7. Lineární rekurentní posloupnosti

Nekonečnou posloupnost $\{s_i\}_{i\geq 0}\in\mathbb{F}_q^\omega$ nazveme *lineární rekurentní posloupností řádu k*, jestliže existují prvky $a_o,\dots,a_k,a\in\mathbb{F}_q$ splňující pro každé $n\geq 0$ *rekurentní vztah*

$$(*)\qquad s_{n+k}=a+\sum_{i=0}^{k-1}a_i s_{n+i}$$

Jestliže je $a=0$ mluvíme o *homogenní lineární rekurentní posloupnosti.*

Příklad 7.1. (1) Konstantní posloupnost je homogenní lineární rekurentní posloupností řádu 1 s rekurentním vztahem $s_{n+1}=s_n$.

(2) Posloupnost $\{1,1,0,1,1,0,\dots\}$ nad tělesem $\mathbb{F}_2$ je homogenní lineární rekurentní posloupností s rekurentním vztahem $s_{n+2}=s_n+s_{n+1}$.

Všimněme si, že u řádu lineární rekurentní posloupnosti nevyžadujeme žádnou podmínku minimality, konstantní posloupnost tak můžeme samozřejmě považovat za lineární rekurentní posloupností s rekurentním vztahem $s_{n+k}=s_n$ pro libovolné k.

Posloupnost $\{s_i\}_{i\geq 0}\in\mathbb{F}_q^\omega$ se nazývá *skoro periodická s periodou r*, jestliže existuje takové n_0, že $s_{n+r}=s_n$ pro každé $n\geq n_0$. Nejmenšímu takovému r budeme říkat nejmenší perioda. Posloupnost $\{s_i\}_{i\geq 0}\in\mathbb{F}_q^\omega$ je *periodická*, existuje-li perioda r tak, že $s_{n+r}=s_n$ pro každé $n\geq 0$.

Pozorování. Nechť $\{s_i\}_{i\geq 0}\in\mathbb{F}_q^\omega$ je skoro periodická posloupnost s nejmenší periodou r_1. Pak

(1) r_1 dělí každou periodu $\{s_i\}$,
(2) $\{s_i\}$ je periodická, právě když $s_{n+r_1}=s_n$ pro každé $n\geq 0$.

Důkaz. (1) Pro periodu r vydělíme se zbytkem polynomy $r=qr_1+t$, kde $t<r_1$. Pak existuje takové n_0, že pro každé $n\geq n_0$

$$s_n=s_{n+r}=s_{n+qr_1+t}=s_{n+(q-1)r_1+t}=\cdots=s_{n+t}.$$

Z minimality r_1 plyne, že $t=0$, tedy r_1 dělí r.

(2) Stačí dokázat přímou implikaci.

Ukážeme, že $s_n=s_{n+r_1}$ pro každé $n\geq 0$. Je-li r perioda $\{s_i\}$ jako periodické posloupnosti, existuje n_0, že $s_n=s_{n+r_1}$ pro každé $n\geq n_0$. Zvolíme-li libovolné $n\geq 0$, pak existuje $m\geq n_0$, pro které $n\equiv m(mod\, r)$. Proto $n+r_1\equiv m+r_1(mod\, r)$ a tudíž

$$s_{n+r_1}=s_{m+r_1}=s_m=s_n.$$

pro každé $n\geq 0$. □

Poznámka 7.2. *Je-li $\{s_i\}_{i\geq 0}\in\mathbb{F}_q^\omega$ lineární rekurentní posloupností řádu k s rekurentním vztahem $s_{n+k}=a+\sum_{i=0}^{k-1}a_i s_{n+i}$, pak*

(1) *$\{s_i\}$ je skoro periodická posloupnost s nejmenší periodou $\leq q^k$,*
(2) *je-li $\{s_i\}$ homogenní má nejmenší periodu $\leq q^k-1$,*
(3) *jestliže $a_0\neq 0$, je $\{s_i\}$ periodická.*

