Riešenie prvej prémiovej úlohy

Peter Kostolányi

18. decembra 2017

Zadanie. Nájdite jazyk $L \subseteq \{a\}^*$ taký, že jazyk L^* nie je regulárny, alebo dokážte, že taký jazyk neexistuje.

Riešenie. Dokážeme, že taký jazyk neexistuje. Nech teda $L \subseteq \{a\}^*$ je jazyk. Ukážeme, že jeho iterácia L^* musí patriť do $\mathscr{R}$. Ak $L \in \{\emptyset, \{\varepsilon\}\}$, tak $L^* = \{\varepsilon\} \in \mathscr{R}$. Nech teda $L \notin \{\emptyset, \{\varepsilon\}\}$.

Nech d je najväčší spoločný deliteľ čísel z množiny $E_L = \{k \in \mathbb{N} \mid a^k \in L\}$. Ak potom $w = a^m$ patrí do L^*, musí platiť $w = a^m = a^{k_1} \dots a^{k_s}$, kde $a^{k_1}, \dots, a^{k_s}$ sú slová z L; pre číslo m teda platí $m = k_1 + \ldots + k_s$, kde $k_1, \dots, k_s$ patria do E_L. V dôsledku toho ľahko vidieť, že číslo d je deliteľom čísla m. Pre jazyk L^* teda platí $L^* \subseteq \{a^{nd} \mid n \in \mathbb{N}\} = \{a^d\}^*$.

V nasledujúcom dokážeme, že existuje $n_0 \in \mathbb{N}$ také, že *všetky* slová a^{nd} s $n \geq n_0$ patria do L^*. Potom už bude dôkaz hotový, keďže z uvedeného vyplýva, že $L^* = \{a^d\}^* \cap L_{fin}^C$, kde L_{fin} je konečný jazyk – jazyk L^* je teda regulárny vďaka regularite všetkých konečných jazykov a uzavretosti triedy $\mathscr{R}$ na iteráciu, prienik a komplement.

Keďže d je najväčší spoločný deliteľ čísel z množiny E_L, nutne musí existovať $r \in \mathbb{N}$ a čísla $d_1, \dots, d_r \in E_L$ s najväčším spoločným deliteľom d.[1] Dokážeme, že pre každé $n \geq d_1 \cdot \ldots \cdot d_r$ deliteľné číslom d existujú čísla $i_1, \dots, i_r \in \mathbb{N}$ také, že $n = i_1 d_1 + \ldots + i_r d_r$. Indukciou na r.

1. Ak $r = 1$, tak $d_1 = d$ a tvrdenie je triviálne.

2. Nech tvrdenie platí pre $r = t$. Ukážeme, že platí aj pre $r = t + 1$.

   Nech teda $r = t+1$ a $n' = d_1 \cdot \ldots \cdot d_t$. Bez ujmy na všeobecnosti predpokladajme, že najväčší spoločný deliteľ čísel n' a d_{t+1} je d; čísla n'/d a d_{t+1}/d sú teda nesúdeliteľné.

   Pre $i = 0, \dots, n'/d - 1$ označme

   $$p(i) := n/d - i d_{t+1}/d.$$

   Keby existovali čísla $i_1, i_2 \in \{0, \dots, n'/d-1\}$ také, že $i_1 < i_2$ a $p(i_1) \equiv p(i_2) \pmod{n'/d}$, mali by sme $i_1 d_{t+1}/d \equiv i_2 d_{t+1}/d \pmod{n'/d}$, a teda číslo $(i_2 - i_1) d_{t+1}/d$ by muselo byť deliteľné číslom n'/d. Keďže sú čísla n'/d a d_{t+1}/d nesúdeliteľné, musí byť číslom n'/d deliteľné číslo $i_2 - i_1$. To je ale spor, keďže $0 \leq i_2 - i_1 \leq n'/d - 1$.

   Čísla $p(0), \dots, p(n'/d - 1)$ teda musia mať po dvoch rôzne zvyšky modulo n'/d. Keďže zvyškov je rovnako veľa ako čísel, musí existovať aj $j \in \{0, \dots, n'/d - 1\}$ také, že platí $p(j) \equiv 0 \pmod{n'/d}$. Inými slovami: číslo n'/d musí deliť číslo $n/d - j d_{t+1}/d$. Preto existuje $j' \in \mathbb{N}$ také, že $j' n'/d = n/d - j d_{t+1}/d$, a teda $n/d = j d_{t+1}/d + j' n'/d$, z čoho

   $$n = j' n' + j d_{t+1}. \tag{1}$$

   Z indukčného predpokladu potom vyplýva existencia čísel $i'_1, \dots, i'_t$ takých, že

   $$n' = i'_1 d_1 + \ldots + i'_t d_t. \tag{2}$$

   Z (1) a (2) nakoniec dostávame

   $$n = j' i'_1 d_1 + \ldots + j' i'_t d_t + j d_{t+1}$$

   a tvrdenie je dokázané pre $i_1 = j' i'_1, \dots, i_t = j' i'_t$ a $i_{t+1} = j$.

Nech teraz $n_0 := d_1 \cdot \ldots \cdot d_r/d$. Ukážeme, že pre všetky $n \geq n_0$ platí $a^{nd} \in L^*$. Skutočne, vďaka dokázanému existujú $i_1, \dots, i_r \in \mathbb{N}$ tak, že $nd = i_1 d_1 + \ldots + i_r d_r$. Platí teda $a^{nd} = (a^{d_1})^{i_1} \dots (a^{d_r})^{i_r}$. Keďže navyše $d_1, \dots, d_r \in E_L$, nutne $a^{d_1}, \dots, a^{d_r} \in L$, a teda $a^{nd} \in L^*$. □

[1] Takéto čísla možno nájsť napríklad nasledovne: nech d_1 je ľubovoľný prvok E_L. Ak $d_1 = d$, stačí vziať $r = 1$. Ak $d_1 > d$, nutne musí existovať $d_2 \in E_L$ také, že najväčší spoločný deliteľ d'_2 čísel d_1 a d_2 je menší ako d_1. Ak $d'_2 = d$, stačí vziať $r = 2$. Ak $d'_2 > d$, nutne musí existovať $d_3 \in E_L$ také, že najväčší spoločný deliteľ d'_3 čísel d_1, d_2 a d_3 je menší ako d'_2, atď. Je zrejmé, že pokračovaním v tomto procese možno skonštruovať nanajvýš konečnú postupnosť deliteľov $d_1 > d'_2 > d'_3 > \ldots > d'_r$, pričom nutne $d'_r = d$ (alebo $d_1 = d$, ak $r = 1$).