

# Automaták irányítása

Iván Szabolcs

2009. szeptember 22.

# Véges automaták

## Automata

**Automata:** egy  $M = (Q, A, \delta)$  hármass, ahol

- $Q$  a véges, nemüres **állapothalmaz**;
- $A$  a véges, nemüres **input ábécé**;
- $\delta : Q \times A \rightarrow Q$  az **átmenetfüggvény**.

$q \cdot u$

A szokott módon  $\delta$  kiterjeszhető egy  $\delta : Q \times A^* \rightarrow Q$  leképezéssé.

$\delta(p, u)$  helyett egyszerűen  $p \cdot u$  vagy  $pu$  szerepel majd, ha  $\delta$  egyértelműen kiderül a környezetből.

$Pu$

Ha  $P \subseteq Q$  és  $u \in A^*$ , legyen  $Pu = \{pu : p \in P\}$ .

# Véges automaták

## Automata

**Automata:** egy  $M = (Q, A, \delta)$  hármass, ahol

- $Q$  a véges, nemüres **állapothalmaz**;
- $A$  a véges, nemüres **input ábécé**;
- $\delta : Q \times A \rightarrow Q$  az **átmenetfüggvény**.

## $q \cdot u$

A szokott módon  $\delta$  kiterjeszhető egy  $\delta : Q \times A^* \rightarrow Q$  leképezéssé.

$\delta(p, u)$  helyett egyszerűen  $p \cdot u$  vagy  $pu$  szerepel majd, ha  $\delta$  egyértelműen kiderül a környezetből.

## $Pu$

Ha  $P \subseteq Q$  és  $u \in A^*$ , legyen  $Pu = \{pu : p \in P\}$ .

# Véges automaták

## Automata

**Automata:** egy  $M = (Q, A, \delta)$  hármas, ahol

- $Q$  a véges, nemüres **állapothalmaz**;
- $A$  a véges, nemüres **input ábécé**;
- $\delta : Q \times A \rightarrow Q$  az **átmenetfüggvény**.

## $q \cdot u$

A szokott módon  $\delta$  kiterjeszhető egy  $\delta : Q \times A^* \rightarrow Q$  leképezéssé.

$\delta(p, u)$  helyett egyszerűen  $p \cdot u$  vagy  $pu$  szerepel majd, ha  $\delta$  egyértelműen kiderül a környezetből.

## $Pu$

Ha  $P \subseteq Q$  és  $u \in A^*$ , legyen  $Pu = \{pu : p \in P\}$ .

## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa

## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa

## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa

# Írányítás (J. Černý, 1964.)

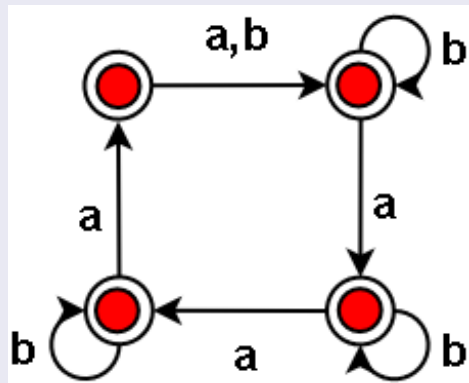
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa





# Írányítás (J. Černý, 1964.)

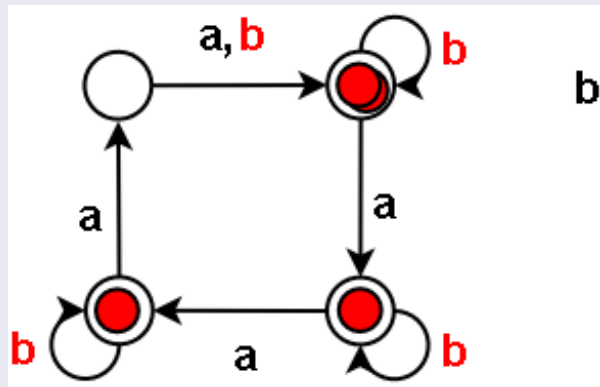
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



# Írányítás (J. Černý, 1964.)

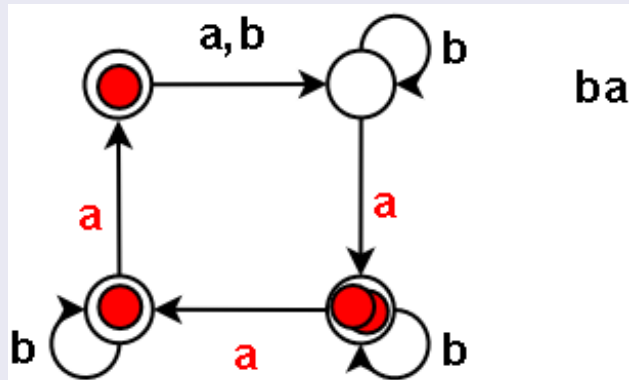
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



# Írányítás (J. Černý, 1964.)

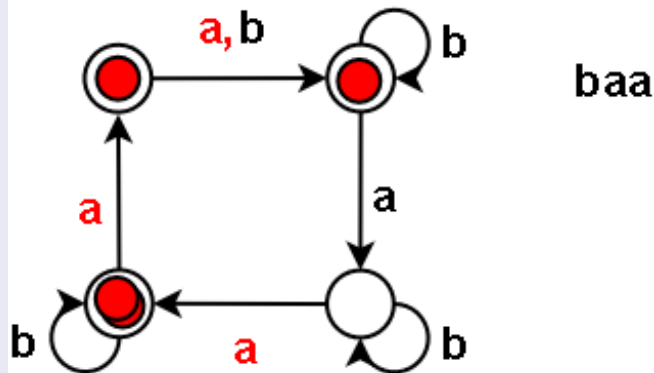
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



# Írányítás (J. Černý, 1964.)

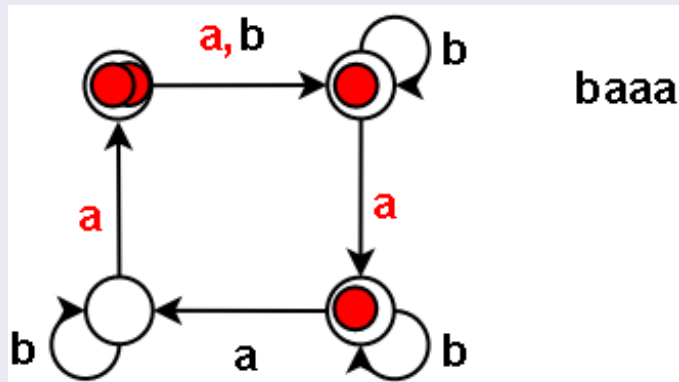
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



# Írányítás (J. Černý, 1964.)

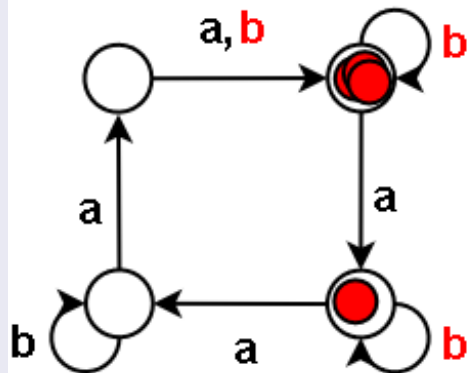
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



baaab

# Írányítás (J. Černý, 1964.)

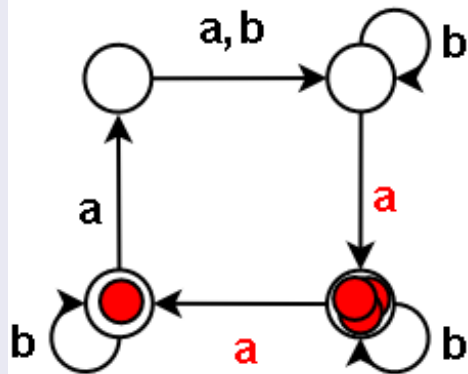
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



baaaba

# Írányítás (J. Černý, 1964.)

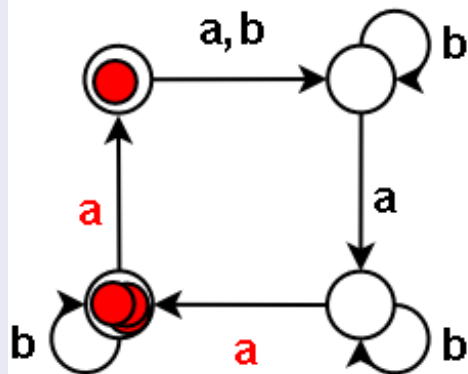
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



baaaba

# Írányítás (J. Černý, 1964.)

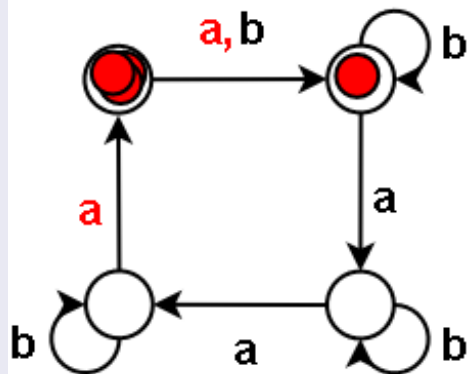
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



baaaba



# Írányítás (J. Černý, 1964.)

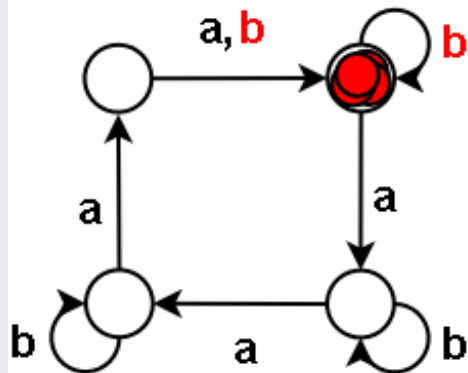
## Írányító szó

Az  $M = (Q, A, \delta)$  automatának  $u \in A^*$  **írányító szava**, ha  $|Qu| = 1$ .

Vagyis ha  $\forall p, q : pu = qu$ .

$M$  **írányítható**, ha van írányító szava.

## Példa



**baaabaab**

# $d(M), d(n)$

## $d(M)$

Ha  $M$  irányítható, legyen

$$d(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

Az előbbi példa automatára  $d(M) = 9$ .

