

1 Definície

Nech $\Sigma = \{a_1, \dots, a_m\}$ je abeceda, a $w = w_1 \dots w_n$ je slovo nad Σ . Potom pre w definujeme relačnú štruktúru $\underline{w} = (M, \leq^w, S^w, First^w, Last^w, a_1^w, \dots, a_m^w)$, kde $M = \{1, \dots, |w|\}$ je množina všetkých pozícií slova w , $\leq^w$ je relácia $\leq$ na množine M , $a_1^w, \dots, a_m^w$ sú unárne relácie na M také, že pre $i = 1, \dots, m$ platí $a_i^w = \{j \in M \mid w_j = a_i\}$. $S^w = \{(x, y) \in M^2 \mid y = x+1\}$. $First^w = \{(1)\}$, $Last^w = \{(|w|)\}$.

2 Veta: Jazyk je regulárny $\Leftrightarrow$ môže byť opísaný formulou v MSO.

2.1 Lema: Jazyk je regulárny $\Rightarrow$ môže byť opísaný formulou v MSO.

Nech L je regulárny jazyk. Potom existuje DKA $A = (K, \Sigma, \delta, q_0, F)$ taký, že $L(A) = L$, $K = \{q_0, q_1, \dots, q_n\}$. Majme MSO formulu ϕ :

$$\exists X_{q_0}, \dots, \exists X_{q_n}$$

$$\forall x \bigvee_{0 \leq i \leq n} (x \in X_{q_i}) \quad (i)$$

$$\wedge \forall x \bigwedge_{(p \in K)(q \in K)p \neq q} ((x \in X_p) \Rightarrow \neg(x \in X_q)) \quad (ii)$$

$$\wedge \forall x First(x) \Rightarrow (x \in X_{q_0}) \quad (iii)$$

$$\wedge \bigwedge_{(p \in K)(q \in K)(a \in \Sigma)} (\forall x)(\forall y)((q = \delta(p, a) \wedge S(x, y) \wedge x \in X_p \wedge a(x) \Rightarrow y \in X_q) \quad (iv)$$

$$\wedge \forall x Last(x) \Rightarrow \bigvee_{(p \in K)(q \in F)(a \in \Sigma)} (x \in X_p \wedge a(x) \wedge q \in \delta(p, a)) \quad (v)$$

$$\wedge (X_{q_0} = \emptyset) \Rightarrow (q_0 \in F) \quad (vi)$$

Jazyk definovaný formulou ϕ je $L(\phi) = \{w \in \Sigma^* \mid \underline{w} \models \phi\}$. Chceme dokázať, že $L(A) = L(\phi)$

2.1.1 Lema

Následne dokážeme lemu:

Nech $A = (K, \Sigma, \delta, q_0, F)$ je DKA, $K = \{q_0, \dots, q_n\}$ a nech $w = w_1 \dots w_k$ kde $w_1, \dots, w_k \in \Sigma, w \neq \varepsilon$. Ak pre w a $x \in \{1, \dots, k\}(\exists X_{q_0}^w, \dots, \exists X_{q_n}^w)$ také, že platí (i) - (iv), a platí $(q_0, w) \vdash_A^* (q_j, w_x w_{x+1} \dots w_k)$, tak $x \in X_{q_j}^w$.

D: MI na x

1° $x = 1$. Z (iii) $\rightarrow x \in X_{q_0}^w$

2° $x = l \rightarrow x = l + 1$

Ak $(q_0, w_1 \dots w_k) \vdash_A^* (q_j, w_{l+1} \dots w_k)$, tak keďže A je DKA, tak $\exists q_i \in K$ také, že $(q_0, w) \vdash_A^* (q_i, w_1 \dots w_k) \vdash_A (q_j, w_{l+1} \dots w_k)$, pričom $\delta(q_i, w_l) = q_j$. Z IP potom platí $l \in X_{q_i}^w$. Z (iv) vieme, že ak $l \in X_{q_i}^w$ a zároveň $w_l^w(l)$ a $S(x, y)$, tak $x \in X_{q_j}^w$.

2.1.2 $w \in L(A) \Rightarrow w \in L(\phi)$

Najprv dokážeme, že ak $\exists q \in K$ a $\exists m \in \mathbb{N}$ také, že $(q_0, w) \vdash_A^m (q, \epsilon)$, tak $(\exists X_{q_0}^w, \exists X_{q_1}^w, \dots, \exists X_{q_n}^w)$ také, že platí (i) - (iv).

