

Končni avtomati

1. Jeziki in operacije nad jeziki

A - množica (končna in eprazna) abeceda
Jezik nad A je podmnožica množice A^*
vseh besed nad A .

Prazna beseda: λ ali 1

A^* je monoid, operacija je konkatencija
(stik) besed.

A^* je prosti monoid nad A .

(če je $S \subseteq A^*$ generiran monoid, potem

preslikava $\iota: A \rightarrow S$

$$\iota: a \mapsto a$$

se razširi do homeomorfizma $A^* \rightarrow S$)

Primer

$$a \mapsto a$$

$$b \mapsto b$$

$$a \mapsto a \quad \leadsto \quad ab \mapsto ab$$

$$b \mapsto b \quad \leadsto \quad abbab \mapsto abbab$$

$\vee S$ se lahko zgod $a^2b = baab \dots$

Operacije

① Booleve operacije

- presek jezikov $\cap$
- unija $\cup$
- komplement c
- razlika $-$
- simetrična razlika

② Produkt: $L_1, L_2 \subseteq A^*$

$$L_1 L_2 = \{ uv ; u \in L_1, v \in L_2 \}$$

Potenciranje:

$$L^0 = \{\lambda\}, L^1 = L, \dots L^{n+1} = L^n \cdot L$$

③ Zvezda in plus $L \subseteq A^*$

$$L^* = \bigcup_{n \geq 0} L^n = \lambda \cup L \cup L^2 \cup \dots$$

(Pišemo a namesto $\{a\}$)

$$L^+ = \bigcup_{n \geq 1} L^n$$

Lastnosti

1. Produkt je asociativen, λ je enota za množenje $\{\lambda\}$

$$(L_1 L_2) L_3 = L_1 (L_2 L_3)$$

2. Distributivnost:

$$L (L_1 \cup L_2) = L L_1 \cup L L_2$$

$$(L_1 \cup L_2) L = L_1 L \cup L_2 L$$

Trditev: Množica jezikov nad A tvorí polkalobar glede na operacije $\cup$ in $\cdot$.

$$0 = \emptyset \quad 1 = \{\lambda\}$$

Polkalobar $(K, +, \cdot)$ kjer velja

1. $(K, +)$ je komutativen monoid z enoto 0

2. $(K, \cdot)$ je monoid z enoto 1

3. Distributivnost: $a(b+c) = ab+ac$, $(a+b)c = ac+bc$

4. $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in K$

Množenje jezikov ni komutativno. $\{a\} \cdot \{b\} \neq \{b\} \cdot \{a\}$

Včasih pišemo $L_1 + L_2$ namesto $L_1 \cup L_2$

Primeri: polkolobarjev

1.) $(\mathbb{N}_0, +, \cdot)$

2.) jeziki nad A

3.) $B = \{0, 1\}$ Boolev polkolobar

$\cdot$	0	1
0	0	0
1	0	1

$+$	0	1
0	0	1
1	1	1

4.) Trojski polkolobar (min-plus kolobar)

$$\mathcal{M} = (\mathbb{N}_0 \cup \{\infty\}, \min, +)$$

$$\min\{a, \infty\} = a, \quad a + \infty = \infty$$

5.) $(\mathbb{N}_0 \cup \{\infty\}, \cdot, +)$

$$0 \cdot \infty = 0 \quad a + \infty = \infty$$

$$a \cdot \infty = \infty \quad \forall a \in \mathbb{N}$$

Operacije (nadeljevanje)

④ Levi in desni kvocient

$$L \subseteq A^* \quad u \in A^*$$

Definiramo $u^{-1}L = \{v; uv \in L\}$ levi
podobno $Lu^{-1} = \{v; vu \in L\}$ desni

Trditve:

$$① \quad (uv)^{-1}L = v^{-1}(u^{-1}L)$$

$$L(uv)^{-1} = (Lv^{-1})u^{-1}$$

$$② \quad u^{-1}(L_1 + L_2) = u^{-1}L_1 + u^{-1}L_2$$

$$③ \quad u^{-1}(L_1 \cap L_2) = u^{-1}L_1 \cap u^{-1}L_2$$

$$④ \quad u^{-1}(L_1 - L_2) = u^{-1}L_1 - u^{-1}L_2$$

$$⑤ \quad a \in A. \quad a^{-1}(L_1 L_2) = \begin{cases} (a^{-1}L_1)L_2; & \lambda \notin L_1 \\ (a^{-1}L_1)L_2 + a^{-1}L_2; & \lambda \in L_1 \end{cases}$$

$$⑥ \quad a \in A. \quad a^{-1}L^* = (a^{-1}L)L^*$$

Dokaz:

$$a^{-1}L^* = a^{-1}(\lambda + L^+) = a^{-1} \cdot L \cdot L^* = \begin{cases} (a^{-1}L)L^* & \lambda \notin L \quad \checkmark \\ (a^{-1}L)L^* + a^{-1}L^*, & \lambda \in L \end{cases}$$

$$\begin{aligned} \hookrightarrow &= a^{-1}(\lambda + L^+) + a^{-1}L^* = a^{-1}(\lambda + L^+ + L^*) = \\ &= a^{-1}(L^* + L^*) = a^{-1}L^* \end{aligned}$$