## $d(n)$

Ha  $n \geq 1$ , legyen

$$d(n) = \max\{d(M) : M \text{ irányítható, } n\text{-állapotú automata}\}.$$

## $d(n)$ kis $n$ -ekre

- $d(1) = 0$ .
- $d(2) = 1$ .
- $d(3) = 4$ .
- $d(4) = 9$ .

# $d(M), d(n)$

## $d(M)$

Ha  $M$  irányítható, legyen

$$d(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

Az előbbi példa automatára  $d(M) = 9$ .

## $d(n)$

Ha  $n \geq 1$ , legyen

$$d(n) = \max\{d(M) : M \text{ irányítható, } n\text{-állapotú automata}\}.$$

$d(n)$  kis  $n$ -ekre

- $d(1) = 0$ .
- $d(2) = 1$ .
- $d(3) = 4$ .
- $d(4) = 9$ .

# $d(M), d(n)$

## $d(M)$

Ha  $M$  irányítható, legyen

$$d(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

Az előbbi példa automatára  $d(M) = 9$ .

## $d(n)$

Ha  $n \geq 1$ , legyen

$$d(n) = \max\{d(M) : M \text{ irányítható, } n\text{-állapotú automata}\}.$$

## $d(n)$ kis $n$ -ekre

- $d(1) = 0$ .
- $d(2) = 1$ .
- $d(3) = 4$ .
- $d(4) = 9$ .

# $d(M), d(n)$

## $d(M)$

Ha  $M$  irányítható, legyen

$$d(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

Az előbbi példa automatára  $d(M) = 9$ .

## $d(n)$

Ha  $n \geq 1$ , legyen

$$d(n) = \max\{d(M) : M \text{ irányítható, } n\text{-állapotos automata}\}.$$

## $d(n)$ kis $n$ -ekre

- $d(1) = 0$ .
- $d(2) = 1$ .
- $d(3) = 4$ .
- $d(4) = 9$ .

# $d(M), d(n)$

## $d(M)$

Ha  $M$  irányítható, legyen

$$d(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

Az előbbi példa automatára  $d(M) = 9$ .

## $d(n)$

Ha  $n \geq 1$ , legyen

$$d(n) = \max\{d(M) : M \text{ irányítható, } n\text{-állapotú automata}\}.$$

## $d(n)$ kis $n$ -ekre

- $d(1) = 0$ .
- $d(2) = 1$ .
- $d(3) = 4$ .
- $d(4) = 9$ .

# $d(M), d(n)$

## $d(M)$

Ha  $M$  irányítható, legyen

$$d(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

Az előbbi példa automatára  $d(M) = 9$ .

## $d(n)$

Ha  $n \geq 1$ , legyen

$$d(n) = \max\{d(M) : M \text{ irányítható, } n\text{-állapotú automata}\}.$$

## $d(n)$ kis $n$ -ekre

- $d(1) = 0$ .
- $d(2) = 1$ .
- $d(3) = 4$ .
- $d(4) = 9$ .

# $d(M), d(n)$

## $d(M)$

Ha  $M$  irányítható, legyen

$$d(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

Az előbbi példa automatára  $d(M) = 9$ .

## $d(n)$

Ha  $n \geq 1$ , legyen

$$d(n) = \max\{d(M) : M \text{ irányítható, } n\text{-állapotú automata}\}.$$

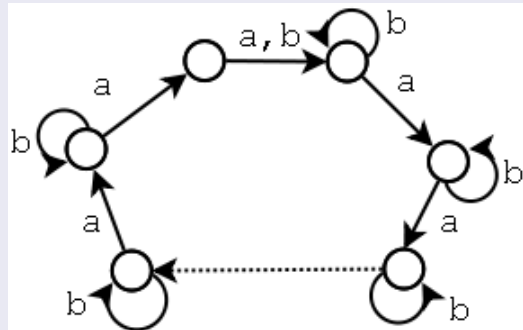
## $d(n)$ kis $n$ -ekre

- $d(1) = 0$ .
- $d(2) = 1$ .
- $d(3) = 4$ .
- $d(4) = 9$ .



# A Sejtés

$d(n) \geq (n-1)^2$  (Černý, 1964)



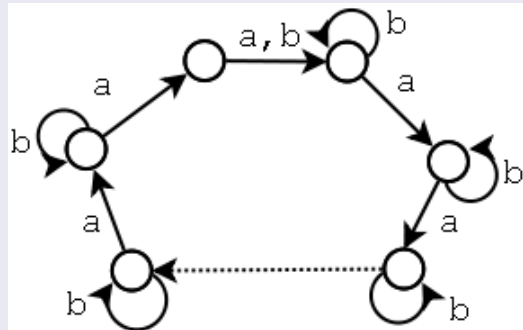
Legrövidebb irányító szó:  $(ba^{n-1})^{n-2}b$ , hossza  $(n-1)^2$

A Černý-sejtés

$$d(n) \stackrel{?}{=} (n-1)^2$$

# A Sejtés

$d(n) \geq (n-1)^2$  (Černý, 1964)



Legrövidebb irányító szó:  $(ba^{n-1})^{n-2}b$ , hossza  $(n-1)^2$

## A Černý-sejtés

$$d(n) \stackrel{?}{=} (n-1)^2$$

$$d(n) \leq 2^n - n - 1$$

## Hatványautomata

Legyen  $P_M = (P(Q), A, \delta')$  az  $M$  hatványautomatája:

$$\delta'(P, a) = \{\delta(p, a) : p \in P\}.$$

## Észrevétel

$$\begin{aligned} u \text{ irányítja } M\text{-et} &\Leftrightarrow |\delta(Q, u)| = 1 \\ &\Leftrightarrow |\delta'(Q, u)| = 1 \\ &\Leftrightarrow P_M\text{-ben } u \text{ egyelemű halmazba viszi } Q\text{-t.} \end{aligned}$$

Tehát  $d(M)$  ugyanannyi, mint  $P_M$ -ben a  $Q$ -ból a  $\{\{q\} : q \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $2^n - n - 1$ .

$$d(n) \leq 2^n - n - 1$$

## Hatványautomata

Legyen  $P_M = (P(Q), A, \delta')$  az  $M$  hatványautomatája:

$$\delta'(P, a) = \{\delta(p, a) : p \in P\}.$$

## Észrevétel

$$\begin{aligned} u \text{ irányítja } M\text{-et} &\Leftrightarrow |\delta(Q, u)| = 1 \\ &\Leftrightarrow |\delta'(Q, u)| = 1 \\ &\Leftrightarrow P_M\text{-ben } u \text{ egyelemű halmazba viszi } Q\text{-t.} \end{aligned}$$

Tehát  $d(M)$  ugyanannyi, mint  $P_M$ -ben a  $Q$ -ból a  $\{\{q\} : q \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $2^n - n - 1$ .

$$d(n) \leq 2^n - n - 1$$

## Hatványautomata

Legyen  $P_M = (P(Q), A, \delta')$  az  $M$  hatványautomatája:

$$\delta'(P, a) = \{\delta(p, a) : p \in P\}.$$

## Észrevétel

$$\begin{aligned} u \text{ irányítja } M\text{-et} &\Leftrightarrow |\delta(Q, u)| = 1 \\ &\Leftrightarrow |\delta'(Q, u)| = 1 \\ &\Leftrightarrow P_M\text{-ben } u \text{ egyelemű halmazba viszi } Q\text{-t.} \end{aligned}$$

Tehát  $d(M)$  ugyanannyi, mint  $P_M$ -ben a  $Q$ -ból a  $\{\{q\} : q \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $2^n - n - 1$ .

$$d(n) \leq 2^n - n - 1$$

## Hatványautomata

Legyen  $P_M = (P(Q), A, \delta')$  az  $M$  hatványautomatája:

$$\delta'(P, a) = \{\delta(p, a) : p \in P\}.$$

## Észrevétel

$$\begin{aligned} u \text{ irányítja } M\text{-et} &\Leftrightarrow |\delta(Q, u)| = 1 \\ &\Leftrightarrow |\delta'(Q, u)| = 1 \\ &\Leftrightarrow P_M\text{-ben } u \text{ egyelemű halmazba viszi } Q\text{-t.} \end{aligned}$$

Tehát  $d(M)$  ugyanannyi, mint  $P_M$ -ben a  $Q$ -ból a  $\{\{q\} : q \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $2^n - n - 1$ .

## Észrevétel

$M$  irányítható  $\Leftrightarrow$  minden  $p, q \in Q$ -ra van  $u$ , amire  $pu = qu$ .

- $\Rightarrow$ : triviális
- $\Leftarrow$ : ha  $|P| \geq 2$ , akkor legyen  $p \neq q \in P$ .  
Vegyünk egy  $u$  szót, amire  $pu = qu$ .  
Akkor  $|Pu| < |P|$ . Innen indukció  $|P|$  szerint.

## Észrevétel

$M$  irányítható  $\Leftrightarrow$  minden  $p, q \in Q$ -ra van  $u$ , amire  $pu = qu$ .

- $\Rightarrow$ : triviális
- $\Leftarrow$ : ha  $|P| \geq 2$ , akkor legyen  $p \neq q \in P$ .  
Vegyünk egy  $u$  szót, amire  $pu = qu$ .  
Akkor  $|Pu| < |P|$ . Innen indukció  $|P|$  szerint.



## Észrevétel

$M$  irányítható  $\Leftrightarrow$  minden  $p, q \in Q$ -ra van  $u$ , amire  $pu = qu$ .

- $\Rightarrow$ : triviális
- $\Leftarrow$ : ha  $|P| \geq 2$ , akkor legyen  $p \neq q \in P$ .

Vegyünk egy  $u$  szót, amire  $pu = qu$ .

Akkor  $|Pu| < |P|$ . Innen indukció  $|P|$  szerint.

## Észrevétel

$M$  irányítható  $\Leftrightarrow$  minden  $p, q \in Q$ -ra van  $u$ , amire  $pu = qu$ .

- $\Rightarrow$ : triviális
- $\Leftarrow$ : ha  $|P| \geq 2$ , akkor legyen  $p \neq q \in P$ .

Vegyünk egy  $u$  szót, amire  $pu = qu$ .

Akkor  $|Pu| < |P|$ . Innen indukció  $|P|$  szerint.

## Észrevétel

$M$  irányítható  $\Leftrightarrow$  minden  $p, q \in Q$ -ra van  $u$ , amire  $pu = qu$ .

