

Języki, automaty i obliczenia

Wykład 4: Minimalizacja automatów skończonych

Sławomir Lasota

Uniwersytet Warszawski

18 marca 2015

- 1 Twierdzenie Myhill-Nerode'a
- 2 Minimalizacja automatów deterministycznych
- 3 *Automaty a monoidy

Notacja

$w^{-1}L$ zamiast $\{w\}^{-1}L = \{u \in A^* : wu \in L\}$

Język $L \subseteq A^*$ określa relację równoważności w A^* :

$$\begin{aligned}w \sim_L v &\iff w^{-1}L = v^{-1}L \\ &\iff \forall u \in A^*. (wu \in L \iff vu \in L)\end{aligned}$$

Fakt ($\sim_L$ jest L -niezmiennicza)

$$w \sim_L v \implies (w \in L \iff v \in L)$$

rysunek

Dowód:

$$w \in L \iff \varepsilon \in w^{-1}L$$

$$w \sim_L v \iff \forall u \in A^*. (wu \in L \iff vu \in L)$$

Przykład

$$A = \{a, b\}$$

$$\varepsilon^{-1}L = L$$

$$\varepsilon \sim_L ab \sim_L abab$$

$$L = (ab)^*$$

$$a^{-1}L = bL$$

$$a \sim_L aba \sim_L ababa$$

$$b^{-1}L = \emptyset$$

$$b \sim_L aa \sim_L abb$$

$$A = \{a, b\}$$

$$(a^k)^{-1}L = \{a^n b^{n+k} : n \in \mathbb{N}\}$$

$$L = \{a^n b^n : n \in \mathbb{N}\}$$

Twierdzenie (Myhill-Nerode 1958)

Niech $L \subseteq A^*$. Następujące warunki są równoważne:

- L jest regularny
- $\sim_L$ ma skończony indeks

Niech $\mathcal{A} = (A, Q, \{q_0\}, F, \delta)$ automat deterministyczny rozpoznający L .

Fakt

$L_{\widehat{\delta}(q_0, w)}(\mathcal{A}) = w^{-1}L$, dla każdego $w \in A^*$.

Zdefiniujmy relację równoważności $\sim_{\mathcal{A}}$ na A^* :

$$w \sim_{\mathcal{A}} v \iff \widehat{\delta}(q_0, w) = \widehat{\delta}(q_0, v).$$

Relacja ta ma skończony indeks. Używamy faktu powyżej, by dowieść

$$w \sim_{\mathcal{A}} v \implies w \sim_L v.$$

Czyli indeks relacji $\sim_L$ jest nie większy niż indeks relacji $\sim_{\mathcal{A}}$.

Wniosek

Każdy automat deterministyczny rozpoznający język L ma przynajmniej indeks($\sim_L$) stanów.

Fakt ($\sim_L$ jest prawą kongruencją)

$$w \sim_L v \implies w a \sim_L v a$$

Dowód:

$$(w a)^{-1} L = a^{-1} (w^{-1} L) = a^{-1} (v^{-1} L) = (v a)^{-1} L$$

Konstruujemy automat deterministyczny $\mathcal{A}_L$:

- $Q' = A^* / \sim_L = \{[w]_{\sim_L} : w \in A^*\}$
- $q'_0 = [\varepsilon]_{\sim_L}$
- $F' = \{[w]_{\sim_L} : w \in L\}$
- $\delta'([w]_{\sim_L}, a) = [w a]_{\sim_L}$

Fakt

$$L(\mathcal{A}_L) = L$$

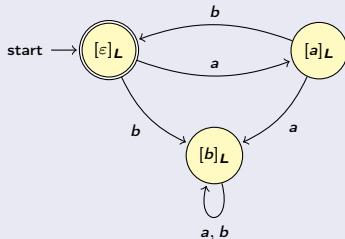
Dowód:

$$\hat{\delta}'([\varepsilon]_{\sim_L}, w) = [w]_{\sim_L} \in F \iff w \in L$$

- $Q' = A^*/\sim_L = \{[w]_{\sim_L} : w \in A^*\}$
- $q'_0 = [\varepsilon]_{\sim_L}$
- $F' = \{[w]_{\sim_L} : w \in L\}$
- $\delta'([w]_{\sim_L}, a) = [w a]_{\sim_L}$

