10. gyakorlat – Mintaillesztés és moduláris hatványozás

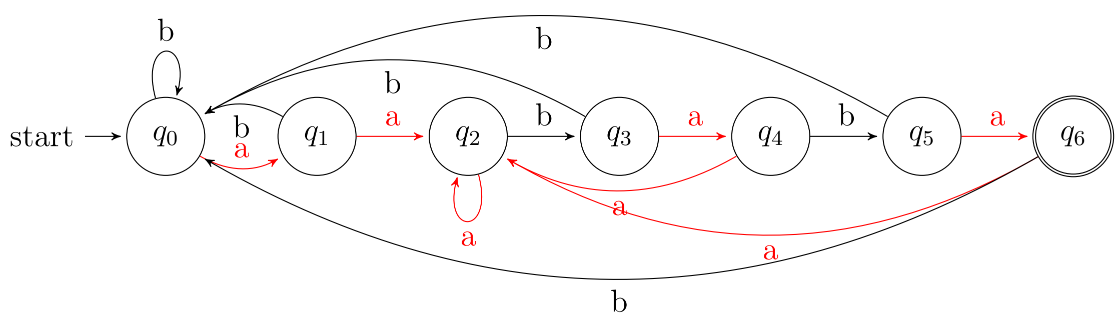
1. Adjunk meg egy véges állapotú determinisztikus automatát, ami a `P='aababa'` minta illesztését hajtja végre!

$$\begin{array}{ll}
\delta(q_0,a)=q_1 & \delta(q_0,b)=q_0\\
\delta(q_1,a)=q_2 & \delta(q_1,b)=q_0\\
\delta(q_2,a)=q_2 & \delta(q_2,b)=q_3\\
\delta(q_3,a)=q_4 & \delta(q_3,b)=q_0\\
\delta(q_4,a)=q_2 & \delta(q_4,b)=q_5\\
\delta(q_5,a)=q_6 & \delta(q_5,b)=q_0\\
\delta(q_6,a)=q_2 & \delta(q_6,b)=q_0
\end{array}$$

vagy kicsit olvashatóbban

$Q \backslash \Sigma$	a	b
q_0	q_1	q_0
q_1	q_2	q_0
q_2	q_2	q_3
q_3	q_4	q_0
q_4	q_2	q_5
q_5	q_6	q_0
q_6	q_2	q_0

1. táblázat. `P` minta illesztését vizsgáló automata δ állapotátmenet-függvénye.



Milyen állapotokat érint az automata a `T='aaabaababa'` input feldolgozása során?

i	0	1	2	3	4	5	6	7	8	9	10
T[i]	–	a	a	a	b	a	a	b	a	b	a
q_i	q_0	q_1	q_2	q_2	q_3	q_4	q_2	q_3	q_4	q_5	$\boxed{q_6}$

2. Adjuk meg a Knuth-Morris-Pratt algoritmus által a `P` mintához meghatározott $\pi : \{1,2,\ldots,m\} \to \{0,1,\ldots,m-1\}$ prefixfüggvényt!

Előtte egy kis emlékeztető.

$\mathtt{P}_i$ jelölje `P`-nek az i hosszúságú prefixét (kezdőszeletét), azaz pl. $\mathtt{P}_3 = aab$, $\mathtt{P}_2 = aa$, $\mathtt{P}_1 = a$, illetve $\mathtt{P}_0 = \epsilon$, ahol ϵ az üres szót jelöli.

$\texttt{X} \sqsupset \texttt{Y}$ jelölje azt, ha $\texttt{X}$ sztring szuffixe $\texttt{Y}$-nak (azaz teljesül, hogy $\texttt{Y}$ végződése megegyezik magával $\texttt{X}$-szel). (Pl. $\underline{\texttt{aaba}} \sqsupset \texttt{cac}\underline{\texttt{aaba}}$, ugyanakkor $\underline{\texttt{aaba}} \not\sqsupset \texttt{cac}\underline{\texttt{aabb}}$.)

Megjegyzés: Az $\texttt{Y} \sqsupset \texttt{Y}$, valamint az $\epsilon \sqsupset \texttt{Y}$ relációk triviálisan teljesülnek minden $\texttt{Y}$-ra.

Ezek után legyen $\pi[q] = \max\{k : k < q \wedge \texttt{P}_k \sqsupset \texttt{P}_q\}$, azaz a q-hoz rendelt prefixfüggvény értéke legyen $\texttt{P}$ azon leghosszabb (q-nál rövidebb) prefixének hosszával egyenlő, ami valódi (vele nem megegyező) szuffixe $\texttt{P}_q$-nak.

Pl. $\pi[4] = 1$, mivel

- $\underline{aab} = \texttt{P}_3 \not\sqsupset \texttt{P}_4 = a\underline{aba}$
- $\underline{aa} = \texttt{P}_2 \not\sqsupset \texttt{P}_4 = aa\underline{ba}$
- $\underline{a} = \texttt{P}_1 \sqsupset \texttt{P}_4 = aab\underline{a}$.

i	0	1	2	3	4	5	6
P[i]	–	a	a	b	a	b	a
$\pi[i]$		0	1	0	1	0	1

3. Rabin-Karp algoritmussal döntsük el, hogy a `T=3613203214` input kapcsán mely indexeiről kezdődhet a `P=321` mintára való illeszkedés a $h(x) = x \mod 11$ hasítófüggvény használata mellett?

0. index: $361 \mod 11 = 9$
1. index: $613 \mod 11 = 10 * (9 - 1 * 3) + 3 \mod 11 = 8$
2. index: $132 \mod 11 = 10 * (8 - 1 * 6) + 2 \mod 11 = 0$
3. index: $320 \mod 11 = 10 * (0 - 1 * 1) + 0 \mod 11 = 1$
4. index: $203 \mod 11 = 10 * (1 - 1 * 3) + 3 \mod 11 = 5$
5. index: $032 \mod 11 = 10 * (5 - 1 * 2) + 2 \mod 11 = 10$
6. index: $321 \mod 11 = 10 * (10 - 1 * 0) + 1 \mod 11 = 2$
7. index: $214 \mod 11 = 10 * (2 - 1 * 3) + 4 \mod 11 = 5$

Milyen karakternek kéne a `T` minta következő pozícióján álljon, hogy a Rabin-Karp algoritmus tévesen megvizsgálja az illeszkedést?

$14y \mod 11 = 10 * (5 - 1 * 2) + y \mod 11 = 2$

4. Moduláris hatványozás segítségével határozzuk meg a $d = 7^{13} \mod 17$ kifejezés értékét?

$13 = 1101b$

$d = 1 \xrightarrow{1/a} d = (1 * 1) \mod 17 = 1 \xrightarrow{1/b} d = (1 * 7) \mod 17 = 7 \xrightarrow{2/a} d = (7 * 7) \mod 17 = 15 \xrightarrow{2/b} d = (15 * 7) \mod 17 = 3 \xrightarrow{3/a} d = (3 * 3) \mod 17 = 9 \xrightarrow{4/a} d = (9 * 9) \mod 17 = 13 \xrightarrow{4/b} d = (13 * 7) \mod 17 = 91 \mod 17 = \boxed{6}$