Primer

$$(L_1 \cap L_2) \cdot L \neq L_1 L \cap L_2 L$$

$$\underbrace{(\{b\} \cap \{ba\})}_{\emptyset} \cdot \{a, aa\} = \{b\} \cdot \{a, aa\} \cap \{ba\} \cdot \{a, aa\} = \{baa\}$$

Primer:

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

$L = A^* aba A^*$ - besede, ki vsebujejo podbesedo aba

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

$$b^{-1} L = b^{-1} A^* \underbrace{a}_{L_1} \underbrace{ba}_{L_2} A^* = \underbrace{b^{-1} A^*}_{L} a ba A^* + \underbrace{b^{-1} (aba A^*)}_{=\emptyset} =$$

Lastnost nam ne pomaga

$$a^{-1} L = a^{-1} A^* \underbrace{a}_{L} ba A^* = \underbrace{a^{-1} A^*}_{L} a ba A^* + a^{-1} (aba A^*) =$$

$$(ab)^{-1} L = (ab)^{-1} A^* a ba A^* + \underbrace{(ab)^{-1} (aba A^*)}_{a A^*}$$

$$X \subseteq A^* \quad L \subseteq A^*$$

$$X^{-1}L = \bigcup_{u \in X} u^{-1}L \quad \text{lev: kvocient z } X$$

$$LX^{-1} = \bigcup_{u \in X} L u^{-1}$$

Primeri

$$1) (x+y)^{-1}L = X^{-1}L + Y^{-1}L$$

$$2) (xy)^{-1}L = Y^{-1}(X^{-1}L)$$

$$(X^*)^{-1}L = L + (X^*)^{-1}(X^{-1}L)$$

Prednosti:

$$1) L^*, L^+, L^c$$

$$2) L_1 L_2, u^{-1}L_1, L u^{-1}$$

$$3) L_1 + L_2, L_1 \cap L_2$$

2. Racionalni jeziki

A - končna neprazna abeceda.

Množica racionalnih jezikov $\mathcal{F}$ je najmanjša podmnožica jezikov, ki zadošča

1) $\emptyset \in \mathcal{F}$, $\forall a \in A$. $\{a\} \in \mathcal{F}$

2) $\mathcal{F}$ je zaprta za končne unije, produkt in zvezdo

Množico vseh racionalnih jezikov nad A označimo $\text{Rat}(A^*)$

Dobra definiranoost? vsi jeziki nad A zadoščajo

1) in 2). Al: obstaja najmanjša

če $\mathcal{F}_i$ zadošča 1) in 2), potem tudi $\bigcap_i \mathcal{F}_i$
zadošča 1) in 2)

Sledi: $\mathcal{F}$ je presek vseh podmnožic A^* , ki zadoščajo
1) in 2)

$\forall$ končni jezik je racionalen

Naj bo $\mathcal{F}_0$ množica vseh končnih jezikov

Naj bo $n \geq 0$

$\mathcal{F}_{n+1}$ je množica jezikov oblike $L_1 + L_2, L_1 L_2, L_1^*$,
kjer $L_1, L_2 \in \mathcal{F}_n$

Dobimo $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \dots$

$$\mathcal{F} = \bigcup_{n \geq 0} \mathcal{F}_n$$

$$\text{Trditev } \mathcal{F} = \bigcup_{n \geq 0} \mathcal{F}_n = \text{Rat}(A^*)$$

Dokaz: $\mathcal{F}$ zadošča 1) in 2)

$$\Rightarrow \mathcal{F} \supseteq \text{Rat}(A^*)$$

Naj bo X množica jezikov, ki zadošča 1) in 2)

Potem $X \supseteq \mathcal{F}_0$

Zaradi 2) je $X \supseteq \mathcal{F}_1 \Rightarrow \forall k \in \mathbb{N}_0, X \supseteq \mathcal{F}_k$

$$\Rightarrow X \supseteq \mathcal{F}$$

$$\Rightarrow \text{Rat}(A^*) \supseteq \mathcal{F}$$

$$\Rightarrow \mathcal{F} = \text{Rat}(A^*)$$

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

1) $L_1 = (a+ab+ba)^*$

2) $L_2 = A^* u A^* \quad u \in A^*$

3) $L_3 = p A^* \quad ; p \in A^*$

4) Množica vseh besed sode dolžine $= (A^2)^*$

5) Množica vseh besed lihe dolžine $= (A^2)^* \cdot A$

Racionalen izraz je definiran rekurzivno:

1) 1 in 0 sta racionalna izraza

2) $\forall a \in A$ je racionalen izraz

3) če sta e_1, e_2 racionalna izraza,
 $(e_1 + e_2), (e_1 e_2)$ sta racionalna izraza