Przykład

$L = (a b)^*$



Konstruujemy automat deterministyczny $\mathcal{A}_L$:

- $Q' = \{w^{-1}L : w \in A^*\}$
- $q'_0 = L = \varepsilon^{-1}L$
- $F' = \{M \in Q' : \varepsilon \in M\}$
- $\delta'(M, a) = a^{-1}M$

Fakt

$$\widehat{\delta}'(q'_0, w) = w^{-1}L$$

Dowód:

$$a^{-1}(w^{-1}L) = (wa)^{-1}L$$

Fakt

$$L(\mathcal{A}_L) = L$$

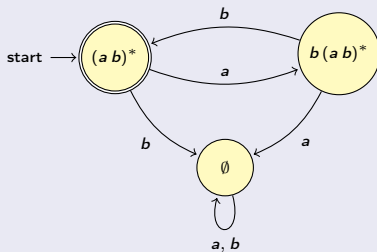
Dowód:

$$w \in L(\mathcal{A}_L) \iff \widehat{\delta}'(q'_0, w) \in F' \iff \varepsilon \in w^{-1}L \iff w \in L$$

- $Q' = \{w^{-1}L : w \in A^*\}$
- $q'_0 = L = \varepsilon^{-1}L$
- $F' = \{M \in Q' : \varepsilon \in M\}$
- $\delta'(M, a) = a^{-1}M$

Przykład

$L = (ab)^*$



Wniosek

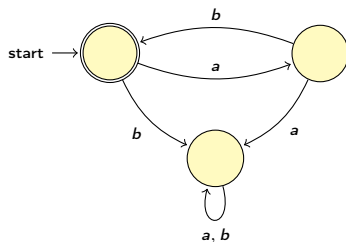
*Każdy automat deterministyczny rozpoznający L ma przynajmniej $\text{indeks}(\sim_L)$ stanów.
Automat $\mathcal{A}_L$ ma $\text{indeks}(\sim_L)$ stanów.*

*Czyli $\mathcal{A}_L$ to **minimalny** automat deterministyczny rozpoznający język L .*

Pytanie

Czy automat minimalny jest wyznaczony jednoznacznie?

Niech $L = (ab)^*$. Czy ten automat jest minimalny?



Każdy automat deterministyczny rozpoznający $L = (ab)^*$ ma przynajmniej 3 stany.

Dowód:

	ϵ	a	b
ϵ	$\times$	b	ab
a	$\times$	$\times$	b
b	$\times$	$\times$	$\times$

$\epsilon b \notin L$ $ab \in L$

$\epsilon ab \in L$ $bab \notin L$

$ab \in L$ $bb \notin L$

- 1 Twierdzenie Myhill-Nerode'a
- 2 Minimalizacja automatów deterministycznych
- 3 *Automaty a monoidy

Niech $\mathcal{A} = (A, Q, \{q_0\}, F, \delta)$ automat deterministyczny.

Kongruencja w $\mathcal{A}$ to relacja równoważności $R \subseteq Q \times Q$ taka, że

- $R(q, p) \implies (q \in F \iff p \in F)$
- $R(q, p) \implies r(\delta(q, a), \delta(p, a))$, dla każdego $a \in A$

Automat ilorazowy $\mathcal{A}/R$:

- $A' = A$
- $Q' = \{[q]_R : q \in Q\} = Q/R$
- $q'_0 = [q_0]_R$
- $F' = \{[q]_R : q \in F\} = F/R$
- $\delta'([q]_R, a) = [\delta(q, a)]_R$

Fakt

$$L(\mathcal{A}/R) = L(\mathcal{A})$$

Dowód:

$$\widehat{\delta'}([q_0]_R) = [\widehat{\delta}(q_0)]_R$$

Niech $\mathcal{A} = (A, Q, \{q_0\}, F, \delta)$ automat deterministyczny. Niech $L = L(\mathcal{A})$.
Założmy, że wszystkie stany automatu $\mathcal{A}$ są osiągalne.

