IB107 Vyčíslitelnost a složitost

prostorová složitost, vztahy složitostních tříd, TQBF

Jan Strejček

Fakulta informatiky
Masarykova univerzita

prostorová složitost algoritmu

- paměť použitá při výpočtu
- závisí na vstupu
- jako základní model použijeme Turingův stroj
- zkoumáme nejhorší případ, tedy maximální počet přečtených políček pásky v závislosti na délce vstupu
- lze zkoumat i průměrný případ

prostorová složitost Turingova stroje

Definice (prostorová složitost deterministického TM)

Nechť $\mathcal{M}$ je úplný deterministický (jednopáskový nebo vícepáskový) Turingův stroj se vstupní abecedou Σ. Pro každé $w \in \Sigma^*$ definujeme $s_{\mathcal{M}}(w)$ jako počet políček pásky, které stroj $\mathcal{M}$ čte při výpočtu na vstupu w. Prostorová složitost stroje $\mathcal{M}$ je pak funkce $S_{\mathcal{M}} : \mathbb{N} \to \mathbb{N}$ definovaná vztahem

$$S_{\mathcal{M}}(n) = \max\{s_{\mathcal{M}}(w) \mid w \in \Sigma^n\}.$$

Definice (prostorová složitost nedeterministického TM)

Definice prostorové složitosti úplného nedeterministického Turingova stroje se liší jen tím, že $s_{\mathcal{M}}(w)$ označuje maximální počet políček pásky, které stroj $\mathcal{M}$ čte při nějakém výpočtu na vstupu w.

Příklad

$$\mathcal{M} = (\{q_0, q_1, q_{acc}, q_{rej}\}, \{0, 1\}, \{0, 1, \rhd, \sqcup\}, \rhd, \sqcup, \delta, q_0, q_{acc}, q_{rej})$$

δ	$\rhd$	0	1	$\sqcup$
q_0	$(q_0, \rhd, R)$	$(q_0, 0, R)$	$(q_1, 1, R)$	$(q_{acc}, -, -)$
q_1		$(q_{rej}, -, -)$	$(q_1, 1, R)$	$(q_{acc}, -, -)$

komprese prostoru

Věta

Pro každý deterministický úplný TM $\mathcal{M}$ a pro každé $m > 1$ lze zkonstruovat deterministický úplný TM $\mathcal{M}'$ tak, že $L(\mathcal{M}) = L(\mathcal{M}')$ a

$$S_{\mathcal{M}'}(n) = \left\lceil \frac{S_{\mathcal{M}}(n)}{m} \right\rceil + n + 2.$$

Důkaz:

■

Protože prostor lze komprimovat, používáme asymptotickou notaci.

prostorové složitostní třídy problémů

prostorová složitost problému = nejmenší prostorová složitost, s jakou lze daný problém rozhodnout

Definice (prostorové složitostní třídy problémů)

Každá funkce $f : \mathbb{N} \to \mathbb{R}^+$ definuje prostorové složitostní třídy problémů:

$$SPACE(f(n)) = \{L \mid L \text{ je rozhodovaný nějakým det. TM } \mathcal{M} \text{ s prostorovou složitostí } S_{\mathcal{M}}(n) = \mathcal{O}(f(n))\}$$

$$NSPACE(f(n)) = \{L \mid L \text{ je rozhodovaný nějakým nedet. TM } \mathcal{N} \text{ s prostorovou složitostí } S_{\mathcal{N}}(n) = \mathcal{O}(f(n))\}$$

$SAT \in \mathrm{SPACE}(n)$

$SAT = \{\langle\varphi\rangle \mid \varphi$ je splnitelná výroková formule$\}$

SAT může být rozhodován deterministickým třípáskovým TM $\mathcal{M}$:

- na 2. pásku postupně zapisujeme všechna ohodnocení proměnných
- na 3. pásce pro dané ohodnocení ověříme, zda splňuje φ
- akceptujeme, pokud narazíme na splňující ohodnocení
- zamítneme, pokud žádné ohodnocení není splňující

Prostor lze použít opakovaně.