- $\Rightarrow$ : triviális
- $\Leftarrow$ : ha  $|P| \geq 2$ , akkor legyen  $p \neq q \in P$ .  
Vegyünk egy  $u$  szót, amire  $pu = qu$ .  
Akkor  $|Pu| < |P|$ . Innen indukció  $|P|$  szerint.

## Észrevétel

$M$  irányítható  $\Leftrightarrow$  minden  $p, q \in Q$ -ra van  $u$ , amire  $pu = qu$ .

- $\Rightarrow$ : triviális
- $\Leftarrow$ : ha  $|P| \geq 2$ , akkor legyen  $p \neq q \in P$ .  
Vegyünk egy  $u$  szót, amire  $pu = qu$ .  
Akkor  $|Pu| < |P|$ . Innen indukció  $|P|$  szerint.

$$d(n) = O(n^3)$$

## Segédautomata $M$ -hez

Legyen  $M^2 = (Q^2, A, \delta^2)$ , ahol  $\delta^2((p, q), a) = (\delta(p, a), \delta(q, a))$ .  
(Direkt szorzat önmagával.)

## Észrevétel

$pu = qu$  pontosan akkor, ha  $M^2$ -ben  $(p, q)u = (r, r)$  valamilyen  $r$ -re.  
Tehát a  $\{p, q\}$  halmazt összeajtó legrövidebb szó hossza ugyanannyi, mint  $M^2$  gráfjában a  $(p, q)$ -ból a  $\{(r, r) : r \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $n^2 - n$ .

## Következmény

$$d(n) \leq (n^2 - n)(n - 1) = n^3 - 2n^2 + n.$$

$$d(n) = O(n^3)$$

## Segédautomata $M$ -hez

Legyen  $M^2 = (Q^2, A, \delta^2)$ , ahol  $\delta^2((p, q), a) = (\delta(p, a), \delta(q, a))$ .  
(Direkt szorzat önmagával.)

## Észrevétel

$pu = qu$  pontosan akkor, ha  $M^2$ -ben  $(p, q)u = (r, r)$  valamilyen  $r$ -re.  
Tehát a  $\{p, q\}$  halmazt összeajtó legrövidebb szó hossza ugyanannyi, mint  $M^2$  gráfjában a  $(p, q)$ -ból a  $\{(r, r) : r \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $n^2 - n$ .

## Következmény

$$d(n) \leq (n^2 - n)(n - 1) = n^3 - 2n^2 + n.$$

$$d(n) = O(n^3)$$

## Segédautomata $M$ -hez

Legyen  $M^2 = (Q^2, A, \delta^2)$ , ahol  $\delta^2((p, q), a) = (\delta(p, a), \delta(q, a))$ .  
(Direkt szorzat önmagával.)

## Észrevétel

$pu = qu$  pontosan akkor, ha  $M^2$ -ben  $(p, q)u = (r, r)$  valamilyen  $r$ -re.  
Tehát a  $\{p, q\}$  halmazt összeajtó legrövidebb szó hossza ugyanannyi, mint  $M^2$  gráfjában a  $(p, q)$ -ból a  $\{(r, r) : r \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $n^2 - n$ .

## Következmény

$$d(n) \leq (n^2 - n)(n - 1) = n^3 - 2n^2 + n.$$

$$d(n) = O(n^3)$$

## Segédautomata $M$ -hez

Legyen  $M^2 = (Q^2, A, \delta^2)$ , ahol  $\delta^2((p, q), a) = (\delta(p, a), \delta(q, a))$ .  
(Direkt szorzat önmagával.)

## Észrevétel

$pu = qu$  pontosan akkor, ha  $M^2$ -ben  $(p, q)u = (r, r)$  valamilyen  $r$ -re.  
Tehát a  $\{p, q\}$  halmazt összejtő legrövidebb szó hossza ugyanannyi, mint  $M^2$  gráfjában a  $(p, q)$ -ból a  $\{(r, r) : r \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $n^2 - n$ .

## Következmény

$$d(n) \leq (n^2 - n)(n - 1) = n^3 - 2n^2 + n.$$



$$d(n) = O(n^3)$$

## Segédautomata $M$ -hez

Legyen  $M^2 = (Q^2, A, \delta^2)$ , ahol  $\delta^2((p, q), a) = (\delta(p, a), \delta(q, a))$ .  
(Direkt szorzat önmagával.)

## Észrevétel

$pu = qu$  pontosan akkor, ha  $M^2$ -ben  $(p, q)u = (r, r)$  valamilyen  $r$ -re.  
Tehát a  $\{p, q\}$  halmazt összeajtó legrövidebb szó hossza ugyanannyi, mint  $M^2$  gráfjában a  $(p, q)$ -ból a  $\{(r, r) : r \in Q\}$  halmazba vezető legrövidebb út hossza.

Ez legfeljebb  $n^2 - n$ .

## Következmény

$$d(n) \leq (n^2 - n)(n - 1) = n^3 - 2n^2 + n.$$

## Algoritmus

- 1 Kezdetben legyen  $S = Q$  és  $u = \varepsilon$ .
- 2 Ha  $|S| = 1$ , vége,  $u$  irányítja  $M$ -et.
- 3 Legyen  $v \in A^*$  egy legrövidebb olyan szó, amire  $|Sv| < |S|$ .
- 4  $S := Sv$ ,  $u := uv$ , menjünk a 2. pontra.

## Tények

Az algoritmus irányító szót ad vissza.

Nem mindig a legrövidebbet!

## Algoritmus

- 1 Kezdetben legyen  $S = Q$  és  $u = \varepsilon$ .
- 2 Ha  $|S| = 1$ , vége,  $u$  irányítja  $M$ -et.
- 3 Legyen  $v \in A^*$  egy legrövidebb olyan szó, amire  $|Sv| < |S|$ .
- 4  $S := Sv$ ,  $u := uv$ , menjünk a 2. pontra.

## Tények

Az algoritmus irányító szót ad vissza.

Nem mindig a legrövidebbet!

## Algoritmus

- 1 Kezdetben legyen  $S = Q$  és  $u = \varepsilon$ .
- 2 Ha  $|S| = 1$ , vége,  $u$  irányítja  $M$ -et.
- 3 Legyen  $v \in A^*$  egy legrövidebb olyan szó, amire  $|Sv| < |S|$ .
- 4  $S := Sv$ ,  $u := uv$ , menjünk a 2. pontra.

## Tények

Az algoritmus irányító szót ad vissza.

Nem mindig a legrövidebbet!

## Algoritmus

- 1 Kezdetben legyen  $S = Q$  és  $u = \varepsilon$ .
- 2 Ha  $|S| = 1$ , vége,  $u$  irányítja  $M$ -et.
- 3 Legyen  $v \in A^*$  egy legrövidebb olyan szó, amire  $|Sv| < |S|$ .
- 4  $S := Sv$ ,  $u := uv$ , menjünk a 2. pontra.

## Tények

Az algoritmus irányító szót ad vissza.

Nem mindig a legrövidebbet!

## Algoritmus

- 1 Kezdetben legyen  $S = Q$  és  $u = \varepsilon$ .
- 2 Ha  $|S| = 1$ , vége,  $u$  irányítja  $M$ -et.
- 3 Legyen  $v \in A^*$  egy legrövidebb olyan szó, amire  $|Sv| < |S|$ .
- 4  $S := Sv$ ,  $u := uv$ , menjünk a 2. pontra.

## Tények

Az algoritmus irányító szót ad vissza.

Nem mindig a legrövidebbet!

## Algoritmus

- 1 Kezdetben legyen  $S = Q$  és  $u = \varepsilon$ .
- 2 Ha  $|S| = 1$ , vége,  $u$  irányítja  $M$ -et.
- 3 Legyen  $v \in A^*$  egy legrövidebb olyan szó, amire  $|Sv| < |S|$ .
- 4  $S := Sv$ ,  $u := uv$ , menjünk a 2. pontra.

## Tények

Az algoritmus irányító szót ad vissza.

Nem mindig a legrövidebbet!

## Algoritmus

- 1 Kezdetben legyen  $S = Q$  és  $u = \varepsilon$ .
- 2 Ha  $|S| = 1$ , vége,  $u$  irányítja  $M$ -et.
- 3 Legyen  $v \in A^*$  egy legrövidebb olyan szó, amire  $|Sv| < |S|$ .
- 4  $S := Sv$ ,  $u := uv$ , menjünk a 2. pontra.

## Tények

Az algoritmus irányító szót ad vissza.

Nem mindig a legrövidebbet!



## Algoritmus

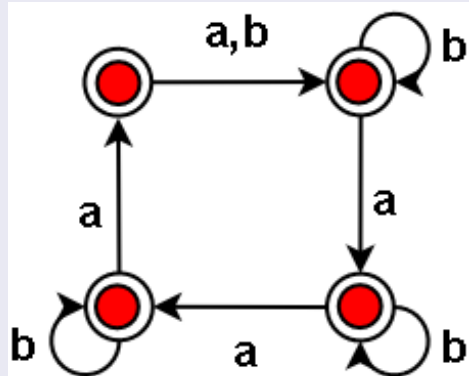
- 1 Kezdetben legyen  $S = Q$  és  $u = \varepsilon$ .
- 2 Ha  $|S| = 1$ , vége,  $u$  irányítja  $M$ -et.
- 3 Legyen  $v \in A^*$  egy legrövidebb olyan szó, amire  $|Sv| < |S|$ .
- 4  $S := Sv$ ,  $u := uv$ , menjünk a 2. pontra.

## Tények

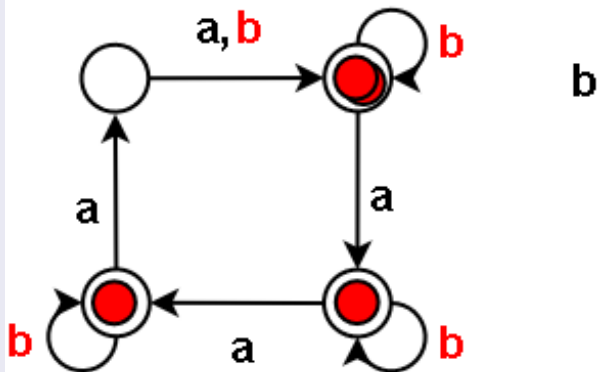
Az algoritmus irányító szót ad vissza.

Nem mindig a legrövidebbet!