D: MI na m:

1° $m = 0$. Ak $(q_0, w) \vdash_A^0 (q, \epsilon)$, tak nutne $q = q_0, w = \epsilon$. Takže (i) - (iv) platí, pretože $M = \emptyset$, a teda v každej časti (i) - (iv) kvantifikujeme všeobecným kvantifikátorom cez prázdnu množinu.

2° $m = k \rightarrow m = k + 1$

Ak $(q_0, w) \vdash_A^{k+1} (q, \epsilon)$, tak keďže A je deterministický, tak posledný krok musel byť na písmeno, a teda $(q_0, uc) \vdash_A^k (q_j, c) \vdash_A (q, \epsilon)$ pre nejaké $q_j \in K, u \in \Sigma^+, c \in \Sigma$ také, že $w = uc$ a zároveň $\delta(q_j, c) = q$. Keďže každý krok bol na písmeno, tak $|w| = k + 1, |u| = k$. Platí $c^w(k + 1)$. Z IP pre u vieme, že $\exists X_{q_0}^u, \exists X_{q_1}^u, \dots, \exists X_{q_n}^u$ také, že platia (i) - (iv). Položme $X_{q_0}^w = X_{q_0}^u, \dots, X_{q_{j-1}}^w = X_{q_{j-1}}^u, X_{q_j}^w = X_{q_j}^u \cup \{k + 1\}, X_{q_{j+1}}^w = X_{q_{j+1}}^u, \dots, X_{q_n}^w = X_{q_n}^u$. Dokážeme, že pre $\forall x \in \{1, \dots, k\}$ a $X_{q_0}^w, \dots, X_{q_n}^w$ platí (i) - (iv).

(i) - (iv) pre $x \in \{1, \dots, k\}$

(i) Keďže $u \in L(\phi)$, tak $\forall x \in \{1, \dots, k\} (\bigvee_{0 \leq i \leq k} x \in X_{q_i}^u)$. Keďže $\forall i \in \{1, \dots, n\}$ platí $X_{q_i}^u \subseteq X_{q_i}^w$, tak platí $\forall x \in \{1, \dots, k\} \bigvee_{0 \leq i \leq k} x \in X_{q_i}^w$.

(ii) Podľa IP $\rightarrow (\forall x \in \{1, \dots, k\}) \bigwedge_{(p \in K)(q \in K)p \neq q} (x \in X_p^u \Rightarrow \neg(x \in X_q^u))$.

Chceme dokázať $\forall x \in \{1, \dots, k\} \bigwedge_{(p \in K)(q \in K)p \neq q} (x \in X_p^w \Rightarrow \neg(x \in X_q^w))$. Môžu nastať 3 možnosti:

1. $X_p^w = X_{q_j}^w$.

Chceme dokázať, že $\forall x \in \{1, \dots, k\} \bigwedge_{(q \in K)(q \neq q_j)} (x \in X_{q_j}^w \Rightarrow \neg(x \in X_q^w))$.

Ak $x \in \{1, \dots, k\}$, tak $x \neq k + 1$, a teda ak $x \in X_{q_j}^w$ tak $x \in X_{q_j}^u$. Z IP $\rightarrow \bigwedge_{(q \in K)(q \neq q_j)} \neg(x \in X_q^u)$. Ak $q \neq q_j$, tak $X_q^u = X_q^w$, a teda platí $\bigwedge_{(q \in K)(q \neq q_j)} \neg(x \in X_q^w)$.

2. $X_p^w \neq X_{q_j}^w \wedge X_q^w = X_{q_j}^w$

Chceme dokázať, že $\forall x \in \{1, \dots, k\} \bigwedge_{(p \in K)(p \neq q_j)} (x \in X_p^w \Rightarrow \neg(x \in X_{q_j}^w))$. Z IP

platí $\bigwedge_{(p \in K)(p \neq q_j)} (x \in X_p^u \Rightarrow \neg(x \in X_{q_j}^u))$. Platí, že ak $X_p^w \neq X_{q_j}^w$, tak $X_p^w = X_p^u$, a keďže $X_{q_j}^w = X_{q_j}^u \cup \{k + 1\}$, a $x \neq k + 1$, tak ak $\neg(x \in X_{q_j}^u)$ tak $\neg(x \in X_{q_j}^w)$.

Z toho vyplýva $\forall x \in \{1, \dots, k\} \bigwedge_{(p \in K)(p \neq q_j)} (x \in X_p^w \Rightarrow \neg(x \in X_{q_j}^w))$.

