# Konečné automaty - základy

Šimon Sádovský

*Poznámka* 1. V uvedených dôkazoch sa vyskytuje formulácia „je analogické“. Táto formulácia sa v matematických textov vyskytuje zvyčajne, avšak môže byť zradná a treba s ňou narábať opatrne. Skúste si premyslieť, prečo v uvedených prípadoch môžeme tvrdiť že niečo je analogické niečomu inému. Taktiež si ako cvičenie premyslite, čo by bolo treba doplniť do uvedených dôkazov, keby sme požadovali, aby sme nepoužívali formuláciu „je analogické“.

### Deterministický konečný automat

**Úloha 1.** Zostrojte deterministický alebo nedeterministický automat akceptujúci jazyk

$$L = \{a^{3k} \mid k \in \mathbb{N}\}.$$

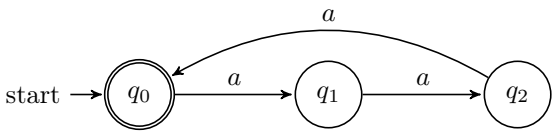
Správnosť svojej konštrukcie *poriadne* dokážte.

**Označenie 1.** Operáciu „sčítanie modulo 3“ budeme pre potreby tejto úlohy označovať $\oplus$.

*Dôkaz.* Jazyk $L$ budeme akceptovať deterministickým konečným automatom. Definujeme DKA $A = (K, \Sigma, \delta, q_0, F)$ kde:

- $K = \{q_i \mid i \in \mathbb{Z}_3\}$
- $\Sigma = \{a\}$
- $F = \{q_0\}$
- $(\forall i \in \mathbb{Z}_3)\ \delta(q_i, a) = q_{i\oplus 1}$.

Pre lepšiu čitateľnosť uvádzame aj prechodový diagram automatu $A$.




Teraz potrebujeme dokázať, že platí $L = L(A)$. To spravíme tak, že dokážeme nasledovnú sadu invariantov pre jednotlivé stavy automatu $A$ z ktorých požadovaná rovnosť následne vyplynie.

(i) $(\forall k \in \mathbb{N})\ (q_0, a^k) \vdash^* (q_0, \varepsilon) \Leftrightarrow k \bmod 3 = 0$

(ii) $(\forall k \in \mathbb{N})\ (q_0, a^k) \vdash^* (q_1, \varepsilon) \Leftrightarrow k \bmod 3 = 1$

(iii) $(\forall k \in \mathbb{N})\ (q_0, a^k) \vdash^* (q_2, \varepsilon) \Leftrightarrow k \bmod 3 = 2$

*Poznámka* 2. Pred samotným dokazovaním uvedených invariantov si uvedomme nasledovné. Každý invariant nejak charakterizuje slová, ktoré pri výpočte skončia v stave popisovanom daným invariantom. Práve toto využijeme pri samotnom dôkaze $L = L(A)$.

Teraz prejdime k dôkazu platnosti uvedených invariantov. Najprv dokážeme implikácie „z ľava do prava“, všetky naraz, indukciou na dĺžku výpočtu.

1°: Uvažujme ľubovoľný nulakrokový výpočet $(q_0, a^k) \vdash^0 (p, \varepsilon)$ kde $p \in K$. Takýto výpočet v skutočnosti existuje iba jeden a nutne musí platiť $k = 0$ a $p = q_0$, teda ide o výpočet $(q_0, \varepsilon) \vdash^0 (q_0, \varepsilon)$. Teda platí lavá strana invariatnu (i). Navyše platí $0 = 0 \bmod 3$, teda pravá strana invariantu (i) platí tiež. Z toho vyplýva, že pre nulakrokové výpočty invariant (i) platí. Z uvedeného taktiež vyplýva, že pre žiadne nulakrokové výpočty nemôže platiť ľavá strana invariatov (ii) a (iii) a teda pre nulakrokové výpočty sú tieto invarianty platné triviálne. Týmto je báza indukcie dokázaná.

2°: Nech $n \in \mathbb{N}$. Uvažujme, že uvedené invarianty platia pre všetky výpočty dĺžky nanajvýš $n$. Dokážeme, že potom platia aj pre všetky výpočty dĺžky $n+1$.