4) če je e racionalni izraz $\Rightarrow e^*$ je racionalen

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

$$(a^*(ba)^*(bb^*))^*$$

Primer: $e_1 = (a+b)^*$ $e_2 = (a^*b)^* a^*$, $e_3 = 1 + (a+b)(a+b)^*$

racionalni izrazi:

e_1, e_2, e_3 definirajo isti jezik A^*

Velja identiteta $(a+b)^* = (a^*b)^* a^*$

(ni končne baze identitet)

KONČNI AUTOMATI IN PREPOZNAVNI JEZIKI

Definicija: **končni avtomat** je $\mathcal{A} = (A, Q, E, I, F)$

kjer: A - končna abeceda

Q - množica stanj ^{končna množica}

E - množica povezav ^(prehodov oz. tranzicij) $E \subseteq Q \times A \times Q$

$I \subseteq Q$ množica začetnih stanj

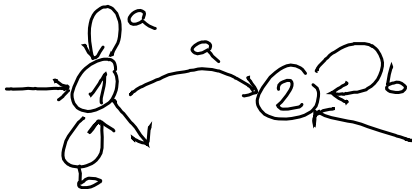
$F \subseteq Q$ množica končnih stanj (final states)

Primer

$A = \{a, b\}$ $Q = \{1, 2\}$

$I = \{1, 2\}$ $F = \{1\}$

$E = \{(1, a, 1), (1, b, 1), (1, a, 2), (2, b, 2)\}$



Bolj kompaktno:

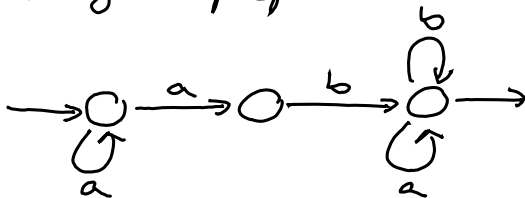
- (x, a, y) in (u, b, v) sta **sosednji** če $u=y$
- **Pot** v $\mathcal{A}$ je zaporedje zaporednih povezav
- Dolžina poti je število povezav v poti
- **Prazna pot** v $q \in Q$ (q, λ, q)
- Pot p je **začetna**, če se prične v začetnem stanju
- Pot p je **končna**, če se konča v končnem stanju
- Pot p je **uspešna**, če je začetna in končna
- **Oznake poti** $p: a_1 a_2 \dots a_n \in A^*$
- Naj $u = a_1 \dots a_n \in A^*$. Automat $\mathcal{A}$ **sprejme** besedo u , če obstaja uspešna pot katere oznaka je u
 $l(p) \dots$ oznake poti
- Naj bo $L(\mathcal{A}) = \{u \in A^*; \mathcal{A} \text{ sprejme } u\}$
jezik, ki ga sprejme automat (oz prepozna)
- Naj bo L nek jezik. L je prepoznaven če obstaja končni automat, ki ga prepozna ($L = L(\mathcal{A})$)

Primer

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

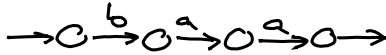
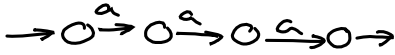
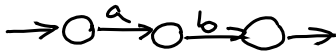
$$L = a^* a b A^*$$

Ali je L prepoznaven



Primer 2:

$$L = \{ab, aaa, baa\}$$



Vsak končen jezik je prepoznaven

Stanje q je **dosegljivo**, če lahko iz začetnega stanja prideš v stanje q

Stanje q je **nedosegljivo**, če obstaja pot iz q v neko končno stanje

Automat $\mathcal{A}$ je **trimmed** če je vsako stanje dosegljivo in nedosegljivo

Automata $\mathcal{A}$ in $\mathcal{B}$ sta **ekvivalentna** če

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

Kako dokazati, da L ni prepoznaven?

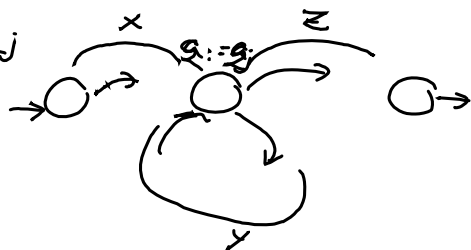
Predpostavimo, da je $L \subseteq A^*$ prepoznaven in
ga sprejme avtomat, ki ima $|p| \geq n$ stanj
Naj bo p uspešna pot v δ^*



$\exists 0 \leq i < j \leq n$ da je $q_i = q_j$

Torej imamo zanko

$l(p) = xyz$



Potem velja $xy^nz; n \in \mathbb{N}_0$ je v našem jeziku

Trditveni lema o črpanju (pumping lemma)

Naj bo L prepoznaven. Potem obstaja $n \in \mathbb{N}$, da
velja $\forall u \in L$ z dolžino vsaj $|u| \geq n$ obstaja zapis

