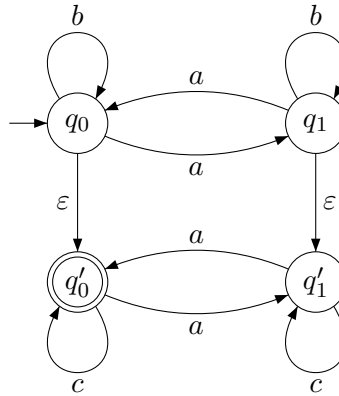


Riešené úlohy: konečné automaty

Peter Kostolányi

29. októbra 2026

Úloha 1. Nech $A = (K, \Sigma, \delta, q_0, F)$ je nedeterministický konečný automat s $K = \{q_0, q_1, q'_0, q'_1\}$, $\Sigma = \{a, b, c\}$, $F = \{q'_0\}$ a s prechodovou funkciou δ danou nasledujúcim diagramom.



- Nájdite a pomocou korektného množinového zápisu vyjadrite jazyk $L(A)$. Svoje tvrdenie nemusíte dokazovať.
- Pre každý stav q automatu A sformulujte invariant charakterizujúci jazyk všetkých slov $w \in \Sigma^*$ takých, že $(q_0, w) \vdash_A^* (q, \varepsilon)$.
- Zostrojte regulárnu gramatiku G takú, že $L(G) = L(A)$. Túto rovnosť netreba dokazovať v prípade použitia štandardnej konštrukcie; v opačnom prípade je dôkaz nutný.

Riešenie.

- Je $L(A) = \{uv \mid u \in \{a, b\}^*; v \in \{a, c\}^*; \#_a(uv) \equiv 0 \pmod{2}\}$. Ekvivalentne možno tento jazyk vyjadriť aj ako $L(A) = (aa)^* \sqcup b^*c^*$.
- Pre všetky $w \in \Sigma^*$ a $i \in \{0, 1\}$ je

$$(q_0, w) \vdash_A^* (q_i, \varepsilon) \iff w \in \{a, b\}^* \wedge \#_a(w) \equiv i \pmod{2}$$

a

$$(q_0, w) \vdash_A^* (q'_i, \varepsilon) \iff \exists u \in \{a, b\}^* \exists v \in \{a, c\}^* : w = uv \wedge \#_a(uv) \equiv i \pmod{2}.$$

- Štandardnou konštrukciou z prednášky dostávame regulárnu gramatiku $G = (N, T, P, \sigma)$, kde $N = \{q_0, q_1, q'_0, q'_1\}$, $T = \{a, b, c\}$, $\sigma = q_0$ a

$$\begin{aligned}
 P = \{ & q_0 \rightarrow aq_1 \mid bq_0 \mid q'_0 \\
 & q_1 \rightarrow aq_0 \mid bq_1 \mid q'_1 \\
 & q'_0 \rightarrow aq'_1 \mid cq'_0 \mid \varepsilon \\
 & q'_1 \rightarrow aq'_0 \mid cq'_1 \}.
 \end{aligned}$$

□

Úloha 2. Nech $m \in \mathbb{N}$ je ľubovoľné pevne dané prirodzené číslo. Zostrojte (deterministický alebo nedeterministický) konečný automat A_m akceptujúci jazyk

$$L_m = \{w \in \{a, b\}^* \mid \#_a(w) = m\}.$$

Správnosť svojej konštrukcie dokážte matematickou indukciou.

Riešenie. Dokážeme, že jazyk L_m zo zadania je akceptovaný deterministickým konečným automatom $A_m = (K, \Sigma, \delta, q_0, F)$, kde: $K = \{0, \dots, m+1\}$; $\Sigma = \{a, b\}$; pre všetky $q \in K$ je

$$\delta(q, a) = \begin{cases} q+1 & \text{ak } q \in \{0, \dots, m\}, \\ q & \text{ak } q = m+1, \end{cases}$$

$$\delta(q, b) = q;$$

$q_0 = 0$; a $F = \{m\}$.

Sformulujeme teraz invarianty, ktorých platnosť budeme dokazovať pre jednotlivé stavy automatu A_m . Pre všetky $q \in \{0, \dots, m\}$ dokážeme invariant

$$I_q: \forall w \in \Sigma^* : (0, w) \vdash^* (q, \varepsilon) \iff \#_a(w) = q;$$

pre stav $m+1$ napokon dokážeme invariant

$$I_{m+1}: \forall w \in \Sigma^* : (0, w) \vdash^* (m+1, \varepsilon) \iff \#_a(w) \geq m+1.$$