Důkaz. (1) Označme $\mathbf{s}_n:=(s_n,\dots,s_{n+k-1})\in\mathbb{F}_q^n$ n-tý *stavový vektor* lineární rekurentní posloupností. Pak $|\{\mathbf{s}_n|n\geq 0\}|\leq|\mathbb{F}_q^n|=q^n$, proto existuje $u<v$, pro něž

$v - u \leq q^n$ a $\mathbf{s}_u = \mathbf{s}_v$. Proto

$$s_{u+k} = a + \sum_{i=0}^{k-1} a_i s_{u+i} = a + \sum_{i=0}^{k-1} a_i s_{v+i} = s_{v+k}.$$

Protože $s_{u+k} = s_{v+k}$, máme $\mathbf{s}_{u+1} = \mathbf{s}_{v+1}$. Indukčním argumentem dostáváme, že $s_{u+l} = s_{v+l}$ pro každé $l \geq 0$. Položíme-li nyní $r := v - u$, vidíme, že $s_n = s_{n+r}$ pro každé $n \geq u$.

(2) Existuje-li stavový vektor $\mathbf{s}_n := (0, \dots, 0)$, pak je posloupnost skoro konstantní, tedy má periodu 1. V opačném případě zopakujeme důkaz (1) pro $u < v$, pro které $v - u \leq |\{\mathbf{s}_n\}| \leq |\mathbb{F}_q^n \setminus \{0\}| = q^n - 1$ a $\mathbf{s}_u = \mathbf{s}_v$.

(3) Buď r_1 nejmenší perioda a n_0 nejmenší takové, že $s_n = s_{n+r_1}$ pro každé $n \geq n_0$. Kdyby $n_0 > 0$, pak by $s_{n_0+k-1} = a + \sum_{i=0}^{k-1} a_i s_{n_0+i-1}$, a proto by $s_{n_0-1} =$

$$= a_0^{-1}(s_{n_0+k-1} - a - \sum_{i=1}^{k-1} a_i s_{n_0+i-1}) = a_0^{-1}(s_{n_0+r_1+k-1} - a - \sum_{i=1}^{k-1} a_i s_{n_0+r_1+i-1}) =$$

$= s_{n_0-1+r_1}$, což by bylo ve sporu s minimalitou n_0 □

Pozorování. Uvažujme posloupnost $\{s_i\}_{i \geq 0} \in \mathbb{F}_q^\omega$

1. (1) Jestliže $s_0 \neq 0$ a $s_i = 0$ pro $i > 0$, je $\{s_i\}$ homogenní skoro periodická posloupnost lineární rekurentní posloupnost řádu 2 s rekurentním vztahem $s_{n+2} = s_{n+1}$, která není periodická.
2. (2) Je-li $\{s_i\}$ skoro periodická posloupnost splňující $s_n = s_{n+r}$ pro všechna $n \geq n_0$ je lineární rekurentní posloupností s rekurentním vztahem $s_{n+n_0} = s_{n+n_0+r}$.
3. (3) $\{s_i\}$ je lineární rekurentní posloupnost, právě když je skoro periodická.

Je-li $\{s_i\}_{i \geq 0} \in \mathbb{F}_q^\omega$ homogenní lineární rekurentní posloupností s rekurentním vztahem $s_{n+k} = \sum_{i=0}^{k-1} a_i s_{n+i}$, pak $c = x^k - \sum_{i=0}^{k-1} a_i x^i \in \mathbb{F}_q[x]$ se nazývá *charakteristický polynom* $\{s_i\}$.