$u = xyz$, kjer $|xy| \leq n$, $|y| \geq 1$

tako da $xy^kz \in L$ za $\forall k \in \mathbb{N}_0$

Primer: $L = \{a^n b^n; n \geq 1\}$ $A = \{a, b\}$

L ni prepoznaven

če je L prepoznaven, obstaja n z lme

Vzememo besedo $u = a^n b^n$

obstaja zapi $u = xyz$

$$|xy| \leq n$$

$$x = a^l, y = a^t \quad z = a^s b^n$$

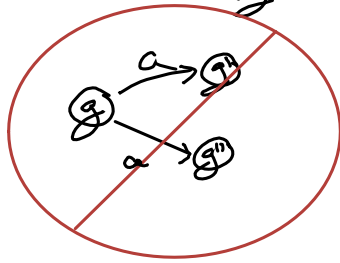
$$k = 2n$$

$$xy^kz = a^{l+2nt+s} b^n$$

$l+2nt+s > n$ torej to ne leži
v našem jeziku

Deterministični automati

Automat $\mathcal{A} = (Q, A, E, I, F)$ je determinističen, če za vsa stanja $q \in Q$ in vsako $a \in A$ $\exists$ največ ena preizkušnja oblike (q, a, q')



Pišemo $q \cdot a = q'$ če obstaja preizkušnja (q, a, q')

Trditev: V končen avtomata je ekvivalenten determinističnemu končnemu avtomatu

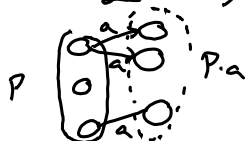
Dokaz: Naj bo $\mathcal{A} = (Q, A, E, I, F)$ in L njegov jezik.

Definirajmo $\mathcal{A}' = (\mathcal{P}(Q), A, E', I, F')$

↑
element
potenčne
množice
(eno začetno stanje)

Naj bo $P \subseteq Q$ in $a \in A$

$$P \cdot a = \{ g \in Q ; \exists (p, a, g) \in E, p \in P \}$$



$$E' = \{ (P, a, P \cdot a), P \in \mathcal{P}(Q), a \in A \}$$

Tu drži $\forall p \in P. \exists (p, a, P \cdot a) \Rightarrow \mathcal{A}'$ je kompletan determinističen

$$F' = \{ P \in \mathcal{P}(Q) ; P \cap F \neq \emptyset \}$$

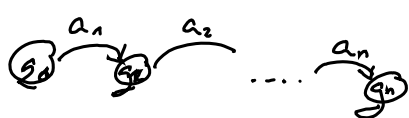
vse podmnožice, ki imajo vsaj eno končno stanje

$\mathcal{A}'$ je determinističen po konstrukciji

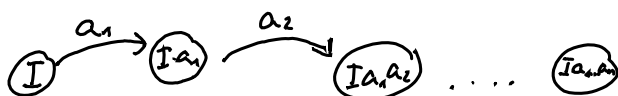
$$\underline{\underline{L(\mathcal{A}') = L(\mathcal{A})}}$$

$$L(\mathcal{A}) \subseteq L(\mathcal{A}')$$

Naj bo $u \in L(\mathcal{A})$, torej $\exists$ pot $\in \mathcal{A}$ $a_1 \dots a_n$



Po definiciji je v $\mathcal{A}'$



$$\text{ker } q_0 \in I \Rightarrow q_1 \in Ia_1 \Rightarrow q_2 \in Ia_1a_2 \Rightarrow \dots$$

$$\Rightarrow \dots \Rightarrow q_n \in Ia_1 \dots a_n \Rightarrow Ia_1 \dots a_n \in F'$$

Dobili smo pot z oznako u v $\mathcal{A}'$, ki je uspešna

$$\Rightarrow \mathcal{A}' \text{ sprejme } u \Rightarrow L(\mathcal{A}) \subseteq L(\mathcal{A}')$$

2) še za prazne besede

$$L(\mathcal{A}') \subseteq L(\mathcal{A})$$



Naj bo $u \in L(\mathcal{A}')$

$$1) u = \lambda \Rightarrow I \in F' \Rightarrow I \cap F \neq \emptyset \Rightarrow \lambda \in L(\mathcal{A})$$

2) $u = a_1 \dots a_n$. V $\mathcal{A}$ obstaja uspešna pot



$$\text{ker } p_n \in F' \Rightarrow P_n \cap F \neq \emptyset \Rightarrow \exists g_n \in P_n \cap F$$