Fakt

$L_{\widehat{\delta}(q_0, w)}(\mathcal{A}) = w^{-1}L$, dla każdego $w \in A^*$.

Definiujemy kongruencję w $\mathcal{A}$ następująco:

$$R_{\mathcal{A}}(q, p) \text{ wtw. gdy } L_q(\mathcal{A}) = L_p(\mathcal{A})$$

Fakt

Automaty $\mathcal{A}/R_{\mathcal{A}}$ i $\mathcal{A}_L$ są izomorficzne.

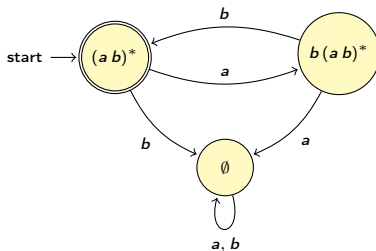
Dowód:

- | | |
|--|---|
| • $Q' = \{L_q(\mathcal{A}) : q \in Q\}$ | • $Q' = \{w^{-1}L : w \in A^*\}$ |
| • $q'_0 = L_{q_0}(\mathcal{A})$ | • $q'_0 = L = \varepsilon^{-1}L$ |
| • $F' = \{L_q(\mathcal{A}) : q \in F\}$ | • $F' = \{M \in Q' : \varepsilon \in M\}$ |
| • $\delta'(L_q(\mathcal{A}), a) = L_{\delta(q, a)}(\mathcal{A})$ | • $\delta'(M, a) = a^{-1}M$ |

Wniosek

Automat minimalny $\mathcal{A}_L$ jest wyznaczony jednoznacznie (z dokładnością do izomorfizmu).

$$L = (ab)^*$$



Problem obliczeniowy

Dane: automat deterministyczny $\mathcal{A}$

Wynik: automat (izomorficzny do automatu) $\mathcal{A}_L$

Algorytm

usuń stany nieosiągalne z automatu $\mathcal{A}$

oblicz relację $R_{\mathcal{A}}$

oblicz automat ilorazowy $\mathcal{A}/R_{\mathcal{A}}$

Niech $\mathbb{P}$ będzie podziałem zbioru Q .

Dla $X, Y \in \mathbb{P}$ i $a \in A$ powiemy, że (a, Y) łamie X jeśli

rysunek

- $X_{a,Y}^{\text{tak}} = \{q \in X : \delta(q, a) \in Y\} \neq \emptyset$,
- $X_{a,Y}^{\text{nie}} = \{q \in X : \delta(q, a) \notin Y\} \neq \emptyset$.

Niech $\mathbb{P}_{X,a,Y} = P - X \cup \{X_{a,Y}^{\text{tak}}, X_{a,Y}^{\text{nie}}\}$.

Podział $\mathbb{P}$ jest *stabilny* jeśli nie ma $X, Y \in \mathbb{P}$ i $a \in A$ t.ż. (a, Y) łamie X .

Fakt

Relacja R_A odpowiada największemu stabilnemu podziałowi.

Algorytm

$\mathbb{P} := \{F, Q - F\}$

dopóki $\mathbb{P}$ nie jest stabilny, powtarzaj

znajdź $X, Y \in P$ oraz $a \in A$, t.ż. (a, Y) łamie X

$\mathbb{P} := \mathbb{P}_{X,a,Y}$

- 1 Twierdzenie Myhilla-Nerode'a
- 2 Minimalizacja automatów deterministycznych
- 3 *Automaty a monoidy

Monoid $\mathbb{M} = (M, \cdot, 1)$ to

- zbiór M
- łączna operacja $\cdot : M^2 \rightarrow M$, tzn.

$$(m \cdot n) \cdot k = m \cdot (n \cdot k), \text{ dla } m, n, k \in M.$$

- element neutralny $1 \in M$, tzn.

$$1 \cdot m = m \cdot 1 = m, \text{ dla } m \in M$$

Przykład

$$(A^*, \cdot, \varepsilon) \quad (\mathcal{P}(A^*) - \emptyset, \cdot, \{\varepsilon\}) \quad (\mathbb{N}, +, 0) \quad (\{0 \dots k-1\}, +_k, 0)$$

Homomorfizm z $\mathbb{M}$ do $\mathbb{M}'$ to funkcja $h : M \rightarrow M'$ t.ż.