Predpokladajme, že platí ľavá strana invariantu (i). Teda platí $(q_0, a^k) \vdash^{n+1} (q_0, \varepsilon)$ pre nejaké $k \in \mathbb{N}$. Tento výpočet vieme rozpísať ako

$$\underbrace{(q_0, a^{k-1}a) \vdash^n (p, a)}_{\text{Časť 1}} \vdash (q_0, \varepsilon)$$

pre nejaké $p \in K$. Teraz skúmajme posledný krok tohto výpočtu. Z definície prechodovej funkcie $\delta$ vyplýva, že platí $p = q_2$. Keďže Časť 1 uvedeného výpočtu je dĺžky $n$, vzťahuje sa na ňu indukčny predpoklad. Z uvedeného vyplýva, že Časť 1 spĺňa pravú stranu invariantu (iii), teda poďla IP musí platiť $(k-1) \bmod 3 = 2$. Teraz je už zjavné, že platí $k \bmod 3 = 0$ a pre výpočty dĺžky $n+1$ je implikácia „z ľava do prava“ invariantu (i) dokázaná.

Dôkaz implikácii „z ľava do prava“ invariantov (ii) a (iii) je analogický k uvedenému dôkazu implikácie „z ľava do prava“ invariantu (i). Týmto je uvedená sada invariantov „z ľava do prava“ dokázaná.

Teraz chceme dokázať sadu invariantov „z prava do ľava“. Môžeme si všimnúť, že pravé strany invariantov sú „disjunktné“ v zmysle, že pre žiadne vstupné slovo automatu $A$ nemôže platiť naraz viac ako jedna z uvedených pravých strán. Práve túto vlastnosť v dôkaze využijeme.

Sporom dokážeme implikáciu „z prava do ľava“ invariatnu (i). Predpokladajme, že platí pravá strana invariantu (i), teda uvažujme ľubovolné $k \in \mathbb{N}$ také, že $k \bmod 3 = 0$. Pre spor ale predpokladajme, že ľavá strana invariantu (i) neplatí. Teda neplatí $(q_0, a^k) \vdash^* (q_0, \varepsilon)$. Na slove $a^k$ však musí existovať nejaký výpočet automatu $A$. Teda musí platiť alebo $(q_0, a^k) \vdash^* (q_1, \varepsilon)$ alebo $(q_0, a^k) \vdash^* (q_2, \varepsilon)$. V prvom prípade by však podľa už dokázanej implikácie „z ľava doprava“ invariantu (ii) muselo platiť $k \bmod 3 = 1$, čo je v spore s prepokladom, že $k \bmod 3 = 0$. Analogicky by sme dospeli k sporu v druhom prípade použitím implikácie „z ľava doprava“ invariantu (iii). Pre implikácie „z prava do ľava“ invariatnov (ii) a (iii) je dôkaz analogický.

Teraz sme úspešne dokázali platnosť uvedenej sady invariantov.

Ostáva dokázať, že platí $L(A) = L$. Dokážeme obe inklúzie danej rovnosti.

$\subseteq$: Nech $w \in L(A)$. Teda musí existovať akceptačný výpočet automatu $A$ na slove $w$. Keďže $q_0$ je jediný akceptačný stav automatu $A$, musí platiť $(q_0, w) \vdash^* (q_0, \varepsilon)$. Keďže $w$ je vstupné slovo automatu $A$, tak musí platiť $w \in \Sigma^*$, teda $w = a^k$ pre nejaké $k \in \mathbb{N}$. Z implikácie „z ľava do prava“ invariantu (i) potom vyplýva, že $k \bmod 3 = 0$. Teda zjavne $w \in L$.

$\supseteq$: Nech $w \in L$. Teda existuje $l \in \mathbb{N}$ také, že $w = a^{3l}$. Zjavne platí $3l \mod 3 = 0$, preto podľa implikácie „z prava do ľava“ invariantu (i) platí $(q_0, w) \vdash^* (q_0, \varepsilon)$. Keďže $q_0 \in F$, tak uvedený výpočet je akceptačný a platí $w \in L(A)$.