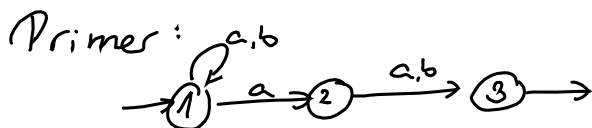


ker $g_n \in P_n \exists$ povezave (g_{n-1}, a_n, g_n)

ker $g_{n-1} \in P_{n-1} \exists$ povezave $(g_{n-2}, a_{n-1}, g_{n-1})$

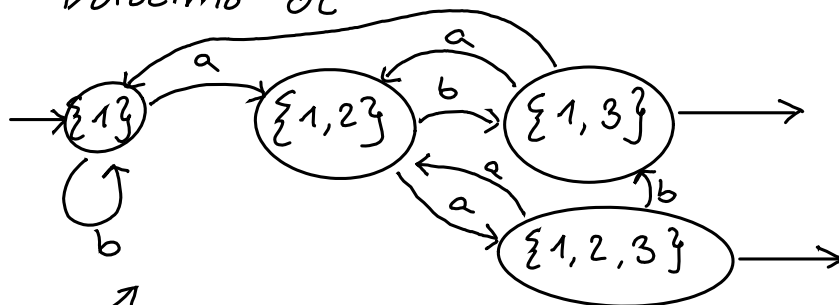
Na koncu v $\mathcal{A}$ dobimo pot.

ker $g_0 \in I$ je g_0 začetno stanje

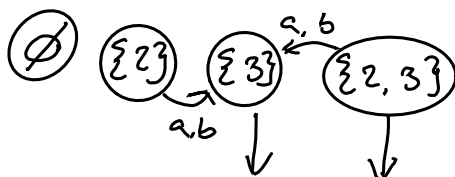


ni determinističen

Določimo A'



obrezan
avtomat
 A''



A'' avtomat je determinističen

Kompletnost: Iz vsakega stanja za vsako
črko dostajajo puščice

DN: Dokazi, da je vsak determinističen avtomat
ekvivalenten obreznemu determinističnemu

Definicija: $\mathcal{A}$ je **standarden**, če nobena povezava nima konca v začetnem stanju

Trditev: Poljuben deterministični avtomat je ekvivalenten standardnemu determinističnemu

Dokaz: Naj bo $\mathcal{A} = (Q, A, \overset{\text{delovanje}}{\circ}, q_-, F)$ deterministični avtomat. Predpostavimo, da $\mathcal{A}$ ni standardni.

Definiramo nov avtomat $\mathcal{A}' = \{Q \cup \{p\}, A, \circ, p, F'\}$;
 $p \notin Q$

E so povezave v $\mathcal{A}$

$$E' = E \cup \{(p, a, q); (q_-, a, q) \in E, a \in A\}$$

$$F' = \begin{cases} F; & q_- \notin F \\ F \cup \{p\}; & q_- \in F \end{cases}$$

$\mathcal{A}'$ je determinističen in standarden

$\forall q \in Q. \forall a \in A \exists$ kvečjemu ena povezava (q, a, r)

Za p : če (q, a, r) in (a, a, r') $\vdash$

(q_-, a, r) in (q_-, a, r') ker je prepuščeno

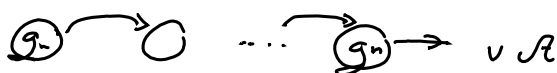
Pokažimo $L(\mathcal{A}) = L(\mathcal{A}')$

$u \in L(\mathcal{A})$

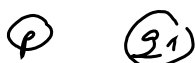
1) $u = 1 \Rightarrow q_- \in F \Rightarrow 1 \in L(\mathcal{A}')$ ker $p \in F'$

2) $u \neq 1 \quad u = a_1 \dots a_n \quad n \geq 1$

Potem



Potem v $\mathcal{A}'$ imamo

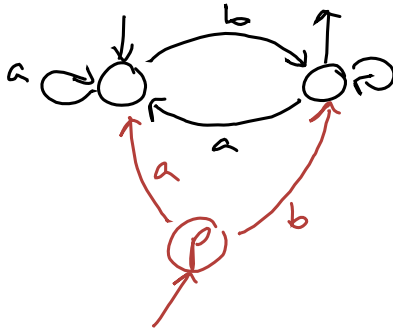
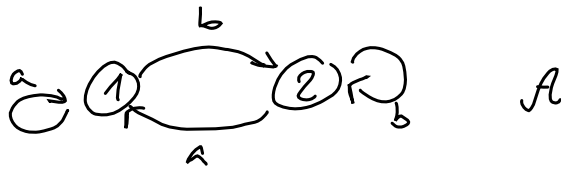


Torej $L(\mathcal{A}) \subseteq L(\mathcal{A}')$

Naj bo $u \in L(\mathcal{A}')$ 1) $u = 1$ podobno kot prej

2) Podobno kot prej

Primer



Cilj: Kleenejev izrek:

jezik $L = A^*$ je racionalen $\Leftrightarrow L$ je prepoznaven

Operacije nad prepovednimi jeziki:

Preseki:

Trditev: Če sta L_1, L_2 prepovedni, potem je tudi njun presek $L_1 \cap L_2$ prepoveden

Dokaz: Naj bo $L_1 = L(\mathcal{A}_1)$ in $L_2 = L(\mathcal{A}_2)$

$$\mathcal{A}_1 = (Q_1, A, E_1, I_1, F_1) \quad \mathcal{A}_2 = (Q_2, A, E_2, I_2, F_2)$$

Definirajmo avtomat $\mathcal{B} = (Q_1 \times Q_2, A, E, I_1 \times I_2, F_1 \times F_2)$

v $\mathcal{B}$ je povezava

$$E \ni (g_1, g_2), a, (r_1, r_2) \Leftrightarrow (g_1, a, r_1) \in E_1 \wedge (g_2, a, r_2) \in E_2$$

s tem je E definirana

Naj bo

$(g_1, g_2) \xrightarrow{a_1} \dots \rightarrow (r_1, r_2)$ uspešna pot
v $\mathcal{B}$. Potem mora dosegati uspešna pot v

$\mathcal{A}_1$ in $\mathcal{A}_2$ definirane s projekcijo.