$\Rightarrow$: Matematickou indukciou vzhľadom na n dokážeme, že pre všetky $n \in \mathbb{N}$ platia implikácie

$$I'_q: \forall w \in \Sigma^* : (0, w) \vdash^n (q, \varepsilon) \Rightarrow \#_a(w) = q$$

pre všetky $q \in \{0, \dots, m\}$, ako aj implikácia

$$I'_{m+1}: \forall w \in \Sigma^* : (0, w) \vdash^n (m+1, \varepsilon) \Rightarrow \#_a(w) \geq m+1.$$

1. Pre $n = 0$ môže byť ľavá strana pravdivá iba pri implikácii I'_0 . V takom prípade je $w = \varepsilon$ a $q = 0$, pričom $\#_a(w) = \#_a(\varepsilon) = 0 = q$.
2. Predpokladajme platnosť implikácií $I'_0, \dots, I'_{m+1}$ pre $n = k$ a uvažujme $n = k+1$.
Pre $n = k+1$ najprv dokážeme implikácie $I'_0, \dots, I'_m$. Uvažujme teda situáciu, keď pre nejaké $q \in \{0, \dots, m\}$ a $w \in \Sigma^*$ je $(0, w) \vdash^{k+1} (q, \varepsilon)$. Potom existujú $u \in \Sigma^*$ a $c \in \Sigma$ také, že $w = uc$ a

$$(0, uc) \vdash^k (p, c) \vdash (q, \varepsilon)$$

pre nejaký stav $p \in K$. V takom prípade nutne $\delta(p, c) = q$ a z definície prechodovej funkcie automatu A_m teda vyplýva, že buď $p = q$ a $c = b$, alebo $q > 0$, $p = q-1$ a $c = a$. V prvom prípade je z indukčného predpokladu $\#_a(u) = p = q$, a teda aj $\#_a(w) = \#_a(uc) = \#_a(ub) = q$. V zostávajúcim prípade zas $\#_a(u) = p = q-1$, z čoho opäť $\#_a(w) = \#_a(uc) = \#_a(ua) = q$. Implikácia I'_q je teda dokázaná aj pre $n = k+1$.

Zostáva pre $n = k+1$ dokázať aj poslednú implikáciu I'_{m+1} . Nech teda $w \in \Sigma^*$ je také, že $(0, w) \vdash^{k+1} (m+1, \varepsilon)$. Potom existujú $u \in \Sigma^*$ a $c \in \Sigma$ také, že $w = uc$ a

$$(0, uc) \vdash^k (p, c) \vdash (m+1, \varepsilon)$$

pre nejaký stav $p \in K$. Z toho $\delta(p, c) = m+1$ a z definície prechodovej funkcie vidíme, že môžu nastať tri možnosti: $p = m$ a $c = a$, $p = m+1$ a $c = a$, alebo $p = m+1$ a $c = b$. V prvom prípade z indukčného predpokladu dostávame $\#_a(u) = m$, z čoho $\#_a(w) = \#_a(ua) \geq m+1$. Vo zvyšných dvoch prípadoch zas z indukčného predpokladu máme $\#_a(u) \geq m+1$, a teda aj $\#_a(w) = \#_a(uc) \geq m+1$. Pre $n = k+1$ sme teda dokázali aj implikáciu I'_{m+1} .

$\Leftarrow$: Z úplnosti prechodovej funkcie deterministického konečného automatu A_m vyplýva, že pre každé slovo $w \in \Sigma^*$ existuje stav $q \in K$ taký, že $(0, w) \vdash^* (q, \varepsilon)$. Ak $\#_a(w) = p$ pre nejaké $p \in \{0, \dots, m\}$, nutne musí byť $q = p$; v opačnom prípade by totiž z implikácií $I'_0, \dots, I'_{m+1}$ dokázaných vyššie vyplývalo, že musí byť buď $\#_a(w) = q \neq p$ (ak $q \in \{0, \dots, m\}$), alebo $\#_a(w) \geq m+1 > p$ (ak $q = m+1$). V oboch prípadoch by išlo o spor s rovnosťou $\#_a(w) = p$. Podobne ak $\#_a(w) \geq m+1$, musí byť $q = m+1$, pretože v opačnom prípade by sme vďaka implikáciám $I'_0, \dots, I'_{m+1}$ dostali $\#_a(w) = q < m+1$, čo je opäť spor.

Keďže je m jediným akceptačným stavom automatu A_m , slovo $w \in \Sigma^*$ patrí do jazyka $L(A_m)$ práve vtedy, keď $(0, w) \vdash^* (m, \varepsilon)$. To ale vďaka invariantu I_m nastane práve vtedy, keď $\#_a(w) = m$, čiže keď $w \in L_m$. Skutočne teda $L(A_m) = L_m$. $\square$

Úloha 3. Zostrojte (deterministický alebo nedeterministický) konečný automat akceptujúci jazyk

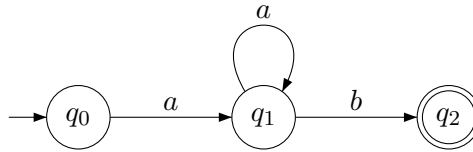
$$L = a^+b.$$

Správnosť svojej konštrukcie dokážte poriadnou matematickou indukciou.

