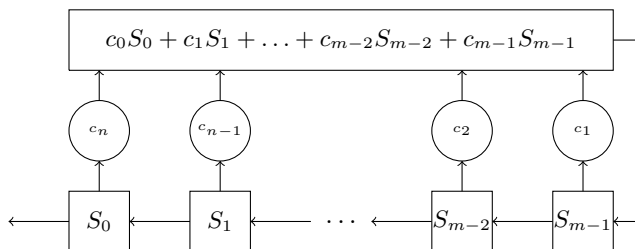


Лекция 4

Рекурентни редици и поточни шифри

В тази глава ще разгледаме линейни рекурентни редици. Те са важни за криптографията с това, че те са изключително лесни за генериране и анализ. Ще разглеждаме линейни рекурентни редици над $F = \text{GF}(q)$ за произволно q , аа на отделни места и за произволно поле F , макар за практиката от изключителен интерес да е случая $q = 2$.

Линейни рекурентни редици могат да се генерират от устройства, наречени *линейни регистри с обратна връзка* (linear feedback shift registers). Едно такова устройство, работещо над поле с q елемента е представено на фигурата по-долу. В случая то е с дължина n , т.е. състои се от n клетки, всяка от които пази стойност от полето F . Регистърът работи на дискретни тактове, при което на всеки такт съдържанието на клетките се измества вляво. Съдържанието на най-лявата клетка отива на изхода, а най-дясната клетка приема нова стойност, която е линейна комбинация на съдържанието на всички клетки.



Ако дискретните моменти означим с $t = 0, 1, 2, \dots$, а $S_i(t)$ означава съдържанието на i -тата клетка, то работата на регистъра се описва от равенствата

$$\begin{aligned} S_i(t+1) &= S_{i+1}(t), \quad i = 0, 1, \dots, n-2, \\ S_{n-1}(t+1) &= c_1 S_{n-1}(t) + c_2 S_{n-2}(t) + \dots + c_0 S_0(t) \end{aligned}$$

Ако в началния момент регистърът съдържа вектора $(a_0, a_1, \dots, a_{n-1})$, то той очевидно ще генерира редица (a_i) , удовлетворяваща уравнението

$$a_{n+t} = c_1 a_{n+t-1} + c_2 a_{n+t-2} + \dots + c_n a_t.$$

Ясно е, че редиците, генерирани от линейни регистри са точно линейните рекурентни редици и в тази глава ще изследваме техните свойства.

4.1 Основни резултати за линейни рекурентни редици

Ще започнем с изложението на някои резултати, които са в сила за линейни рекурентни редици над произволно поле.

Нека n е естествено число, а $c_0, c_1, \dots, c_{n-1}$ са елементи от произволно поле F . Една редица $\mathbf{a} = (a_k)_{k \geq 0}$, удовлетворяваща уравнение от вида

$$a_{k+n} = \sum_{i=0}^{n-1} c_i a_{k+i}, \quad k \geq 0, \quad (4.1)$$

наричаме *линейна рекурентна редица (от ред n) над F* . Самото уравнение (4.1) наричаме *линейно рекурентно уравнение от ред n* . Първите n члена на редицата $\mathbf{a}$ я определят еднозначно и се наричат нейни *начални стойности*.

Всяка линейна рекурентна редица $\mathbf{a}$ може да бъде породена с помощта на физическо устройство наречено *линеен регистър с обратна връзка* (linear feedback shift-register (LFSR)). Схематично един линеен регистър с обратна връзка е изобразен на Фигура ???. Той се състои от n клетки D_j , $j = 0, 1, \dots, n-1$, всяка от които съдържа елемент от $\mathbb{F}$, n мултипликатора, и $n-1$ суматора. Регистърът работи в дискретни моменти от време. За удобство ще считаме, че той започва работа в момента $t = 0$. В началото на работата всяка клетка D_j съдържа някакъв елемент a_j от $\mathbb{F}$. Ако съдържанието на D_j в момента t означим с $D_j(t)$, то след извършване на един такт, т.е. в момента $t+1$, съдържанието на клетките на регистъра се задава с равенствата:

$$\begin{aligned} D_j(t+1) &= D_{j+1}(t), \quad j = 0, 1, \dots, n-2; \\ D_{n-1}(t+1) &= \sum_{i=0}^{n-1} c_i D_i(t). \end{aligned}$$

[PICTURE: LFSR (L-N, vol.2, p.497)]

Ясно е, че след k такта съдържанието на D_j ще бъде a_{k+j} . Векторът $\mathbf{a}^{(k)} = (a_k, a_{k+1}, \dots, a_{k+n-1})$ наричаме *вектор на k -тото състояние на редицата $\mathbf{a}$ или вътрешно състояние на регистъра на k -тия такт*. Вектора $\mathbf{a}^{(0)}$ наричаме вектор на началното състояние.