To pomeni: $u \in L(\mathcal{B}) \Leftrightarrow u \in L_1 \cap L_2$

Torej: $L(\mathcal{B}) = L_1 \cap L_2$

Unija

Trditev: L_1, L_2 prepoznavna $\Rightarrow L_1 \cup L_2$ prepoznavna

Dokaz združimo dva avtomata

$$B = A_1 \cup B_2 \quad (\text{ampak ni determinističen})$$

Lahko bi definirali Σ deterministične

$$B = (Q_1 \times Q_2, A, E, (i_1, i_2), F_1 \times Q_2 \cup Q_1 \times F_2)$$

$\Leftrightarrow \exists A_1$ obstaja

... Filipovi zapiski

Komplement

Trditev: L prepoznaven $\Rightarrow A^*L$ prepoznaven

Dokaz: Naj bo $L = L(A)$, kjer je A determinističen in kompleten

$$A = (Q, A, E, i, F)$$

$$A^* = (Q, A, E, i, Q - F)$$

Produkt

Trditev 1: Naj bosta L_1, L_2 prepoznavna. Potem je $L_1 L_2$ prepoznaven

Dokaz $L_1 = L(\mathcal{A}_1)$ $L_2 = L(\mathcal{A}_2)$

Ker je $\mathcal{A}_2$ standardni deterministični

$$\mathcal{A}_1 = (Q_1, A, E_1, I_1, F_1) \quad \mathcal{A}_2 = (Q_2, A, E_2, i, F_2)$$

Definiramo $\mathcal{A} = (Q, A, E, I_1, F)$

$$Q = Q_1 \cup (Q_2 - \{i\})$$

$$E = E_1 \cup (E_2 - \{(i, a, 2) \in E_2\}) \cup \{(z', a, 2); z' \in F_1, g \in Q_2, (i, a, 2) \in E_2\}$$

$$F = \begin{cases} F_1 \cup (F_2 - \{i\}); & i \in F_2 \\ F_2 & ; i \in F_2 \end{cases}$$

Pokažemo da $L(\mathcal{A}) = L_1 L_2$

$\supseteq$ Naj bo $u_1 \in L_1, u_2 \in L_2$ $u_1 u_2 \in L_1 L_2$

1.) Naj bo $u_2 = 1$ torej $i \in F_2$

$$u_1 u_2 = u_1 \quad \text{ker } u \in L(\mathcal{A}_1) \Rightarrow u_1 \in L(\mathcal{A})$$

2) $u_2 \neq 1$ ker $u_1 \in L(\mathcal{A}_1)$ v $\mathcal{A}_1$ obstaja uspešna pot

$$\text{pot } i_1 \xrightarrow{u_1} z_1 \in F_1$$

Naj bo $u_2 = a \cdot u_2$ kjer $a \in A$

ker $u_2 \in L(\mathcal{A}_2)$ v $\mathcal{A}_2$ obstaja uspešna pot

$$i \xrightarrow{a} z' \in F_2$$

Potem v $\mathcal{A}$ imamo

$$z_1 \xrightarrow{a} z' \quad \text{ker je } \mathcal{A}_2 \text{ standarden}$$

Sledi $u_1 u_2 \in L(\mathcal{A})$

$\subseteq$ Naj bo $u \in L(\mathcal{A})$

$$z_1 \xrightarrow{\quad} z_2 \in F$$

$$1.) i \in F_2 \Leftrightarrow F = F_1 \cup (F_2 - \{i\})$$

$$1.1) z_2 \in F_1$$

Pozornost: vsaka uspešna pot ima obliko

Filipovi zaščitni

Zvezda

May bo L prepoznaven. Potem je tudi L^* prepoznavna

Dokaz: Filip

Toditev: Naj bo L prepoznaven. Potem ~~je~~ sta $K^{-1}L$ in LK^{-1} tudi prepoznavna