Riešenie. Jazyk L je akceptovaný nedeterministickým¹ konečným automatom $A = (K, \Sigma, \delta, q_0, F)$, kde $K = \{q_0, q_1, q_2\}$, $\Sigma = \{a, b\}$, $F = \{q_2\}$ a

$$\begin{aligned} \delta(q_0, a) &= \{q_1\}, & \delta(q_1, a) &= \{q_1\}, & \delta(q_2, a) &= \emptyset, \\ \delta(q_0, b) &= \emptyset, & \delta(q_1, b) &= \{q_2\}, & \delta(q_2, b) &= \emptyset, \\ \delta(q_0, \varepsilon) &= \emptyset, & \delta(q_1, \varepsilon) &= \emptyset, & \delta(q_2, \varepsilon) &= \emptyset. \end{aligned}$$

Prechodový diagram automatu A je na obrázku 1.



Obr. 1: Prechodový diagram nedeterministického konečného automatu A .

Pre stavy automatu A dokážeme nasledujúce invarianty:

$$\begin{aligned} I_0: \forall w \in \Sigma^* : (q_0, w) \vdash^* (q_0, \varepsilon) &\iff w = \varepsilon \\ I_1: \forall w \in \Sigma^* : (q_0, w) \vdash^* (q_1, \varepsilon) &\iff w \in a^+, \\ I_2: \forall w \in \Sigma^* : (q_0, w) \vdash^* (q_2, \varepsilon) &\iff w \in a^+b. \end{aligned}$$

$\Rightarrow$: Matematickou indukciou vzhľadom na n dokážeme, že pre všetky $n \in \mathbb{N}$:

$$\begin{aligned} I'_0: \forall w \in \Sigma^* : (q_0, w) \vdash^n (q_0, \varepsilon) &\Rightarrow w = \varepsilon, \\ I'_1: \forall w \in \Sigma^* : (q_0, w) \vdash^n (q_1, \varepsilon) &\Rightarrow w \in a^+, \\ I'_2: \forall w \in \Sigma^* : (q_0, w) \vdash^n (q_2, \varepsilon) &\Rightarrow w \in a^+b. \end{aligned}$$

Pre $n = 0$ môže byť ľavá strana pravdivá iba pri implikácii I'_0 . V takom prípade tiež nutne $w = \varepsilon$.

Predpokladajme teda pravdivosť uvedených implikácií pre $n = k \in \mathbb{N}$ a uvažujme $n = k + 1$.

I'_0 : Pre $w \in \Sigma^*$ spĺňajúce $(q_0, w) \vdash^{k+1} (q_0, \varepsilon)$ musia existovať $q \in K$, $u \in \Sigma^*$ a $z \in \Sigma \cup \{\varepsilon\}$ také, že $w = uz$ a $(q_0, uz) \vdash^k (q, z) \vdash (q_0, \varepsilon)$ – a teda $q_0 \in \delta(q, z)$. Do stavu q_0 však v automate A nevedie žiaden prechod. Ľavá strana implikácie I'_0 tak pre $n = k + 1$ nemôže byť splnená a implikácia ako celok je teda pravdivá.

I'_1 : Nech $w \in \Sigma^*$ je slovo také, že $(q_0, w) \vdash^{k+1} (q_1, \varepsilon)$. Potom $(q_0, uz) \vdash^k (q, z) \vdash (q_1, \varepsilon)$ pre nejaké $q \in K$, $u \in \Sigma^*$ a $z \in \Sigma \cup \{\varepsilon\}$ také, že $w = uz$.

Nutne teda $q_1 \in \delta(q, z)$ a z definície prechodovej funkcie δ ľahko vidieť, že $z = a$, pričom $q = q_0$ alebo $q = q_1$. V prvom prípade je z indukčného predpokladu $u = \varepsilon$, z čoho $w = ua = a \in a^+$; v zostávajúcim prípade je z indukčného predpokladu $u \in a^+$, a teda aj $w = ua \in a^+$.

I'_2 : Nech $w \in \Sigma^*$ je slovo také, že $(q_0, w) \vdash^{k+1} (q_2, \varepsilon)$. Potom $(q_0, uz) \vdash^k (q, z) \vdash (q_2, \varepsilon)$ pre nejaké $q \in K$, $u \in \Sigma^*$ a $z \in \Sigma \cup \{\varepsilon\}$ také, že $w = uz$.

Keďže nutne $q_2 \in \delta(q, z)$, z definície prechodovej funkcie δ vyplýva, že $z = b$ a $q = q_1$. Z indukčného predpokladu teda dostávame $u \in a^+$, z čoho $w = ub \in a^+b$.

