

Rozoznávanie jazykov konečnými monoidmi

Ročníkový projekt

Michaela Janitorová

1.12.2024

Obsah

1	Definície	5
2	Rozoznávanie jazykov monoidmi	7
3	Syntaktický monoid	9

Kapitola 1

Definície

Na úvod definujeme základné pojmy používané v tomto texte.

Definícia 1.0.1. Abeceda je ľubovoľná konečná neprázdna množina. Prvky abecedy nazývame symboly alebo písmená.

Definícia 1.0.2. Slovo nad abecedou Σ je konečná postupnosť symbolov množiny Σ . Prázdnu postupnosť (prázdne slovo) označujeme ε .

Definícia 1.0.3. Jazyk nad abecedou Σ je ľubovoľná množina slov nad abecedou Σ .

Definícia 1.0.4. Pologrupa je dvojica $(M, *)$ kde M je množina a $*$ je asociatívna binárna operácia na množine M .

Definícia 1.0.5. Neutrálny prvok pologrupy $(M, *)$ je prvok $e \in M$ taký, že pre všetky $x \in M$ platí

$$e * x = x = x * e$$

Neutrálne prvky budeme označovať ako e alebo 1 .

Definícia 1.0.6. Monoid je pologrupa obsahujúca neutrálny prvok. (Monoid budeme zapisovať aj ako trojicu $(M, *, e)$).

Príklad 1.0.7. Medzi monoidy patrí napríklad $(\mathbb{N}, +, 0)$ alebo $(\Sigma^*, \cdot, \varepsilon)$ kde $\cdot$ je operácia zretiazenia slov.

Príklad 1.0.8. Konečným monoidom je napr. $(\mathbb{Z}_n, +, 0)$ alebo tiež $(F, \circ, \text{Id}_S)$ kde F je množina funkcií $f : S \rightarrow S$, $\circ$ je operácia skladania funkcií a Id_S je identické zobrazenie na konečnej množine S .

Definícia 1.0.9. Konečný monoid je monoid $(M, *, e)$ taký, že množina M je konečná.

Definícia 1.0.10. Akcia Pod akciou monoidu $(S, \cdot, 1)$ rozumieme zobrazenie $\delta : Q \times S \rightarrow Q$ také, že pre $\forall x, y \in S$ a pre $\forall q \in Q$ platí $\delta(\delta(q, x), y) = \delta(q, xy)$ a zároveň $\forall q \in Q : \delta(q, 1) = q$.

Definícia 1.0.11. Deterministický konečný automat je päťica $A = (\Sigma, Q, \delta, q_0, F)$, kde Σ je abeceda, Q je konečná množina stavov, $\delta : Q \times \Sigma \rightarrow Q$ je akcia na $(\Sigma^*, \cdot, \varepsilon)$, $q_0 \in Q$ je počiatočný stav a $F \subseteq Q$ je množina akceptačných stavov. **Jazyk** akceptovaný automatom A je množina $L(A) = \{x \in \Sigma^* \mid \delta(q_0, x) \in F\}$.

Definícia 1.0.12. Konfigurácia deterministického konečného automatu je prvok (q, w) kde q je stav automatu a w je nespracovaná časť vstupného slova.

Definícia 1.0.13. Prechodový monoid Nech A je konečný automat $A = (\Sigma, Q, \delta, q_0, F)$. Označme $M_A = (\{\delta_x \mid x \in \Sigma^*\}, \circ, \delta_\varepsilon)$ kde δ_x je funkcia z Q do Q definovaná ako $\delta_x(q) = \delta(x, q)$. Potom M_A nazveme prechodovým monoidom.

Definícia 1.0.14. Homomorfizmus h definujeme ako také zobrazenie z A do B , že pre $\forall x, y \in A$ platí $h(x \cdot y) = h(x) \cdot h(y)$. Pod obrazom jazyka L pri zobrazení homomorfizmom h rozumieme $h(L) = \{h(w) \mid w \in L\}$. **Homomorfizmus monoidov:** Pod homomorfizmom z monoidu $(M, \cdot, e)$ do monoidu $(N, *, 1)$ rozumieme zobrazenie $h : M \rightarrow N$ s nasledovnými vlastnosťami:

- i. pre všetky $x, y \in M$ platí $h(x \cdot y) = h(x) * h(y)$
- ii. $h(e) = 1$.