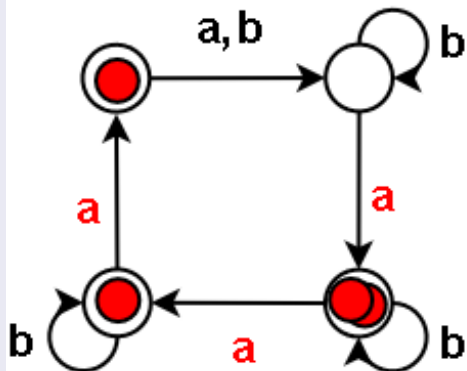
## Példa



## Példa

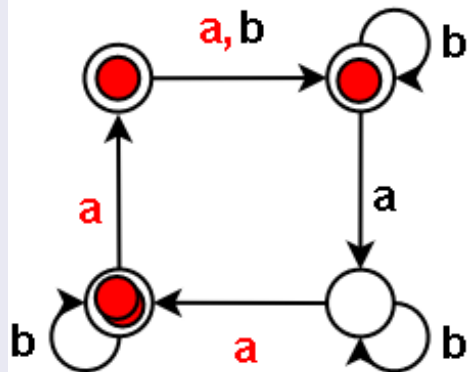


## Példa



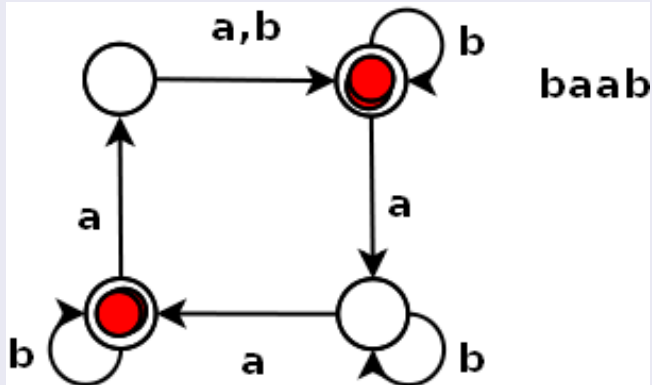
ba

## Példa

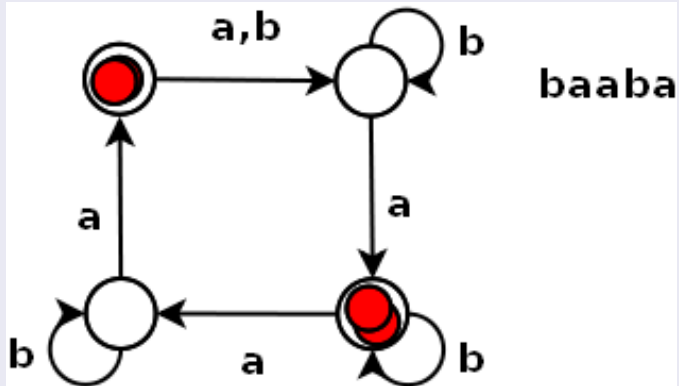


baa

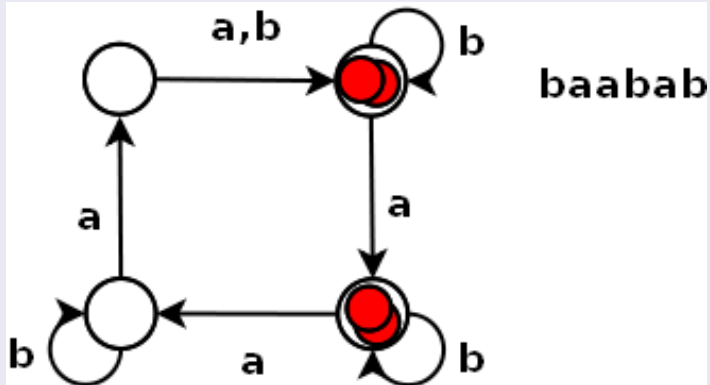
## Példa



## Példa



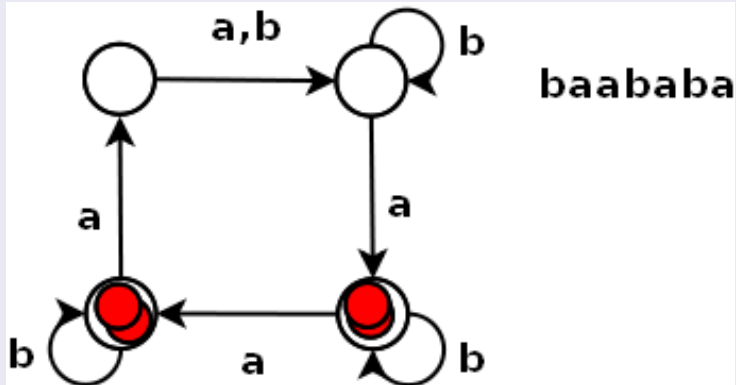
## Példa



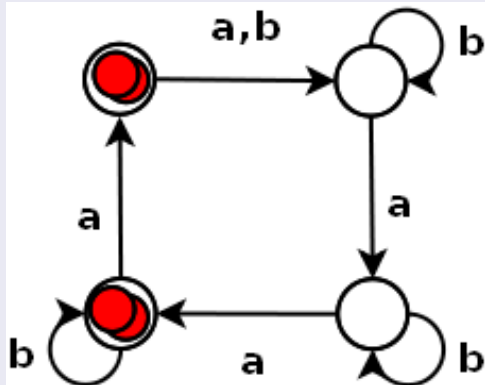
baabab



## Példa

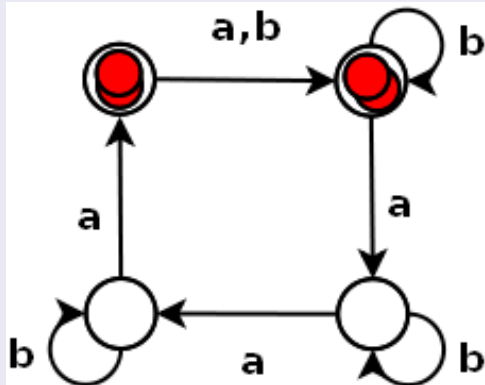


## Példa



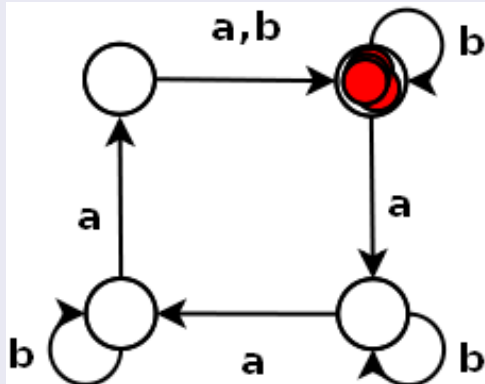
**baababaa**

## Példa



**baababaaa**

## Példa



**baababaaab**

10 hosszú!

## Tétel (Frankl, 1982)

Ha  $A_1, \dots, A_m$   $r$ -elemű,  $B_1, \dots, B_m$  pedig  $s$ -elemű halmazok úgy, hogy

- minden  $i$ -re  $A_i \cap B_i = \emptyset$  és
- minden  $i < j$ -re  $A_i \cap B_j \neq \emptyset$ ,

akkor  $m \leq \binom{r+s}{s}$ .

## Következmény (Pin, 1983)

$$d(n) \leq \frac{n^3 - n}{6}$$

Hogy?

A mohó algoritmus elemzésével.

## Tétel (Frankl, 1982)

Ha  $A_1, \dots, A_m$   $r$ -elemű,  $B_1, \dots, B_m$  pedig  $s$ -elemű halmazok úgy, hogy

- minden  $i$ -re  $A_i \cap B_i = \emptyset$  és
- minden  $i < j$ -re  $A_i \cap B_j \neq \emptyset$ ,

akkor  $m \leq \binom{r+s}{s}$ .

## Következmény (Pin, 1983)

$$d(n) \leq \frac{n^3 - n}{6}$$

Hogy?

A mohó algoritmus elemzésével.

## Tétel (Frankl, 1982)

Ha  $A_1, \dots, A_m$   $r$ -elemű,  $B_1, \dots, B_m$  pedig  $s$ -elemű halmazok úgy, hogy

- minden  $i$ -re  $A_i \cap B_i = \emptyset$  és
- minden  $i < j$ -re  $A_i \cap B_j \neq \emptyset$ ,

akkor  $m \leq \binom{r+s}{s}$ .

## Következmény (Pin, 1983)

$$d(n) \leq \frac{n^3 - n}{6}$$

## Hogy?

A mohó algoritmus elemzésével.

# Itt tartunk!

Eddig tehát ennyi ismert:

$$(n-1)^2 \leq d(n) \leq \frac{n^3 - n}{6}.$$

## Speciális esetek

A sejtés igaz, ha  $M$ ...

- ...prím darab állapotú és benne egy betű ciklikus permutációt indukál (Pin, 1978);
- ...akárhány állapotú és benne egy betű ciklikus permutációt indukál (Dubuc, 1998);
- ...átmenetgráfjában van Euler-kör (Kari, 2003);
- ...aperiodikus (Trahtman, 2007);
- ...

...de az általános esetben továbbra is nyitott a kérdés.



# Itt tartunk!

Eddig tehát ennyi ismert:

$$(n-1)^2 \leq d(n) \leq \frac{n^3 - n}{6}.$$

## Speciális esetek

A sejtés igaz, ha  $M$ ...

- ...prím darab állapotú és benne egy betű ciklikus permutációt indukál (Pin, 1978);
- ...akárhány állapotú és benne egy betű ciklikus permutációt indukál (Dubuc, 1998);
- ...átmenetgráfjában van Euler-kör (Kari, 2003);
- ...aperiodikus (Trahtman, 2007);
- ...

...de az általános esetben továbbra is nyitott a kérdés.

## Parciális automaták irányítása

## Parciális automata

**Parciális automata:** egy  $M = (Q, A, \delta)$  hármas, ahol

- $Q, A$ : mint korábban;
- $\delta : Q \times A \rightarrow Q$  **parciális** függvény.

$pu, Pu$

$\delta$  ismét kiterjeszhető egy  $\delta : Q \times A^* \rightarrow Q$  **parciális** függvénnyé.

$pu = q$ :  $\delta(p, u)$  értelmezett és eredménye  $q$ .

$Pu = R$ :  $\delta(p, u)$  értelmezett minden  $p \in P$ -re és  $R = \{pu : p \in P\}$ .

## Parciális automata

**Parciális automata:** egy  $M = (Q, A, \delta)$  hármas, ahol

- $Q, A$ : mint korábban;
- $\delta : Q \times A \rightarrow Q$  **parciális** függvény.