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

$\Leftarrow$: Nech $w \in \Sigma^*$. Implikácia

$$I_0'': w = \varepsilon \Rightarrow (q_0, w) \vdash^* (q_0, \varepsilon)$$

je triviálne pravdivá. Dokážeme teraz implikáciu

$$I_1'': w \in a^+ \Rightarrow (q_0, w) \vdash^* (q_1, \varepsilon).$$

Každé $w \in a^+$ možno zapísať ako $w = a^n$ pre nejaké $n \in \mathbb{N} - \{0\}$. Implikáciu tak môžeme dokázať indukciou vzhľadom na takéto n . Pre $n = 1$ je $(q_0, a^1) \vdash (q_1, \varepsilon)$, pretože $q_1 \in \delta(q_0, a)$. Ak teraz pre $n = k \in \mathbb{N} - \{0\}$ platí $(q_0, a^k) \vdash^* (q_1, \varepsilon)$, tak aj pre $n = k + 1$ zisťujeme, že $(q_0, a^{k+1}) \vdash^* (q_1, a) \vdash (q_1, \varepsilon)$, keďže $q_1 \in \delta(q_1, a)$. Implikácia

$$I_2'': w \in a^+b \Rightarrow (q_0, w) \vdash^* (q_2, \varepsilon)$$

je napokon bezprostredným dôsledkom predchádzajúcej implikácie: ak $w \in a^+b$, existuje $u \in a^+$ také, že $w = ub$. Podľa I_1'' potom $(q_0, u) \vdash^* (q_1, \varepsilon)$, z čoho $(q_0, ub) \vdash^* (q_1, b) \vdash (q_2, \varepsilon)$, keďže $q_2 \in \delta(q_1, b)$.

Keďže je q_2 jediným akceptačným stavom automatu A , slovo $w \in \Sigma^*$ patrí do $L(A)$ práve vtedy, keď $(q_0, w) \vdash^* (q_2, \varepsilon)$. To vďaka invariantu I_2 nastane práve vtedy, keď $w \in a^+b$. Skutočne teda $L(A) = L$. $\square$

Úloha 4. Zostrojte (deterministický alebo nedeterministický) konečný automat akceptujúci jazyk

$$L = \{xycyz \mid x, y, z \in \{a, b\}^*; \#_a(x) + \#_b(y) \equiv |z| \pmod{2}\}$$

(nad abecedou $\Sigma = \{a, b, c\}$). Správnosť svojej konštrukcie dokážte poriadnou matematickou indukciou.

Riešenie. Dokážeme, že $L = L(A)$ pre nedeterministický² konečný automat $A = (K, \Sigma, \delta, q_0, F)$, kde $K = \mathbb{Z}_2 \times \{1, 2, 3\}$,

$$\begin{aligned} \delta([p, 1], a) &= \{[p + 1, 1]\} & \forall p \in \mathbb{Z}_2, & \delta([p, 2], a) = \{[p, 2]\} & \forall p \in \mathbb{Z}_2, \\ \delta([p, 1], b) &= \{[p, 1]\} & \forall p \in \mathbb{Z}_2, & \delta([p, 2], b) = \{[p + 1, 2]\} & \forall p \in \mathbb{Z}_2, \\ \delta([p, 1], c) &= \{[p, 2]\} & \forall p \in \mathbb{Z}_2, & \delta([p, 2], c) = \{[p, 3]\} & \forall p \in \mathbb{Z}_2, \end{aligned}$$

$$\begin{aligned} \delta([p, 3], a) &= \{[p - 1, 3]\} & \forall p \in \mathbb{Z}_2, \\ \delta([p, 3], b) &= \{[p - 1, 3]\} & \forall p \in \mathbb{Z}_2, \\ \delta([p, 3], c) &= \emptyset & \forall p \in \mathbb{Z}_2, \end{aligned}$$

$\delta(q, \varepsilon) = \emptyset$ pre všetky $q \in K$, $q_0 = [0, 1]$ a $F = \{[0, 3]\}$. Všetky operácie sčítania a odčítania prvkov $\mathbb{Z}_2$ sú, samozrejme, modulo 2. Rovnosť $L(A) = L$ vyplynie z nasledujúcich invariantov pre jednotlivé stavy automatu.

- a) Pre $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ je $([0, 1], w) \vdash^* ([p, 1], \varepsilon)$ práve vtedy, keď $w \in \{a, b\}^*$ a $\#_a(w) \equiv p \pmod{2}$.
- b) Pre $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ je $([0, 1], w) \vdash^* ([p, 2], \varepsilon)$ práve vtedy, keď $w = xcy$ pre nejaké $x, y \in \{a, b\}^*$ také, že $\#_a(x) + \#_b(y) \equiv p \pmod{2}$.
- c) Pre $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ je $([0, 1], w) \vdash^* ([p, 3], \varepsilon)$ práve vtedy, keď $w = xcycz$ pre nejaké $x, y, z \in \{a, b\}^*$ také, že $\#_a(x) + \#_b(y) - |z| \equiv p \pmod{2}$.

