

TAL přednáška
30.4.2019

Jazyk L_p a L_S : L_p je jazyk všech prvočísel počínaje binární.
 L_S je jazyk všech složených čísel počínaje binární.
 Předpokládejme "1" do L_p , potom máme $L_S = L_p$, $\overline{L_S} = \overline{L_p}$

Tvrzení: Jazyk L_S leží ve třídě NP

Zdůvodnění: Ještě říkáme, že n je složené, snadno! To, že má dělíteli r , pro nějž platí $1 < r < n$. Známe-li nejmenšího dělíteli r , jsme schopni dělením čísla n číslem r ověřit, že n je opravdu složené číslo. Pro prvočíslo žádoucí faktor dělitel nelze existovat. Při ověřování čísla n gitemyeme počty čísla r , kde $k = \lg(n)$ je délka binárního slova, a $r \in O(k)$. Faktorů r je exponenciálně.

Důsledek: Jazyk L_p je ve třídě co-NP

Tvrzení: Jazyk L_p leží ve třídě NP a coNP

Důsledek: Jazyk L_S leží ve třídě co-NP.

Jazyky L_p a L_S leží v průniku tříd NP a coNP

Miller-Rabinův test prvočiselnosti: Pokud n je prvočíslo, výsledek ANO, pokud n není prvočíslo, výsledek ANO nebo NE. Odpověď NE je vždy správná, odpověď ANO je správná s pravděpodobností aspoň $\frac{1}{2}$.

Budeme potřebovat algebry: možna

- $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ je slyšitelně třídič modulo n
- $a \oplus b = c$, kde $c = (a+b) \text{ mod } n$
- $a \odot b = c$, kde $c = (a \cdot b) \text{ mod } n$
- $(\mathbb{Z}_n, \oplus, 0)$ je komutativní grupa.
- $(\mathbb{Z}_n, \odot, 1)$ je monoid
- Malá Fermatova věta: $a^{p-1} \equiv 1 \pmod{n}$
- Je-li H podgrupa grupy G , tak $|H|/|G|$
- operace sčítání, nasobení, množením a dělení tvorí polynomickou

Algoritmus:

1. spočítáme $n-1 = 2^l \cdot m$, kde m je liché
2. náhodně vybereme $a \in \{0, 1, 2, \dots, n-1\}$
3. spočítáme $a^m \pmod{n}$. Ještě říkáme $a^m = 1$, výsledek je ANO
ještě říkáme $a^m \neq 1$, pokračujeme
4. spočítáme a^{2m} . Ještě říkáme $a^{2m} \neq 1$, výsledek je NE
5. opakování možnosti (a^m) na druhou. Vrátíme k faktoru, že $a^{2^k m} \neq 1$, ale $a^{2^{k+1} m} = 1$. Ještě říkáme $a^{2^k m} = -1$, výsledek je ANO. Jinak je výsledek NE.

Věta: Ještě říkáme pro výsledek n dle MR algoritmu výsledek NE, pak je n složné!

Dk: Výsledek NE musíme doslat v krok 4 nebo 5.

Krok 4: $a^{2^k m} = a^{n-1} = 1$, dle Fermatovy věty pro a respektive s n . Pokud to všechno jde, pak je a, n soudobé, a tedy n není prvočíslo.

Krok 5: $a^{2^k m} = x$, $a^{2^{k+1} m} = x^2 = 1$, $x \neq 1$. Máme $x^2 = 1$, ale v této možnosti faktor polynomu pouze dva kořeny, 1 a -1. Pokud tedy $x \neq 1$, nejdé v této možnosti a a n ji složené.

Věta: Je-li n složné, doskáhne odpověď ANO s pravděpodobností $\leq \frac{1}{2}$.

Dk: spočítáme, kolik je a , která dají správnou odpověď. $a \in \{1, 2, \dots, n-1\}$

- když a je soudobé s n : nemůže doshat odpověď ANO
- když a je nesoudobé s n , pak a má inverzi, tj. $a^t = 1$ pro $t > 0$, $a \cdot a^{-1} = 1$, $a^{-1} = a^{t-1}$

- když n je Carmichaelovo, pak platí, že $a^{n-1} = 1$. Důkaz pro tato čísla je těžký, když ho vysvětlíme, je v MKR.
- když n není Carmichaelovo, pak existuje a neoddělné s m , že $a^{n-1} \neq 1$

Uvažme K množinu všech a neoddělných s n , kde $a^{n-1} = 1$, $K = \{a \mid a \in \mathbb{Z}_{n-1}^*\}$, $\gcd(a, n) = 1$, $a^{n-1} = 1\}$. $(K, \cdot, 1)$ je podgrupa, přitom $|K| / |\mathbb{Z}_n^*|$, $K \subseteq \mathbb{Z}_n^*$

$$\frac{|\mathbb{Z}_n^*|}{|K|} \geq 2, \text{ tj. } |\mathbb{Z}_n^*| \geq 2 \cdot |K| \Rightarrow \text{Pro } \forall a \notin \mathbb{Z}_n^* \text{ neto } a \in \mathbb{Z}_n^* \rightarrow K \text{ dostane mezi správnou odpověď}$$

Randomizovaný Turingův stroj: TM se dvěma páskami, kde první je stejná jako páška běžného TM, a druhá páška obsahuje náhodnou posloupnost 0 a 1. Na rozdíl od běžného TM má hlava tři instrukce: L, R a S (stří).

