Teorie algoritmů — 10. týden

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

21. 4. 2026

Třída co-$\mathcal{NP}$

Definice.

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

Rozhodovací úloha $\mathcal{U}$ patří do třídy co-$\mathcal{NP}$, jestliže jazyk $L_{\mathcal{U}}$ patří do co-$\mathcal{NP}$.

Příklad.

Nesplnitelnost booleovských formulí v CNF.

Třída co-$\mathcal{NP}$

Není známo, zda co-$\mathcal{NP} = \mathcal{NP}$.

Lemma.

Máme dva jazyky L_1 a L_2 pro které $L_1 \lhd_p L_2$. Pak také platí $\overline{L_1} \lhd_p \overline{L_2}$.

Tvrzení.

Platí co-$\mathcal{NP} = \mathcal{NP}$ právě tehdy, když existuje $\mathcal{NP}$ úplný jazyk L pro který $\overline{L}$ je ve třídě $\mathcal{NP}$.

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

$$\mathcal{P}\text{SPACE} = \mathcal{NP}\text{SPACE}.$$

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 ⊢ J then return TRUE
         else return FALSE
   end
   else (rekursivní část)
         for každé ID K do
         if REACH(I, K; ⌊m/2⌋) a REACH(K, J; ⌈m/2⌉) then
               return TRUE
         return FALSE
   end
end
```

Pravděpodobnostní algoritmy

Miller-Rabinův test prvočíselnosti

Jedná se o pravděpodobnostní algoritmus, který pro dané velké liché číslo N:

- Je-li N prvočíslo, tak to algoritmus vždy potvrdí.
- Je-li N složené, tak to algoritmus potvrdí s pravděpodobností alespoň $0,5$.

Pravděpodobnostní algoritmy

Vstup: Velké liché číslo N

Výstup: „prvočíslo“, „složené“

1. Vypočítáme $N - 1 = 2^r\, m$, kde m je liché.
2. Vybereme náhodně $a \in \{1, 2, \ldots, N-1\}$
   Je-li a^m mod N rovno 1, výstup „prvočíslo“.
3. Spočítáme a^{2m} mod N, $a^{2^2\, m}$ mod N,..., $a^{2^r\, m}$ mod N.
4. Je-li $a^{2^r\, m}$ mod N různé od 1, výstup „složené“.
5. Vezmeme $b = a^{2^k\, m}$ mod N poslední, které není 1.
   Je-li $b = -1$, výstup „prvočíslo“, jinak výstup „složené“.

Pravděpodobnostní algoritmy

Věta. Jestliže Miller Rabinův test prvočíselnosti dá výstup „složené“, pak N je složené.

Jestliže Miller Rabinův test prvočíselnosti dá výstup „prvočíslo“, tak N je prvočíslo s pravděpodobností větší než $0,5$.