Dokážeme teraz jednotlivé implikácie.

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

- a) Pre všetky $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ také, že $([0, 1], w) \vdash^n ([p, 1], \varepsilon)$, je $w \in \{a, b\}^*$ a súčasne $\#_a(w) \equiv p \pmod{2}$.
- b) Pre všetky $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ také, že $([0, 1], w) \vdash^n ([p, 2], \varepsilon)$, je $w = xcy$ pre nejaké $x, y \in \{a, b\}^*$ spĺňajúce $\#_a(x) + \#_b(y) \equiv p \pmod{2}$.
- c) Pre všetky $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ také, že $([0, 1], w) \vdash^n ([p, 3], \varepsilon)$, je $w = xcycz$ pre nejaké $x, y, z \in \{a, b\}^*$ spĺňajúce $\#_a(x) + \#_b(y) - |z| \equiv p \pmod{2}$.

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 $\#_a(w) \equiv 0 \pmod{2}$. Vo zvyšných dvoch tvrdeniach 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 $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ sú také, že $([0, 1], w) \vdash^{k+1} ([p, 1], \varepsilon)$, musia existovať $s \in K$, $u \in \Sigma^*$ a $v \in \Sigma \cup \{\varepsilon\}$ také, že $w = uv$ a $([0, 1], uv) \vdash^* (s, v) \vdash ([p, 1], \varepsilon)$; stadiaľ $[p, 1] \in \delta(s, v)$. Bud' teda $s = [p - 1, 1]$ a $v = a$, alebo $s = [p, 1]$ a $v = b$. V prvom prípade je z indukčného predpokladu $u \in \{a, b\}^*$ a $\#_a(u) \equiv p - 1 \pmod{2}$; v dôsledku toho aj $w = ua \in \{a, b\}^*$ a $\#_a(w) = \#_a(u) + 1 \equiv p \pmod{2}$. V druhom prípade je $u \in \{a, b\}^*$ a $\#_a(u) \equiv p \pmod{2}$; preto aj $w = ub \in \{a, b\}^*$ a $\#_a(w) = \#_a(u) \equiv p \pmod{2}$.

²Konštruovaný automat bude v podstate deterministický, ale nebude mať úplnú prechodovú funkciu; budeme ho preto formálne považovať za nedeterministický konečný automat.

Nech ďalej $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ sú také, že $([0, 1], w) \vdash^{k+1} ([p, 2], \varepsilon)$. Pre nejaké $s \in K$, $u \in \Sigma^*$ a $v \in \Sigma \cup \{\varepsilon\}$ potom $w = uv$ a $([0, 1], uv) \vdash^* (s, v) \vdash ([p, 2], \varepsilon)$. Nutne teda $[p, 2] \in \delta(s, v)$, čo môže nastať v troch rôznych prípadoch: pre $s = [p, 2]$ a $v = a$, pre $s = [p - 1, 2]$ a $v = b$ a pre $s = [p, 1]$ a $v = c$. Ak $s = [p, 2]$ a $v = a$, je z indukčného predpokladu $u = xcy'$ pre nejaké $x, y' \in \{a, b\}^*$ také, že $\#_a(x) + \#_b(y') \equiv p \pmod{2}$; ak teda položíme $y = y'a$, je skutočne $w = xcy$, kde $x, y \in \{a, b\}^*$ a $\#_a(x) + \#_b(y) = \#_a(x) + \#_b(y') \equiv p \pmod{2}$. Podobne ak $s = [p - 1, 2]$ a $v = b$, je $u = xcy'$ pre $x, y' \in \{a, b\}^*$ také, že $\#_a(x) + \#_b(y') \equiv p - 1 \pmod{2}$; pre $y = y'b$ tak $w = xcy$, kde $x, y \in \{a, b\}^*$ a $\#_a(x) + \#_b(y) = \#_a(x) + \#_b(y') + 1 \equiv p \pmod{2}$. Ak $s = [p, 1]$ a $v = c$, je z indukčného predpokladu $u \in \{a, b\}^*$, pričom $\#_a(u) \equiv p \pmod{2}$; pre $x = u$ a $y = \varepsilon$ preto naozaj $w = xcy$, pričom $\#_a(x) + \#_b(y) = \#_a(u) \equiv p \pmod{2}$.