С всяка линейна рекурентна редица $\mathbf{a}$ над $\mathbb{F}$, удовлетворяваща уравнението (4.1) асоциираме матрица $\mathbf{A}$ от ред n над F :

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 & c_0 \\ 1 & 0 & & & 0 & c_1 \\ 0 & 1 & \ddots & \ddots & 0 & c_2 \\ \vdots & \vdots & & & \vdots & \vdots \\ \vdots & \vdots & & & 0 & c_{n-2} \\ 0 & 0 & & & 1 & c_{n-1} \end{pmatrix}. \quad (4.2)$$

Лесно се проверява, че за всяко $t = 0, 1, \dots$ е изпълнено $\mathbf{a}^{(t+1)} = \mathbf{a}^{(t)} \mathbf{A}$, откъдето

$$\mathbf{a}^{(t)} = \mathbf{a}^{(0)} \mathbf{A}^t. \quad (4.3)$$

Нека $\mathbf{a}$ е линейна рекурентна редица, удовлетворяваща уравнението (4.1). Последното може да бъде записано във вида

$$a_{k+n} - c_{n-1}a_{k+n-1} - c_{n-2}a_{k+n-2} - \dots - c_0a_k = 0, \quad k \geq 0, \quad (4.4)$$

Полиномът

$$f(x) = x^n - c_{n-1}x^{n-1} - \dots - c_1x - c_0 \quad (4.5)$$

се нарича *характеристичен полином* за редицата $\mathbf{a}$. Той зависи единствено от рекурентното уравнение (4.1). Ако $\mathbf{A}$ е матрицата, определена в (4.4), то $f(x)$ съвпада с характеристичния полином на $\mathbf{A}$, т.е. $f(x) = \det(x\mathbf{I} - \mathbf{A})$. От друга страна $\mathbf{A}$ може да бъде разглеждана като съпровождаща матрица на нормирания полином $f(x)$. Нека $f^*(x) = x^{\deg f} f(\frac{1}{x})$ е реципрочния полином за $f(x)$. В случаите, когато $f(0) \neq 0$ степента на $f^*(x)$ съвпада със степента на $f(x)$. По-нататък ще разглеждаме редици с характеристични полиноми изпълняващи това условие.¹

Характеристичният полином f , реципрочния му f^* и асоциираната матрица $\mathbf{A}$ описват в еднаква степен линейната рекурентна редица (a_i) , зададена с уравнението (4.1). Тези обекти не зависят от началните условия. Така при зададен характеристичен полином съществува семейство от линейни рекурентни редици, които се получават при задаване на различни начални условия.

Сега ще преставим една важна характеристика на линейните рекурентни редици над поле $\mathbb{F}$. За тази цел с всяка редица $\mathbf{a} = (a_k)$ над полето $\mathbb{F}$, свързваме формален степенен ред:

$$a(x) = \sum_{i=0}^{\infty} a_i x^i \in \mathbb{F}[[x]].$$

В сила е следния фундаментален резултат, играещ централна роля в по-нататъшното изложение.

¹Това не е ограничение на общността, тъй като редица с характеристичен полином f , за който $f(0) = 0$ съвпада (от някое място нататък) с редица, имаща характеристичен полином f' от по-ниска степен, за който $f'(0) \neq 0$.

Теорема 4.1. Нека $\mathbf{a} = (a_k)$ е редица над полето $\mathbb{F}$ и нека $a(x) \in \mathbb{F}[[x]]$ е асоциираният с нея формален степенен ред. Редицата $\mathbf{a}$ е линейна рекурентна редица с характеристичен полином $f \in \mathbb{F}[x]$, $\deg f < n$, тогава и само тогава, когато съществува полином $g(x) \in \mathbb{F}[x]$ с $\deg g < \deg f$, за който

$$a(x) = \frac{g(x)}{f^*(x)}. \quad (4.6)$$

Съответствието между редиците $\mathbf{a}$ с характеристичен полином f и полиномите g е биективно.

Доказателство. Нека $f(x) = x^n - c_{n-1}x^{n-1} - \dots - c_1x - c_0$. Ще запишем $f(x)$ и $g(x)$ като елементи на $\mathbb{F}[[x]]$:

$$f^*(x) = -\sum_{k=0}^{\infty} c_k^* x^k, \quad g(x) = \sum_{k=0}^{\infty} b_k x^k.$$

Ясно е, че $c_0^* = -1$ и $c_k^* = 0$ за $k > n$. Уравнението

$$a(x)f^*(x) = g(x) \quad (4.7)$$

над $\mathbb{F}[[x]]$ определя еднозначно $g(x)$:

$$b_j = -\sum_{i=0}^j c_i^* a_{j-i} \quad j \geq 0. \quad (4.8)$$

Полагайки $j = l + n$ в (4.8), получаваме

$$b_{l+n} = -\sum_{i=0}^{l+n} c_i^* a_{l+n-i} = \sum_{i=0}^n c_{n-i} a_{l+n-i} = \sum_{i=0}^n c_i a_{l+i}. \quad (4.9)$$

Ако $\mathbf{a}$ удовлетворява линейно рекурентно уравнение с характеристичен полином f , то $b_k = 0$ за $k \geq n$. Следователно $\deg g < n$. Обратно, нека $\deg g < n$. Тогава $b_k = 0$ за всяко $k \geq n$. Редът $a(x)$ се определя чрез (4.7) или, еквивалентно, чрез (4.8). В матричен запис (4.8) сепредставено като

$$(b_0, \dots, b_{n-1}) = (a_0, \dots, a_{n-1}) \begin{pmatrix} 1 & -c_{n-1} & -c_{n-2} & \dots & -c_2 & -c_1 \\ 0 & 1 & -c_{n-1} & & -c_3 & -c_2 \\ 0 & 0 & 1 & \ddots & -c_4 & -c_3 \\ \vdots & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 1 & -c_{n-1} \\ 0 & 0 & 0 & \ddots & 0 & 1 \end{pmatrix}.$$

Това равенство определя еднозначно a_k , тъй като матрицата вдясно е неособена. При $k \geq n$ имаме $b_k = 0$ и условието (4.8) се свежда до рекурентната връзка (4.4). Получената редица е единствена, откъдето следва и еднозначността между редиците с характеристичен полином f и полиномите g от степен по-малка от $\deg f$. $\square$

Следствие 4.2. Нека $\mathbf{a} = (a_k)$ е редица над $\mathbb{F}$ и нека $a(x) \in \mathbb{F}[[x]]$ е асоциираният с $\mathbf{a}$ формален степенен ред. Редицата $\mathbf{a}$ е линейна рекурентна редица тогава и само тогава, когато $a(x)$ принадлежи на $\mathbb{F}(x)$ – полето от рационални функции над $\mathbb{F}$.