- $f(m \cdot n) = f(m) \cdot' f(n)$,
- $f(1) = 1'$

Przykład

$$a \mapsto \{a\} \quad L \mapsto \min\{|w| : w \in L\} \quad n \mapsto n \bmod k$$

Monoid $\mathbb{M} = (M, \cdot, 1)$ rozpoznaje język $L \subseteq A^*$ jeśli istnieje homomorfizm z A^* na $\mathbb{M}$:

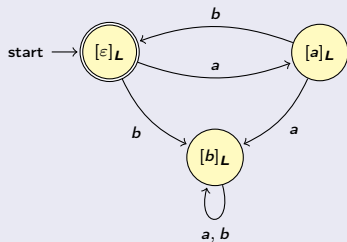
$$h : A^* \rightarrow \mathbb{M}$$

i podzbiór $X \subseteq M$ t.że

$$L = h^{-1}(X).$$

Przykład

$$L = (ab)^*$$



$$M = \{\varepsilon, a, b, ba, aa\}$$

$$1 = \varepsilon$$

	ε	a	b	ba	aa
ε					
a		aa	ε	a	
b		ba	aa	aa	
ba		aa	b	ba	
aa					

$$X = \{\varepsilon\}$$

Twierdzenie

Niech $L \subseteq A^$. Następujące warunki są równoważne:*

- *L jest regularny*
- *L jest rozpoznawany przez skończony monoid*

Niech $\mathcal{A} = (A, Q, I, F, \delta)$.

Słowo $w \in A^*$ determinuje relację $\delta_w \subseteq Q \times Q$:

$$\delta_\varepsilon = \{(q, q) : q \in Q\} \quad \delta_a = \{(q, q') : (q, a, q') \in \delta\} \quad \delta_{aw} = \delta \circ \delta_w$$

Definiujemy *monoid przejść* $\mathbb{M} = (M, \circ, \delta_\varepsilon)$, gdzie

$$M = \{\delta_w : w \in A^*\} \subseteq \mathcal{P}(Q \times Q),$$

homomorfizm $h : A^* \rightarrow \mathbb{M}$ z A^* na $\mathbb{M}$

$$w \mapsto \delta_w,$$

oraz podzbiór $X \subseteq M$:

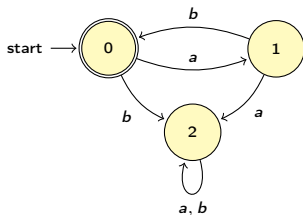
$$X = \{r \in M : \exists q \in I, q' \in F. r(q, q')\}.$$

Fakt

$$w \in L(\mathcal{A}) \iff h(w) \in X$$

Dowód:

$$w \in L(\mathcal{A}) \iff \exists q \in I, q' \in F. (q, q') \in \delta_w \iff \delta_w = h(w) \in X$$

Automat $\mathcal{A}$ 

$$\mathbb{M} = (\{\delta_\varepsilon, \delta_a, \delta_b, \delta_{ba}, \delta_{aa}\}, \circ, \delta_\varepsilon)$$

$$\delta_\varepsilon = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\delta_a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \delta_b = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\delta_{ba} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \delta_{aa} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$X = \{\delta_\varepsilon\}$$

$\circ$	ε	a	b	ba	aa
ε					
a		aa	ε	a	
b		ba	aa	aa	
ba		aa	b	ba	
aa					

Niech $\mathbb{M} = (M, \cdot, 1)$ będzie skończonym monoidem, $h : A^* \rightarrow \mathbb{M}$, oraz $X \subseteq M$.