Dokaz: Naj bo $L = L(\mathcal{A})$

$\mathcal{A} = (Q, A, \cdot, q_0, F)$ deterministični avtomat

$$\begin{array}{c} uv \\ (q_0) \rightsquigarrow (q) \end{array}$$

$$(q_0) \xrightarrow{u} (qu) \xrightarrow{v} (q)$$

Definiramo $\mathcal{A}' = (Q, A, \cdot, q_0 \cdot u, F)$

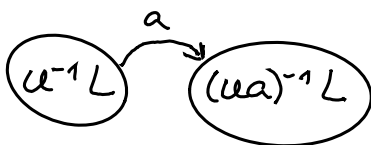
$$\begin{aligned} v \in L(\mathcal{A}') &\Leftrightarrow (q_0 \cdot u) \cdot v \in F \Leftrightarrow q_0 \cdot (uv) \in F \Leftrightarrow uv \in L(\mathcal{A}) \\ &\Leftrightarrow v \in u^{-1}L(\mathcal{A}) \end{aligned}$$

$K^{-1}L = \bigcup_{u \in K} u^{-1}L$ sestavimo slehraj avtomate kot pri:
dokaže se unijo

Minimizacija in Nerodeov avtomat

$L \subseteq A^*$ jezik

Definirajmo $R(L) = \{Q, A, \cdot, L, F\}$,
kjer $\cdot Q = \{u^{-1}L; u \in A^*\}$ ↖ začetno stanje
 $\cdot u^{-1}L \cdot a = a^{-1}u^{-1}L = (ua)^{-1}L$



$\cdot F = \{u^{-1}L; u \in L\}$

$R(L)$ se imenuje **Nerodeov avtomat**

V splošnem je $R(L)$ neskončen avtomat, torej

Q ni nujno končen

$R(L)$ je determinističen, kompleten, dosegljiv

Izreke (Myhill-Nerodeov)

L je prepoznaven $\Leftrightarrow \mathcal{A}(L)$ je končen avtomat
če je L prepoznaven, ga $\mathcal{A}(L)$ prepozna

Dokaz:

($\Leftarrow$) Recimo, da je $\mathcal{A}(L)$ končen, torej

$Q = \{u^{-1}L; u \in A^*\}$ je končna množica

Pokažimo da $\mathcal{A}(L)$ prepozna L $\underline{L} = \underline{L}(\underline{\mathcal{A}(L)})$

($\subseteq$) $u \in L$

① $u \xrightarrow{u} \text{②}$ g končno?

$u = a_1 \dots a_n$

$g = L \cdot u$

$L \cdot u = u^{-1}L \Rightarrow g$ je končno

($\supseteq$) $u \in L(\mathcal{A}(L))$

$\Rightarrow u^{-1}L$ je končno stanje

$\Rightarrow u$ je pot od L do $u^{-1}L \Rightarrow u$ je prepoznaven

$\Rightarrow u \in L$

Opomba: to deluje tudi če je naš avtomat neskončen

($\Rightarrow$) Naj bo L prepoznaven $L = L(\mathcal{A})$ za nek končen avtomat $\mathcal{A}$ (izbrano determinističnega

$\mathcal{A} = (Q, A, \cdot, \underline{g}, F)$, $|Q| < \infty$

Vemo: za $u \in A^*$ $u^{-1}L$ prepozna avtomat

$(Q, A, \cdot, \underline{g} \cdot u)$

ker je končno mnogo takih stanj $\underline{g} \cdot u \in Q$ imamo končno mnogo kvocientov.

Če $u^{-1}L$ in $r^{-1}L$ prepozna $(Q, A, \cdot, \underline{g} \cdot u, \underline{g} \cdot r, F)$

$\Rightarrow u^{-1}L = r^{-1}L$

$\Rightarrow \mathcal{A}(L)$ je končen avtomat

Ali je $\mathcal{A}(L)$ kodosegljiv (in s tem tudi dobrozan)



$$u^{-1}L \cdot w = (uw)^{-1}L = v^{-1}L$$

$\mathcal{A}(L)$ je kodosegljiv $\Leftrightarrow \forall u \in A^* \exists w \in A^* . uw \in L$
 $\Leftrightarrow$ vsaka beseda $u \in A^*$ je predpona neke besede
 iz $L \Leftrightarrow \forall u \in A^* , u^{-1}L \neq \emptyset$

Ureditve na determinističnih kanoničnih avtomatih

Definirajmo $A' \leq A$ če obstaja preslikava

$p: Q \rightarrow Q'$, da je $p(q \cdot a) = p(q) \cdot a$, $p^{-1}(F') = F$,

$$q_1 \xrightarrow{a} q_2 \quad p(q_1) \xrightarrow{a} p(q_2)$$

$$q_1 \cdot a = q_2 \Rightarrow p(q_1) \cdot a = p(q_2)$$

$\Leftarrow$ je delna ureditve

Izreči:

Naj bo L prepoznaven jezik, potem je $A(L)$ najmanjši dosegljiv determinističen avtomat, ki prepozna L , in sicer $A(L)$ je dosegljiv determinističen komplet avtomat z najmanjšim možnim številom ostenj, ki prepozna L .

Dokaz: Naj bo $A = (Q, A, \cdot, q_-, F)$ kanonen avtomat, ki prepozna L in je dosegljiv, determinističen, komplet $L = L(A)$. Za $\forall g \in Q$ naj bo L_g jezik, ki ga prepozna $A_g = (Q, A, \cdot, g, F)$ in sicer $L = A_g$.