Pr: Je dán RTM M , kde $Q = \{q_0, q_1, q_2, q_3, q_F\}$, $\Gamma = \{0, 1, B\}$ a S daná tabulkou

	0, 0	1, 0	0, 1	1, 1	B, 0	B, 1
q_0	$q_1, 0, R, S$	$q_2, 1, R, S$	$q_3, 0, S, R$	$q_3, 1, S, R$	—	—
q_1	$q_1, 0, R, S$	—	—	—	q_F, B, S, S	—
q_2	—	$q_2, 1, R, S$	—	—	—	q_F, B, S, S
q_3	$q_3, 0, R, R$	—	—	$q_3, 1, R, R$	q_F, B, S, S	q_F, B, S, S
q_F	—	—	—	—	—	—

← (první páška, náhodná páška)

posuny hlav jsou dané lamy v horní řadě pořadí

na náhodnou pášku se napsí!

Tento RTM má následné funkce podle prvního libu náhodné pášky:

- první bit je nula: na vstupu je slovo 0^n (stav q_1) neto 1^n (stav q_2)
- první bit je jedna: na vstupu je stejné slovo jako v náhodné posloupnosti (q_3)

- Jaká je pravděpodobnost, že M se zastaví v q_F ?

- pro $w = \emptyset$: pravděpodobnost je nula, proto $p = 0$
- pro $w = 0^n$ nebo $w = 1^n$ ← první bit = 0: $\frac{1}{2} \cdot 1 = \frac{1}{2}$ první bit = 1: $\frac{1}{2} \cdot (\frac{1}{2})^{|w|} = \frac{1}{2} \cdot \frac{1}{2^{|w|}}$ $p = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2^{|w|+1}}$
- pro $|w|_0 > 0, |w|_1 > 0$: ← první bit = 0: $\frac{1}{2} \cdot 0 = 0$ první bit = 1: $\frac{1}{2} \cdot \frac{1}{2^{|w|}} = \frac{1}{2^{|w|+1}}$ $p = \frac{1}{2}$

Definice: Jazyk L patří do třídy RP (Randomized Polynomial), jestliže existuje RTM M takový,

- 1) Jestliže $w \notin L$, pak M se zastaví v q_F a $p = 0$
- 2) Jestliže $w \in L$, pak M se zastaví v q_F a $p \geq \frac{1}{2}$
- 3) Existuje polynom $p(n)$, že když napsíte M se zastaví najmíň po $p(n)$ kroích.

Pr: Miller-Rabinův test a třída RP

Když n je prvočíslo, může mít správnou odpověď NE
Když n je složené, dostane odpověď NE s pravděpodobností $\geq \frac{1}{2}$

L_S je třída složených čísel
 $L_S \in RP$

Definice: RTM splňující podmínky 1 a 2 nazýváme stroj typu Monte Carlo.

Tvrdění: Je dán jazyk $L \in RP$. Pak pro každou konstantu $0 < c < \frac{1}{2}$ existuje ← RTM s polynomickou složitostí takový, že: Monte Carlo TM nemůže být polynomický

- 1) Jestliže $w \notin L$, pak M skončí v q_F s pravděpodobností 0.
- 2) —||— $w \in L$, —||— aranž. $1-c$.

Dokazování správnosti: Uvažme RTM M' typu Monte Carlo s polynomickou složitostí. Zde je $w \in L(M')$, udělá cyklu s pravd. 0. Jinak udělá cyklu s pravd. nejmíň $\frac{1}{2}$.

Takovém TM M opakovaně spustíme M' . Pokud M' rozhodne ANO, konkrétně i M ANO. Jinak spustíme M' znova.

Při k spuštěních je cykla $< \frac{1}{2^k} < c$, $\frac{1}{c} < 2^k$, $\lg(\frac{1}{c}) \leq k$.

Definice: Jazyk L patří do třídy ZPP (zero-error probabilistic polynomial), pokud existuje RTM M takový, že:

- 1) Ještě $w \notin L$, shod M se nejprve zadání s pravděpodobností 0.
- 2) Ještě $w \in L$,
- 3) Hlavní hmotnost počtu kroků M na jednom řešení je $p(n)$, kde $p(n)$ je polynom a n je délka vstupního slova.
a M není déle čtyřnáct krát delší, než je délka vstupního slova.

Definice: RTM splňující podmínky níže se nazývá shod typu Las Vegas.

Tvrzení: Ještě L patří do ZPP, pak i \bar{L} patří do ZPP. (prohodíme konecovou mohoucí hodiny)

Definice: Jazyk L patří do třídy co-RP iff \bar{L} patří do třídy RP.

Věta: Platí: $PS \subseteq ZPP$, $RP \subseteq NP$, $co\text{-}RP \subseteq co\text{-}NP$.

Věta: $ZPP = RP \cap co\text{-}RP$. Když tedy $RP = co\text{-}RP$, tak $ZPP = RP$.
dokaz bude příště.