Definiujemy automat deterministyczny $\mathcal{A}$:

- $Q = M$
- $I = \{1\}$
- $F = X$
- $\delta(m, a) = m \cdot h(a) \qquad \hat{\delta}(m, w) = m \cdot h(w)$

Fakt

$$w \in L(\mathcal{A}) \iff h(w) \in X$$

Dowód:

$$w \in L(\mathcal{A}) \iff \hat{\delta}(1, w) \in X \iff 1 \cdot h(w) \in X \iff h(w) \in X$$

Kongruencja w A^* to relacja równoważności $R \subseteq A^* \times A^*$, która jest substytutowna:

$$(w, v) \in R \wedge (w', v') \in R \implies ((w w'), (v v')) \in R.$$

Niech $L \subseteq A^*$. Relacja równoważności R jest L -niezmiennicza jeśli

$$(w, v) \in R \implies (w \in L \iff v \in L).$$

Fakt

Niech $L \subseteq A^*$. Następujące warunki są równoważne:

- L jest rozpoznawany przez skończony monoid
- istnieje L -niezmiennicza kongruencja w A^* o skończonym indeksie

Dowód:

$$\begin{array}{ccc} h & & A^*/R \\ \vdots & & \uparrow \\ \checkmark & & \vdots \\ \ker(h) & & R \end{array}$$

Notacja

$$L w^{-1} L = \{ \langle u, u' \rangle \in A^* \times A^* : u w u' \in L \}$$

Język $L \subseteq A^*$ określa relację równoważności w A^* :

$$\begin{aligned} w \approx_L v &\iff L w^{-1} L = L v^{-1} L \\ &\iff \forall u, u' \in A^*. (u w u' \in L \iff u v u' \in L) \end{aligned}$$

Przykład

$$A = \{a, b\}$$

$$L = (ab)^*$$

$$\epsilon \approx_L ab \approx_L abab$$

$$a \approx_L aba \approx_L ababa$$

$$b \approx_L bab \approx_L babab$$

$$ba \approx_L baba \approx_L bababa$$

$$aa \approx_L abb \approx_L aab \approx_L bba$$

Kongruencje w A^* są uporządkowane przez relację inkluzji.

Fakt

$\approx_L$ jest największą L -niezmienniczą kongruencją w A^* .

Dowód:

- $\approx_L$ jest kongruencją:

$$L w^{-1} L = L v^{-1} L \wedge L w'^{-1} L = L v'^{-1} L \implies L (w w')^{-1} L = L (v v')^{-1} L$$

- $\approx_L$ jest L -niezmiennicza:

$$w \in L \iff (\varepsilon, \varepsilon) \in L w^{-1} L$$

- $\approx_L$ jest największa:

$$(w, v) \in R \implies (\forall u, u'. (u w u', u v u') \in R) \implies w \approx_L v$$

Wniosek

Niech $L \subseteq A^*$. Następujące warunki są równoważne:

- L jest regularny
- $\approx_L$ ma skończony indeks

Monoid syntaktyczny $\mathbb{M}_L = A^*/\approx_L$

Przykład

$$L = (ab)^*$$

$$\mathbb{M}_L = (\{\varepsilon, a, b, ba, aa\}, \cdot, \varepsilon)$$

$\cdot$	ε	a	b	ba	aa
ε	ε				
a		aa	ε	a	
b		ba	aa	aa	
ba		aa	b	ba	
aa					

Wniosek

Monoid syntaktyczny $\mathbb{M}_L$ rozpoznaje język L .

Twierdzenie (automat minimalny a monoid syntaktyczny)

Monoid przejść automatu minimalnego jest izomorficzny z monoidem syntaktycznym.

Twierdzenie

Niech $L \subseteq A^*$. Następujące warunki są równoważne:

- L jest regularny
- $\sim_L$ ma skończony indeks
- L jest rozpoznawany przez skończony monoid
- monoid syntaktyczny $\mathbb{M}_L$ jest skończony
- $\approx_L$ ma skończony indeks