3. $X_p^w \neq X_{q_j}^w \wedge X_q^w \neq X_{q_j}^w$.

Ostáva dokázať, $\forall x \in \{1, \dots, k\} \bigwedge_{(p \in K)(q \in K)(p \neq q \wedge p \neq q_j \wedge q \neq q_j)} (x \in X_p^w \Rightarrow \neg(x \in X_q^w))$. Keďže z IP platí $\bigwedge_{(p \in K)(q \in K)(p \neq q \wedge p \neq q_j \wedge q \neq q_j)} (x \in X_p^u \Rightarrow \neg(x \in X_q^u))$, a

$(\forall q \in K)((q \neq q_j) \Rightarrow (X_q^w = X_q^u))$, tak tvrdenie platí.

(iii) Z IP vieme, že pre u platí $First(x) \Rightarrow x \in X_{q_0}^u$. Teda ak $|u| \geq 1$, tak $1 \in X_{q_0}^u$. Keďže $X_{q_0}^u \subseteq X_{q_0}^w$, tak $First(x) \Rightarrow x \in X_{q_0}^w$. Ak $|u| = 0$, tak $w = c$. Teda platilo $(q_0, c) \vdash_A^0 (q_0, c)$, a teda $X_{q_0}^w = X_{q_0}^u \cup \{1\} = \{1\}$, $1 \in X_{q_0}^w$.

(iv) Dokážeme pre všetky $x \in \{1, \dots, k-1\}$. Keďže $w = uc$, tak $\forall x \in \{1, \dots, k\}$ $a^w(x) \Leftrightarrow a^u(x)$. Ak $x \in X_p^w$, $x \neq k+1$, tak $x \in X_p^u$. Čiže ak $x \in \{1, \dots, k-1\} \wedge a^w(x) \wedge S(x, y) \Rightarrow x \in X_p^u \wedge a^u(x) \wedge S(x, y)$. Ak navyše $\delta(p, a) = q$, tak z IP pre u platí $y \in X_q^u \subseteq X_q^w$, a teda $y \in X_q^w$.

(i) - (iv) pre $x = k + 1$

Teraz dokážeme (i) - (iii) pre $x = k + 1$ a $X_{q_0}^w, \dots, X_{q_n}^w$, a (iv) pre $x = k$, $x = k + 1$.

(i) Keďže $X_{q_j}^w = X_{q_j}^u \cup \{k+1\}$, tak $x \in X_{q_j}^w$.

(ii) Chceme dokázať, že $\bigwedge_{(p \in K)(q \in K)p \neq q} ((x \in X_p^w) \Rightarrow \neg(x \in X_q^w))$ Vieme, že $x \in X_{q_j}^w$. Keďže $(\forall q \in K)((q \neq q_j) \Rightarrow (X_q^w = X_q^u))$, a platí $X_{q_i}^u \subseteq \{1, \dots, k\}$ tak $\forall q((q \neq q_j) \Rightarrow \neg(x \in X_q^w))$. Takže jediný prípad, kedy bude ľavá strana implikácie platiť bude, ak $X_p^w = X_{q_j}^w$. Potom platí, že $\bigwedge_{(q \in K)p \neq q} ((x \in X_{q_j}^w) \Rightarrow \neg(x \in X_q^w))$.

(iii) Jediný prípad kedy bude splnený predpoklad $First(x)$ bude, ak $k = 0$. Potom $|u| = 0$, takže $w = c$. Teda platilo $(q_0, c) \vdash_A^0 (q_0, c)$, a $X_{q_0}^w = X_{q_0}^u \cup \{1\} = \{1\}$, $1 \in X_{q_0}^w$.