Доказателство. Необходимостта на условието следва от Теорема 4.1. Обратно, нека приемем, че $a(x) \in \mathbb{F}(x)$, т.е.

$$a(x) = \frac{g(x)}{f^*(x)},$$

за някакъв полином f , за който $\gcd(f^*, g) = 1$. Съществуват полиноми u и v , за които $uf^* + vg = 1$. Заместваме $g = af^*$ и получаваме $(u + va)f^* = 1$. Следователно f^* е обратим във $\mathbb{F}[[x]]$ и има свободен член $c_0^* \neq 0$. Без ограничение на общността $f^*(x) = -\sum_{k=0}^{\infty} c_k^* x^k$, където $c_0^* = -1$ и за почти всички k , $c_k^* = 0$. Да положим $n = \max(\deg f^*, 1 + \deg g)$. Прилагайки още веднъж Теорема 4.1, получаваме, че $a(x)$ е асоцииран с линейна рекурентна редица с характеристичен полином f . $\square$

Пример 4.3. Да вземем за пример редицата на ФИБОНАСИ. Тя се задава чрез рекурентното уравнение $a_k = a_{k-1} + a_{k-2}$ и началните условия $a_0 = a_1 = 1$. Характеристичният полином е $f(x) = x^2 - x - 1$ и степенният ред може да бъде записан като

$$a(x) = \frac{1}{1 - x - x^2}.$$

Развивайки този ред, получаваме очаквания резултат

$$1 + x + 2x^2 + 3x^3 + 5x^4 + 8x^5 + 13x^6 + 21x^7 + 34x^8 + 55x^9 + \dots$$

До момента не отбелязвахме очевидния факт, че линейна рекурентна редица може да удовлетворява повече от една рекурентна връзка. Като тривиален пример ще посочим нулевата редица, която може да бъде получена от произволна рекурентна връзка с начални стойности $(0, 0, \dots, 0)$. Друг пример е редицата на ФИБОНАСИ, която може да бъде получена от рекурентното уравнение $a_k = a_{k-1} + a_{k-3} + a_{k-4}$ при начално условие $(1, 1, 2, 3)$.

Теорема 4.4. Нека $\mathbf{a} = (a_k)$ е линейна рекурентна редица над полето $\mathbb{F}$ и нека $a(x) \in \mathbb{F}[[x]]$ е формалният степенен ред, асоцииран с $\mathbf{a}$. Съществува единствен полином f_0 със старши коефициент 1, за който е изпълнено условието: $\mathbf{a}$ удовлетворява линейно рекурентно уравнение с характеристичен полином f тогава и само тогава, когато f е кратен на f_0 .

Доказателство. Нека f е характеристичен полином за някакво рекурентно уравнение, удовлетворявано от $\mathbf{a}$. Съгласно Теорема 4.1 съществува полином g , за който е в сила $a(x) = g/f^*$. Да положим $d(x) = \gcd(f^*, g)$. Тогава $f^* = df_0^*$ и $g = dg_0$. Твърдим, че f_0 е търсеният полином.

Всеки полином hf_0 , кратен на f_0 , съответства на линейно рекурентно уравнение, което поражда $\mathbf{a}$. Наистина от Теорема 4.1 имаме

$$\frac{h^*g_0}{h^*f_0^*} = \frac{g_0}{f_0^*} = \frac{dg_0}{df_0^*} = \frac{g}{f^*} = a(x).$$

Обратно, нека f_1 е характеристичен полином за линейно рекурентно уравнение, пораждащо $\mathbf{a}$. Съществува полином g_1 , за който $a(x) = g_1/f_1^*$. Следователно, $g_1f_0^* = g_0f_1^*$, откъдето f_0 дели f_1 (f_0^* и g_0 са взаимно прости). $\square$

Следствие 4.5. Нека $\mathbf{a} = (a_k)$ е линейна рекурентна редица над полето $\mathbb{F}$ и нека $a(x) \in \mathbb{F}[[x]]$ е формалния степенен ред, асоцииран с $\mathbf{a}$. Съществува единствен полином m със старши коефициент 1, за който е изпълнено условието: $\mathbf{a}$ удовлетворява линейно рекурентно уравнение с характеристичен полином f тогава и само тогава, когато f е кратен на m .

Еднозначно определеният полином в Следствие 4.5, наричаме *минимален полином* за редицата $\mathbf{a}$. Приемаме, че минималният полином на нулевата редица $a_k = 0$, $k \geq 0$, е равен на 1. Всички други линейни рекурентни редици имат минимален полином $m(x)$ от ненулева степен. Бихме могли да дефинираме минимален полином на линейна рекурентна редица като характеристичния полином, получен от линейно рекурентно уравнение от минимален ред, което се удовлетворява от съответната редица. В Раздел 4.5 ще опишем ефективен алгоритъм за определяне на минималния полином на дадена редица.

