$ P/poly.

■ **Dôkaz.**

- BPP stroj M, na n-bitovom vstupe sa pomýli s pp. $\leq 1/2^{(n+1)}$.
- $\Pr_r[M \text{ sa mýli na } x] \leq 1/2^{(n+1)}$
- $\Pr_r[M$ sa mýli na *nejakom* vstupe$] \leq 2^n \times (1/2^{(n+1)}) \leq 1/2$
- pre polovicu r sa M nepomýli na žiadnom vstupe
- $\Rightarrow$ existuje také r; môžeme ho použiť ako radu pre M

□

- príklad aplikácie: testovanie prvočísel

Veta (Adleman)

BPP $\subseteq$ P/poly.

Dôkaz.

- BPP stroj M, na n-bitovom vstupe sa pomýli s pp. $\leq 1/2^{(n+1)}$.
- $\Pr_r[M \text{ sa mýli na } x] \leq 1/2^{(n+1)}$
- $\Pr_r[M \text{ sa mýli na } \textit{nejakom} \text{ vstupe}] \leq 2^n \times (1/2^{(n+1)}) \leq 1/2$
- pre polovicu r sa M nepomýli na žiadnom vstupe
- $\Rightarrow$ existuje také r; môžeme ho použiť ako radu pre M

$\square$

- príklad aplikácie: testovanie prvočísel

Veta (Adleman)

BPP $\subseteq$ P/poly.

Dôkaz.

- BPP stroj M, na n-bitovom vstupe sa pomýli s pp. $\leq 1/2^{(n+1)}$.
- $\Pr_r[M \text{ sa mýli na } x] \leq 1/2^{(n+1)}$
- $\Pr_r[M \text{ sa mýli na } \textit{nejakom} \text{ vstupe}] \leq 2^n \times (1/2^{(n+1)}) \leq 1/2$
- pre polovicu r sa M nepomýli na žiadnom vstupe
- $\Rightarrow$ existuje také r; môžeme ho použiť ako radu pre M

$\square$

- príklad aplikácie: testovanie prvočísel

Veta (Adleman)

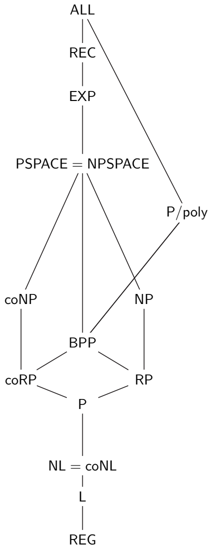
BPP $\subseteq$ P/poly.

■ **Dôkaz.**

- BPP stroj M, na n-bitovom vstupe sa pomýli s pp. $\leq 1/2^{(n+1)}$.
- $\Pr_r[M \text{ sa mýli na } x] \leq 1/2^{(n+1)}$
- $\Pr_r[M \text{ sa mýli na } \textit{nejakom} \text{ vstupe}] \leq 2^n \times (1/2^{(n+1)}) \leq 1/2$
- pre polovicu r sa M nepomýli na žiadnom vstupe
- $\Rightarrow$ existuje také r; môžeme ho použiť ako radu pre M

$\square$

- príklad aplikácie: testovanie prvočísel


ALL
REC
EXP
PSPACE = NPSPACE
P/poly
coNP
NP
BPP
coRP
RP
P
NL = coNL
L
REG