Věta 7.3. *Jestliže charakteristický polynom c homogenní lineární rekurentní posloupností $\{s_n\}$ s rekurentním vztahem $s_{n+k} = \sum_{i=0}^{k-1} a_i s_{n+i}$ nemá v rozkladovém nadtělese $\mathbb{K}$ vícenásobné kořeny a $\alpha_1, \dots \alpha_k \in \mathbb{K}$ jsou všechny kořeny c, pak existují taková $\beta_1 \dots, \beta_k \in \mathbb{K}$, že $s_n = \sum_{j=1}^{k} \beta_j \alpha_j^n$ pro všechna $n \geq 0$.*

Důkaz. Položme $\mathbf{s}_0 := (s_0, \dots, s_{k-1}) \in \mathbb{F}_q^n$ a $\mathbf{A} := \begin{pmatrix} \alpha_1^0 & \alpha_2^0 & \dots & \alpha_k^0 \\ \alpha_1^1 & \alpha_2^1 & \dots & \alpha_k^1 \\ . & . & \dots & . \\ . & . & \dots & . \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_k^{k-1} \end{pmatrix}$.

Protože je Vandermondova matice $\mathbf{A}$ regulární, existuje (jednoznačně určený) vektor $\beta = (\beta_1, \dots, \beta_k) \in \mathbb{K}^k$, pro který $\mathbf{A}\beta^T = \mathbf{s}_0^T$.

Vidíme, že $s_n = \sum_{j=1}^{k} \beta_j \alpha_j^n$ pro všechna $n < k$. Nyní využijeme indukci a za předpokladu, že tento vztah platí pro všechny hodnoty menší než $n + k$, dokážeme jeho platnost pro $n + k$:

$$\sum_{j=1}^{k} \beta_j \alpha_j^{n+k} - s_{n+k} = \sum_{j=1}^{k} \beta_j \alpha_j^{n+k} - \sum_{i=0}^{k-1} a_i s_{n+i} =$$

$$= \sum_{j=1}^{k} \beta_j \alpha_j^{n+k} - \sum_{i=0}^{k-1} a_i \sum_{j=1}^{k} \beta_j \alpha_j^{n+i} = \sum_{j=1}^{k} \beta_j \alpha_j^n c(\alpha_j) = 0.$$

□

Příklad 7.4. Uvažujme homogenní lineární rekurentní posloupností s rekurentním vztahem $s_{n+2} = s_{n+1} + s_n$ nad tělesem $\mathbb{F}_2$. Její charakteristický polynom je x^2+x+1 s rozkladovým nadtělesem $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ a kořeny α, $\alpha+1$. Nyní stejně jako v důkazu předchozí Věty vyřešíme soustavu

$$\begin{pmatrix} 1 & 1 \\ \alpha & \alpha+1 \end{pmatrix} \cdot \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

a dostaneme $\beta_1 = \alpha$ a $\beta_2 = \alpha + 1$. Proto $s_n = \alpha^{n+1} + (\alpha+1)^{n+1}$.

Věta 7.5. *Nechť $c = x^k - \sum_{i=0}^{k-1} a_i x^i \in \mathbb{F}_q[x]$ je charakteristický polynom nenulové homogenní lineární rekurentní posloupnosti $\{s_i\} \in \mathbb{F}_q^\omega$. Jestliže je c ireducibilní nad F_q a α jeho kořen v kořenovém nadtělese $\mathbb{K}$, který má v grupě $\mathbb{K}^*$ řád r, potom je $\{s_i\}$ periodická s nejmenší periodou rovnou r.*

Důkaz. Protože je posloupnost $\{s_i\}$ nenulová a c ireducibilní, 0 není kořenem c a podle 7.2(3) je posloupnost $\{s_i\}$ periodická. Z Poznámky 3.1 víme, že $c = m_{\alpha,\mathbb{F}_q} = \prod_{i=0}^{k-1}(x - \alpha^{q^i})$, proto $\mathbb{K} = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^k}$ je rozkladové nadtěleso polynomu c a všechny jeho kořeny mají stejný řád v grupě $\mathbb{K}^*$.