Следващата теорема дава прост критерий, по който можем да определим дали характеристичния полином на рекурентна редица, зададена с някакво линейно рекурентно уравнение е минималния полином за тази редица.

Теорема 4.6. Нека $\mathbf{a} = (a_k)$ е линейна рекурентна редица над полето $\mathbb{F}$ с характеристичен полином f от степен n . Полиномът f е минимален за $\mathbf{a}$ тогава и само тогава, когато векторите $\mathbf{a}^{(0)}, \mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n-1)}$ са линейно независими.

Доказателство. Нека f е минимален полином и да допуснем, че

$$\lambda_0 \mathbf{a}^{(0)} + \lambda_1 \mathbf{a}^{(1)} + \dots + \lambda_{n-1} \mathbf{a}^{(n-1)} = \mathbf{0}.$$

Умножаваме двете страни на горното равенство с $\mathbf{A}^t$ и получаваме

$$\lambda_0 \mathbf{a}^{(t)} + \lambda_1 \mathbf{a}^{(t+1)} + \dots + \lambda_{n-1} \mathbf{a}^{(t+n-1)} = \mathbf{0}.$$

По-специално,

$$\lambda_0 a_t + \lambda_1 a_{t+1} + \dots + \lambda_{n-1} a_{t+n-1} = 0, \quad t \geq 0.$$

Това е рекурентно уравнение от ред не по-голям от $n-1$, в противоречие с дефиниращото свойство на минималния полином. Обратно, векторите $\mathbf{a}^{(0)}, \mathbf{a}^{(1)}, \dots, \mathbf{a}^{(n-1)}$ не могат да бъдат линейно зависими, ако минималният полином е от степен $< n$. $\square$

Пример 4.7. Редицата $(0, 1, 1, 1, \dots)$ удовлетворява линейно рекурентно уравнение от втори ред $a_k = a_{k-1} + a_{k-2}$???

Теорема 4.8. Дадено е рекурентното уравнение

$$a_{k+n} = \sum_{i=0}^{n-1} c_i a_{k+i}, \quad k \geq n, \quad (4.10)$$

от ред n с характеристичен полином

$$f(x) = x^n - c_{n-1}x^{n-1} - \dots - c_1x - c_0 \quad (4.11)$$

над крайното поле $\mathbb{F}$. Ако $\alpha_1, \dots, \alpha_t$ са различните корени на f (в някакво разширение $\mathbb{E}$ на $\mathbb{F}$), то редицата $\mathbf{s} = (s_k)$ със

$$s_k = \lambda_1 \alpha_1^k + \dots + \lambda_t \alpha_t^k \quad (k \in \mathbb{N}_0) \quad (4.12)$$

е решение на (4.10) над $\mathbb{E}$ (за произволни $\lambda_1, \dots, \lambda_t \in \mathbb{E}$). Решенията, зададени с (4.12) образуват линейно пространство с размерност t над E .

Доказателство. Редиците от вида (4.12) образуват линейно пространство. Следователно достатъчно е да докажем твърдението в специалния случай $t = 1$, $\lambda_1 = 1$. Да положим $\alpha = \alpha_1$. Тогава

$$0 = f(\alpha) = \alpha^n - \sum_{i=1}^n c_i \alpha^i,$$

откъдето

$$\alpha^{n+t} = \sum_{i=1}^n c_i \alpha^{n+t-i}$$

за всяко $t \geq 0$. С това проверихме, че редицата (a_i) наистина е решение. Размерността на линейното пространство, породено от редиците от вида (4.12) не надминава t . Сега е достатъчно да докажем, че редиците $(\alpha_1^i), \dots, (\alpha_t^i)$ са линейно независими. Ако допуснем, че

$$\lambda_1 \alpha_1^k + \lambda_2 \alpha_2^k + \dots + \lambda_t \alpha_t^k = 0$$

за всяко $k \geq 0$, то $(\lambda_1, \dots, \lambda_t)$ е решение на системата

$$x_1 \alpha_1^k + x_2 \alpha_2^k + \dots + x_t \alpha_t^k = 0, \quad k = 0, \dots, t-1.$$

Матрицата от коефициентите е матрица на Вандермонд и тъй като корените $\alpha_1, \dots, \alpha_t$ са различни, то системата има единствено тривиалното решение $\lambda_1 = \dots = \lambda_t = 0$. $\square$

Следствие 4.9. Ако линейното рекурентно уравнение (4.10) с характеристичен полином f има различни корени $\alpha_1, \dots, \alpha_n$ в полето си на разлагане E , то всички решения на (4.10) на E са от вида (4.12) с $t = n$. $\square$

Пример 4.10. Рекурентното уравнение за числата на FIBONACCI $a_n = a_{n-1} + a_{n-2}$ има характеристичен полином $f(x) = x^2 - x - 1$. Корени на f са $\alpha_{1,2} = (1 \pm \sqrt{5})/2$ и следователно всички редици удовлетворяващи имат $a_n = a_{n-1} + a_{n-2}$ вида

$$s_k = \lambda_1 \left(\frac{1 + \sqrt{5}}{2} \right)^k + \lambda_2 \left(\frac{1 - \sqrt{5}}{2} \right)^k.$$

За класическите числа на FIBONACCI се получава $\lambda_1 = 1/\sqrt{5}$, $\lambda_2 = -1/\sqrt{5}$.

