Teorie algoritmů — 11. týden

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

28. 4. 2026

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 B;
- 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
$M = (Q, \Sigma, \Gamma, \delta, q_0, B, F)$, kde

- Q, Σ, Γ, q_0, B a F mají stejný význam jako v případě TM.
- přechodová funkce δ je parciální zobrazení $(Q \setminus F) \times \Gamma \times \{0, 1\}$ 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 obsah 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

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

Nerozhodnutelnost

Rekurzivně spočetné (v angličtině Recursively Enumerable) jazyky.

Jazyk L je rekurzivně spočetný, označujeme RS (též RE), jestliže existuje Turingův stroj M, který přijímá jazyk L, tj. pro který $L = L(M)$.

Rekurzivní jazyky.

Jazyk L je rekurzivní, jestliže existuje Turingův stroj M, který rozhoduje jazyk L.

Nerozhodnutelnost

Poznámka.

Jazyky, které nejsou rekurzivní, se také nazývají algoritmicky neřešitelné nebo nerozhodnutelné. Podobně mluvíme o nerozhodnutelných nebo algoritmicky neřešitelných úlohách. Rozhodovací úloha se obvykle nazývá nerozhodnutelná, termín algoritmicky neřešitelná se používá obvykle pro optimalizační úlohy.

Tvrzení.

Je-li L rekurzivní jazyk, pak je rekurzivní i jeho doplněk $\overline{L}$.

Tvrzení.

Jestliže jazyk L i jeho doplněk $\overline{L}$ jsou oba rekurzivně spočetné, pak jsou i rekurzivní.

Nerozhodnutelnost

Věta.

Je dán jazyk L, pak nastane jedna z následujících možností:

- L a $\overline{L}$ jsou oba rekurzivní.
- Jeden z jazyků L a $\overline{L}$ je rekurzivně spočetný a druhý není rekurzivně spočetný.
- L a $\overline{L}$ nejsou rekurzivně spočetné.

Nerozhodnutelnost

Kód Turingova stroje.

Máme Turingův stroj $M = (Q, \Sigma, \Gamma, \delta, q_0, B, F)$, kde

- $Q = \{q_1, q_2, \ldots, q_n\}$,
- $\Sigma = \{0, 1\}$,
- $\Gamma = \{X_1, X_2, \ldots, X_m\}$, zde $X_1 = 0$, $X_2 = 1$ a $X_3 = B$,
- $q_0 = q_1$,
- $F = \{q_2\}$.
- Označme $D_1 := R$ a $D_2 := L$.

Nerozhodnutelnost

Jedné hodnotě přechodové funkce δ

$$\delta(q_i, X_j) = (q_k, X_l, D_r)$$

přiřadíme následující slovo

$$t = 0^i 10^j 10^k 10^l 10^r.$$

Kód M, značíme ho $\langle M \rangle$, je

$$\langle M \rangle = 111\, t_1\, 11\, t_2\, 11 \ldots 11\, t_p\, 111,$$

kde $t_1, \ldots, t_p$ jsou slova odpovídající všem hodnotám přechodové funkce M.

Nerozhodnutelnost

Seřazení binárních slov do posloupnosti je možné na příklad takto:

Dané binární slovo w bude na pozici k, kde k je přirozené číslo s binárním zápisem $1w$.

Výše jsme vlastně popsali uspořádání nejprve podle délky a pak pro slova stejné délky lexikografické uspořádání.

Konvence.

Jestliže binární slovo w nemá tvar kódu nějakého Turingova stroje, považujeme ho za kód Turingova stroje M, který nemá definovaný žádný přechod, tedy nepřijímá žádné slovo.

Nerozhodnutelnost

Diagonální jazyk.

Diagonální jazyk L_d je definován:

$$L_d = \{\langle M \rangle \mid \ M \text{ nepřijímá } w = \langle M \rangle\}.$$

Věta.

Neexistuje Turingův stroj, který by přijímal diagonální jazyk L_d.
Jinými slovy, $L_d \neq L(M)$ pro každý Turingův stroj M.