Teorie algoritmů — 11. týden

Marie Demlová
http://math.fel.cvut.cz/en/people/demlova

30. 4. 2024

Třídy $\mathcal{P}$SPACE a $\mathcal{NP}$SPACE

Věta.

Je dán Turingův stroj M (deterministický nebo nedeterministický), který přijímá L s paměťovou složitostí $p(n)$ (p je polynom). Pak existuje konstanta c taková, že M přijme slovo w délky n po nejvýše $c^{p(n)+1}$ krocích.

Třídy $\mathcal{P}$SPACE a $\mathcal{NP}$SPACE

Věta.

Jestliže jazyk L patří do $\mathcal{P}$SPACE ($\mathcal{NP}$SPACE), pak L je rozhodován deterministickým (nedeterministickým) Turingovým strojem M s polynomiální paměťovou složitostí a který se zastaví na každém slově délky n po maximálně $c^{q(n)}$ krocích ($q(n)$ je vhodný polynom a c je konstanta).

Třídy $\mathcal{P}$SPACE a $\mathcal{NP}$SPACE

Savitchova věta.

Platí
$$\mathcal{P}\mathtt{SPACE} = \mathcal{NP}\mathtt{SPACE}.$$

Třídy $\mathcal{P}$SPACE a $\mathcal{NP}$SPACE

Rekursivní procedura REACH(I, J, m)**:**

Vstup: ID I a J NTM M a kladné přirozené číslo m.

Výstup:

- TRUE, jestliže z I je možné přejít do J po maximálně m krocích,
- FALSE v opačném případě.

Třídy $\mathcal{P}$SPACE a $\mathcal{NP}$SPACE

REACH$(I, J; m)$

begin
    if $m = 1$ then
        if $I = J$ nebo $I \vdash J$ then return TRUE
        else return FALSE
    end
    else (*rekursivní část*)
        for každé ID K do
        if REACH$(I, K; \lfloor \frac{m}{2} \rfloor)$ a REACH$(K, J; \lceil \frac{m}{2} \rceil)$ then
            return TRUE
        return FALSE
    end
end

Třídy založené na pravděpodobnostních algoritmech

Randomizovaný Turingův stroj.

Neformálně: Randomizovaný Turingův stroj (RTM) je Turingův stroj M se dvěma nebo více páskami, kde první páska má stejnou roli jako u deterministického Turingova stroje a druhá páska obsahuje posloupnost 0 a 1 generovanou náhodně, obsahuje 0 nebo 1 se stejnou pravděpodobností rovnou $\frac{1}{2}$).

Třídy založené na pravděpodobnostních algoritmech

Na začátku práce:

- M je v počátečním stavu q_0;
- první páska obsahuje vstupní slovo w, ostatní pole B;
- druhá páska obsahuje náhodně generovanou posloupnost 0 a 1;
- ostatní pásky (jsou-li) obsahují Bs;
- každá hlava čte první pole své pásky.

Třídy založené na pravděpodobnostních algoritmech

Podle stavu q, ve kterém řídící jednotka M je, a podle obsahu čtených polí pásek, přechodová funkce δ TM M určí, zda se M zastaví nebo provede jeden krok, tj. následující akce:

- změní stav řídící jednotky,
- přepíše obsah čteného pole první pásky (nebo třetí a další) (**ale nezmění obsah pole druhé pásky**),
- pohne každou svou hlavou doprava, doleva nebo ji nechá na čteném poli (pohyby hlav jsou nezávislé).

Třídy založené na pravděpodobnostních algoritmech

Formálně. a randomizovaný Turingův stroj je $M = (Q, \Sigma, \Gamma, \delta, q_0, F)$, kde

- Q, Σ, Γ, q_0, B a F mají stejný význam jako v případě TM.
- přechodová funkce δ je parciální zobrazení $Q \times \Gamma \times \{0, 1\}$ do $Q \times \Gamma \times \{L, R, S\}^2$.

Třídy založené na pravděpodobnostních algoritmech

Je-li M ve stavu q a první hlava čte X, druhá čte $a \in \{0,1\}$ a

$$\delta(q, X, a) = (p, Y, D_1, D_2), \quad p \in Q, Y \in \Gamma, D_1, D_2 \in \{L, R, S\},$$

pak M přejde do stavu p; na první pásce napíše Y a i-tou hlavou pohne doprava, jestliže $D_i = R$, nebo doleva, jestliže $D_i = L$, nebo se nepohne, jestliže $D_i = S$.