4.2 Периодични редици

Редицата $\mathbf{a}$ наричаме *периодична* ако съществуват естествени числа $r > 0$ и $k_0 > 0$, че $a_{k+r} = a_k$ за всички $k \geq k_0$. Числото r наричаме *период* на $\mathbf{a}$. Най-малкият от всички възможни периоди наричаме *минимален период* з $\mathbf{a}$.

Лема 4.11. *Всеки период на периодична редица се дели на минималния ѝ период.*

Доказателството на този факт е очевидно. Редица $\mathbf{a}$ с минимален период r наричаме *строго периодична*, ако $a_{k+r} = a_k$ за всяко $k = 0, 1, \dots$

Лема 4.12. *Редицата $\mathbf{a} = (a_i)$ е строго периодична тогава и само тогава, когато съществува такова цяло число $r > 0$, за което $a_{k+r} = a_k$ за всяко $k = 0, 1, \dots$*

Доказателство. Необходимостта е очевидна. Обратно, ако условието на лемата се изпълнява, то $\mathbf{a}$ е периодична. Следователно тя има минимален период r_0 като равенството $a_{k+r_0} = a_k$ се изпълнява за всяко $k \geq k_0$, $k_0 \in \mathbb{N}$. Нека k е произволно естествено число и да изберем $m \geq k_0$, за което $m \equiv k \pmod{r}$. Тогава $a_{k+r_0} = a_{m+r_0} = a_m = a_k$, откъдето следва, че $\mathbf{a}$ е строго периодична. $\square$

Нека $\mathbf{a} = (a_i)$ е периодична редица с минимален период r . Най-малкото неотрицателно k_0 , за което е изпълнено $a_{k+r} = a_k$ за всяко $k \geq k_0$, наричаме *предпериод* на $\mathbf{a}$. Ясно е, че една периодична редица е строго периодична тогава и само тогава, когато предпериодът ѝ е 0.

Всяка периодична редица удовлетворява някакво линейно рекурентно уравнение и е следователно линейна рекурентна редица.

Теорема 4.13. *Нека $\mathbf{a} = (a_i)$ е редица над полето F и нека $a(x) \in F[[x]]$ е свързаният с нея формален степенен ред. Редицата (a) е периодична тогава и само тогава, когато $(1 - x^r)a(x)$ е полином над $\mathbb{F}$.*

Доказателство. Нека $\mathbf{a}$ е периодична с период r : $a_{k+r} = a_k$ за $k \geq N$. Това може да бъде записано като

$$a(x) = (a_0 + \dots + a_{N-1}x^{N-1}) + x^N(a_N + \dots + a_{N+r-1}x^{N+r-1})(1 + x^r + x^{2r} + \dots).$$

Използвайки тъждеството $1 + x^r + x^{2r} + \dots = (1 - x^r)^{-1}$ получаваме

$$(1 - x^r)a(x) = (a_0 + \dots + a_{N-1}x^{N-1})(1 - x^r) + x^N(a_N + \dots + a_{N+r-1}x^{N+r-1}),$$

откъдето следва, че $(1 - x^r)a(x) \in F[x]$. Обратно, нека $(1 - x^r)a(x)$ е полином над F . Тогава можем да запишем

$$(1 - x^r)a(x) = g(x) = (1 - x^r)u(x) + v(x), \quad 0 \leq \deg v(x) < r,$$

откъдето

$$a(x) = u(x) + v(x)(1 + x^r + x^{2r} + \dots),$$

което показва, че $a_{k+r} = a_k$ за всяко $k \geq \deg u + 1$. $\square$

Следствие 4.14. *Всяка периодична редица над поле е линейна рекурентна редица.*

Доказателство. Теорема 4.13 и Следствие 4.2. $\square$

Следствие 4.15. *Нека $\mathbf{a} = (a_i)$ е строго периодична редица с период r над полето $\mathbb{F}$, $a(x) \in F[[x]]$ е свързаният с нея формален степенен ред. Тогава в сила е полиномното тъждество*

$$f^*(x)s(x) = (1 - x^r)g(x),$$

където $f(x) = c_n x^n - c_{n-1} x^{n-1} - \dots - c_0$, а полиномите $s(x)$ и $g(x)$ са дефинирани чрез

$$\begin{aligned} s(x) &= a_0 + a_1 x + \dots + a_{r-1} x^{r-1}, \\ g(x) &= \sum_{j=0}^{n-1} \left(\sum_{i=0}^j c_{n-i} a_{j-i} \right) x^j. \end{aligned}$$

Доказателство. Теорема 4.1 и равенството

$$a(x) = s(x)(1 + x^r + x^{2r} + \dots) = s(x)(1 - x^r)^{-1}.$$

□

Теорема 4.16. *Нека $\mathbf{a}$ е строго периодична линейна рекурентна редица от ред n с характеристичен полином f над полето F . Полиномът f е минимален полином за $\mathbf{a}$ тогава и само тогава, когато кои да е n последователни вектора на състоянието са линейно независими.*

4.3 Линейни рекурентни редици над крайни полета

В този раздел ще разглеждаме линейни рекурентни редици над фиксирано крайно поле $F = \mathbb{F}_q$.

Една линейна рекурентна редица от ред n е винаги периодична като минималният ѝ период r удовлетворява неравенството $r \leq q^n - 1$. Повече яснота относно дължината на периода внася следната лема.