□

*Poznámka* 3. Čo sú to tie invarianty? Pozrime sa na slovo invariant etymologicky. Toto slovo vieme rozložiť na predponu „in“ a jeho základ „variant“. Slovo „variant“ má blízko k „variable“, čo dobre poznáme z programovania a značí to premenú. Skutočne, „variant“ označuje niečo, čo je meniace-sa. Predpona „in“ v angličtine neguje význam slova za ňou. Teda slovo invariant bude znamnať „niečo, čo sa nemení“, resp. inak povedané „niečo, čo sa zachováva“. Tvrdenia, ktoré sme nazvali v dôkaze invariantmi naozaj hovoria toľko, že istá vlastnosť je pre všetky slová, ktoré skončia v tom-ktorom stave automatu nemenná, resp. zachovaná. Teda „stav zachováva (resp. nemení) nejakú vlastnosť slov, ktoré v ňom skončia“.

*Poznámka* 4. Trošku hlbšie sa zamyslime nad dôkazom implikácií „z prava do ľava“ našich invariantov. Využili sme fakt, že pravé strany sú v nejakom zmysle „disjunktné“, teda že o žiadnom slove neplatila naraz viac ako jedna z pravých strán. V skutočnosti pre každé vstupné slovo platila práve jedna z pravých strán. Toto je dôsledok toho, že nami definovaný konečný automat je

deterministický. DKA majú tú vlastnosť, že pre každé vstupné slovo existuje práve jeden výpočet. Preto každé slovo je daným DKA dočítané jednoznačne v jednom z jeho stavov. Preto pre ľubovoľný DKA bude mať sada k nemu prislúchajúcich invariantov túto „disjunktnú vlastnosť“. Toto nebude platiť, ak budeme pracovať s nedeterministickými konečnými automatmi, ako vidíme v ďalšom príklade.

*Poznámka* 5. Všimnime si, že v samotnom „finále dôkazu“, teda pri dôkaze rovnosti $L(A) = L$ sme využívali iba invariant (i), ktorý sa týkal akceptačného stavu a ostatné invarianty sme v tejto fáze dôkazu nevyužili. Avšak ak by sme dokazovali iba tento invariant sám o sebe, niekde v indukcii, ktorú sme robili, by sme natrafili na problém. Zamyslite sa, kde by tento problém nastal. Potom by už malo byť jasné, prečo sme potrebovali dokazovať celú sadu invariantov a nie iba tento jeden osamote.

*Poznámka* 6. Môžeme si všimnúť, že všetky invarianty majú podobnú štruktúru a dali by sa zapísať aj inak. Konkrétne by sme namieto troch invariantov mohli dokazovať tvrdenie

$$(\forall i \in \mathbb{Z}_3)(\forall k \in \mathbb{N})(q_0, a^k) \vdash^* (q_i, \varepsilon) \Leftrightarrow k \bmod 3 = i$$

Toto tvrdenie je presne to isté, čo naše tri invarianty, akurát zapísané stručnejšie. Z pedagogických dôvodov boli v príklade uvedené všetky tri invarianty. Avšak takto zostručniť zápis je dobrý zvyk. Ak by sme potrebovali zostrojiť DKA napríklad pre jazyk $L = \{a^{1991k} \mid k \in \mathbb{N}\}$, tak verím, že je jasné, ktorý typ zápisu chceme použiť v dôkaze.

### Nedeterministický konečný automat

**Úloha 2.** Zostrojte deterministický alebo nedeterministický automat akceptujúci jazyk

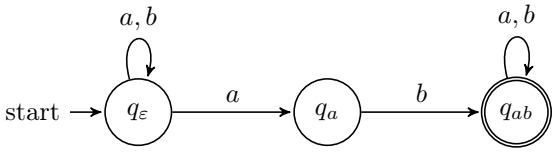
$$L = \{uabv \mid u, v \in \{a, b\}^*\}.$$

Správnosť svojej konštrukcie *poriadne* dokážte.

*Dôkaz.* Jazyk $L$ budeme akceptovať nedeterministickým konečným automatom. Definujeme NKA $A = (K, \Sigma, \delta, q_\varepsilon, F)$ kde $K = \{q_\varepsilon, q_a, a_{ab}\}$, $\Sigma = \{a, b\}$, $F = \{q_{ab}\}$ a prechodová funkcia $\delta$ je definovaná ako

$$\begin{aligned}
\delta(q_\varepsilon, b) &= \{q_\varepsilon\} \\
\delta(q_\varepsilon, a) &= \{q_\varepsilon, q_a\} \\
\delta(q_a, b) &= \{q_{ab}\} \\
\delta(q_{ab}, c) &= \{q_{ab}\} \text{ pre } c \in \{a, b\}
\end{aligned}$$

pričom iné ako uvedené prechody v automate $A$ neexistujú. Pre lepšiu čitateľnosť uvádzame aj prechodový diagram automatu $A$.