determinismus a nedeterminismus, čas a prostor

Věta

Pro každou funkci $f : \mathbb{N} \to \mathbb{R}^+$ *platí:*

1. $TIME(f(n)) \subseteq NTIME(f(n))$
2. $SPACE(f(n)) \subseteq NSPACE(f(n))$
3. $TIME(f(n)) \subseteq SPACE(f(n))$
4. $NTIME(f(n)) \subseteq NSPACE(f(n))$
5. $SPACE(f(n)) \subseteq TIME(k^{f(n)})$ *pro vhodné* $k \in \mathbb{N}$
6. $NSPACE(f(n)) \subseteq NTIME(k^{f(n)})$ *pro vhodné* $k \in \mathbb{N}$

Důkaz:

■

Savitchova věta

Věta (Savitchova věta)

Pro každou funkci $f : \mathbb{N} \to \mathbb{R}^+$ *splňující* $f(n) \geq n$ *platí:*

$$NSPACE(f(n)) \subseteq SPACE(f^2(n))$$

Standardní převod nedet. TM na deterministický nefunguje:

Savitchova věta

Důkaz: Nechť $\mathcal{N}$ je nedet. TM s prostorovou složitostí $f(n)$. Stroj upravíme tak, aby před akceptováním smazal pásku a posunul hlavu zcela vlevo. Má tedy jen jednu akceptující konfiguraci c_{acc}. Výpočet stroje má maximálně $k^{f(n)}$ kroků.

Ekvivalentní deterministický stroj $\mathcal{M}$ implementuje proceduru $comp(c_1, c_2, t)$, která akceptuje, pokud lze ve stroji $\mathcal{N}$ během nejvýše t kroků přejít z konfigurace c_1 do c_2, jinak zamítá. Je-li c_w iniciální konfigurace stroje $\mathcal{N}$ pro w, stačí tedy spustit $comp(c_w, c_{acc}, k^{f(n)})$.

$comp(c_1, c_2, t)$ lze implementovat rekurzivně:

Savitchova věta

Algoritmus pro $comp(c_1, c_2, t)$:

$t = 1$: Otestujeme, zda platí $c_1 = c_2$ nebo $c_1 \vdash_{\mathcal{N}} c_2$.

Pokud platí, akceptujeme, jinak zamítneme.

$t > 1$: Pro každou konfiguraci c' stroje $\mathcal{N}$ využívající nejvýše $f(n)$ políček

- spustíme $comp(c_1, c', \lceil \frac{t}{2} \rceil)$ a $comp(c', c_2, \lceil \frac{t}{2} \rceil)$,
- pokud obojí akceptuje, akceptujeme.

Pokud žádné c' nevedlo k akceptování, zamítneme.

Prostorová složitost:

- *comp* potřebuje prostor na c_1, c_2, c' a t (a něco konstantního):
- hloubka rekurzivního volání:
- celkem:

$\blacksquare$

polynomiální prostorové složitostní třídy

$$\mathrm{PSPACE} = \bigcup_{k \in \mathbb{N}} \mathrm{SPACE}(n^k) \qquad \mathrm{NPSPACE} = \bigcup_{k \in \mathbb{N}} \mathrm{NSPACE}(n^k)$$

Věta

$PSPACE = NPSPACE$

Důkaz: Plyne přímo z definice ($\subseteq$) a ze Savitchovy věty ($\supseteq$). ■

sublineární prostorové složitostní třídy

- chceme podchytit prostor využívaný nad rámec vstupu
- upravíme výpočetní model:
  - (vícepáskový) Turingův stroj se speciální vstupní páskou
  - vstupní páska je konečná, za vstupem je koncová značka $\lhd$
  - vstupní pásku lze pouze číst, nelze na ni zapsat
  - čtení ze vstupní pásky se nezapočítává do počtu přečtených políček $s_{\mathcal{M}}(w)$
- v tomto modelu je každý regulární jazyk v SPACE(1)

$$\mathrm{L} = \mathrm{LOGSPACE} = \mathrm{SPACE}(\log n)$$

$$\mathrm{NL} = \mathrm{NLOGSPACE} = \mathrm{NSPACE}(\log n)$$

Příklad: $\{0^k 1^k \mid k \geq 0\} \in L$

vztahy prostorových a časových tříd

$$\mathrm{L} \subseteq \mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{NPSPACE} = \mathrm{PSPACE} \subseteq \mathrm{EXPTIME} \subseteq \mathrm{NEXPTIME}$$