## $\rho u, P u$

$\delta$  ismét kiterjeszhető egy  $\delta : Q \times A^* \rightarrow Q$  **parciális** függvénnyé.

$\rho u = q$ :  $\delta(p, u)$  értelmezett és eredménye  $q$ .

$P u = R$ :  $\delta(p, u)$  értelmezett **minden**  $p \in P$ -re és  $R = \{\rho u : p \in P\}$ .

## Parciális automata

**Parciális automata:** egy  $M = (Q, A, \delta)$  hármas, ahol

- $Q, A$ : mint korábban;
- $\delta : Q \times A \rightarrow Q$  **parciális** függvény.

## $\rho u, P u$

$\delta$  ismét kiterjeszhető egy  $\delta : Q \times A^* \rightarrow Q$  **parciális** függvénnyé.

$\rho u = q$ :  $\delta(p, u)$  értelmezett és eredménye  $q$ .

$P u = R$ :  $\delta(p, u)$  értelmezett **minden**  $p \in P$ -re és  $R = \{\rho u : p \in P\}$ .

## Parciális automata

**Parciális automata:** egy  $M = (Q, A, \delta)$  hármas, ahol

- $Q, A$ : mint korábban;
- $\delta : Q \times A \rightarrow Q$  **parciális** függvény.

## $\rho u, P u$

$\delta$  ismét kiterjeszhető egy  $\delta : Q \times A^* \rightarrow Q$  **parciális** függvénnyé.

$\rho u = q$ :  $\delta(p, u)$  értelmezett és eredménye  $q$ .

$P u = R$ :  $\delta(p, u)$  értelmezett **minden**  $p \in P$ -re és  $R = \{\rho u : p \in P\}$ .

## Irányító szó

Az  $u$  szó **irányítja** az  $M$  parciális automatát, ha  $|Qu| = 1$ .

( $pu$  minden  $p \in Q$ -ra értelmezett kell legyen!)

$M$  **irányítható**, ha van irányító szava.

$d_p(M)$

Ha  $M$  irányítható, legyen

$$d_p(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

$d_p(n)$

Ha  $n \geq 1$ , legyen

$$d_p(n) = \max\{d_p(M) : M \text{ irányítható, } n\text{-állapotos parc. automata}\}.$$

## Irányító szó

Az  $u$  szó **irányítja** az  $M$  parciális automatát, ha  $|Qu| = 1$ .

( $pu$  minden  $p \in Q$ -ra értelmezett kell legyen!)

$M$  **irányítható**, ha van irányító szava.

$d_p(M)$

Ha  $M$  irányítható, legyen

$$d_p(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

$d_p(n)$

Ha  $n \geq 1$ , legyen

$$d_p(n) = \max\{d_p(M) : M \text{ irányítható, } n\text{-állapotos parc. automata}\}.$$



## Irányító szó

Az  $u$  szó **irányítja** az  $M$  parciális automatát, ha  $|Qu| = 1$ .

( $pu$  minden  $p \in Q$ -ra értelmezett kell legyen!)

$M$  **irányítható**, ha van irányító szava.

$d_p(M)$

Ha  $M$  irányítható, legyen

$$d_p(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

$d_p(n)$

Ha  $n \geq 1$ , legyen

$$d_p(n) = \max\{d_p(M) : M \text{ irányítható, } n\text{-állapotos parc. automata}\}.$$

## Irányító szó

Az  $u$  szó **irányítja** az  $M$  parciális automatát, ha  $|Qu| = 1$ .

( $pu$  minden  $p \in Q$ -ra értelmezett kell legyen!)

$M$  **irányítható**, ha van irányító szava.

## $d_p(M)$

Ha  $M$  irányítható, legyen

$$d_p(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

## $d_p(n)$

Ha  $n \geq 1$ , legyen

$$d_p(n) = \max\{d_p(M) : M \text{ irányítható, } n\text{-állapotos parc. automata}\}.$$

## Irányító szó

Az  $u$  szó **irányítja** az  $M$  parciális automatát, ha  $|Qu| = 1$ .

( $pu$  minden  $p \in Q$ -ra értelmezett kell legyen!)

$M$  **irányítható**, ha van irányító szava.

## $d_p(M)$

Ha  $M$  irányítható, legyen

$$d_p(M) = \min\{|u| : u \text{ irányítja } M\text{-et}\}.$$

## $d_p(n)$

Ha  $n \geq 1$ , legyen

$$d_p(n) = \max\{d_p(M) : M \text{ irányítható, } n\text{-állapotos parc. automata}\}.$$

$$d_p(n) = O(2^n)$$

Hogy?

A hatványautomatás konstrukció itt is működik.

Javítás?

A páronkénti összeejthetőség most kevés.

Példa

$$d_p(n) = O(2^n)$$

Hogy?

A hatványautomatás konstrukció itt is működik.

Javítás?

A páronkénti összeejthetőség most kevés.

Példa

$$d_p(n) = O(2^n)$$

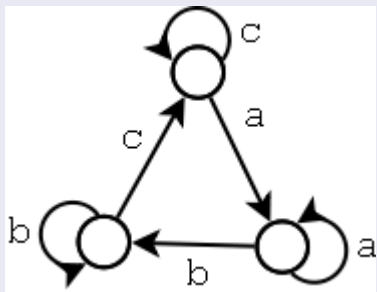
Hogy?

A hatványautomatás konstrukció itt is működik.

Javítás?

A páronkénti összeejthetőség most kevés.

Példa



$$d_p(n) = \Omega(\sqrt{2}^n) \text{ (Ito-Tsuji, 2004)}$$

## Konstrukció

Legyen  $n = 2m$  páros,  $Q = \{0, 1, \dots, n-1\}$ ,  $A = \{a, b_1, \dots, b_m, c\}$  és  $\delta$  a következő:

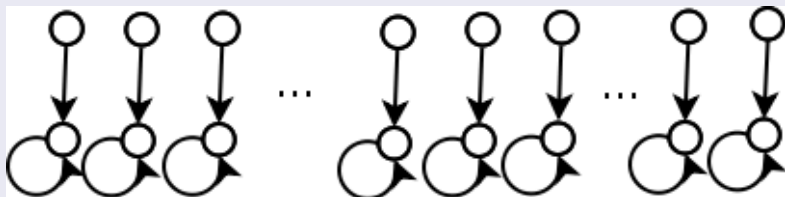
Az  $a$  betűhöz tartozó átmenet

$$d_p(n) = \Omega(\sqrt{2}^n) \text{ (Ito-Tsuji, 2004)}$$

## Konstrukció

Legyen  $n = 2m$  páros,  $Q = \{0, 1, \dots, n-1\}$ ,  $A = \{a, b_1, \dots, b_m, c\}$  és  $\delta$  a következő:

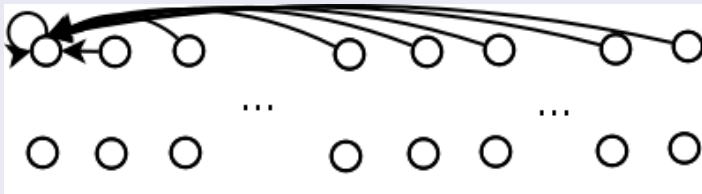
## Az $a$ betűhöz tartozó átmenet





$$d_p(n) = \Omega(\sqrt{2^n}) \text{ (Ito-Tsuji, 2004)}$$

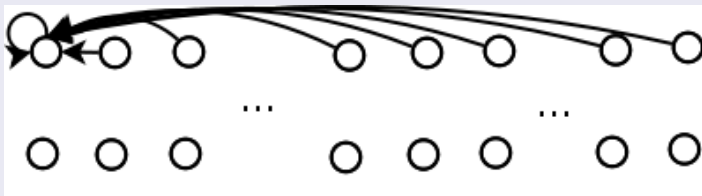
A  $c$  betűhöz tartozó átmenet



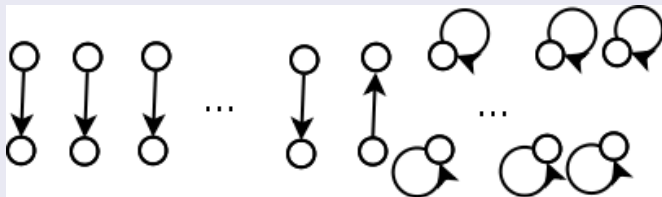
A  $b_i, 1 \leq i \leq m$  betűhöz tartozó átmenet

$$d_p(n) = \Omega(\sqrt{2}^n) \text{ (Ito-Tsuji, 2004)}$$

A  $c$  betűhöz tartozó átmenet

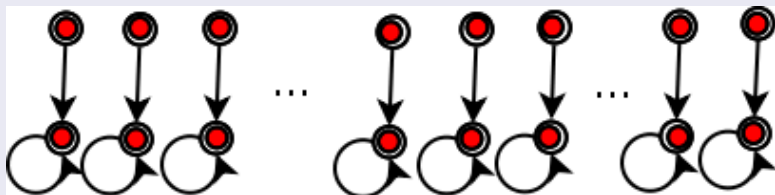


A  $b_i, 1 \leq i \leq m$  betűhöz tartozó átmenet



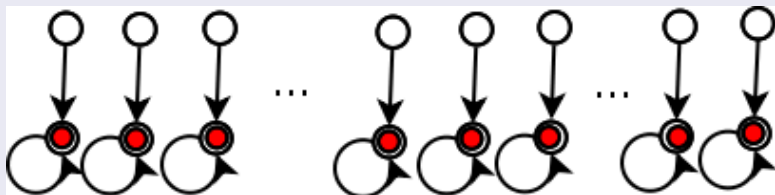
# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



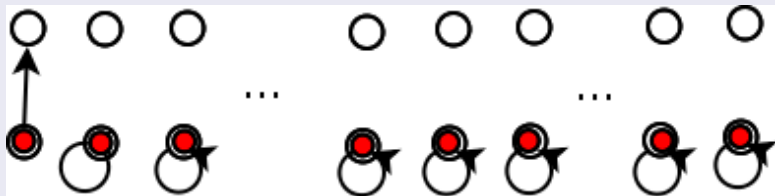
# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



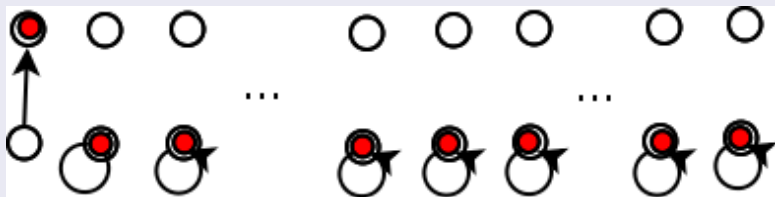
# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