Ker je A dosegljiv, determinističen, komplet, obstaja pot $q_- \xrightarrow{u} g$ in naj bo $g_- \cdot u = g$ od prej vemo $u^{-1}L$

Definiramo preslikavo $p: Q \rightarrow \{u^{-1}L; u \in A^*\}$
 $g \mapsto L(A_g)$

p je surjektivna: $\forall u \in A^*, u^{-1}L \in \text{im } p$, saj $u^{-1}L = p(g_-) = L(A_{g_-})$
 $(g_-) \xrightarrow{u} g$

Pokažimo $p: Q \rightarrow \{u^{-1}L; u \in A^*\}$ morfizem iz A v $A(L)$

$$p(g_-) = 1^{-1}L = L$$



$$p^{-1}(\{u^{-1}L; u \in L\}) = F$$

$$\text{če } p(g_-) = u^{-1}L, u \in L$$

$$(g_-) \xrightarrow{u} g \Leftrightarrow g \in F$$

$$g_1 \cdot a = g_2 \text{ v } A$$

$$\text{preverimo } p(g_1) \cdot a = p(g_2)$$

$$A_{g_1}^a = u^{-1}L \cdot a = (ua)^{-1}L = A_{g_2} = A_{g_2} \quad \checkmark$$

izbrano
tak u

Primer

$$L = (a(ab)^*)^* + (ba)^* \quad \text{konstrukcija od } L$$

$$p^{-1}L = L = L_1$$

$$\begin{aligned} a^{-1}L &= a^{-1}((a(ab)^*)^* + (ba)^*) = \\ &= a^{-1} \cdot a(ab)^*(a(ab)^*)^* + 0 = \\ &= (ab)^*(a(ab)^*)^* = L_2 \end{aligned}$$

$$b^{-1}L_1 = a(ba)^* = L_3$$

$$a^{-1}L_2 = b(ab)^*(a(ab)^*)^* + (ab)^*(a(ab)^*)^* = bL_2 + L_2 = L_4$$

$$b^{-1}L_2 = 0$$

$$a^{-1}L_3 = (ba)^* = L_5$$

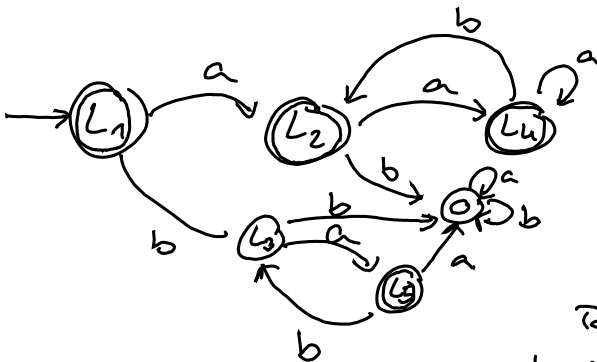
$$b^{-1}L_3 = 0$$

$$a^{-1}L_4 = a^{-1}bL_2 + a^{-1}L_2 = L_4$$

$$b^{-1}L_4 = L_2 + b^{-1}L_2 = L_2 + 0 = L_2$$

$$a^{-1}L_5 = 0$$

$$b^{-1}L_5 = a(ba)^* = L_3$$



Ta automet ni
 kodirano, ker iz
 0 ni izhoda, cc
 demo 0 stran ne
 b: bil kompleten

$$a \in L \Rightarrow 1^{-1}L \in F$$

$$a \in L \Rightarrow L_2 \in F$$

$$L_3 = L \cdot b \quad b \notin L \Rightarrow L_3 \notin F$$

$$L_4 = L \cdot a^2, \quad a^2 \in L \Rightarrow L_4 \in F$$

$$L_5 = L \cdot ba \quad ba \in L \Rightarrow L_5 \in F$$

Kleenejev izrek:

$L \subseteq A^*$ je prepoznaven $\Leftrightarrow L$ je racionalen

Dokaz:

Če je L racionalen, je prepoznaven

$\{a\}$, unija, produkt, *

↓
prepoznaven od prej

Predpostavimo, da je L prepoznaven $L = L(A)$
 A je končen avtomat.

1. konstrukcija:

Poden je jezik $L = L(A)$

$A = (Q, A, \cdot, q_0, F)$

Naj bo $A_2 = (Q, A, \cdot, q_0, F)$

$L_2 = L(A_2)$

Cilj: Sistem enačb z n neznanimi, kjer
 $n = |Q|$, katerega rešitve so natanko L_2 ; $q \in Q$

Oglejmo si enačbo $KX + L = X$

$K, L \subseteq A^*$ da fiksen podoben, X pa je
neznan

Toditev (Ardenova rešitev)

Predpostavimo, da $1 \notin K$, potem ima enačba

$KX + L = X$ ime eno samo rešitev:

$$X = K^*L$$