Nech napokon $p \in \mathbb{Z}_2$ a $w \in \Sigma^*$ sú také, že $([0, 1], w) \vdash^{k+1} ([p, 3], \varepsilon)$. Pre nejaké $s \in K$, $u \in \Sigma^*$ a $v \in \Sigma \cup \{\varepsilon\}$ potom $w = uv$ a $([0, 1], uv) \vdash^* (s, v) \vdash ([p, 3], \varepsilon)$. Nutne teda $[p, 3] \in \delta(s, v)$, čo môže nastať v troch rôznych prípadoch: pre $s = [p + 1, 3]$ a $v = a$, pre $s = [p + 1, 3]$ a $v = b$ a pre $s = [p, 2]$ a $v = c$. Ak $s = [p + 1, 3]$ a $v \in \{a, b\}$, je z indukčného predpokladu $u = xcycz'$ pre nejaké $x, y, z' \in \{a, b\}^*$ také, že $\#_a(x) + \#_b(y) - |z'| \equiv p + 1 \pmod{2}$; ak teda položíme $z = z'v$, je skutočne $w = xcycz$, kde $x, y, z \in \{a, b\}^*$ a

$$\#_a(x) + \#_b(y) - |z| = \#_a(x) + \#_b(y') - |z'| - 1 \equiv p \pmod{2}.$$

Ak $s = [p, 2]$ a $z = c$, je z indukčného predpokladu $u = xcy$ pre nejaké $x, y \in \{a, b\}^*$ také, že $\#_a(x) + \#_b(y) \equiv p \pmod{2}$; pre $z = \varepsilon$ preto naozaj $w = xcycz$, pričom

$$\#_a(x) + \#_b(y) - |z| = \#_a(x) + \#_b(y) \equiv p \pmod{2}.$$

$\Leftarrow$: Dokážeme nasledujúce tri tvrdenia:

- a) Pre všetky $p \in \mathbb{Z}_2$ a $x \in \{a, b\}^*$ spĺňajúce $\#_a(x) \equiv p \pmod{2}$ je $([0, 1], x) \vdash^* ([p, 1], \varepsilon)$.
- b) Pre všetky $p \in \mathbb{Z}_m$ a $x, y \in \{a, b\}^*$ spĺňajúce $\#_a(x) + \#_b(y) \equiv p \pmod{2}$ je $([0, 1], xcy) \vdash^* ([p, 2], \varepsilon)$.
- c) Pre všetky $p \in \mathbb{Z}_m$ a $x, y, z \in \{a, b\}^*$ spĺňajúce $\#_a(x) + \#_b(y) - |z| \equiv p \pmod{2}$ je $([0, 1], xcycz) \vdash^* ([p, 3], \varepsilon)$.

Prvé z tvrdení dokážeme indukciou vzhľadom na $|x|$. Ak $|x| = 0$, nutne $x = \varepsilon$, z čoho $p = 0$, a teda aj $([0, 1], w) \vdash^* ([p, 1], \varepsilon)$. Nech teda tvrdenie platí pre všetky $x \in \{a, b\}^*$ dĺžky $k \in \mathbb{N}$ a uvažujme prípad, keď $x \in \{a, b\}^{k+1}$; nech $\#_a(x) \equiv p \pmod{2}$. Pre nejaké $u \in \{a, b\}^k$ potom $x = ua$ alebo $x = ub$. V prvom prípade nutne $\#_a(u) \equiv p - 1 \pmod{2}$ a z indukčného predpokladu tak dostávame $([0, 1], u) \vdash^* ([p - 1, 1], \varepsilon)$, z čoho

$$([0, 1], x) = ([0, 1], ua) \vdash^* ([p - 1, 1], a) \vdash ([p, 1], \varepsilon).$$

V druhom je $\#_a(u) \equiv p \pmod{2}$ a vďaka indukčnému predpokladu teda $([0, 1], u) \vdash^* ([p, 1], \varepsilon)$; z toho

$$([0, 1], x) = ([0, 1], ub) \vdash^* ([p, 1], b) \vdash ([p, 1], \varepsilon).$$

Druhé tvrdenie dokážeme indukciou vzhľadom na $|y|$. Pre $|y| = 0$ nutne $y = \varepsilon$. Ako dôsledok prvého tvrdenia tak pre všetky $x \in \{a, b\}^*$ spĺňajúce $\#_a(x) + \#_b(y) = \#_a(x) \equiv p \pmod{2}$ skutočne dostávame $([0, 1], xcy) = ([0, 1], xc) \vdash^* ([p, 1], c) \vdash ([p, 2], \varepsilon)$. Predpokladajme ďalej, že tvrdenie platí pre všetky $y \in \{a, b\}^*$ dĺžky $k \in \mathbb{N}$ a uvažujme prípad, keď $y \in \{a, b\}^{k+1}$; nech $x \in \{a, b\}^*$ je ľubovoľné a nech $\#_a(x) + \#_b(y) \equiv p \pmod{2}$. Pre nejaké $u \in \{a, b\}^k$ potom $y = ua$ alebo $y = ub$. V prvom prípade je $\#_a(x) + \#_b(u) \equiv p \pmod{2}$ a z indukčného predpokladu tak dostávame $([0, 1], xcu) \vdash^* ([p, 2], \varepsilon)$, z čoho

$$([0, 1], xcy) = ([0, 1], xcua) \vdash^* ([p, 2], a) \vdash ([p, 2], \varepsilon).$$