Jestliže $\delta(q, X, a)$ není definováno, pak se M zastaví.

M se zastaví úspěšně právě tehdy, když vstoupí do akceptující (koncového) stavu $q \in F$.

Třídy založené na pravděpodobnostních algoritmech

Příklad.

Je dán RTM M, kde $Q = \{q_0, q_1, q_2, q_3, q_4\}$, $\Gamma = \{0, 1, B\}$, $F = \{q_4\}$ a přechodová funkce δ je definována tabulkou:

Třídy založené na pravděpodobnostních algoritmech

	$0,0$	$1,0$	$0,1$
$\rightarrow q_0$	$(q_1, 0, R, S)$	$(q_2, 1, R, S)$	$(q_3, 0, S, R)$
q_1	$(q_1, 0, R, S)$	—	—
q_2	—	$(q_2, 1, R, S)$	—
q_3	$(q_3, 0, R, R)$	—	—
$\leftarrow q_4$	—	—	—

	$1,1$	$B,0$	$B,1$
$\rightarrow q_0$	$(q_3, 1, S, R)$	—	—
q_1	—	(q_4, B, S, S)	—
q_2	—	(q_4, B, S, S)	—
q_3	$(q_3, 1, R, R)$	(q_4, B, S, S)	(q_4, B, S, S)
$\leftarrow q_4$	—	—	—

Třída $\mathcal{RP}$

Jazyk L patří do $\mathcal{RP}$ iff existuje RTM M takový, že:

1. Jestliže $w \notin L$, pak M se zastaví v $q_f \in F$ s pravděpodobností 0.
2. Jestliže $w \in L$, pak M se zastaví v $q_f \in F$ s pravděpodobností aspoň $\frac{1}{2}$.
3. Existuje polynom $p(n)$ takový, že pro každý výpočet M (tj. pro každý obsahy náhodné pásky) M potřebuje nejvýše $p(n)$ kroků, kde n délka vstupního slova.

Třída $\mathcal{RP}$

Turingův stroj typu Monte-Carlo.

RTM splňující 1 a 2 je Turingův stroj typu Monte-Carlo.

Tvrzení.

Je dán jazyk $L \in \mathcal{RP}$, pak pro každou kladnou konstantu $0 < c < \frac{1}{2}$ existuje RTM M (algoritmus) s polynomiální složitostí takový, že:

1. Jestliže $w \notin L$, pak M skončí v $q_f \in F$ s pravděpodobností 0.
2. Jestliže $w \in L$, pak M skončí v $q_f \in F$ s pravděpodobností alespoň $1 - c$.

Třída $\mathcal{ZPP}$

Jazyk L patří do $\mathcal{ZPP}$ iff existuje RTM M takový, že:

1. Jestliže $w \notin L$, pak M skončí v $q_f \in F$ s pravděpodobností 0.
2. Jestliže $w \in L$, pak M skončí $q_f \in F$ s pravděpodobností 1.
3. Střední hodnota počtu kroků M během jednoho výpočtu nad vstupním slovem délky n je $p(n)$, kde $p(n)$ je vhodný polynom.

Třída $\mathcal{ZPP}$

Turingův stroj typu Las Vegas.

RTM, které splňuje všech tři podmínky, je Las Vegas Turingův stroj.

Tvrzení.

Jestliže jazyk L patří do $\mathcal{ZPP}$, pak také jeho doplněk $\overline{L}$.

Třída co-$\mathcal{RP}$.

Jazyk L patří do třídy co-$\mathcal{RP}$, jestliže jeho doplněk $\overline{L}$ patří do třídy $\mathcal{RP}$.

Věta.

$$\mathcal{ZPP} = \mathcal{RP} \cap \text{ co-}\mathcal{RP}.$$

Věta.

Platí

$$\mathcal{P} \subseteq \mathcal{ZPP}, \quad \mathcal{RP} \subseteq \mathcal{NP}, \quad \text{co-}\mathcal{RP} \subseteq \text{ co-}\mathcal{NP}.$$