# Az automata irányítható

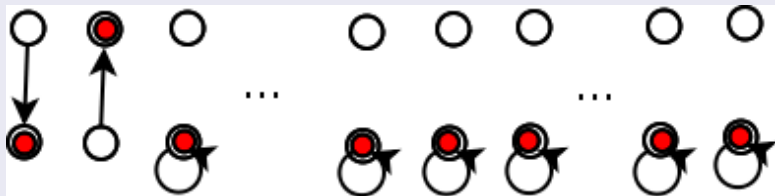
Ezt az automatát a következőképp tudjuk irányítani:





# Az automata irányítható

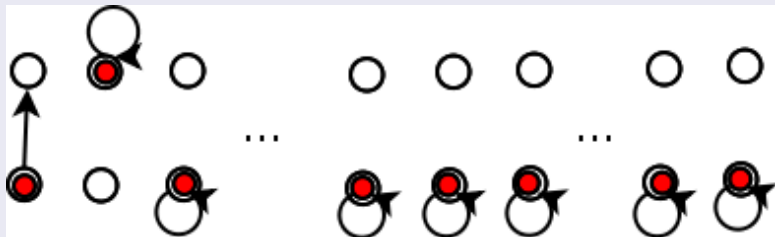
Ezt az automatát a következőképp tudjuk irányítani:





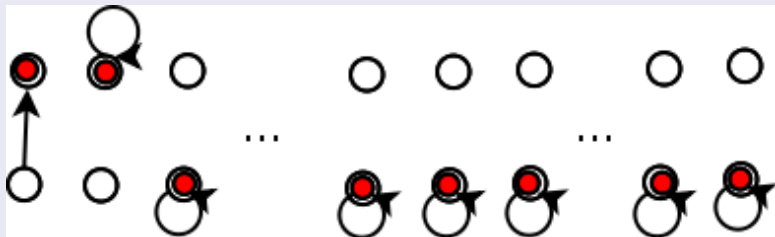
# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



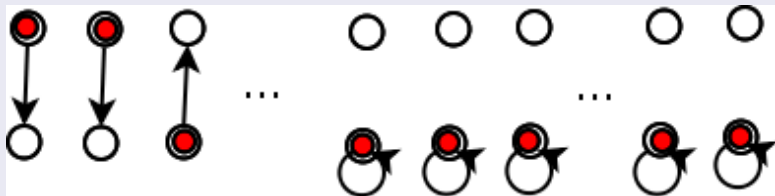
# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



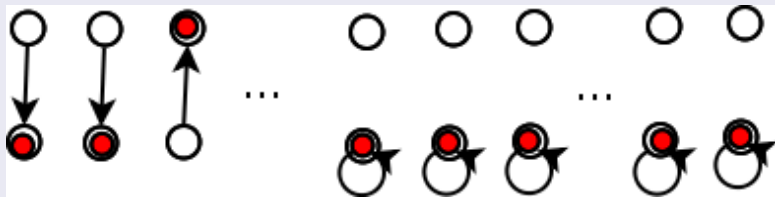
# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



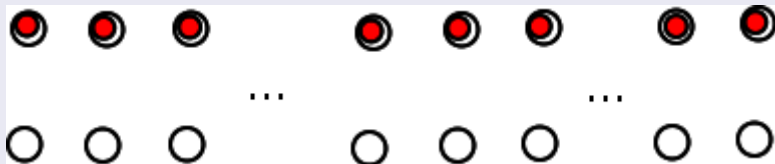
# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



# Az automata irányítható

Ezt az automatát a következőképp tudjuk irányítani:



A szó hossza  $2^m + 1 = 2^{n/2} + 1 = \Omega(\sqrt{2^n})$ .

$d_p(n) = \Omega(\sqrt[3]{3}^n)$  (P. Martyugin, 2005)

Tétel

$$d_p(n) = \Omega(\sqrt[3]{3}^n)$$

Hogy?

Ugyanez hármas számrendszerben...

Írjunk cikket a négyes számrendszerről?

Nem, további variálásával a számrendszernek már nem lesz jobb...

$$d_p(n) = \Omega(\sqrt[3]{3^n}) \text{ (P. Martyugin, 2005)}$$

Tétel

$$d_p(n) = \Omega(\sqrt[3]{3^n})$$

Hogy?

Ugyanez hármas számrendszerben...

Írjunk cikket a négyes számrendszerről?

Nem, további variálásával a számrendszernek már nem lesz jobb...



$$d_p(n) = \Omega(\sqrt[3]{3^n}) \text{ (P. Martyugin, 2005)}$$

Tétel

$$d_p(n) = \Omega(\sqrt[3]{3^n})$$

Hogy?

Ugyanez hármass számrendszerben...

Írjunk cikket a négyes számrendszerről?

Nem, további variálásával a számrendszernek már nem lesz jobb...

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

(Zs. Gazdag, Sz. Iván, J. Nagy-György, 2009)

## Tétel

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n}).$$

A továbbiakban rögzítsünk egy  $M = (Q, A, \delta)$  irányítható parciális automatát, és legyen  $n = |Q|$ .

## Bizonyítás – vázlat

- Először belátjuk, hogy van olyan  $u \in A^*$ , amire  $|Qu| \leq n/3$  és  $|u| \leq n \cdot \sqrt[3]{4^n}$ .
- Aztán ezt a szót használjuk még  $n/3$ -szor.

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

(Zs. Gazdag, Sz. Iván, J. Nagy-György, 2009)

## Tétel

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n}).$$

A továbbiakban rögzítsünk egy  $M = (Q, A, \delta)$  irányítható parciális automatát, és legyen  $n = |Q|$ .

## Bizonyítás – vázlat

- Először belátjuk, hogy van olyan  $u \in A^*$ , amire  $|Qu| \leq n/3$  és  $|u| \leq n \cdot \sqrt[3]{4^n}$ .
- Aztán ezt a szót használjuk még  $n/3$ -szor.

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

(Zs. Gazdag, Sz. Iván, J. Nagy-György, 2009)

## Tétel

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n}).$$

A továbbiakban rögzítsünk egy  $M = (Q, A, \delta)$  irányítható parciális automatát, és legyen  $n = |Q|$ .

## Bizonyítás – vázlat

- Először belátjuk, hogy van olyan  $u \in A^*$ , amire  $|Qu| \leq n/3$  és  $|u| \leq n \cdot \sqrt[3]{4^n}$ .
- Aztán ezt a szót használjuk még  $n/3$ -szor.

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

(Zs. Gazdag, Sz. Iván, J. Nagy-György, 2009)

## Tétel

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n}).$$

A továbbiakban rögzítsünk egy  $M = (Q, A, \delta)$  irányítható parciális automatát, és legyen  $n = |Q|$ .

## Bizonyítás – vázlat

- Először belátjuk, hogy van olyan  $u \in A^*$ , amire  $|Qu| \leq n/3$  és  $|u| \leq n \cdot \sqrt[3]{4^n}$ .
- Aztán ezt a szót használjuk még  $n/3$ -szor.

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

(Zs. Gazdag, Sz. Iván, J. Nagy-György, 2009)

## Tétel

$$d_p(n) = O(n^2 \cdot \sqrt[3]{4^n}).$$

A továbbiakban rögzítsünk egy  $M = (Q, A, \delta)$  irányítható parciális automatát, és legyen  $n = |Q|$ .

## Bizonyítás – vázlat

- Először belátjuk, hogy van olyan  $u \in A^*$ , amire  $|Qu| \leq n/3$  és  $|u| \leq n \cdot \sqrt[3]{4^n}$ .
- Aztán ezt a szót használjuk még  $n/3$ -szor.

## Transzverzális

Legyen  $\Theta$  egy ekvivalencia-reláció  $Q$ -n.  $P \subseteq Q$  egy  $\Theta$ -transzverzális, ha minden  $\Theta$ -osztályból **pontosan egy** elemet tartalmaz.

## Szemitranzverzális

Legyen  $\Theta$  egy ekvivalencia-reláció  $Q$ -n.  $P \subseteq Q$  egy  $\Theta$ -szemitranzverzális, ha minden  $\Theta$ -osztályból **legfeljebb egy** elemet tartalmaz.

## Transzverzális

Legyen  $\Theta$  egy ekvivalencia-reláció  $Q$ -n.  $P \subseteq Q$  egy  $\Theta$ -transzverzális, ha minden  $\Theta$ -osztályból **pontosan egy** elemet tartalmaz.

## Szemitranzverzális

Legyen  $\Theta$  egy ekvivalencia-reláció  $Q$ -n.  $P \subseteq Q$  egy  $\Theta$ -szemitranzverzális, ha minden  $\Theta$ -osztályból **legfeljebb egy** elemet tartalmaz.



## Transzverzális

Legyen  $\Theta$  egy ekvivalencia-reláció  $Q$ -n.  $P \subseteq Q$  egy  $\Theta$ -transzverzális, ha minden  $\Theta$ -osztályból **pontosan egy** elemet tartalmaz.

## Szemitranzverzális

Legyen  $\Theta$  egy ekvivalencia-reláció  $Q$ -n.  $P \subseteq Q$  egy  $\Theta$ -szemitranzverzális, ha minden  $\Theta$ -osztályból **legfeljebb egy** elemet tartalmaz.

## Transzverzális

Legyen  $\Theta$  egy ekvivalencia-reláció  $Q$ -n.  $P \subseteq Q$  egy  $\Theta$ -**transzverzális**, ha minden  $\Theta$ -osztályból **pontosan egy** elemet tartalmaz.

## Szemitranzverzális

Legyen  $\Theta$  egy ekvivalencia-reláció  $Q$ -n.  $P \subseteq Q$  egy  $\Theta$ -**szemitranzverzális**, ha minden  $\Theta$ -osztályból **legfeljebb egy** elemet tartalmaz.

# A (szemi)transzverzálisok száma

## Lemma

Ha  $\Theta$  egy  $k$  indexű ekvivalencia-reláció, akkor **legfeljebb**  $2^{n-k}$  különböző  $\Theta$ -transzverzális létezik.

## Lemma

Ha  $\Theta$  egy  $k$  indexű ekvivalencia-reláció, akkor **legfeljebb**  $\left(\frac{n+k}{k}\right)^k$  különböző  $\Theta$ -szemitranszverzális létezik.

# A (szemi)transzverzálisok száma

## Lemma

Ha  $\Theta$  egy  $k$  indexű ekvivalencia-reláció, akkor **legfeljebb  $2^{n-k}$**  különböző  $\Theta$ -transzverzális létezik.

## Lemma

Ha  $\Theta$  egy  $k$  indexű ekvivalencia-reláció, akkor **legfeljebb  $\left(\frac{n+k}{k}\right)^k$**  különböző  $\Theta$ -szemitranszverzális létezik.

# A (szemi)transzverzálisok száma

## Lemma

Ha  $\Theta$  egy  $k$  indexű ekvivalencia-reláció, akkor **legfeljebb  $2^{n-k}$**  különböző  $\Theta$ -transzverzális létezik.

## Lemma

Ha  $\Theta$  egy  $k$  indexű ekvivalencia-reláció, akkor **legfeljebb  $\left(\frac{n+k}{k}\right)^k$**  különböző  $\Theta$ -szemitranszverzális létezik.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.



# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.

- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.

# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k+1)2^k$ , kész.



# A transzverzálisok köze a témához

## Lemma

Tetszőleges  $1 \leq k < n$ -hez létezik olyan  $u_k$ , amire  $|Qu_k| \leq n - k$  és  $|u_k| \leq k2^{k-1}$ .

## Bizonyítás

Indukció  $k$ -ra.  $k = 1$  triviális, kell legyen egy  $a \in A$ , amire  $|Qa| < n$ .

- Ha  $|Qu_k| < n - k$ , akkor  $u_{k+1} = u_k$  jó lesz.
- Egyébként legyen  $p\Theta q \Leftrightarrow pu_k = qu_k$ .  $\Theta$  egy  $n - k$  indexű ekvivalenciareláció. Jelölje  $P$  a  $Qu_k$  halmazt.

Vegyünk egy legrövidebb  $v$  szót, amire  $Pv$  definiált és melyre létezik  $p \neq q \in P$ :  $pv\Theta qv$ . (Ilyen szó van.)

Akkor  $v$  összes  $v'$  valódi prefixére  $Pv'$  egy  $\Theta$ -transzverzális. Mivel  $v$  legrövidebb, különbözőek.

Tehát  $|v|$  legfeljebb a különböző  $\Theta$ -transzverzálisok száma:  $|v| \leq 2^k$ .

Akkor  $u_{k+1} = u_k v u_k$  jó lesz, a hossza legfeljebb  $2 \cdot k2^{k-1} + 2^k = (k + 1)2^k$ , kész.

$$d_3(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

Legyen  $n = 3m$ . Előző lemma szerint egy  $u$  szóra  $|Qu| \leq m$  és  $|u| \leq m2^{2m}$ . Legyen  $p\Theta q \Leftrightarrow pu = qu$ .

## Algoritmus

- Legyen  $w = u$  és  $P = Qu$ .
- Ha  $|P| = 1$ , vége, adjuk vissza  $w$ -t.
- Különben vegyünk egy legrövidebb olyan  $v$  szót, amire létezik  $p \neq q \in P$  úgy, hogy  $p\Theta qv$ .
- Legyen  $w = wv$  és  $P = Pvu$ . Menjünk a 2. pontra.

$$d_3(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

Legyen  $n = 3m$ . Előző lemma szerint egy  $u$  szóra  $|Qu| \leq m$  és  $|u| \leq m2^{2m}$ . Legyen  $p\Theta q \Leftrightarrow pu = qu$ .

## Algoritmus

- Legyen  $w = u$  és  $P = Qu$ .
- Ha  $|P| = 1$ , vége, adjuk vissza  $w$ -t.
- Különben vegyünk egy legrövidebb olyan  $v$  szót, amire létezik  $p \neq q \in P$  úgy, hogy  $pv\Theta qv$ .
- Legyen  $w = wvu$  és  $P = Pvu$ . Menjünk a 2. pontra.

$$d_3(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

Legyen  $n = 3m$ . Előző lemma szerint egy  $u$  szóra  $|Qu| \leq m$  és  $|u| \leq m2^{2m}$ . Legyen  $p\Theta q \Leftrightarrow pu = qu$ .

## Algoritmus

- Legyen  $w = u$  és  $P = Qu$ .
- Ha  $|P| = 1$ , vége, adjuk vissza  $w$ -t.
- Különben vegyünk egy legrövidebb olyan  $v$  szót, amire létezik  $p \neq q \in P$  úgy, hogy  $pv\Theta qv$ .
- Legyen  $w = wvu$  és  $P = Pvu$ . Menjünk a 2. pontra.

$$d_3(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

Legyen  $n = 3m$ . Előző lemma szerint egy  $u$  szóra  $|Qu| \leq m$  és  $|u| \leq m2^{2m}$ . Legyen  $p\Theta q \Leftrightarrow pu = qu$ .

## Algoritmus

- Legyen  $w = u$  és  $P = Qu$ .
- Ha  $|P| = 1$ , vége, adjuk vissza  $w$ -t.
- Különben vegyünk egy legrövidebb olyan  $v$  szót, amire létezik  $p \neq q \in P$  úgy, hogy  $pv\Theta qv$ .
- Legyen  $w = wvu$  és  $P = Pvu$ . Menjünk a 2. pontra.

$$d_3(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

Legyen  $n = 3m$ . Előző lemma szerint egy  $u$  szóra  $|Qu| \leq m$  és  $|u| \leq m2^{2m}$ . Legyen  $p\Theta q \Leftrightarrow pu = qu$ .

## Algoritmus

- Legyen  $w = u$  és  $P = Qu$ .
- Ha  $|P| = 1$ , vége, adjuk vissza  $w$ -t.
- Különben vegyünk egy legrövidebb olyan  $v$  szót, amire létezik  $p \neq q \in P$  úgy, hogy  $pv\Theta qv$ .
- Legyen  $w = wvu$  és  $P = Pvu$ . Menjünk a 2. pontra.

$$d_3(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

Legyen  $n = 3m$ . Előző lemma szerint egy  $u$  szóra  $|Qu| \leq m$  és  $|u| \leq m2^{2m}$ . Legyen  $p\Theta q \Leftrightarrow pu = qu$ .

## Algoritmus

- Legyen  $w = u$  és  $P = Qu$ .
- Ha  $|P| = 1$ , vége, adjuk vissza  $w$ -t.
- Különben vegyünk egy legrövidebb olyan  $v$  szót, amire létezik  $p \neq q \in P$  úgy, hogy  $p\Theta qv$ .
- Legyen  $w = wvu$  és  $P = Pvu$ . Menjünk a 2. pontra.

$$d_3(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

Legyen  $n = 3m$ . Előző lemma szerint egy  $u$  szóra  $|Qu| \leq m$  és  $|u| \leq m2^{2m}$ . Legyen  $p\Theta q \Leftrightarrow pu = qu$ .

## Algoritmus

- Legyen  $w = u$  és  $P = Qu$ .
- Ha  $|P| = 1$ , vége, adjuk vissza  $w$ -t.
- Különben vegyünk egy legrövidebb olyan  $v$  szót, amire létezik  $p \neq q \in P$  úgy, hogy  $pv\Theta qv$ .
- Legyen  $w = wvu$  és  $P = Pvu$ . Menjünk a 2. pontra.



$$d_3(n) = O(n^2 \cdot \sqrt[3]{4^n})$$

Legyen  $n = 3m$ . Előző lemma szerint egy  $u$  szóra  $|Qu| \leq m$  és  $|u| \leq m2^{2m}$ . Legyen  $p\Theta q \Leftrightarrow pu = qu$ .

## Algoritmus

- Legyen  $w = u$  és  $P = Qu$ .
- Ha  $|P| = 1$ , vége, adjuk vissza  $w$ -t.
- Különben vegyünk egy legrövidebb olyan  $v$  szót, amire létezik  $p \neq q \in P$  úgy, hogy  $pv\Theta qv$ .
- Legyen  $w = wvu$  és  $P = Pvu$ . Menjünk a 2. pontra.

$w$

Egyrészt  $w$  irányítja  $M$ -et.

Másrészt  $|w|$  legfeljebb  $m$ -szer  $|u|$ , plusz a különböző  $\Theta$ -szemitranszverzálisok száma, vagyis

$$\begin{aligned}d_p(M) &\leq m \cdot |u| + \left(\frac{n+m}{m}\right)^m \\ &\leq m^2 \cdot 2^{2m} + \left(\frac{n+m}{m}\right)^m \\ &\leq n^2 \cdot 2^{2n/3} + \left(\frac{4n/3}{n/3}\right)^{n/3} \\ &= O(n^2 \cdot \sqrt[3]{4^n}).\end{aligned}$$

$w$

Egyrészt  $w$  irányítja  $M$ -et.

Másrészt  $|w|$  legfeljebb  $m$ -szer  $|u|$ , plusz a különböző  $\Theta$ -szemitranszverzálisok száma, vagyis

$$\begin{aligned}d_p(M) &\leq m \cdot |u| + \left(\frac{n+m}{m}\right)^m \\ &\leq m^2 \cdot 2^{2m} + \left(\frac{n+m}{m}\right)^m \\ &\leq n^2 \cdot 2^{2n/3} + \left(\frac{4n/3}{n/3}\right)^{n/3} \\ &= O(n^2 \cdot \sqrt[3]{4}^n).\end{aligned}$$

$w$

Egyrészt  $w$  irányítja  $M$ -et.

Másrészt  $|w|$  legfeljebb  $m$ -szer  $|u|$ , plusz a különböző  $\Theta$ -szemitranszverzálisok száma, vagyis

$$\begin{aligned}d_p(M) &\leq m \cdot |u| + \left(\frac{n+m}{m}\right)^m \\ &\leq m^2 \cdot 2^{2m} + \left(\frac{n+m}{m}\right)^m \\ &\leq n^2 \cdot 2^{2n/3} + \left(\frac{4n/3}{n/3}\right)^{n/3} \\ &= O(n^2 \cdot \sqrt[3]{4^n}).\end{aligned}$$

## Ismert korlátok

$$d_p(n) = \Omega(\sqrt[3]{3}^n) \text{ és } d_p(n) = O(n^2 \cdot \sqrt[3]{4}^n).$$

## Szerintünk...

$$d_p(n) = \Theta(p(n) \cdot \sqrt[3]{3}^n)$$

valami  $p(n)$  polinomra.

## Ismert korlátok

$$d_p(n) = \Omega(\sqrt[3]{3}^n) \text{ és } d_p(n) = O(n^2 \cdot \sqrt[3]{4}^n).$$

## Szerintünk...

$$d_p(n) = \Theta(p(n) \cdot \sqrt[3]{3}^n)$$

valami  $p(n)$  polinomra.

Alsó korlát, ha  $A = \{a, b, c\}$

## Konstrukció

Legyen  $\pi$  a  $Q = \{1, \dots, n\}$  halmaz egy permutációja és  $C_1, \dots, C_k$  ennek osztályai. Minden  $1 \leq i \leq k$ -ra legyen  $p_i \in C_i$  egy reprezentáns.

Definiáljuk a következő  $M = (Q, \{a, b, c\}, \delta)$  parciális automatát:

- minden  $q \in Q$ -ra  $qa$  legyen a  $q$  osztályának a reprezentáns eleme;
- minden  $q \in Q$ -ra  $qb$  legyen  $\pi(q)$ ;
- minden  $q \in Q$ -ra  $qc$  pontosan akkor definiált, ha  $\pi(q) = p_i$  valamely  $1 \leq i \leq k$ -ra.

Akkor  $M$  irányítható, a legrövidebb irányító szavának hossza:  $o(\pi) + 1$ , ahol  $o(\pi)$  a  $\pi$  rendje, vagyis a legkisebb  $k \geq 1$ , amire  $\pi^k = \text{id}_Q$ .

## Alsó korlát, ha $A = \{a, b, c\}$

### Konstrukció

Legyen  $\pi$  a  $Q = \{1, \dots, n\}$  halmaz egy permutációja és  $C_1, \dots, C_k$  ennek osztályai. Minden  $1 \leq i \leq k$ -ra legyen  $p_i \in C_i$  egy reprezentáns.

Definiáljuk a következő  $M = (Q, \{a, b, c\}, \delta)$  parciális automatát:

- minden  $q \in Q$ -ra  $qa$  legyen a  $q$  osztályának a reprezentáns eleme;
- minden  $q \in Q$ -ra  $qb$  legyen  $\pi(q)$ ;
- minden  $q \in Q$ -ra  $qc$  pontosan akkor definiált, ha  $\pi(q) = p_i$  valamely  $1 \leq i \leq k$ -ra.

Akkor  $M$  irányítható, a legrövidebb irányító szavának hossza:  $o(\pi) + 1$ , ahol  $o(\pi)$  a  $\pi$  **rendje**, vagyis a legkisebb  $k \geq 1$ , amire  $\pi^k = \text{id}_Q$ .



## Alsó korlát, ha $A = \{a, b, c\}$

### Konstrukció

Legyen  $\pi$  a  $Q = \{1, \dots, n\}$  halmaz egy permutációja és  $C_1, \dots, C_k$  ennek osztályai. Minden  $1 \leq i \leq k$ -ra legyen  $p_i \in C_i$  egy reprezentáns.

Definiáljuk a következő  $M = (Q, \{a, b, c\}, \delta)$  parciális automatát:

- minden  $q \in Q$ -ra  $qa$  legyen a  $q$  osztályának a reprezentáns eleme;
- minden  $q \in Q$ -ra  $qb$  legyen  $\pi(q)$ ;
- minden  $q \in Q$ -ra  $qc$  pontosan akkor definiált, ha  $\pi(q) = p_i$  valamely  $1 \leq i \leq k$ -ra.

Akkor  $M$  irányítható, a legrövidebb irányító szavának hossza:  $o(\pi) + 1$ , ahol  $o(\pi)$  a  $\pi$  **rendje**, vagyis a legkisebb  $k \geq 1$ , amire  $\pi^k = \text{id}_Q$ .

Alsó korlát, ha  $A = \{a, b, c\}$

## Konstrukció

Legyen  $\pi$  a  $Q = \{1, \dots, n\}$  halmaz egy permutációja és  $C_1, \dots, C_k$  ennek osztályai. Minden  $1 \leq i \leq k$ -ra legyen  $p_i \in C_i$  egy reprezentáns.

Definiáljuk a következő  $M = (Q, \{a, b, c\}, \delta)$  parciális automatát:

- minden  $q \in Q$ -ra  $qa$  legyen a  $q$  osztályának a reprezentáns eleme;
- minden  $q \in Q$ -ra  $qb$  legyen  $\pi(q)$ ;
- minden  $q \in Q$ -ra  $qc$  pontosan akkor definiált, ha  $\pi(q) = p_i$  valamely  $1 \leq i \leq k$ -ra.

Akkor  $M$  irányítható, a legrövidebb irányító szavának hossza:  $o(\pi) + 1$ , ahol  $o(\pi)$  a  $\pi$  rendje, vagyis a legkisebb  $k \geq 1$ , amire  $\pi^k = \text{id}_Q$ .

## Alsó korlát, ha $A = \{a, b, c\}$

### Konstrukció

Legyen  $\pi$  a  $Q = \{1, \dots, n\}$  halmaz egy permutációja és  $C_1, \dots, C_k$  ennek osztályai. Minden  $1 \leq i \leq k$ -ra legyen  $p_i \in C_i$  egy reprezentáns.

Definiáljuk a következő  $M = (Q, \{a, b, c\}, \delta)$  parciális automatát:

- minden  $q \in Q$ -ra  $qa$  legyen a  $q$  osztályának a reprezentáns eleme;
- minden  $q \in Q$ -ra  $qb$  legyen  $\pi(q)$ ;
- minden  $q \in Q$ -ra  $qc$  pontosan akkor definiált, ha  $\pi(q) = p_i$  valamely  $1 \leq i \leq k$ -ra.

Akkor  $M$  irányítható, a legrövidebb irányító szavának hossza:  $o(\pi) + 1$ , ahol  $o(\pi)$  a  $\pi$  **rendje**, vagyis a legkisebb  $k \geq 1$ , amire  $\pi^k = \text{id}_Q$ .

Alsó korlát, ha  $A = \{a, b, c\}$

## Konstrukció

Legyen  $\pi$  a  $Q = \{1, \dots, n\}$  halmaz egy permutációja és  $C_1, \dots, C_k$  ennek osztályai. Minden  $1 \leq i \leq k$ -ra legyen  $p_i \in C_i$  egy reprezentáns.

Definiáljuk a következő  $M = (Q, \{a, b, c\}, \delta)$  parciális automatát:

- minden  $q \in Q$ -ra  $qa$  legyen a  $q$  osztályának a reprezentáns eleme;
- minden  $q \in Q$ -ra  $qb$  legyen  $\pi(q)$ ;
- minden  $q \in Q$ -ra  $qc$  pontosan akkor definiált, ha  $\pi(q) = p_i$  valamely  $1 \leq i \leq k$ -ra.

Akkor  $M$  irányítható, a legrövidebb irányító szavának hossza:  $o(\pi) + 1$ , ahol  $o(\pi)$  a  $\pi$  **rendje**, vagyis a legkisebb  $k \geq 1$ , amire  $\pi^k = \text{id}_Q$ .

Alsó korlát, ha  $A = \{a, b, c\}$

## Konstrukció

Legyen  $\pi$  a  $Q = \{1, \dots, n\}$  halmaz egy permutációja és  $C_1, \dots, C_k$  ennek osztályai. Minden  $1 \leq i \leq k$ -ra legyen  $p_i \in C_i$  egy reprezentáns.

Definiáljuk a következő  $M = (Q, \{a, b, c\}, \delta)$  parciális automatát:

- minden  $q \in Q$ -ra  $qa$  legyen a  $q$  osztályának a reprezentáns eleme;
- minden  $q \in Q$ -ra  $qb$  legyen  $\pi(q)$ ;
- minden  $q \in Q$ -ra  $qc$  pontosan akkor definiált, ha  $\pi(q) = p_i$  valamely  $1 \leq i \leq k$ -ra.

Akkor  $M$  irányítható, a legrövidebb irányító szavának hossza:  $o(\pi) + 1$ , ahol  $o(\pi)$  a  $\pi$  **rendje**, vagyis a legkisebb  $k \geq 1$ , amire  $\pi^k = \text{id}_Q$ .

# $S_n$ rendje szuperpolinom

## Tétel (Landau, 1903)

Egy  $n$ -elemű halmazon egy maximális rendű permutáció rendje

$$e^{\Theta(\sqrt{n \cdot \ln n})}.$$

## Következmény

Hárombetűs ábécére megszorítva is,

$$d_p(n) = \Omega(c^{\sqrt{n \cdot \ln n}})$$

alkalmas  $c > 1$  konstansra.

## Nyitott kérdés

Igaz-e, hogy  $d_p(n) = \Omega(c^n)$  valamilyen  $c > 1$ -re ebben az esetben is?

# $S_n$ rendje szuperpolinom

## Tétel (Landau, 1903)

Egy  $n$ -elemű halmazon egy maximális rendű permutáció rendje

$$e^{\Theta(\sqrt{n \cdot \ln n})}.$$

## Következmény

Hárombetűs ábécére megszorítva is,

$$d_p(n) = \Omega(c^{\sqrt{n \cdot \ln n}})$$

alkalmas  $c > 1$  konstansra.

## Nyitott kérdés

Igaz-e, hogy  $d_p(n) = \Omega(c^n)$  valamilyen  $c > 1$ -re ebben az esetben is?

# $S_n$ rendje szuperpolinom

## Tétel (Landau, 1903)

Egy  $n$ -elemű halmazon egy maximális rendű permutáció rendje

$$e^{\Theta(\sqrt{n \cdot \ln n})}.$$

## Következmény

Hárombetűs ábécére megszorítva is,

$$d_p(n) = \Omega(c^{\sqrt{n \cdot \ln n}})$$

alkalmas  $c > 1$  konstansra.

## Nyitott kérdés

Igaz-e, hogy  $d_p(n) = \Omega(c^n)$  valamilyen  $c > 1$ -re ebben az esetben is?



# Házi feladat

Javítsunk meg a következő korlátok közül legalább hármat!

	$\Omega$	$O$
$d(n)$	$(n-1)^2$	$\frac{n^3-n}{6}$
$d_p(n)$	$\sqrt[3]{3}^n$	$n^2 \cdot \sqrt[3]{4}^n$
$d_{p,3}(n)$	$c^{\sqrt{n \cdot \ln n}}$	$n^2 \cdot \sqrt[3]{4}^n$

Köszönöm a figyelmet.