Лема 4.17. *Нека $\mathbf{a}$ е линейна рекурентна редица над $F = \mathbb{F}_q$ с минимален полином $t(x)$, $\deg t(x) = n$. Тогава $\mathbf{a}$ е периодична редица с минимален период $r_1 = q^n - 1$.*

Доказателство. Редицата $\mathbf{a}$ удовлетворява линейно рекурентно уравнение от ред n и нека A е асоциираната с него матрица. Тогава векторите на състоянията $\mathbf{a}^{(t)}$ могат да бъдат получени от $\mathbf{a}^{(0)}$ съгласно формулата (4.3). Можем да предположим, че никой вектор на състояние не е $\mathbf{0}$, тъй като в такъв случай редицата е с период 1. Възможните вектори на състояние са $q^n - 1$ на брой, следователно за някои цели числа $0 \leq s < t \leq q^n - 1$ е изпълнено $\mathbf{a}^{(s)} = \mathbf{a}^{(t)}$. От (4.3) следва, че $\mathbf{a}^{(s+k)} = \mathbf{a}^{(t+k)}$ за $k \geq 0$, т.е. $\mathbf{a}$ е периодична с период $r = t - s \leq q^n - 1$. □

Следствие 4.18. *Класът на периодичните редици над крайно поле F съвпада с класа на линейните рекурентни редици над F .*

Макар линейните рекурентни редици над крайно поле да са винаги периодични, то те не са задължително строго периодични, както показва тривиалният пример $a_{n+2} = a_{n+1}$ с начално условие $(0, 1)$. Следващият резултат дава достатъчно условие за това една линейна рекурентна редица над крайно поле да бъде строго периодична.

Теорема 4.19. *Нека $\mathbf{a}$ е линейна рекурентна редица над крайното поле $F = \mathbb{F}_q$ с характеристичен полином $f(x) = x^n - c_{n-1} x^{n-1} - \dots - c_0$. Ако $c_0 \neq 0$, то $\mathbf{a}$ е строго периодична с минимален период $r \leq q^n - 1$. Освен това асоциираната с $\mathbf{a}$ матрица A е обратима r дели реда на A .*

Доказателство. Матрицата A обратима, тъй като $\det A = \pm c_0 \neq 0$ (4.2). От (4.3) имаме

$$\mathbf{a}^{(t)} = \mathbf{a}^{(0)} A^t = \mathbf{a}^{(0)} A^{t+s} = \mathbf{a}^{(t+s)},$$

за всяко $t \geq 0$, където s е редът на A . Така $\mathbf{a}$ е периодична с период s . Останалата част от теоремата следва непосредствено от Лема 4.11 и Лема 4.17. $\square$

От Теорема 4.19 следва в частност, че минималният период на $\mathbf{a}$ дели $|\mathrm{GL}(n, \mathbb{F}_q)| = q^{(n^2-n)/2}(q^n - 1) \dots (q - 1)$.²

Редица $\mathbf{d}$, удовлетворяваща линейно рекурентно уравнение от вида (4.1) с начално състояние $(0, 0, \dots, 1)$, наричаме *редица, породена от импулс* (за даденото уравнение) или *импулсна редица*.

Теорема 4.20. Нека $\mathbf{d} = (d_i)$ е редица над $F = \mathbb{F}_q$, породена от импулс, и удовлетворяваща уравнението (4.1). Нека A е матрицата, асоциирана с редицата $\mathbf{d}$. Тогава за всеки два вектора $\mathbf{d}^{(s)}$ и $\mathbf{d}^{(t)}$

$$\mathbf{d}^{(s)} = \mathbf{d}^{(t)} \iff A^t = A^s. \quad (4.13)$$

Минималният период на коя да е редица, удовлетворяваща (4.1), дели минималния период на $\mathbf{d}$.

Доказателство. За всяко $t \geq 0$ е в сила $\mathbf{d}^{(t)} = \mathbf{d}^{(0)} A^t$. Следователно $A^s = A^t$ влече $\mathbf{d}^{(s)} = \mathbf{d}^{(t)}$. Обратно, ако $\mathbf{d}^{(s)} = \mathbf{d}^{(t)}$, то $\mathbf{d}^{(s+k)} = \mathbf{d}^{(t+k)}$ за всяко $k \geq 0$. Използвайки (4.3) заключаваме, че $\mathbf{d}^{(k)} A^s = \mathbf{d}^{(k)} A^t$ за всяко $k \geq 0$. Тъй като векторите $\mathbf{d}^{(0)}, \dots, \mathbf{d}^{(n-1)}$ са очевидно линейно независими, то $A^s = A^t$.

Да означим с r минималния период, а с k_0 –редпериода на $\mathbf{d}$. За всяко $k \geq k_0$ имаме $d_{k+r} = d_k$ и $\mathbf{d}^{(k+r)} = \mathbf{d}^{(k)}$. Съгласно (4.13) $A^{k+r} = A^k$ за всяко $k \geq k_0$. Следователно за всяка редица $\mathbf{a}$, удовлетворяваща (??), равенството $\mathbf{a}^{(k+r)} = \mathbf{a}^{(k)}$ е изпълнено за всяко $k \geq k_0$. Това означава, че r е период за $\mathbf{a}$ и Лема 4.11 завършва доказателството. $\square$

Теорема 4.21. Нека $\mathbf{d} = (d_i)$ е импулсна редица над $F = \mathbb{F}_q$, удовлетворяваща линейното рекурентно уравнение (4.1) с характеристичен полином f , $c_0 \neq 0$, и с асоциирана матрица A . Тогава $\mathbf{d}$ е периодична с минимален период r равен на реда на A . Равенството $r = q^n - 1$ е в сила тогава и само тогава, когато f е примитивен полином.

