Riešenia tretej sady bodovaných domácich úloh

29. novembra 2017

Úloha 1. Zostrojte nedeterministický alebo deterministický konečný automat akceptujúci jazyk

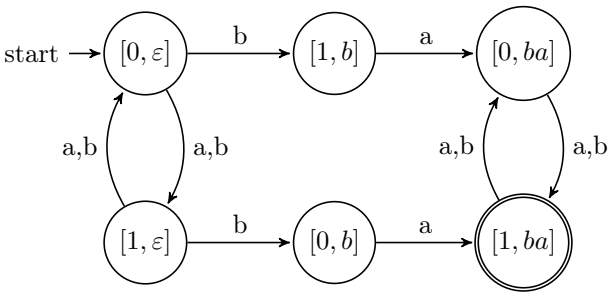
$$L = \{w \in \{a,b\}^* \mid |w| \equiv 1 \ (mod\ 2) \wedge w \textit{ obsahuje podslovo } ba\}.$$

Správnosť svojej konštrukcie *poriadne* dokážte.

Riešenie. Pripomeňme, že symbolom $\oplus$ označujeme „sčítanie modulo 2" a táto operácia je ekvivalentná logickej operácii XOR. Jazyk budeme akceptovať nedeterministickým konečným automatom. Definujeme NKA $A = (K, \{a,b\}, \delta, [0,\varepsilon], \{[1,ba]\})$, kde $K = \{[i,u] \mid i \in \{0,1\}, u \in \{\varepsilon, b, ba\}\}$ a prechodová funkcia je definovaná nasledovne:

- $\forall i \in \{0,1\} : \delta([i,\varepsilon], a) = \{[i \oplus 1, \varepsilon]\}$
- $\forall i \in \{0,1\} : \delta([i,\varepsilon], b) = \{[i \oplus 1, \varepsilon], [i \oplus 1, b]\}$
- $\forall i \in \{0,1\} : \delta([i,b], a) = \{[i \oplus 1, ba]\}$
- $\forall i \in \{0,1\}, c \in \{a,b\} : \delta([i,ba], c) = \{[i \oplus 1, ba]\}$

Pre lepšiu čitateľnosť uvádzame aj diagram automatu A.



Pred tým, ako prejdeme k dôkazu správnosti našej konštrukcie sa chvíľku zamyslime nad tým, ako náš automat funguje. Jeho stavy sú dvojice, v ktorých si náš automat pamätá dve veci. V prvej zložke stavu si pamätá dĺžku dosial spracovanej časti slova, presnejšie jej zvyšok po delení dvomi. V druhej zložke si pamätá, akú časť nami hladaného podslova už videl. Náš automat funguje tak, že najprv strieda stavy $[0,\varepsilon]$ a $[1,\varepsilon]$, potom si nedeterministicky tipne, kedy už môže ísť overiť, že nasleduje nami hľadané podslovo ba. Ak si tipol správne, tak najprv prejde do stavu $[0,b]$ resp. $[1,b]$ a z neho následne do stavu $[1,ba]$ resp. $[0,ba]$. Potom už automat môže byť istý, že vstup obsahuje podslovo ba a iba strieda stavy $[0,ba]$ a $[1,ba]$ aby overil, že dĺžka slova modulo 2 je naozaj 1. Takže poďme dokázať, že $L(A) = L$. Rovnosť dokážeme dôkazom oboch inklúzií.

$\subseteq$: Dokážeme sadu invariantov, z ktorých vyplynie $L(A) \subseteq L$.

Prvý invariant bude dokazovať, voľne povedané, že ak skončí výpočet v nejakom stave, tak prvá zložka stavu nám hovorí, koľko je dĺžka spracovaného slova modulo 2. Formálne dokážeme:

(a) $\forall w \in \{a,b\}^*, [l,v] \in K : ([0,\varepsilon], w) \vdash^* ([l,v], \varepsilon) \Rightarrow |w| \equiv l \pmod 2$

Dokážeme indukciou na dĺžku výpočtu.

1° Ak $([0,\varepsilon], w) \vdash^0 ([l,v], \varepsilon)$, potom nutne $w = \varepsilon$ a $[l,v] = [0,\varepsilon]$, teda platí $|w| = 0 = l$ a teda báza je dokázaná.

2° Predpokladajme, že tvrdenie platí pre výpočty dĺžky n a dokážme tvrdenie pre výpočty dĺžky $n+1$. Nech $([0,\varepsilon],w) \vdash^{n+1} ([l,v],\varepsilon)$. Nech $u \in \{a,b\}^*$, $c \in \{a,b\}$ a platí $w = uc$. Teda výpočet sa dá rozpísať ako $([0,\varepsilon],uc) \vdash^{n} ([l_1,v_1],c) \vdash ([l,v],\varepsilon)$. Tu sa na chviľku zastavme. Posledné tvrdenie platí iba vďaka tomu, že v prechodovej funkcii nemáme žiadne prechody na ε, lebo inak by posledný krok výpočtu mohol byť na ε, prípadne všetky kroky mohli byť na epsilon a w sa ani nedá zapísať ako uc. Takéto „rozpisovanie vstupného slova a výpočtu" budeme v pokračovaní dôkazu používať ešte viac krát. Uvedomme si, že vždy to môžme tak priamočiaro spraviť iba vďaka tomu, že automat neobsahuje žiadne prechody na ε. Všimnime si, že pre prechodovú funkciu nám platí nasledovné:

$$\forall [k_1,v_1] \in K, [k_2,v_2] \in K, c \in \{a,b\} : [k_2,v_2] \in \delta([k_1,v_1],c) \Rightarrow k_2 = k_1 \oplus 1$$

Teda na základe toho, ako vyzerá posledný krok výpočtu musí platiť $l = l_1 \oplus 1$. Z prvej časti výpočtu „od začiatku až po predposledný krok" a IP nám vyplýva, že $|u| \equiv l_1 \pmod 2$. Teda musí platiť $|uc| \equiv l_1 \oplus 1 \pmod 2$. Dajúc do kopy predchádzajúce nám platí $|uc| \equiv l \pmod 2$. A kedže $w = uc$, tak sme s dôkazom tvrdenia (a) hotoví.

Ďalší invariant nám bude hovoriť o tom, že ak sa dopočítame do stavu $[hocico, b]$, tak slovo na vstupe muselo končiť symbolom b. Formálne:

(b) $\forall w \in \{a,b\}^*, l \in \{0,1\} : ([0,\varepsilon],w) \vdash^* ([l,b],\varepsilon) \Rightarrow \exists u \in \{a,b\}^* : w = ub$

Na dôkaz tohto invariantu nám stačí nasledovná úvaha. Nech $w \in \{a,b\}^*, l \in \{0,1\}$ a nech platí $([0,\varepsilon],w) \vdash^* ([l,b],\varepsilon)$. Zjavne tento výpočet musí byť nenulovej dĺžky. Nech $u \in \{a,b\}^*$, $c \in \{a,b\}$ a platí $w = uc$. Potom tento výpočet môžme zapísať nasledovne: $([0,\varepsilon],w) \vdash^* (q,c) \vdash ([l,b],\varepsilon)$ kde q je nejaký stav automatu A. Pozrime sa pozornejšie na posledný krok výpočtu. Ten krok vedie do stavu $[l,b]$. Teda na to aby sme ho mohli spraviť muselo platiť $[l,b] \in \delta(q,c)$. Z definície funkcie δ nám potom vyplýva, že nutne musí platiť $c = b$. A pre to platí $w = uc = ub$, čím sme skompletizovali dôkaz invariantu (b).

Ďalší invariant nám bude hovoriť o tom, že ak sa dopočítame do stavu $[hocico, ba]$, tak slovo na vstupe muselo obsahovať podslovo ba. Formálne:

(c) $\forall w \in \{a,b\}^*, l \in \{0,1\} : ([0,\varepsilon],w) \vdash^* ([l,ba],\varepsilon) \Rightarrow \exists u_1,u_2 \in \{a,b\}^* : w = u_1 ba u_2$

Dokážeme indukciou na dĺžku výpočtu.

1° Báza platí triviálne. Prečo? Uvedomme si, že pre žiadne slovo w nemôže platiť $([0,\varepsilon],w) \vdash^0 ([l,ba],\varepsilon)$. A teda v nami dokazovanej implikácii je „na ľavo FALSE".

2° Predpokladajme, že tvrdenie platí pre výpočty dĺžky n a dokážme tvrdenie pre výpočty dĺžky $n+1$. Nech $w \in \{a,b\}^*, l \in \{0,1\}$ a nech $([0,\varepsilon],w) \vdash^{n+1} ([l,ba],\varepsilon)$. Nech $u \in \{a,b\}^*$, $c \in \{a,b\}$ a platí $w = uc$. Teda výpočet sa dá rozpísať ako $([0,\varepsilon],uc) \vdash^{n} (q,c) \vdash ([l,ba],\varepsilon)$, kde q je nejaký stav automatu A. Z definície funkcie δ platí, že môžu nastať nasledovné dva prípady:

- $\exists l_1 \in \{0,1\} : q = [l_1,b]$, $c = a$.
  V tomto prípade nám z invariantu (b) vyplýva, že existuje slovo $v_1 \in \{a,b\}^*$ také, že $u = v_1 b$. Z predošlého vyplýva, že $w = ua = v_1 ba$, čo nám dokazuje platnosť invariantu v tomto prípade, pretože nami hľadané u_1, u_2 vieme zvoliť $u_1 = v_1, u_2 = \varepsilon$.
- $q = [l \oplus 1, ba]$, $c \in \{a,b\}^*$.
  V tomto prípade nám z IP vyplýva, že existujú slová $v_1, v_2 \in \{a,b\}^*$ také, že $u = v_1 ab v_2$. Teda platí $w = uc = v_1 ab v_2 c$. Teraz už naozaj ľahko vidno, že aj v tomto prípade invariant platí.

Nakoľko iné prípady nastať nemôžu, tak sme s dôkazom invariantu (c) hotoví.

Ako z dokázaných invariantov vyplýva nami dokazované $L(A) \subseteq L$? Nech $w \in L(A)$. Teda existuje nejaký akceptačný výpočet automatu A na slove w. Nakoľko automat A má jediný akceptačný stav $[1, ba]$, tento výpočet musí vyzerať nasledovne: $([0, \varepsilon], w) \vdash^* ([1, ba], \varepsilon)$. Z invariatnu (a) potom vyplýva, že $|w| \equiv 1 \pmod 2$ a z invariantu (c) vyplýva, že w obsahuje podslovo ba. Teda $w \in L$.

$\supseteq$: Potrebujeme dokázať $L \subseteq L(A)$.
Urobíme to tak, že pre ľubovoľné $w \in L$ zostrojíme akceptačný výpočet v automate A. Budeme si pomáhať nasledovným tvrdením (ktoré bude v skutočnosti takpovediac „dva v jednom"):

(d) $\forall w \in \{a, b\}^*, A \in \{\varepsilon, ba\}, l \in \{0, 1\} : |w| \equiv l \pmod 2 \Rightarrow ([0, A], w) \vdash^* ([l, A], \varepsilon)$

Tvrdenie (d) dokážeme indukciou vzhľadom na dĺžku slova w.

1° Ak platí $w = \varepsilon$, potom $|w| \equiv 0 \pmod 2$ a ľahko vidno, že platí $([0, A], w) \vdash^* ([0, A], \varepsilon)$.

2° Uvažujme ľubovoľné $w \in \{a, b\}^*$, ktoré je nenulovej dĺžky a predpokladajme, že tvrdenie platí pre všetky slová, ktoré sú kratšie ako w. Nech $u \in \{a, b\}^*$, $c \in \{a, b\}$ a platí $w = uc$. Nech $l_u \in \{0, 1\}$ a nech platí $|u| \equiv l_u \pmod 2$. Všimnime si, že potom nutne musí platiť $|w| \equiv l_u \oplus 1 \pmod 2$. Slovo u je zjavne kratšie ako slovo w, preto preň platí IP. Teda platí $([0, A], u) \vdash^* ([l_u, A], \varepsilon)$. Z prechdádzajúceho nám vyplýva $([0, A], uc) \vdash^* ([l_u, A], c)$. A z funkcie δ nám vyplýva $([l_u, A], c) \vdash ([l_u \oplus 1, A], \varepsilon)$. Dajúc dokopy predchádzajúce nám platí $([0, A], uc) \vdash^* ([l_u, A], c) \vdash ([l_u \oplus 1, A], \varepsilon)$. A nakoľko $w = uc$ a $|w| \equiv l_u \oplus 1 \pmod 2$, tak sme s dôkazom hotoví.

Teraz zostrojme akceptačný výpočet na ľubovolnom slove $w \in L$. Z toho, že $w \in L$ nám priamo vyplýva, že existujú slová $u, v \in \{a, b\}^*$ také, že $w = ubav$ a navyše $|w| \equiv 1 \pmod 2$.

Pred tým, ako formálne dotiahneme veci, sa chvíľku zamyslime. Z toho aká je dĺžka slova w nám vyplýva o dĺžkach slov u, v niečo. Konkrétne toľko, že súčet ich dĺžok musí dávať po delení 2 zvyšok 1. Teda alebo u je nepárnej dĺžky a v je párnej alebo vice-versa. Uvažujme prvý prípad, keď u je nepárnej dĺžky a v je párnej (pri druhom je úvaha analogická). V tomto prípade zostrojíme výpočet nasledovne - „zjeme"slovo u a skončíme v stave $[1, \varepsilon]$. Následne mám na vstupe podslovo ba. Teda prejdeme cez stav $[0, b]$ do stavu $[1, ba]$. Teraz nám už len ostáva „zjesť"slovo v. Kedže sa nachádzame v stave $[1, ba]$, tak s prehľadom slovo v dočítame taktiež v stave $[1, ba]$, ktorý je akceptačný. Poďme formálne.

Nakoľko $|w| \equiv 1 \pmod 2$, môžu nastať nasledovné dve možnosti:

- $|u| \equiv 1 \pmod 2$, $|v| \equiv 0 \pmod 2$.
  Potom vďaka tvrdeniu (d) platí $([0, \varepsilon], ubav) \vdash^* ([1, \varepsilon], bav)$. Vďaka funkcii δ vieme tento výpočet predĺžiť na $([0, \varepsilon], ubav) \vdash^* ([1, \varepsilon], bav) \vdash ([0, b], av) \vdash ([1, ba], v)$. Teraz môžu nastať dva prípady:
  - $|v| = 0$, teda $v = \varepsilon$ a niet ďalej čo dokazovať, lebo v tomto prípade sme už úspešne zostrojili akceptačný výpočet.
  - $|v| \geq 1$.
    Nech $v_1 \in \{a, b\}^*$, $c_1 \in \{a, b\}$ také, že $v = c_1 v_1$. Uvedomme si, že platí $|v_1| \equiv 1 \pmod 2$. V takom prípade vďaka funkcii δ a tvrdeniu (d) platí: $([1, ba], c_1 v_1) \vdash ([0, ba], v_1) \vdash^* ([1, ba], \varepsilon)$. Dajúc to do kopy s predchádzajúcim vieme zostrojiť výpočet $([0, \varepsilon], ubav) \vdash^* ([1, \varepsilon], bav) \vdash ([0, b], av) \vdash ([1, ba], v) \vdash^* ([1, ba], \varepsilon)$. Teda aj v tomto prípade sme úspešne zostrojili akceptačný výpočet.
- $|u| \equiv 0 \pmod 2$, $|v| \equiv 1 \pmod 2$.
  Potom vďaka tvrdeniu (d) platí $([0, \varepsilon], ubav) \vdash^* ([0, \varepsilon], bav)$. Vďaka funkcii δ vieme tento výpočet predĺžiť na $([0, \varepsilon], ubav) \vdash^* ([1, \varepsilon], bav) \vdash ([1, b], av) \vdash ([0, ba], v)$. No a na záver opäť vďaka tvrdeniu (d) vieme tento výpočet predĺžiť nasledovne: $([0, \varepsilon], ubav) \vdash^* ([1, \varepsilon], bav) \vdash ([1, b], av) \vdash ([0, ba], v) \vdash^* ([1, ba], \varepsilon)$. A teda vidno, že aj v tomto prípade sme úspešne zostrojili akceptačný výpočet.

Nakoľko sme rozobrali všetky možné tvary slova $w \in L$ a v každom prípade sme úspešne zostrojili akceptačný výpočet na slove w, tak ľahko vidno, že naozaj platí $L \subseteq L(A)$.

□

Úloha 2. Nech $A = (K, \Sigma, \delta, q_0, F)$ je ľubovoľný (deterministický alebo nedeterministický) konečný automat. Poriadne dokážte, že platí:

$$\forall p, q \in K \ \forall u, v \in \Sigma^* : (p, uv) \vdash_A^* (q, v) \Leftrightarrow (p, u) \vdash_A^* (q, \varepsilon)$$

Riešenie. Budeme dokazovať obe implikácie a obe budeme dokazovať indukciou na dĺžku výpočtu.

$\Rightarrow$:

1° Nech platí $(p, uv) \vdash_A^0 (q, v)$. Potom nutne $q = p, u = \varepsilon$. Teda lahko vidno, že platí $(p, \varepsilon) \vdash_A^* (p, \varepsilon)$, čo bolo treba dokázať.

2° Predpokladajme, že platí $\forall p, q \in K \ \forall u, v \in \Sigma^* : (p, uv) \vdash_A^n (q, v) \Rightarrow (p, u) \vdash_A^* (q, \varepsilon)$. Poďme dokázať tento výrok pre výpočty dĺžky $n + 1$. Nech teda $p, q \in K,\ u, v \in \Sigma^*$ a nech platí $(p, uv) \vdash_A^{n+1} (q, v)$. Uvažujme $c \in \Sigma \cup \{\varepsilon\},\ u_1 \in \Sigma^*, p_1 \in K$ také, že platí $u = cu_1$ a $(p, cu_1v) \vdash_A (p_1, u_1v) \vdash_A^n (q, v)$. Neformálne povedané, c je symbol alebo epsilon, ktorý sme „zožrali"v prvom kroku výpočtu a p_1 je stav, do ktorého sme sa potom dostali. Z $(p, cu_1v) \vdash_A (p_1, u_1v)$ vyplýva, že $p_1 \in \delta(p, c)$ ak uvažujeme NKA. Ak uvažujeme DKA tak $p_1 = \delta(p, c)$. Z $(p_1, u_1v) \vdash_A^n (q, v)$ a IP vyplýva $(p_1, u_1) \vdash_A^* (q, \varepsilon)$. Dajúc dokopy predchádzajúce nám platí $(p, cu_1) \vdash_A (p_1, u_1) \vdash_A^* (q, \varepsilon)$. Nakoľko $u = cu_1$, tak sme dokázali, čo bolo treba.

$\Leftarrow$:

1° Nech platí $(p, u) \vdash_A^0 (q, \varepsilon)$. Potom nutne $q = p, u = \varepsilon$. Teda lahko vidno, že pre ľuvolné $v \in \Sigma^*$ platí $(p, v) \vdash_A^* (p, v)$, čo bolo treba dokázať.

2° Predpokladajme, že platí $\forall p, q \in K \ \forall u, v \in \Sigma^* : (p, u) \vdash_A^n (q, \varepsilon) \Rightarrow (p, uv) \vdash_A^* (q, v)$. Poďme dokázať tento výrok pre výpočty dĺžky $n + 1$. Nech teda $p, q \in K,\ u \in \Sigma^*$ a nech platí $(p, u) \vdash_A^{n+1} (q, \varepsilon)$. Uvažujme $c \in \Sigma \cup \{\varepsilon\},\ u_1 \in \Sigma^*, p_1 \in K$ také, že platí $u = cu_1$ a $(p, cu_1) \vdash_A (p_1, u_1) \vdash_A^n (q, \varepsilon)$. Tak ako v prvej implikácii aj tu, neformálne povedané, c je symbol alebo epsilon, ktorý sme „zožrali"v prvom kroku výpočtu a p_1 je stav, do ktorého sme sa potom dostali. Z $(p, cu_1) \vdash_A (p_1, u_1)$ vyplýva, že $p_1 \in \delta(p, c)$ ak uvažujeme NKA. Ak uvažujeme DKA tak $p_1 = \delta(p, c)$. Z $(p_1, u_1) \vdash_A^n (q, \varepsilon)$ a IP vyplýva, že pre ľuvolné $v \in \Sigma^*$ platí $(p_1, u_1v) \vdash_A^* (q, v)$. Dajúc dokopy predchádzajúce nám platí $(p, cu_1v) \vdash_A (p_1, u_1v) \vdash_A^* (q, v)$. Nakoľko $u = cu_1$, tak sme dokázali, čo bolo treba.

□