$$\mathrm{NL} \subsetneq \mathrm{PSPACE} \qquad \mathrm{P} \subsetneq \mathrm{EXPTIME}$$

problém TQBF

QBF = kvantifikované výrokové formule (proměnné v doméně $\{0, 1\}$)

$$\exists x \forall y \big((x \vee y) \wedge (\neg x \vee \neg y)\big)$$

Předpokládáme, že QBF formule jsou v prenexní formě
(tedy kvantifikátory jsou pouze na začátku formule).

Definice (problém TQBF (true quantified Boolean formula))

Problém TQBF je problém rozhodnout, zda je daná QBF formule bez volných proměnných pravdivá.

$TQBF = \{\langle\varphi\rangle \mid \varphi$ *je pravdivá QBF formule bez volných proměnných*$\}$

Věta

TQBF je PSPACE-úplný.

TQBF je PSPACE-úplný

Důkaz: $TQBF \in$ PSPACE: lze řešit rekurzivní procedurou $t(\varphi)$:

1. Je-li φ tvaru $\exists x(\varphi')$, spustíme $t(\varphi'[x \mapsto 0])$ a $t(\varphi'[x \mapsto 1])$. Pokud alespoň jedno z volání akceptuje, akceptujeme. Jinak zamítneme.
2. Je-li φ tvaru $\forall x(\varphi')$, spustíme $t(\varphi'[x \mapsto 0])$ a $t(\varphi'[x \mapsto 1])$. Pokud obě volání akceptují, akceptujeme. Jinak zamítneme.
3. Pokud φ neobsahuje kvantifikátory, snadno vyhodnotíme a akceptujeme, pokud je φ pravdivá. Jinak zamítneme.

Prostorová složitost:

- v jednom zavolání t si pamatujeme pouze něco konstantního
- hloubka rekurzivního volání:
- celkem:

TQBF je PSPACE-úplný

TQBF je PSPACE-těžký: ukážeme $A \in \text{PSPACE} \implies A \leq_p \mathit{TQBF}$

Nechť $\mathcal{M}$ je TM s prostorovou složitostí n^k rozhodující A. Tedy $\mathcal{M}$ pracuje v čase $d^{(n^k)}$. Předpokládáme, že $\mathcal{M}$ má jednu akceptující konfiguraci c_{acc}. Důkaz kombinuje myšlenky důkazů NP-těžkosti *SAT*u a Savitchovy věty.

Pro každé slovo w sestrojíme QBF formuli Φ, která je pravdivá, právě když existuje výpočet stroje $\mathcal{M}$ z iniciální konfigurace pro w c_{start} do akceptující konfigurace c_{acc} s nejvýše $d^{(n^k)}$ kroky.

TQBF je PSPACE-úplný

Induktivně definujeme formuli $\Phi'_{c_1,c_2,t}$ říkající, že existuje výpočet stroje $\mathcal{M}$ z c_1 do c_2 s nejvýše t kroky:

$t = 1$: $\Phi'_{c_1,c_2,1}$ je pravdivá, právě když $c_1 = c_2$ nebo $c_1 \vdash_{\mathcal{M}} c_2$.

$t > 1$: $\Phi'_{c_1,c_2,t} \; = \; \exists m \, \forall (c_3, c_4) \in \{(c_1, m), (m, c_2)\} \left(\Phi'_{c_3,c_4,\lceil \frac{t}{2} \rceil}\right)$

Pak $\Phi = \exists c_1, c_2 \left(\Phi_{c_1 = c_{start}} \; \wedge \; \Phi_{c_2 = c_{acc}} \; \wedge \; \Phi'_{c_1,c_2,d^{(n^k)}}\right)$.

$|\Phi|$ je polynomiální vzhledem k $|w| = n$ a Φ je pravdivá $\iff$ $w \in A$

Celkem $A \leq_p TQBF$ pro každé $A \in$ PSPACE. $\blacksquare$