Definícia 1.0.15. Antihomomorfizmus je zobrazenie z A do B , pre ktoré platí, že pre $\forall x, y \in A : h(x \cdot y) = h(y) \cdot h(x)$. **Antihomomorfizmus monoidov** $(M, \cdot, e)$ a $(N, *, 1)$ je zobrazenie $h : M \rightarrow N$ spĺňajúce podmienky:

- i. pre všetky $x, y \in M$ platí $h(x \cdot y) = h(y) * h(x)$
- ii. $h(e) = 1$.

Poznámka 1.0.16. Môžeme si všimnúť, že ak pre automat $A = (S, Q, \delta, q_0, F)$ definujeme zobrazenie $h : S \rightarrow M_A$, kde M_A je prechodový monoid, ako $h(x) = \delta_x$ a pod operáciou $\circ$ budeme rozumieť také skladanie zobrazení, že $(g \circ f)(x) = g(f(x))$, potom zobrazenie h bude antihomomorfizmom. Z definície akcie totiž platí, že $\delta_{xy} = \delta_y \circ \delta_x$. Z tohto dôvodu budeme často predpokladať, že sa zobrazenia skladajú v opačnom poradí, teda že $(g \cdot f)(x) = f(g(x))$. Pri takomto skladaní bude δ_{xy} rovné $\delta_x \cdot \delta_y$ a zobrazenie h teda bude homomorfizmom. Namiesto zápisu $h(x)(q)$ resp. $\delta_x(q)$ potom môžeme používať stručnejší zápis $q \cdot x$.

Príklad 1.0.17. Majme monoid $A = (\Sigma^*, \cdot, \varepsilon)$, monoid $B = (\mathbb{N}, +, 0)$ a homomorfizmus $f : \Sigma^* \rightarrow \mathbb{N}$ definovaný ako $f(w) = |w|$. Potom f je homomorfizmom monoidov A a B .

Kapitola 2

Rozoznávane jazykov monoidmi

Definícia 2.0.1. Jazyk rozoznávaný homomorfizmom: Hovoríme, že jazyk $L \subseteq \Sigma^*$ je rozoznávaný homomorfizmom $h : \Sigma^* \rightarrow M$, ak existuje $X \subseteq M$ také, že $L = h^{-1}(X)$

Definícia 2.0.2. Jazyk rozoznávaný monoidom: Jazyk $L \subseteq \Sigma^*$ je rozoznávaný monoidom $(M, \cdot, e)$, ak existuje homomorfizmus $h : \Sigma^* \rightarrow M$ rozoznávajúci jazyk L .

Veta 2.0.3. *Jazyk L je regulárny $\Leftrightarrow$ je rozoznávaný nejakým konečným monoidom*