(iv) Nech $x = k$. Ak $k = 0$, tak predpoklad nie je splnený, pretože $x = 0$. Ak $k \geq 1$ a platí $(q_0, w) \vdash^* (q_j, w_{k+1})$, a A je DKA, tak $\exists q_p \in K$ také, že $(q_0, w) \vdash_A^* (q_p, w_k w_{k+1}) \vdash (q_j, w_{k+1})$, a platí $\delta(q_p, w_k) = q_j$. Keďže platí $(q_0, w_1 \dots w_{k+1}) \vdash_A^* (q_p, w_k w_{k+1})$ a pre $u = w_1 \dots w_k$ platí (i) - (iv), tak podľa lemy $x = k \in X_{q_p}^u \subseteq X_{q_p}^w$. Keďže $x \in X_{q_p}^w$, tak z (ii) vieme, $(\forall q \in K)((q \neq q_p) \Rightarrow \neg(x \in X_q^w))$. Keďže platí $w_k^w(k)$, a na jednej pozícii nemôže byť viac znakov, tak $(\forall a \in \Sigma)((a \neq w_k) \Rightarrow \neg(a^w(k)))$. Teda predpoklad môže platiť len pre $X_p^w = X_{q_p}^w$ a pre $a = w_k$. Vieme, že $(k+1) \in X_{q_j}^w$, a teda ak $y = k + 1$, tak $y \in X_{q_j}^w$. Skutočne teda platí $x \in X_{q_p}^w \wedge w_k^w(k) \wedge S(x, y) \Rightarrow y \in X_{q_j}^w$. Ak $x = k + 1$, tak neexistuje $y \in X^w$ aby platilo $y = x + 1$. A preto predpoklad nikdy nie je splnený, a teda tvrdenie platí.

(v) a (vi)

Teraz dokážeme, že ak $w \in L(A)$, tak pre $X_{q_0}^w, \dots, X_{q_n}^w$ platí (v) a (vi).

Ak $w \in L(A)$, tak platí $(q_0, w) \vdash_A^* (q, \varepsilon)$ pre nejaké $q \in F$. Ak $w = \varepsilon$, tak platí (v), pretože $M = \emptyset$, a teda kvantifikujeme cez prázdnu množinu. Navyše platí $(q_0, \varepsilon) \vdash_A^0 (q_0, \varepsilon)$, a teda $q_0 \in F$, je teda splnená aj (vi).

Ak $w \in \Sigma^+$, tak potom $w = uc$ pre nejaké $u \in \Sigma^*$, $c \in \Sigma$ a ak A je DKA, tak $\exists p \in K$ take, že $(q_0, uc) \vdash^* (p, c) \vdash (q, \varepsilon)$ a platí $\delta(p, c) = q$. Keďže $q \in F$, tak

$\delta(p, c) \in F$. Nech $|w| = k$. Potom platí $c^w(k)$ a $Last^w(k)$, a $\forall l \in X^w (l \neq k)$ neplatí $Last^w(l)$, pretože $k > l$. Keďže pre w platí (i) - (iv), tak z lemy vieme, že $k \in X_p^w$. Teda skutočne platí $\forall x (Last^w(x) \Rightarrow \bigvee_{\delta(p,c) \in F} (x \in X_p^w \wedge c^w(x)))$. Ak $w \neq \varepsilon$, tak $|w| \geq 1$. Potom z (iii) platí, že $1 \in X_{q_0}^w$, $X_{q_0}^w \neq \emptyset$, a teda v (vi) nie je splnený predpoklad, a tvrdenie platí.

2.1.3 $w \in L(A) \Leftarrow w \in L(\phi)$

Ak $w = \varepsilon$, tak $M = \emptyset$, a teda $X_{q_0}^w = \emptyset$. Z (vi) teda vyplýva, že $q_0 \in F$. Platí $(q_0, \varepsilon) \vdash_A^0 (q_0, \varepsilon)$, a teda $w \in L(A)$.

$w \in \Sigma^+$. Nech $w = w_1 \dots w_k$. Keďže A je deterministický, tak $\exists q \in K$ také, že $(q_0, w) \vdash_A^* (q_i, w_k)$. Platí $Last^w(k)$, a vďaka (v) $k \in X_p^w \wedge a^w(k)$ pre nejaké $p \in K$ a $a \in \Sigma$ také, že $\delta(p, a) \in F$. Keďže pre w platí (i) - (iv), tak z lemy $k \in X_{q_i}^w$. Z (ii) vyplýva, že ak $(k \in X_{q_i}^w \wedge k \in X_p^w)$, tak $q_i = p$. Keďže $w = w_1 \dots w_k$, tak platí $w_k^w(k)$ a keďže na jednej pozícii nemôže mať viac písmen, tak $a = w_k$. Takže $\delta(q_i, w_k) = q \in F$. A teda $(q_0, w) \vdash^* (q_i, w_k) \vdash (q, \varepsilon)$ a $q \in F$ a teda $w \in L(A)$.

2.1.4 Záver

Týmto sme dokázali, že slová vyhovujúce MSO formule M sú presne slová, ktoré akceptuje automat A . Takže ak L je regulárny, tak existuje MSO formula, ktorá ho opisuje.