V druhom prípade je $\#_a(x) + \#_b(u) \equiv p - 1 \pmod{2}$ a z indukčného predpokladu teda vyplýva $([0, 1], xcu) \vdash^* ([p - 1, 2], \varepsilon)$, z čoho

$$([0, 1], xcy) = ([0, 1], xcub) \vdash^* ([p - 1, 2], b) \vdash ([p, 2], \varepsilon).$$

Zostáva dokázať tretie tvrdenie, a to indukciou na $|z|$. Pre $|z| = 0$ nutne $z = \varepsilon$. Z druhého tvrdenia tak pre všetky $x, y \in \{a, b\}^*$ spĺňajúce $\#_a(x) + \#_b(y) - |z| = \#_a(x) + \#_b(y) \equiv p \pmod{2}$ dostávame $([0, 1], xcycz) = ([0, 1], xcy) \vdash^* ([p, 2], c) \vdash ([p, 3], \varepsilon)$. Predpokladajme ďalej, že tvrdenie platí pre všetky $z \in \{a, b\}^*$ dĺžky $k \in \mathbb{N}$ a uvažujme prípad, keď $z \in \{a, b\}^{k+1}$; nech $x, y \in \{a, b\}^*$ sú ľubovoľné a nech $\#_a(x) + \#_b(y) \equiv p \pmod{2}$. Pre nejaké $u \in \{a, b\}^k$ a $v \in \{a, b\}$ potom $z = uv$. Preto $\#_a(x) + \#_b(y) - |u| \equiv p + 1 \pmod{2}$ a z indukčného predpokladu tak dostávame $([0, 1], xcycu) \vdash^* ([p + 1, 3], \varepsilon)$, z čoho

$$([0, 1], xcycz) = ([0, 1], xcycuv) \vdash^* ([p + 1, 3], v) \vdash ([p, 3], \varepsilon).$$

Slovo $w \in \Sigma^*$ teraz patrí do jazyka $L(A)$ práve vtedy, keď $([0, 1], w) \vdash^* ([0, 3], \varepsilon)$. To ale podľa dokázaného nastane práve vtedy, keď $w = xcycz$ pre nejaké $x, y, z \in \{a, b\}^*$ také, že $\#_a(x) + \#_b(y) - |z| \equiv 0 \pmod{2}$, t. j. $\#_a(x) + \#_b(y) \equiv |z| \pmod{2}$. Táto podmienka je ekvivalentná príslušnosti slova w do jazyka L . $\square$

Úloha 5. Nech $G = (N, T, P, \sigma)$ je regulárna gramatika s $N = \{\sigma, \alpha, \beta\}$, $T = \{a, b\}$ a

$$\begin{aligned} P = \{ & \sigma \rightarrow aa\sigma \mid b\alpha \mid baa \\ & \alpha \rightarrow a\alpha \mid \beta \mid \varepsilon \\ & \beta \rightarrow a\alpha \mid b\}. \end{aligned}$$

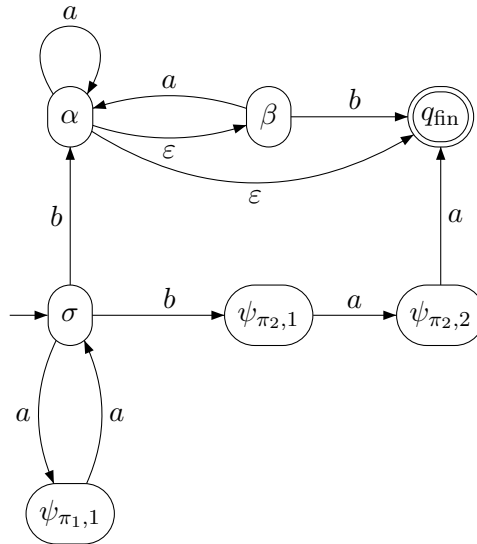
Zostrojte nedeterministický konečný automat A taký, že $L(A) = L(G)$. Túto rovnosť nie je potrebné dokazovať v prípade použitia štandardnej konštrukcie; v opačnom prípade je dôkaz nutný.