Protože ireducibilní polynomy nad konečným tělesem nemají žádné vícenásobné kořeny, můžeme pro $\alpha_i \alpha^{q^{i-1}}$, $i = 1, \dots, k$, použít Větu 7.3, která zaručuje existenci takových čísel $\beta_1 \dots, \beta_k \in \mathbb{K}$, že pro všechna $n \geq 0$ $s_n = \sum_{j=1}^{k} \beta_j \alpha_j^n$. Z předpokladu nenulovosti $\{s_i\}$ potom plyne, že alespoň jedno β_{i_0} je nenulové.

Všimněme si, že t je perioda, právě když pro každé $n \geq 0$ platí

$$0 = s_{n+t} - s_n = \sum_{j=1}^{k} \beta_j \alpha_j^{n+t} - \beta_j \alpha_j^n = \sum_{j=1}^{k} \beta_j \alpha_j^n (\alpha_j^t - 1).$$

Odtud okamžitě vidíme, že r je perioda, neboť $\alpha_j^r - 1 = 0$,

Naopak zapíšeme-li vztah $0 = s_{n+t} - s_n$ pro $n = 0, \dots, k-1$ pro libovolnou periodu maticově, dostaneme součin

$$\begin{pmatrix} \alpha_1^0 & \alpha_2^0 & \dots & \alpha_k^0 \\ \alpha_1^1 & \alpha_2^1 & \dots & \alpha_k^1 \\ . & . & \dots & . \\ . & . & \dots & . \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_k^{k-1} \end{pmatrix} \cdot \begin{pmatrix} \beta_1(\alpha_1^t - 1) \\ \beta_2(\alpha_2^t - 1) \\ . \\ . \\ \beta_k(\alpha_k^t - 1) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ . \\ . \\ 0 \end{pmatrix}$$

Součin můžeme interpretovat jako matici homogenní soustavy rovnic s regulární (Vandermondovou) maticí levých stran. Ta má pouze triviální řešení, proto pro všechna $i = 1, \dots, k$ dostáváme, že $\beta_i(\alpha_i^t - 1)$. Zbývá připomenout, že $\beta_{i_0} \neq 0$, a proto $\alpha_{i_0}^t = 1)$ a tudíž řád r dělí t. Tím jsme ověřili, že r je nejmenší perioda homogenní lineární rekurentní posloupnosti $\{s_i\}$ □

Důsledek 7.6. *Je-li α primitivní prvek tělesa $\mathbb{F}_{q^k}$ a $c = m_{\alpha,\mathbb{F}_q}$ minimální polynom α nad tělesem $\mathbb{F}_q$, pak je každá nenulové homogenní lineární rekurentní posloupnosti $\{s_i\} \in \mathbb{F}_q^\omega$ s charakteristickým polynomem c periodická s (maximální možnou) nejmenší periodou $q^k - 1$.*

Příklad 7.7. Nad tělesem $\mathbb{F}_2$ máme právě tři ireducibilní polynomy stupně 4: $c_1 = x^4 + x + 1$, $c_2 = x^4 + x^3 + 1$, $c_3 = x^4 + x^3 + x^2 + x + 1$ Spočítáme řády kořenů α jednotlivých polynomů v multiplikativní grupě rozkladového nadtělesa $\mathbb{F}_2(\alpha)^* = \mathbb{F}_{16}^*$: Podle Lagrangeovy věty stačí spočítat α^3 a α^5. Zřejmě přitom $\alpha^3 \neq 1$ pro žádný kořen α a $\alpha^5 = 1$ pro kořeny polynomu c_3 neboť

$$0 = \alpha(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = \alpha^5 + 1 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^5 + 1.$$

To znamená, že čtyři kořeny polynomu c_3 jsou právě všechny prvky řádu 5 v patnáctiprvkové cyklické grupě $\mathbb{F}_{16}^*$, tudíž osm kořenů polynomů c_1 a c_2 jsou právě řádu všechny generátory grupy $\mathbb{F}_{16}^*$. Tedy podle Důsledku 7.6. Je každá homogenní lineární rekurentní posloupnosti s nenulovými počátečními podmínkami a rekurentním vztahem $s_{n+4} = s_{n+1} + s_n$ nebo $s_{n+4} = s_{n+3} + s_n$, které odpovídají charakteristickým polynomům c_1 a c_2, periodická s periodou 15.