Доказателство. Съгласно Теорема ?? $\mathbf{d}$ е периодична с период r , делящ реда на A . Следователно $\mathbf{d}^{(r)} = \mathbf{d}^{(0)}$, $A^r = I$ и r е точно равен на реда на A . Но редът на една матрица A е $q^n - 1$ точно когато тя е подобна на съпровождащата матрица на примитивен полином от степен n над F .^{3 4} Това доказва теоремата. $\square$

От Теорема 4.21 следва в частност, че за всяка степен на просто число q и всяко естествено число n съществува линейна рекурентна редица над $\mathbb{F}_q$ с период $q^n - 1$, удовлетворяваща линейно рекурентно уравнение от ред n . Такава редица наричаме *псевдошумова редица*, *PN-редица* или *редица с максимален период*. Импулсните редици, удовлетворяващи линейно рекурентно уравнение с примитивен характеристичен полином са с точност до циклично изместване единствените PN-редици.

²Възможните редове на обратими $(n \times n)$ -матрици над $\mathbb{F}_q$ са определени от NIVEN в [40].

³Да се докаже!!

⁴Да се докаже че f^* е примитивен тогава и само тогава, когато f е примитивен (Теорема 1.5.8 в Юнгникел).

Две редици $\mathbf{a} = (a_i)$ и $\mathbf{b} = (b_i)$ наричаме *циклично еквивалентни*, ако съществува такова цяло число r , че $b_{k+r} = a_k$ за всяко $k \geq 0$. В сила е следния резултат.

Теорема 4.22. Нека $\mathbf{a} = (a_i)$ е PN -редица над $F = \mathbb{F}_q$, удовлетворяваща линейното рекурентно уравнение (4.1) с характеристичен полином f и асоциирана матрица A . Тогава f е примитивен полином и $\mathbf{a}$ е циклично еквивалентна на импулсна редица за даденото линейно рекурентно уравнение. Освен това всяка редица, удовлетворяваща (4.1), различна от нулевата редица $\mathbf{0}$, е циклично еквивалентна на $\mathbf{a}$.

Доказателство. Векторите на състоянията на $\mathbf{a}$ пробягват всички ненулеви вектори с дължина n над F . В частност векторът $(0, 0, \dots, 1)$ вектор на състояние за $\mathbf{a}$. $\square$

Сега ще разгледаме задачата за определяне на всички редици, удовлетворяващи дадено линейно рекурентно уравнение. В случая, когато характеристичният полином f е примитивен, този въпрос се решава от Теорема 4.21. Да разгледаме случая, когато f е неразложим. Ще отбележим, че ако $\deg f = n$, то съществуват точно n различни редици, удовлетворяващи линейно рекурентно уравнение с характеристичен полином f .

Теорема 4.23. Дадено е линейното рекурентно уравнение (4.1) от ред n над $F = \mathbb{F}_q$ с $c_0 \neq 0$, имащо неразложим характеристичен полином f . Нека α е корен на f в някакво разширение E на F . Всяка редица $\mathbf{s} = (s_k)$, удовлетворяваща уравнението (4.1), има вида

$$s_k = \text{Tr}_{E/F}(\theta \alpha^k), \quad k \geq 0, \quad (4.14)$$

където θ е произволен елемент от E . Елементът θ се определя еднозначно от редицата $\mathbf{s}$. С изключение на нулевата редица $\mathbf{0}$, редиците $\mathbf{s}$ са периодични с минимален период $r = \text{ord } f$ и се разбиват на $(q^n - 1)/r$ класа на еквивалентност (по отношение на цикличната еквивалентност) с по r редици всеки.

Доказателство. Първо да отбележим, че всички членове на редиците от вида (4.14) са елементи на F . Съгласно Теорема Апендиш ⁵ E е поле на разлагане за f и негови корени са елементите $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$. От Теорема 4.8 и Следствие 4.9 заключаваме, че всички решения на (4.1) над E образуват линейно пространство с размерност n над E и всяко решение може да бъде записано по единствен начин във вида

$$s_k = \lambda_0 \alpha^k + \lambda_1 \alpha^{kq} + \dots + \lambda_{n-1} \alpha^{kq^{n-1}}, \quad k \geq 0, \quad (4.15)$$

за някакви $\lambda_0, \dots, \lambda_{n-1} \in E$. Ако изберем

$$\lambda_0 = \theta, \lambda_1 = \theta^q, \dots, \lambda_{n-1} = \theta^{q^{n-1}}.$$

получаваме редицата $\mathbf{s} = \mathbf{s}_\theta$, дефинирана в (4.14). С това получаваме q^n различни редици $\mathbf{s}_\theta$, удовлетворяващи (4.1) и първата част на теоремата е доказана.

Съгласно Теорема 4.19 редиците $\mathbf{s}_\theta$ са периодични. Използвайки представянето (??) получаваме

$$s_{k+r} = s_k \iff \text{Tr}_{E/F}(\theta \alpha^{k+r}) = \text{Tr}_{E/F}(\theta \alpha^k) \iff \text{Tr}_{E/F}(\theta \alpha^k (1 - \alpha^r)) = 0.$$

⁵вж. Теорема 1.2.3 в Юнгникел

Последното е в сила за всички $k \geq 0$ тогава и само тогава, когато $\alpha^r = 1$ или $\theta = 0$. Така минималният период на s_θ с $\theta \neq 0$ е редът на α , т.е. редът на f . Останалата част на теоремата е очевидна. $\square$

Теорема 4.23 се обобщава безпроблемно за случая, когато f има различни корени, т.е. f е произведение на различни неразложими многочлени над F със старши коефициент единица.