Riešenie. Skonstruujeme najprv regulárnu gramatiku $G' = (N', T, P', \sigma)$ ekvivalentnú gramatike G takú, že $P' \subseteq N' \times (TN' \cup N' \cup T \cup \{\varepsilon\})$. Za týmto účelom zavedme nasledujúce označenia pravidiel:

$$\begin{aligned} \pi_1 &:= (\sigma \rightarrow aa\sigma), \\ \pi_2 &:= (\sigma \rightarrow baa). \end{aligned}$$

Potom $N' = \{\sigma, \alpha, \beta, \psi_{\pi_1,1}, \psi_{\pi_2,1}, \psi_{\pi_2,2}\}$ a

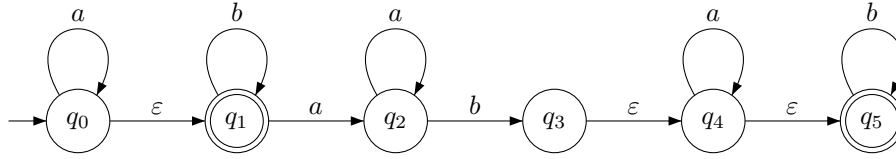
$$\begin{aligned} P = \{ & \sigma \rightarrow a\psi_{\pi_1,1} \mid b\alpha \mid b\psi_{\pi_2,1} \\ & \alpha \rightarrow a\alpha \mid \beta \mid \varepsilon \\ & \beta \rightarrow a\alpha \mid b \\ & \psi_{\pi_1,1} \rightarrow a\sigma \\ & \psi_{\pi_2,1} \rightarrow a\psi_{\pi_2,2} \\ & \psi_{\pi_2,2} \rightarrow a\}. \end{aligned}$$



Obr. 2: Nedeterministický konečný automat A ekvivalentný gramatike G .

Nedeterministický konečný automat A ekvivalentný gramatike G je následne daný diagramom na obrázku 2. □

Úloha 6. Uvažujme nedeterministický konečný automat A nad abecedou $\Sigma = \{a, b\}$ daný nasledujúcim diagramom.



Nájdite nedeterministický konečný automat A' neobsahujúci prechody na prázdne slovo taký, že $L(A') = L(A)$. Túto rovnosť nie je potrebné dokazovať v prípade použitia štandardnej konštrukcie; v opačnom prípade je dôkaz nutný.

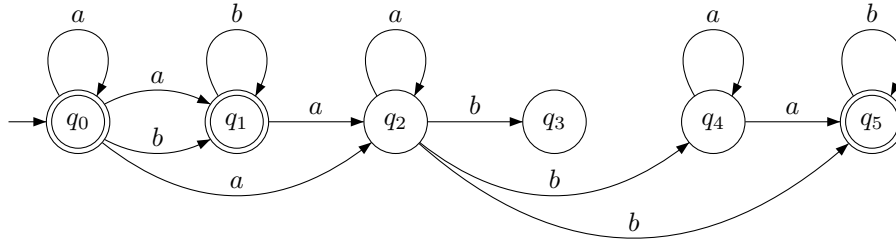
Riešenie. Nech $A = (K, \Sigma, \delta, q_0, F)$. Pre každý stav $q \in K$ najprv nájdeme „epsilonový chvost“ $[q]_\varepsilon$:

$$\begin{aligned} [q_0]_\varepsilon &= \{q_0, q_1\}, & [q_1]_\varepsilon &= \{q_1\}, & [q_2]_\varepsilon &= \{q_2\}, \\ [q_3]_\varepsilon &= \{q_3, q_4, q_5\}, & [q_4]_\varepsilon &= \{q_4, q_5\}, & [q_5]_\varepsilon &= \{q_5\}. \end{aligned}$$

Následne odstránime prechody na ε vedúce z q_0 do q_1 , z q_3 do q_4 a z q_4 do q_5 .

Pre všetky stavy $q \in K \setminus \{q_0\}$ a $c \in \Sigma$ ďalej pre všetky $q' \in \delta(q, c)$ povedieme nové prechody na c zo stavu q aj do všetkých stavov $p \in [q']_\varepsilon$. Takto pribudnú prechody na b z q_2 do q_4 a q_5 a prechod na a z q_4 do q_5 .

V rámci ďalšieho kroku pre všetky $q \in [q_0]_\varepsilon$, $c \in \Sigma$ a $q' \in \delta(q, c)$ povedieme nové prechody na c zo stavu q_0 do všetkých stavov $p \in [q']_\varepsilon$. Takto dostaneme prechody na a aj na b z q_0 do q_1 , ako aj prechod na a z q_0 do q_2 .



Obr. 3: Prechodový diagram nedeterministického konečného automatu A' .

V poslednom kroku sa stane akceptačným aj stav q_0 , pretože $q_1 \in [q_0]_\varepsilon \cap F$. Výsledný automat $A' = (K', \Sigma', \delta', q'_0, F')$ je potom znázornený diagramom na obrázku 3. $\square$