Označme $\mathbb{K}[[x]]$ okruh formálních mocninných řad nad tělesem $\mathbb{K}$ Okruh polynomů $\mathbb{K}[x]$ budeme chápejme v přirozeném smyslu jako podokruh okruhu $\mathbb{K}[[x]]$ (tj. polynomy jsou ty formální mocninné řady, které mají skoro všechny koeficienty nulové). Připomeňme dobře známý fakt z počítačové algebry:

Pozorování. Mocninná řada $\sum_{n\geq 0} a_n x^n \in \mathbb{K}[[x]]$ nad tělesem $\mathbb{K}$ je invertibilní, právě když $a_0 \neq 0$.

Připomeňme pro libovolný polynom $f = \sum_{n=0}^{d} f_n x^n$ stupně $d \geq 0$ značení $f^* = \sum_{n=0}^{d} f_{n-d} x^n$. Z předchozího pozorování plyne, že pro každý nenulový polynom $f \in \mathbb{K}[x]$ existuje inverzní formální mocninná řada $(f^*)^{-1} \in \mathbb{K}[[x]]$

Nechť $\{s_i\} \in \mathbb{F}_q^\omega$ je homogenní lineární rekurentní posloupnost. Potom mocninnou řadu $\sum_{n\geq 0} s_n x^n \in \mathbb{F}_q[[x]]$ nazveme *generující funkcí* lineární rekurentní posloupnosti.

Následující tvrzení nám umožňuje spočítat generující funkci pomocí invertování v oboru mocninných řad, tedy mimo jiné pomocí (mírně modifikovaného) algoritmu dělení se zbytkem.

Věta 7.8. *Nechť* $c = x^k - \sum_{i=0}^{k-1} a_i x^i \in \mathbb{F}_q[x] \setminus |\{0\}$ *a položme* $a_k = -1$.

(1) *Jestliže G je generující funkce homogenní lineární rekurentní posloupnosti $\{s_i\}_{i\geq 0}$ nad tělesem $\mathbb{F}_q$ s charakteristickým polynomem c a platí-li, že $g = -\sum_{j=0}^{k-1}(\sum_{i=0}^{j} a_{i+k-j} s_i) x^j$, pak $G = g \cdot (c^*)^{-1}$.*

(2) *Je-li $g \in \mathbb{F}_q[x]$ a $\deg g < k$, pak $G = g \cdot (c^*)^{-1}$ je generující funkce homogenní lineární rekurentní posloupnosti s charakteristickým polynomem c.*

Důkaz. (1) Vidíme, že $c^* = -\sum_{i=0}^{k} a_{k-i} x^i$. Stačí, abychom ověřili, že $G \cdot c^* = g$:

$$G \cdot c^* = -(\sum_{n\geq 0} s_n x^n) \cdot (\sum_{i=0}^{k} a_{k-i} x^i) = g - \sum_{j\geq k} (\sum_{i=j-k}^{j} a_{i+k-j} s_i) x^j = g,$$

neboť $\sum_{i=j-k}^{j} a_{i+k-j} s_i = s_j - \sum_{\nu=0}^{k-1} a_{k-\nu} s_{j-k+\nu} = 0$ pro každé $j \geq k$

(2) Definujeme-li pro $g = \sum_{i=0}^{k-1} g_i x^i$ induktivně $s_j := g_j + \sum_{i=0}^{j-1} a_{i+k-j} s_i$, pak z posledního výpočtu v (1) plyne, že $s_j = \sum_{\nu=0}^{k-1} a_{k-\nu} s_{j-k+\nu}$ pro každé $j \geq k$, tedy že je G generující funkce homogenní lineární rekurentní posloupnosti s charakteristickým polynomem c. $\square$