Teraz potrebujeme dokázať, že platí $L = L(A)$. To spravíme tak, že dokážeme nasledovnú sadu invariantov pre jednotlivé stavy automatu $A$ z ktorých požadovaná rovnosť následne vyplynie.

(i) $(\forall w \in \Sigma^*)\ (q_\varepsilon, w) \vdash^* (q_\varepsilon, \varepsilon)$

(ii) $(\forall w \in \Sigma^*)\ (q_\varepsilon, w) \vdash^* (q_a, \varepsilon) \Leftrightarrow (\exists u \in \Sigma^*)\ w = ua$

(iii) $(\forall w \in \Sigma^*)\ (q_\varepsilon, w) \vdash^* (q_{ab}, \varepsilon) \Leftrightarrow (\exists u, v \in \Sigma^*)\ w = uabv$

Najprv dokážeme invariant (i). Pred samotným dokazovaním si všimnime, že tento invariant je iný ako ostatné invarianty v zmysle, že neobsahuje žiadnu ekvivalenciu. Dal by sa formulovať aj v štýle „s ekvivalenciou“ takto „$(\forall w \in \Sigma^*)\ (q_\varepsilon, w) \vdash^* (q_\varepsilon, \varepsilon) \Leftrightarrow w \in \Sigma^*$“. Veríme, že po chvíľkovom zamyslení je čitateľovi jasné, prečo sme spokojne mohli zvoliť takú formuláciu, ako sme zvolili.

Teraz prejdime k dôkazu invariantu (i). Indukciou na dĺžku slova $w$.

1°: Nech $|w| = 0$, teda $w = \varepsilon$. Zjavne platí $(q_\varepsilon, \varepsilon) \vdash^* (q_\varepsilon, \varepsilon)$.

2°: Nech $|w| = n+1$ pre nejaké $n \in \mathbb{N}$ a predpokladajme, že tvrdenie platí pre všetky slová dĺžky nanajvýš $n$. Rozpíšme slovo $w$ ako $w = uc$ kde $u \in \Sigma^*$ a $c \in \Sigma$. Zjavne platí $|u| \leq n$, teda na slovo $u$ sa vzťahuje indukčný predpoklad. Teda platí $(q_\varepsilon, uc) \vdash^* (q_\varepsilon, c)$. Tento výpočet môžeme vďaka definícii prechodovej funkcie delta predĺžiť nasledovne $(q_\varepsilon, uc) \vdash^* (q_\varepsilon, c) \vdash (q_\varepsilon, \varepsilon)$.

Teraz dokážeme implikácie „z ľava do prava“ invariantov (ii) a (iii), postupne, jednu po druhej.

(ii) Uvažujme $w \in \Sigma^*$ také, že $(q_\varepsilon, w) \vdash^* (q_a, \varepsilon)$. Tento výpočet vieme rozpísať ako $(q_\varepsilon, uc) \vdash^* (p, c) \vdash (q_a, \varepsilon)$ kde $u \in \Sigma^*$, $c \in \Sigma$ a $w = uc$. Tu si musíme uvedomiť, že takto to môžeme rozpísať iba vďaka tomu, že NKA $A$ neobsahuje prechody na $\varepsilon$. Inak by sme museli uvažovať $c \in \Sigma \cup \{\varepsilon\}$. Z prechodovej funkcie $\delta$ vyplýva, že nutne $p = q_\varepsilon$ a $c = a$. Teda platí $w = ua$ čím je dôkaz implikácie „z ľava do prava“ tohto invariantu hotový.