Dôkaz. $\boxed{\Leftarrow}$ Nech L je jazyk rozoznávaný monoidom $(M, \cdot, e)$ cez homomorfizmus h a množinu X . Chceme dokázať, že potom jazyk L musí byť regulárny. Vieme, že jazyk L je regulárny $\Leftrightarrow$ existuje konečný automat A , pre ktorý platí $L(A) = L$. Ukážeme, že takýto automat naozaj existuje. Nech $A_M = (\Sigma^*, M, \delta, e, X)$ kde prechodová funkcia δ je definovaná ako $\delta(m, a) = m \cdot h(a)$, kde m je stav a a je znak vstupnej abecedy Σ . Potom pre každé $a_1, a_2, \dots, a_n \in \Sigma$ platí $\delta(m, a_1 a_2 \dots a_n) = m \cdot h(a_1) \cdot h(a_2) \cdot \dots \cdot h(a_n)$. Keďže na začiatku čítania slova je stav (m) automatu A_M počiatočný stav e , ktorý je zároveň neutrálnym prvkom vzhľadom na operáciu $\cdot$, automat každé vstupné slovo $w = a_1 \dots a_n$ dočíta v stave $e \cdot h(a_1 \dots a_n) = h(a_1 \dots a_n) = h(w)$. Vieme, že slovo w patrí do jazyka automatu práve vtedy, keď existuje akceptačný výpočet na slove w , teda ak sa automat po dočítaní slova w nachádza v nejakom zo svojich akceptačných stavov. Množina akceptačných stavov automatu A_M zodpovedá množine X , pre ktorú platí $L = h^{-1}(X)$ (teda $L = \{x \in \Sigma^* \mid h(x) \in X\}$). Jazyk automatu A_M je teda rovný množine slov w nad abecedou Σ , pre ktoré platí $h(w) \in X$, čiže $L(A_M) = \{w \in \Sigma^* \mid h(w) \in X\}$. Zrejme platí rovnosť $L(A_M) = L$, takže sme naozaj zostrojili konečný automat akceptujúci jazyk L , a jazyk L je naozaj regulárny.

$\boxed{\Rightarrow}$ Predpokladajme teraz, že L je regulárny jazyk; dokážeme, že existuje konečný monoid, ktorý ho rozoznáva. Ak L je regulárny jazyk, potom existuje deterministický konečný automat $A = (\Sigma^*, Q, \delta, q_0, F)$ taký, že $L(A) = L$. Nech $M_A = (M, \cdot, Id_K)$ je prechodový monoid, $M = \{\delta_x \mid x \in \Sigma^*\}$ a nech h je homomorfizmus zo Σ^* do M definovaný ako $h(x) = \delta_x$ (pozri poznámku). Homomorfizmus h teda každému vstupnému slovu priradí funkciu, ktorá pre dané vstupné slovo a stav, v ktorom sa automat nachádza na začiatku čítania slova, vráti stav, v ktorom bude automat, keď slovo dočíta. Nech ďalej X je podmnožina M , pre ktorú platí $X = \{\delta_x \mid \delta_x(q_0) \in F\}$. X je teda množina práve tých funkcií od slova x , že automat A dočíta x v nejakom zo svojich akceptačných stavov. Potom $h^{-1}(X)$ je zrejme $= L(A)$, pretože $h^{-1}(X)$ zodpovedá množine slov, na ktorých výpočet automatu A skončí v stave $q \in F$. Jazyk L je teda skutočne rozoznávaný konečným monoidom. $\square$

Kapitola 3

Syntaktický monoid

Definícia 3.0.1. Kontext slova: Nech L je jazyk nad abecedou Σ . Kontextom slova w v jazyku L nazývame ľubovoľný prvok množiny $c_L(w) = \{(x, y) \in \Sigma^* \times \Sigma^* \mid xwy \in L\}$. Pod **pravým kontextom** slova w rozumieme prvok množiny $c_L^r(w) = \{x \in \Sigma^* \mid wx \in L\}$ a pod **ľavým kontextom** slova w rozumieme prvok z $c_L^l(w) = \{x \in \Sigma^* \mid xw \in L\}$.

Definícia 3.0.2. Kongruencia: Nech $\equiv$ je relácia na monoide $(M, \cdot, 1)$ taká, že pre všetky u, v patriace monoidu M platí

$$u \equiv v \implies \forall x, y \in M : x \cdot u \cdot y \equiv x \cdot v \cdot y \quad (3.1)$$

Potom reláciu $\equiv$ nazývame kongruenciou (alebo tiež obojstranne invariantnou reláciou ekvivalencie).

Definícia 3.0.3. Syntaktická ekvivalencia: Majme jazyk L nad abecedou Σ . Potom binárnu reláciu $\sim_L$ na Σ^* indukovanú jazykom L nazývame **syntaktická ekvivalencia** (alebo tiež **syntaktická kongruencia**), ak pre všetky $u, v \in \Sigma^*$ platí:

$$u \sim_L v \iff (\forall x, y \in \Sigma^* : xuy \in L \iff xvy \in L) \quad (3.2)$$

Definícia 3.0.4. Relácia ekvivalencie **nasycuje** množinu L práve vtedy, keď L je zjednotením niekoľkých tried ekvivalencie danej relácie. To znamená, že každá trieda ekvivalencie obsahuje buď iba prvky množiny L , alebo iba prvky mimo L .

