1 Berlekampov-Masseyov algoritmus

Definícia 1. Nech je $\{s_i\}_{i\geq 0}$ binárna postupnosť. Symbolom $L_k(\{s_i\}_{i\geq 0})$ označíme dĺžku najkratšieho registra s lineárnou spätnou väzbou, ktorý generuje $s_0, s_1, \ldots, s_{k-1}$. Charakteristický polynóm zodpovedajúci tomuto registru označíme $c^{(k)}(x)$.

Hodnotu $L_k(\{s_i\}_{i\geq 0})$ nazývame lineárna zložitosť postupnosti $s_0, \ldots, s_{k-1}$. V ďalšom budeme pojem „posuvný register s lineárnou spätnou väzbou“ nahradzovať pojmom „register“, prípadne LFSR. Lineárna zložitosť má nasledujúce vlastnosti.

Lema 1. *Nech $\{s_i\}_{i\geq 0}$ a $\{t_i\}_{i\geq 0}$ sú ľubovoľné binárne postupnosti. Nech $k \geq 1$. Potom*

1. $L_k(\{s_i\}_{i\geq 0}) \leq k$.
2. *Ak $s_0 = s_1 = \cdots = s_{k-2} = 0$ a $s_{k-1} = 1$, tak* $L_k(\{s_i\}_{i\geq 0}) = k$.
3. $L_k(\{s_i + t_i\}_{i\geq 0}) \leq L_k(\{s_i\}_{i\geq 0}) + L_k(\{t_i\}_{i\geq 0})$.
4. $L_k(\{s_i\}_{i\geq 0}) \leq L_{k+1}(\{s_i\}_{i\geq 0})$.

Dôkaz. Prvá vlastnosť vyplýva z toho, že stačí zobrať ľubovoľný register dĺžky k a naplniť ho prvými k bitmi. Potom už nezáleží na spätnej väzbe, výstupom registra sú „správne“ bity.

Druhá vlastnosť je dôsledkom faktu, že register sa „cyklí“ v nulovom stave. Preto musí byť dĺžka registra aspoň k (a zároveň k stačí, podľa prvej vlastnosti).

Tretia vlastnosť vyplýva z vety o sčítavaní výstupov dvoch LFSR.

Platnosť štvrtého tvrdenia je triviálna. □

V situáciach, keď bude z kontextu zrejmé, ktorú postupnosť myslíme, budeme $L_k(\{s_i\}_{i\geq 0})$ skracovať na L_k.

Lema 2. *Ak $c^{(k+1)}(x) \neq c^{(k)}(x)$, tak*

$$L_{k+1} \geq \max\{L_k, k+1-L_k\}.$$

Dôkaz. Ľahko vidieť, že $L_{k+1} \geq L_k$. Ostáva ukázať, že $L_{k+1} \geq k+1-L_k$. Nech $\{t_i\}_{i\geq 0}$ je postupnosť, kde $t_0 = \cdots = t_{k-1} = 0$ a $t_k = 1$. Potom

$$L_{k+1}(\{s_i + t_i\}_{i\geq 0}) = L_k(\{s_i\}_{i\geq 0}) = L_k,$$

lebo $c^{(k+1)}(x) \neq c^{(k)}(x)$ a teda (ľubovoľný) register pre L_k generoval namiesto s_k hodnotu $1 + s_k$. Využitím vlastností z lemy 1 dostaneme:

$$\underbrace{L_{k+1}(\{t_i\}_{i\geq 0})}_{k+1} \leq \underbrace{L_{k+1}(\{s_i\}_{i\geq 0})}_{L_{k+1}} + \underbrace{L_{k+1}(\{s_i + t_i\}_{i\geq 0})}_{L_k},$$

odkiaľ bezprostredne vyplýva $L_{k+1} \geq k+1-L_k$. □

Lema 2 poskytuje dolný odhad pre lineárnu zložitosť, ak už doposiaľ vytvorený najkratší register nedokáže vygenerovať správne nasledujúci bit. Dá sa ukázať, že vo vzťahu v leme 2 platí rovnosť. Dôkaz tohto tvrdenia bude konštruktívny – je to Berlekampov-Masseyov algoritmus.

Veta 1. *Ak $c^{(k+1)}(x) \neq c^{(k)}(x)$, tak*

$$L_{k+1} \geq \max\{L_k, k+1-L_k\}.$$

Dôkaz. Dôkaz matematickou indukciou. Definujme $L_0 = 0$ a $c^{(0)}(x) = 1$.

Postupnosť $0, \ldots, 0$ (dĺžky k) vieme generovať registrom dĺžky $L_k = 0$ a $c^{(k)}(x) = 1$. Postupnosť $0, \ldots, 0, 1$ (dĺžky $k+1$) vieme generovať registrom dĺžky $L_{k+1} = k+1$ a $c^{(k+1)} = x^{k+1} + 1$ (a kratším registrom sa to nedá). Teda $L_{k+1} = k+1-L_k$.