(iii) Uvažujme $w \in \Sigma^*$ také, že $(q_\varepsilon, w) \vdash^* (q_{ab}, \varepsilon)$. V tomto výpočte si všimnime prvú konfiguráciu obsahujúcu stav $q_{ab}$ a zároveň krok výpočtu, ktorým sme sa do tejto konfigurácie dostali. Takáto konfigurácia nutne musí existovať. Ak aj nie iná, tak minimálne posledná konfigurácia je takáto. Teda formálne môžeme uvedený výpočet rozpísať ako

$$\underbrace{(q_\varepsilon, ucv) \vdash^* (p, cv)}_{\text{Časť 1}} \vdash (q_{ab}, v) \vdash^* (q_{ab}, \varepsilon)$$

kde $p \in K; u, v \in \Sigma^*; c \in \Sigma$ pričom $w = ucv$ a navyše Časť 1 neobsahuje žiadnu konfiguráciu obsahujúcu stav $q_{ab}$. Skúmajme teraz krok výpočtu $(p, cv) \vdash (q_{ab}, v)$. Keďže konfigurácia $(p, cv)$ sa nachádza ešte v Časti 1, tak nutne $p \neq q_{ab}$. Potom z prechodovej funkcie $\delta$ vyplýva, že $p = q_a$ a $c = b$. Teda platí $(q_\varepsilon, u) \vdash^* (q_a, \varepsilon)$. Z už dokázanej implikácie „z ľava do prava“ invariantu (ii) teda dostávame, že existuje nejaké $u_1 \in \Sigma^*$ také, že platí $u = u_1 a$. Dajúc dokopy všetko predchádzajúce dostávame $w = ucv = ubv = u_1 abv$, čo bolo treba dokázať.

Teraz dokážeme platnosť implikácií „z prava do ľava“ invariantov (ii) a (iii), postupne, jednu po druhej. V tomto dôkaze budeme potrebovať nasledovné pomocné tvrdenie:

**Tvrdenie 1.** $(\forall w \in \Sigma^*)\ (q_{ab}, w) \vdash^* (q_{ab}, \varepsilon)$

Môžeme si všimnúť, že toto tvrdenie sa nápadne podobá na invariant (i). Navyše, dôkaz tohto tvrdenia je až na názov stavu uplne rovnaký ako dôkaz invariantu (i), preto ho neuvádzame.

(ii) Uvažujme teda $w \in \Sigma^*$ také, že existuje $u \in \Sigma^*$ také, že platí $w = ua$. Vďaka platnosti invariantu (i) platí $(q_\varepsilon, ua) \vdash^* (q_\varepsilon, a)$. Tento výpočet vieme vďaka definícii prechodovej funkcie $\delta$ predĺžiť nasledovne $(q_\varepsilon, ua) \vdash^* (q_\varepsilon, a) \vdash (q_a, \varepsilon)$, čím je implikácia „z prava do ľava“ invariantu (ii) dokázaná.

(iii) Teraz uvažujme $w \in \Sigma^*$ také, že existujú $u, v \in \Sigma^*$ také, že platí $w = uabv$. Vďaka platnosti práve dokáznej implikácie „z prava do ľava“ invariantu (ii) dostávame, že platí $(q_\varepsilon, uabv) \vdash^* (q_a, bv)$. Tento výpočet môžeme vďaka definícii prechodovej funkcii delta a Tvrdeniu 1 predĺžiť nasledovne $(q_\varepsilon, uabv) \vdash^* (q_a, bv) \vdash (q_{ab}, v) \vdash^* (q_{ab}, \varepsilon)$. Týmto je dôkaz hotový.

Teraz prejdime k samotnému dôkazu rovnosti $L(A) = L$. Dokážeme obe inklúzie tejto rovnosti.

$\subseteq$: Nech $w \in L(A)$. Teda musí existovať akceptačný výpočet automatu $A$ na slove $w$. Keďže $q_{ab}$ je jediný akceptačný stav automatu $A$, musí platiť $(q_\varepsilon, w) \vdash^* (q_{ab}, \varepsilon)$. Z implikácie „z ľava do prava“ invariantu (iii) potom vyplýva, že existujú $u, v \in \Sigma^*$ také, že platí $w = uabv$. Teda zjavne $w \in L$.

$\supseteq$: Nech $w \in L$. Teda existujú $u, v \in \Sigma^*$ také, že platí $w = uabv$. Potom z implikácie „z prava do ľava“ invariantu (iii) vyplýva, že platí $(q_\varepsilon, w) \vdash^* (q_{ab}, \varepsilon)$. Keďže $q_{ab} \in F$, tento výpočet je akceptačný a preto $w \in L(A)$.

□