Tvrdenie 3.0.5. Nech L je jazyk nad abecedou Σ . Potom je syntaktická ekvivalencia $\sim_L$ kongruenciou nasycujúcou L .

Dôkaz. Syntaktická ekvivalencia je zrejme reláciou ekvivalencie, čo vyplýva okrem iného aj z pozorovania, že pre 2 slová $u, v \in \Sigma^*$ platí $u \sim_L v \iff c_L(u) = c_L(v)$. Nech u, v sú slová nad abecedou Σ , pre ktoré platí $u \sim_L v$ a nech $x = y = \varepsilon$. Potom z definície $\sim_L$: $xuy \in L \iff xvy \in L$, teda $u \in L \iff v \in L$, čo znamená, že $\sim_L$ nasycuje jazyk L . Ešte potrebujeme dokázať, že je syntaktická ekvivalencia kongruenciou, teda že ak pre slová $u, v \in \Sigma^*$ platí $u \sim_L v$ tak $\forall x, y \in \Sigma^* : xuy \sim_L xvy$. Nech teda $u, v \in \Sigma^*$ a $u \sim_L v$. Potom $\forall x, y \in \Sigma^* : xuy \in L \iff xvy \in L$. Táto vlastnosť platí pre všetky x, y , teda aj pre $x = \tilde{x}\tilde{x}$ pre nejaké $\tilde{x}$ nad abecedou Σ a tiež pre $y = \tilde{y}\tilde{y}$ pre nejaké $\tilde{y} \in \Sigma^*$. Potom pre všetky $\tilde{x}, \tilde{y}$ platí $\tilde{x}\tilde{x}\tilde{y}\tilde{y} \in L \iff \tilde{x}\tilde{x}\tilde{y}\tilde{y} \in L$, z čoho vyplýva $\tilde{x}\tilde{u}\tilde{y} \sim_L \tilde{x}\tilde{v}\tilde{y}$ pre všetky $\tilde{x}, \tilde{y} \in \Sigma^*$ a teda relácia $\sim_L$ je naozaj kongruenciou. $\square$

Tvrdenie 3.0.6. *Nech L je jazyk nad abecedou Σ , $\equiv$ je ľubovoľná kongruencia na Σ^* nasycujúca L a nech u, v sú slová $\in \Sigma^*$ také, že $u \equiv v$. Potom platí aj $u \sim_L v$, kde $\sim_L$ je syntaktická ekvivalencia.*

Dôkaz. $u \equiv v$, preto z definície kongruencie musí platiť $\forall x, y \in \Sigma^* : xuy \equiv xvy$, teda slová xuy a xvy sa nachádzajú v rovnakej triede ekvivalencie. Keďže relácia nasycuje jazyk L , platí buď $xuy \in L \wedge xvy \in L$ alebo $xuy \notin L \wedge xvy \notin L$, čiže $xuy \in L \Leftrightarrow xvy \in L = u \sim_L v$ $\square$

Tvrdenie 3.0.7. *Nech $\equiv$ je binárna relácia na monoide $(M, \cdot, \varepsilon)$ a nech u, v sú prvky M také, že $u \equiv v$. Potom sú nasledujúce dve tvrdenia ekvivalentné.*

1. $\forall x, y \in M : xuy \equiv xvy$
2. $\forall x \in M : xu \equiv xv \wedge \forall y \in M : uy \equiv vy$

Dôkaz. 1. $\Rightarrow$ 2. Predpokladáme, že platí $\forall x, y \in M : xuy \equiv xvy$. Potom zrejme pre $y = \varepsilon$ platí $\forall x \in M : xu \equiv xv$ a zároveň obdobne pre $x = \varepsilon$ dostaneme $\forall y \in M : uy \equiv vy$

2. $\Rightarrow$ 1. Vieme, že pre ľubovoľné prvky M u, v t.ž. $u \equiv v$ platí 2. To znamená, že pre ľubovoľný prvok x monoidu M sú v relácii aj slová xu a xv , ktoré tiež patria do M a teda spĺňajú podmienky 2. tvdenia. Z neho vyplýva, že pre každé y z M aj $xuy \equiv xvy$ čím sme získali tvrdenie 1.

Dôsledkom tohto tvrdenia je, že by sme kongruenciu mohli ekvivalentne definovať aj pomocou 2. $\square$

Definícia 3.0.8. Faktorový monoid: Majme kongruenciu $\equiv$ a monoid $(M, \cdot, 1)$. Potom vieme definovať **faktorový monoid** ako trojicu $(M/\equiv, \circ, [1]_{\equiv})$ kde $M/\equiv$ je množina všetkých tried ekvivalencie relácie $\equiv$, $\circ$ je asociatívna binárna operácia definovaná pre všetky $x, y \in M$ ako $[x]_{\equiv} \circ [y]_{\equiv} = [x \cdot y]_{\equiv}$ (naozaj, $\forall x, y, z \in M : ([x]_{\equiv} \circ [y]_{\equiv}) \circ [z]_{\equiv} = [x \cdot y]_{\equiv} \circ [z]_{\equiv} = [x \cdot y \cdot z]_{\equiv} = [x]_{\equiv} \circ [y \cdot z]_{\equiv} = [x]_{\equiv} \circ ([y]_{\equiv} \circ [z]_{\equiv})$) a $[1]_{\equiv}$ je neutrálny prvok ($[x]_{\equiv} \circ [1]_{\equiv} = [x \cdot 1]_{\equiv} = [x]_{\equiv} = [1]_{\equiv} \circ [x]_{\equiv} = [1 \cdot x]_{\equiv} = [x]_{\equiv}$)

Táto operácia je definovaná korektne, pretože, ako ukážeme, nezáleží na výbere reprezentantov triedy ekvivalencie. Nech x_1, x_2 sú ľubovoľné prvky patriace M také, že platí $[x_1]_{\equiv} = [x_2]_{\equiv}$, teda $x_1 \equiv x_2$. Potom, podľa definície kongruencie (podľa tvrdenia 3.0.7) pre všetky y patriace M aj $x_1y \equiv x_2y$, t.j. $[x_1y]_{\equiv} = [x_2y]_{\equiv}$. Obdobne, ak pre nejaké y_1, y_2 z M platí $[y_1]_{\equiv} = [y_2]_{\equiv}$, teda $y_1 \equiv y_2$, potom $\forall x \in M : xy_1 \equiv xy_2$, čo znamená $[xy_1]_{\equiv} = [xy_2]_{\equiv}$. Teda keď máme dané 2 triedy ekvivalencie, bez ohľadu na to, ktoré 2 prvky z nich vyberieme na reprezentáciu daných tried, aplikovanie operácie $\circ$ na dve takéto triedy nám určite nevráti 2 rôzne výsledky.

Definícia 3.0.9. Syntaktický monoid: Nech L je regulárny jazyk nad abecedou Σ a nech $\sim_L$ je syntaktická kongruencia k tomuto jazyku. Keďže Σ^* s operáciou zretazovania a prázdny slovom ε tvorí monoid, aj k jazyku L vieme definovať faktorový monoid ako trojicu $(\Sigma^*/\sim_L, \cdot, [\varepsilon]_{\sim_L})$, ktorý budeme nazývať **syntaktický monoid**.