Теорема 4.24. *Дадено е линейното рекурентно уравнение (4.1) от ред n над $F = \mathbb{F}_q$ с $c_0 \neq 0$. Нека характеристичния полином на (4.1) е от вида $f = f_1 \dots f_m$, където f_i са различни неразложими полиноми от степен n_i със старши коефициент 1. Нека α_i е корен на f_i в разширението $E_i = \mathbb{F}_{q^{n_i}}$, $i = 1, \dots, m$. Всяка редица, удовлетворяваща (4.1) се представя по единствен начин във вида*

$$s_k = \text{Tr}_{E_1/F}(\theta_1 \alpha_1^k) + \dots + \text{Tr}_{E_m/F}(\theta_m \alpha_m^k), \quad k \geq 0, \quad (4.16)$$

където $\theta_1, \dots, \theta_m$ са произволни елементи съответно от разширенията $E_1, \dots, E_m$. С Изключение на нулевата редица $\mathbf{0}$, съответстваща на $\theta_1 = \dots = \theta_m = 0$, редицата $\mathbf{s} = \mathbf{s}(\theta_1, \dots, \theta_m)$ е периодична с минимален период r , който е най-малко общо кратно на редовете $\text{ord } f_i$ за онези i , за които $\theta_i \neq 0$.

Следствие 4.25. Минималният период на импулсна редица, удовлетворяваща линейното рекурентно уравнение от Теорема 4.24, е $\text{lcm}\{\text{ord } f_i \mid i = 1, \dots, m\}$.

Задача. теорема 6.3.12 от Юнгникел.

4.4 Двоични псевдослучайни редици

В много криптографски приложения възниква нуждата от двоични случайни редици. Така например един начин за тайно предаване на съобщения е следния: трансформираме съобщението, което ще предаваме в низ $\mathbf{m}$ от нули и единици и към него добавяме (побитово) случайна двоична редица $\mathbf{s}$ скоето получаваме шифрираното съобщение $\mathbf{c} = \mathbf{m} + \mathbf{s}$. Разбоира се, имаме също $\mathbf{m} = \mathbf{c} + \mathbf{m}$, което означава, че получателят може да възстанови изпратеното съобщение, добавяйки към криптитекста $\mathbf{c}$ редицата $\mathbf{s}$. Ако $\mathbf{s}$ е случайна редица ⁶, то получената криптосистема е безусловно сигурна [47]. За съжаление тя не е твърде практична, тъй като изисква генериране, предаване и съхранение на много дълги случайни двоични редици. Така ние се задоволяваме с използването на такава детерминистично генерирана редица, която може да гарантира достатъчно сигурност. Получената криптографска система наричаме *поточен шифър* (stream cipher).

Нашата задача се свежда до детерминистично генериране на дълги редици (за предпочитане от малко входни данни), които *изглеждат* като случайни редици. Това означава, че те повтарят статистическото поведение, което очакваме от случайните редици. Свойствата, които обикновено изискваме, са формулирани за пръв път от ГОЛОМВ [23, 24] и се наричат *постулати на ГОЛОМВ*. Свойството периодичност подчертава неслучайния характер на разглежданите редици, затова е смислено да се

⁶каквото и да означава това

ограничим върху изследването на един техен период. Практически интерес представляват редици с голям период. В изложението по-долу следваме подхода на LIDL-NIEDERREITER, който се отличава малко от подхода на GOLOMB.

Нека $\mathbf{a} = (a_i)$ е периодична редица на д $\mathbb{F}_2$ с минимален период r . При задаена m -орка $\mathbf{b} = (b_1, b_2, \dots, b_m) \in \mathbb{F}_2$ очакваме числото

$$Z_{\mathbf{a}}(\mathbf{b}) := |\{t \mid 0 \leq t \leq r-1, (a_t, a_{t+1}, \dots, a_{t+m-1}) = \mathbf{b}\}|.$$

да бъде независимо от $\mathbf{b}$ за всички дължини m , за които това има смисъл. (т.е. r трябва да е голямо в сравнение с m). По-нататък, ако сравняваме случайна редица $\mathbf{a} = (a_i)$ с нейна шифтувана версия $\mathbf{a}' = (a_i + h)$, очакваме приблизително равен брой съвпадения и несъвпадения, тъй като всяка от двойките $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ трябва да се появява с вероятност приблизително $1/4$. За измерване на степента на различие на една редица $\mathbf{a}$ с нейната шифтувана версия въвеждаме функцията автокорелация $C_{\mathbf{a}}(h)$, която дефинираме чрез

$$c_{\mathbf{a}}(h) = \sum_{i=0}^{r-1} -1(-1)^{a_i - a_{i+h}}. \quad (4.17)$$

Ще казваме, че редицата $\mathbf{a}$ с период r е *псевдослучайна*, ако са изпълнени следните три условия (постулати на GOLOMB):

$$(G1) \quad |Z_{\mathbf{a}}(0) - Z_{\mathbf{a}}(1)| \leq 1;$$

$$(G2) \quad |Z_{\mathbf{a}}(\mathbf{b}) - