Riešenia tretej sady domácich úloh

Peter Kostolányi

10. novembra 2022

Úloha 1. Nech $m \in \mathbb{N} - \{0\}$. Zostrojte (deterministický alebo nedeterministický) konečný automat akceptujúci jazyk

$$L_m = \{ucv \mid u, v \in \{a,b\}^*;\ \#_a(u) \equiv \#_a(v) \pmod m\}$$

(nad abecedou $\Sigma = \{a,b,c\}$). Poriadne dokážte správnosť svojej konštrukcie.

Riešenie. Dokážeme, že $L_m = L(A_m)$ pre nedeterministický[1] konečný automat $A_m = (K, \Sigma, \delta, q_0, F)$, kde $K = \mathbb{Z}_m \cup \mathbb{Z}_m^2$,

$$\begin{array}{llll}
\delta(p,a) = \{p+1\} & \forall p \in \mathbb{Z}_m, & \delta([p,q],a) = \{[p,q+1]\} & \forall p,q \in \mathbb{Z}_m,\\
\delta(p,b) = \{p\} & \forall p \in \mathbb{Z}_m, & \delta([p,q],b) = \{[p,q]\} & \forall p,q \in \mathbb{Z}_m,\\
\delta(p,c) = \{[p,0]\} & \forall p \in \mathbb{Z}_m, & \delta([p,q],c) = \emptyset & \forall p,q \in \mathbb{Z}_m,\\
\delta(p,\varepsilon) = \emptyset & \forall p \in \mathbb{Z}_m, & \delta([p,q],\varepsilon) = \emptyset & \forall p,q \in \mathbb{Z}_m,
\end{array}$$

$q_0 = 0$ a $F = \{[p,p] \mid p \in \mathbb{Z}_m\}$. Všetky operácie sčítania sú, samozrejme, modulo m. Rovnosť $L(A_m) = L_m$ vyplynie z nasledujúcich invariantov pre jednotlivé stavy automatu.

a) Pre $p \in \mathbb{Z}_m$ a $w \in \Sigma^*$ je $(0,w) \vdash^* (p,\varepsilon)$ práve vtedy, keď $w \in \{a,b\}^*$ a $\#_a(w) \equiv p \pmod m$.

b) Pre $p,q \in \mathbb{Z}_m$ a $w \in \Sigma^*$ je $(0,w) \vdash^* ([p,q],\varepsilon)$ práve vtedy, keď $w = ucv$, kde $u,v \in \{a,b\}^*$, $\#_a(u) \equiv p \pmod m$ a $\#_a(v) \equiv q \pmod m$.

Dokážeme teraz jednotlivé implikácie.

$\Rightarrow$: Indukciou vzhľadom na n dokážeme pre všetky $n \in \mathbb{N}$ nasledujúce dve tvrdenia:

a) Pre všetky $p \in \mathbb{Z}_m$ a $w \in \Sigma^*$ také, že $(0,w) \vdash^n (p,\varepsilon)$, je $w \in \{a,b\}^*$ a $\#_a(w) \equiv p \pmod m$.

b) Pre všetky $p,q \in \mathbb{Z}_m$ a $w \in \Sigma^*$ také, že $(0,w) \vdash^n ([p,q],\varepsilon)$, je $w = ucv$, kde $u,v \in \{a,b\}^*$, $\#_a(u) \equiv p \pmod m$ a $\#_a(v) \equiv q \pmod m$.

Pre $n = 0$ môžu byť predpoklady prvého tvrdenia pravdivé iba ak $p = 0$; v takom prípade nutne $w = \varepsilon$, čiže skutočne $w \in \{a,b\}^*$ a $\#_a(w) \equiv 0 \pmod m$. V druhom tvrdení nie sú pre $n = 0$ predpoklady splnené nikdy. Tvrdenia ako celok sú teda pravdivé.

Predpokladajme, že tvrdenia platia pre $n = k \in \mathbb{N}$ a uvažujme $n = k+1$.

Ak $p \in \mathbb{Z}_m$ a $w \in \Sigma^*$ je také, že $(0,w) \vdash^{k+1} (p,\varepsilon)$, musia existovať $s \in K$, $x \in \Sigma^*$ a $z \in \Sigma \cup \{\varepsilon\}$ také, že $w = xz$ a $(0,xz) \vdash^* (s,z) \vdash (p,\varepsilon)$; stade $p \in \delta(s,z)$. Buď teda $s = p-1$ a $z = a$, alebo $s = p$ a $z = b$. V prvom prípade je z indukčného predpokladu $x \in \{a,b\}^*$ a $\#_a(x) \equiv p-1 \pmod m$; teda aj $w = xa \in \{a,b\}^*$ a $\#_a(w) = \#_a(x)+1 \equiv p \pmod m$. V druhom prípade je $x \in \{a,b\}^*$ a $\#_a(x) \equiv p \pmod m$; preto aj $w = xb \in \{a,b\}^*$ a $\#_a(w) = \#_a(x) \equiv p \pmod m$.

Nech ďalej $p,q \in \mathbb{Z}_m$ a $w \in \Sigma^*$ sú také, že $(0,w) \vdash^{k+1} ([p,q],\varepsilon)$. Pre nejaké $s \in K$, $x \in \Sigma^*$ a $z \in \Sigma \cup \{\varepsilon\}$ potom $w = xz$ a $(0,xz) \vdash^* (s,z) \vdash ([p,q],\varepsilon)$. Nutne teda $[p,q] \in \delta(s,z)$, čo môže nastať v najviac troch rôznych prípadoch: pre $s = [p,q-1]$ a $z = a$, pre $s = [p,q]$ a $z = b$ a pokiaľ $q = 0$, tak aj pre $s = p$ a $z = c$.

Ak $s = [p,q-1]$ a $z = a$, je z indukčného predpokladu $x = ucv'$ pre nejaké $u,v' \in \{a,b\}^*$ také, že $\#_a(u) \equiv p \pmod m$ a $\#_a(v') \equiv q-1 \pmod m$; ak teda položíme $v = v'a$, je skutočne $w = ucv$, kde $u,v \in \{a,b\}^*$, $\#_a(u) \equiv p \pmod m$ a $\#_a(v) = \#_a(v')+1 \equiv q \pmod m$. Podobne ak $s = [p,q]$ a $z = b$, je $x = ucv'$ pre $u,v' \in \{a,b\}^*$ také, že $\#_a(u) \equiv p \pmod m$ a $\#_a(v') \equiv q \pmod m$; pre $v = v'b$ teda naozaj $w = ucv$, kde $u,v \in \{a,b\}^*$, $\#_a(u) \equiv p \pmod m$ a $\#_a(v) = \#_a(v') \equiv q \pmod m$. Ak napokon $q = 0$, $s = p$ a $z = c$, je z indukčného predpokladu $x \in \{a,b\}^*$, pričom $\#_a(x) \equiv p \pmod m$; pre $u = x$ a $v = \varepsilon$ preto naozaj $w = ucv$, pričom $\#_a(u) = \#_a(x) \equiv p \pmod m$ a $\#_a(v) = \#_a(\varepsilon) = 0 \equiv q \pmod m$.

[1] Konštruovaný automat bude v podstate deterministický, ale nebude mať úplnú prechodovú funkciu; budeme ho preto formálne považovať za nedeterministický konečný automat.

$\Leftarrow$: Dokážeme nasledujúce dve tvrdenia:

a) Pre všetky $p \in \mathbb{Z}_m$ a $w \in \{a,b\}^*$ spĺňajúce $\#_a(w) \equiv p \pmod m$ je $(0,w) \vdash^* (p,\varepsilon)$.

b) Pre všetky $p,q \in \mathbb{Z}_m$ a $u,v \in \{a,b\}^*$ spĺňajúce $\#_a(u) \equiv p \pmod m$ a $\#_a(v) \equiv q \pmod m$ je $(0,ucv) \vdash^* ([p,q],\varepsilon)$.

Prvé z tvrdení dokážeme indukciou vzhľadom na $|w|$. Ak $|w| = 0$, nutne $w = \varepsilon$, z čoho $p = 0$, a teda aj $(0,w) \vdash^* (p,\varepsilon)$. Nech teda tvrdenie platí pre všetky $w \in \{a,b\}^*$ dĺžky $k \in \mathbb{N}$ a uvažujme prípad, keď $w = x$ pre nejaké $x \in \{a,b\}^{k+1}$ také, že $\#_a(x) \equiv p \pmod m$. Pre nejaké $y \in \{a,b\}^k$ potom $x = ya$ alebo $x = yb$. V prvom prípade nutne $\#_a(y) \equiv p-1 \pmod m$ a z indukčného predpokladu tak dostávame $(0,y) \vdash^* (p-1,\varepsilon)$, z čoho $(0,x) = (0,ya) \vdash^* (p-1,a) \vdash (p,\varepsilon)$. V druhom je $\#_a(y) \equiv p \pmod m$ a vďaka indukčnému predpokladu teda $(0,y) \vdash^* (p,\varepsilon)$; z toho $(0,x) = (0,yb) \vdash^* (p,b) \vdash (p,\varepsilon)$.