Veta 3.0.10. *Nech $L \subseteq \Sigma^*$ je regulárny jazyk, $\sim_L$ je k nemu prislúchajúca syntaktická ekvivalencia a $(\Sigma^*/\sim_L, \cdot, [\varepsilon]_{\sim_L})$ zodpovedajúci syntaktický monoid. Potom $(\Sigma^*/\sim_L, \cdot, [\varepsilon]_{\sim_L})$ je izomorfný s prechodovým monoidom minimálneho automatu akceptujúceho jazyk L .*

Dôkaz. Nech $L \in \mathcal{R}$ je jazyk nad abecedou Σ , $A = (\Sigma^*, Q, \delta, q_0, F)$ je minimálny konečný automat akceptujúci jazyk L a nech $M_A = (\{\delta_x \mid x \in \Sigma^*\}, \cdot, \delta_\varepsilon)$ je prechodový monoid k

automatu A . Ukážeme, že pre všetky $u, v \in \Sigma^*$ platí $u \sim_L v \iff \delta_u = \delta_v$.

$\Rightarrow$ *Sporom*. Nech u, v sú slová nad abecedou Σ . Za účelom sporu predpokladajme, že $u \sim_L v$ a zároveň $\delta_u \neq \delta_v$. To znamená, že existuje stav q taký, že $\delta_u(q) \neq \delta_v(q)$, teda $q \cdot u \neq q \cdot v$. Potom kvôli minimálnosti automatu A musí existovať slovo y nad abecedou Σ t.ž. $(q \cdot uy \in F \wedge q \cdot vy \notin F) \vee (q \cdot uy \notin F \wedge q \cdot vy \in F)$. BUNV nech $q \cdot uy \in F \wedge q \cdot vy \notin F$. Vieme, že v minimálnom automate sú všetky stavy dosiahnuteľné z počiatočného stavu q_0 , preto musí existovať aj slovo x nad abecedou Σ t.ž. $q_0 \cdot x = q$. To znamená, že $q_0 \cdot xuy$ patrí do množiny F a zároveň $q_0 \cdot xvy$ nepatrí do F , inými slovami $\exists x, y \in \Sigma^* : xuy \in L \wedge xvy \notin L$. To je ale spor s vlastnosťou $u \sim_L v$, čím sme dokázali prvú implikáciu.

$\Leftarrow$ *Priamo*. Nech u, v, x, y sú slová nad abecedou Σ a nech $\delta_u, \delta_v, \delta_x, \delta_y$ sú k nim prislúchajúce prvky prechodového monoidu M_A . Nech ďalej z predpokladu platí $\delta_u = \delta_v$. Potom musí platiť aj nasledujúca rovnosť: $\delta_{xuy} = \delta_x \cdot \delta_u \cdot \delta_y = \delta_x \cdot \delta_v \cdot \delta_y = \delta_{xvy}$. To znamená, že pokiaľ automat A v počiatočnom stave q_0 prečíta slová xuy a xvy , dostane sa do rovnakého stavu, teda že $q_0 \cdot xuy = q_0 \cdot xvy = q$ pre nejaký stav q . Pre tento stav môžu zrejme nastať iba 2 možnosti: buď q je akceptačný alebo q nie je akceptačný. Ak je akceptačný, potom platí $xuy \in L \wedge xvy \in L$. V opačnom prípade $xuy \notin L \wedge xvy \notin L$. Očividne teda pre ľubovoľné $x, y \in \Sigma^* : xuy \in L \iff xvy \in L$ a preto platí $u \sim_L v$.

Ukázali sme, že 2 slová w_1, w_2 sú v jednej triede relácie ekvivalencie $\sim_L$, teda že v monoide $(\Sigma^* / \sim_L, \cdot, [\varepsilon]_{\sim_L})$ predstavujú ten istý prvok, práve vtedy, keď sú si k nim prislúchajúce objekty $\delta_{w_1}, \delta_{w_2}$ rovné, teda keď predstavujú ten istý prvok v monoide $M_A = (\{\delta_x \mid x \in \Sigma^*\}, \cdot, \delta_\varepsilon)$. Syntaktický monoid a prechodový monoid teda majú "rovnakú štruktúru" a možno k nim definovať bijektívny homomorfizmus, ktorý na seba zobrazuje zodpovedajúce prvky. Hľadaným zobrazením môže byť napríklad homomorfizmus $h : M_A \rightarrow \Sigma^* / \sim_L$ definovaný ako $\delta_x \mapsto [x]_{\sim_L}$. $\square$