Predpokladajme, že pre všetky j ($L_k \leq j \leq k-1$) platí

$$\begin{aligned} s_j &= \sum_{i=0}^{L_k-1} c_i^{(k)} s_{j-L_k+i} \\ &= c_0^{(k)} s_{j-L_k} + c_1^{(k)} s_{j-L_k+1} + \cdots + c_{L_k-1}^{(k)} s_{j-1}, \end{aligned}$$

teda register s charakteristickým polynómom generuje prvých k bitov postupnosti. Keďže $c^{(k+1)}(x) \neq c^{(k)}(x)$, podľa lemy 2 je $L_{k+1} \geq \max\{L_k, k+1-L_k\}$. Nech m je také číslo, že

1. $1 \leq m < k$,
2. $L_m < L_k$,
3. $L_{m+1} = L_k$.

Hodnota m je jednoznačne definovaná, je to posledná dĺžka postupnosti, pre ktorú bola dĺžka najkratšieho LFSR kratšia ako je teraz. Podľa indukčného predpokladu

$$\sum_{i=0}^{L_m-1} c_i^{(m)} s_{j-L_m+i} = \begin{cases} s_j, & \text{pre } L_m \leq j < m, \\ s_m + 1, & \text{pre } j = m. \end{cases}$$

Vieme, že $L_k = L_m = \max\{L_m, m+1-L_m\} = m+1-L_m$. Definujme $L = \max\{L_k, k+1-L_k\}$. Ukážeme, že

$$c(x) = x^{L-L_k} c^{(k)}(x) + x^{L-(k+1-L_k)} c^{(m)}(x)$$

je dobrá voľba pre $c^{(k+1)}(x)$.

Stupeň $c^{(k)}(x)$ je L_k, preto je stupeň prvého sčítanca L. Stupeň druhého sčítanca je $L-k+m < L$. Teda $\deg(c(x)) = L$. Overme, že register s $c(x)$ naozaj generuje prvých $k+1$ členov postupnosti

$\{s_i\}_{i\geq 0}$. Počítajme pre j ($L \leq j < k$):

$$\sum_{i=0}^{L-1} c_i s_{j-L+i} = \underbrace{\sum_{i=L-L_k}^{L-1} c^{(k)}_{i-(L-L_k)} s_{j-L+i}}_{A} + \underbrace{\sum_{L-k+m-L_m}^{L-k+m} c^{(m)}_{i-(L-k+m-L_m)} s_{j-L+i}}_{B}$$

$$A = \sum_{i=0}^{L_k-1} c^{(k)}_i s_{j-L_k+i}$$

$$B = \sum_{i=0}^{L_m-1} c^{(m)}_i s_{j-L_m-k+m+i} + s_{j-k+m}$$

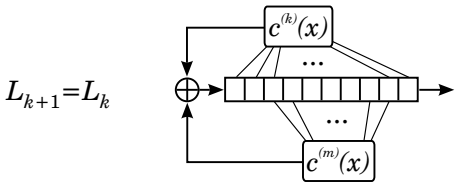
Teda

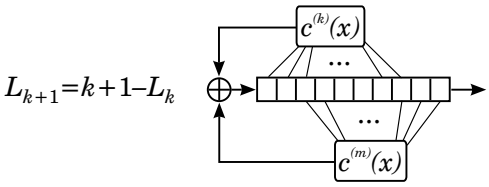
$$A + B = \begin{cases} s_j + 0 = s_j, & \text{pre } L \leq j < k, \\ (s_k + 1) + 1 = s_k, & \text{pre } j = k. \end{cases}$$

□

Veta 1 hovorí o jednoznačnosti stupňa polynómu $c^{(k)}(x)$. Samotný polynóm nemusí byť jednoznačný (môže ich existovať niekoľko).

Nasledujúce obrázky zobrazujú obe situácie, ktoré môžu pri konštrukcii nového charakteristického polynómu vo vete 1 nastať.





Príklad. Máme vstupnú postupnosť 001011011.

k	s_k	L_k	$c^{(k)}(x)$	m
0	–	0	1	–
1	0	0	1	–
2	0	0	1	–
3	1	3	x^3+1	2
4	0	3	x^3+1	2
5	1	3	x^3+x+1	2
6	1	3	x^3+x+1	2
7	0	4	x^4+x^2+x+1	6
8	1	4	$x^4+x^3+x^2$	6
9	1	4	$x^4+x^3+x^2$	6

Príklad. Máme vstupnú postupnosť 1101000

k	s_k	L_k	$c^{(k)}(x)$	m
0	–	0	1	–
1	1	1	$x+1$	0
2	1	1	$x+1$	0
3	0	2	x^2+x+1	2
4	1	2	x^2+x+1	2
5	0	3	x^3+x^2+1	4
6	0	3	x^3+x^2+1	4
7	0	4	$x^4+x^3+x^2+1$	6

Časová zložitosť Berlekampovho-Masseyovho algoritmu je $O(k \cdot L_k)$, kde k je dĺžka spracovanej postupnosti.