Zostáva dokázať druhé tvrdenie, čo možno urobiť indukciou vzhľadom na $|v|$. Pre $|v| = 0$ nutne $v = \varepsilon$ a $q = 0$. Ako bezprostredný dôsledok prvého tvrdenia tak pre všetky $u \in \{a,b\}^*$ spĺňajúce $\#_a(u) \equiv p \pmod m$ skutočne dostávame $(0,ucv) = (0,uc) \vdash^* (p,c) \vdash ([p,0],\varepsilon) = ([p,q],\varepsilon)$. Predpokladajme teda, že tvrdenie platí pre všetky $v \in \{a,b\}^*$ dĺžky $k \in \mathbb{N}$ a uvažujme prípad, keď $v = x$ pre nejaké $x \in \{a,b\}^{k+1}$ také, že $\#_a(x) \equiv q \pmod m$. Pre nejaké $y \in \{a,b\}^k$ potom $x = ya$ alebo $x = yb$. V prvom prípade je $\#_a(y) \equiv q-1 \pmod m$ a z indukčného predpokladu tak pre všetky $u \in \{a,b\}^*$ spĺňajúce $\#_a(u) \equiv p \pmod m$ dostávame $(0,ucy) \vdash^* ([p,q-1],\varepsilon)$, z čoho $(0,ucx) = (0,ucya) \vdash^* ([p,q-1],a) \vdash ([p,q],\varepsilon)$. V druhom prípade je $\#_a(y) \equiv q \pmod m$ a z indukčného predpokladu teda pre všetky $u \in \{a,b\}^*$ spĺňajúce $\#_a(u) \equiv p \pmod m$ vyplýva $(0,ucy) \vdash^* ([p,q],\varepsilon)$, z čoho $(0,ucx) = (0,ucyb) \vdash^* ([p,q],b) \vdash ([p,q],\varepsilon)$.

Slovo $w \in \Sigma^*$ teraz patrí do jazyka $L(A_m)$ práve vtedy, keď existuje stav $s \in F$ taký, že $(0,w) \vdash^* (s,\varepsilon)$. Z definície množiny F vyplýva, že je táto podmienka ekvivalentná existencii $p \in \mathbb{Z}_m$ takého, že $(0,w) \vdash^* ([p,p],\varepsilon)$. To ale podľa dokázaného nastane práve vtedy, keď existuje $p \in \mathbb{Z}_m$ také, že $w = ucv$ pre nejaké $u,v \in \{a,b\}^*$ spĺňajúce $\#_a(u) \equiv p \pmod m$ a $\#_a(v) \equiv p \pmod m$. Táto situácia evidentne nastane práve vtedy, keď $w = ucv$ pre nejaké slová $u,v \in \{a,b\}^*$ spĺňajúce $\#_a(u) \equiv \#_b(v) \pmod m$ – čiže práve vtedy, keď $w \in L_m$. □

Úloha 2. Nech Σ je abeceda, $L \subseteq \Sigma^*$ jazyk a $x \in \Sigma^*$ slovo. *Ľavým kvocientom* jazyka L podľa slova x nazveme jazyk

$$x\backslash L = \{w \in \Sigma^* \mid xw \in L\}.$$

Nech ďalej $A = (K,\Sigma,\delta,q_0,F)$ je ľubovoľný deterministický konečný automat a $q \in K$ jeho stav. *Budúcnosťou stavu* q nazveme jazyk $\mathrm{fut}(q)$ všetkých slov, ktoré automat A akceptuje v prípade, že ich začne čítať zo stavu q – teda

$$\mathrm{fut}(q) = \{w \in \Sigma^* \mid \exists q_F \in F : (q,w) \vdash^* (q_F,\varepsilon)\}.$$

Dokážte, že:

a) Pre každý *deterministický* konečný automat $A = (K,\Sigma,\delta,q_0,F)$ a všetky $x \in \Sigma^*$ existuje stav $q \in K$ taký, že $x\backslash L(A) = \mathrm{fut}(q)$.

b) Pre každý regulárny jazyk $L \subseteq \Sigma^*$ je množina jazykov $\{x\backslash L \mid x \in \Sigma^*\}$ konečná.

Riešenie.

a) Keďže je automat A deterministický, pre každé slovo $x \in \Sigma^*$ existuje *práve jeden* stav $q_x \in K$ taký, že $(q_0,x) \vdash^* (q_x,\varepsilon)$. Dokážeme, že $\mathrm{fut}(q_x) = x\backslash L(A)$.

$\subseteq$: Nech $w \in \mathrm{fut}(q_x)$. Potom existuje stav $q_F \in F$ taký, že $(q_x,w) \vdash^* (q_F,\varepsilon)$, v dôsledku čoho tiež $(q_0,xw) \vdash^* (q_x,w) \vdash^* (q_F,\varepsilon)$. Teda $xw \in L(A)$, z čoho $w \in x\backslash L(A)$.

$\supseteq$: Nech $w \in x\backslash L(A)$. Potom $xw \in L(A)$, a teda existuje $q_F \in F$ také, že $(q_0,xw) \vdash^* (q_F,\varepsilon)$, čo možno vďaka jedinečnosti stavu q_x prepísať ako $(q_0,xw) \vdash^* (q_x,w) \vdash^* (q_F,\varepsilon)$. Teda $(q_x,w) \vdash^* (q_F,\varepsilon)$ a $w \in \mathrm{fut}(q_x)$.

b) Pre každý regulárny jazyk $L \subseteq \Sigma^*$ existuje deterministický konečný automat $A = (K, \Sigma, \delta, q_0, F)$ taký, že $L(A) = L$. Z tvrdenia dokázaného v predchádzajúcej podúlohe potom vyplýva, že

$$\{x\backslash L \mid x \in \Sigma^*\} = \{x\backslash L(A) \mid x \in \Sigma^*\} \subseteq \{\mathrm{fut}(q) \mid q \in K\},$$

pričom množina jazykov na pravej strane je očividne konečná. □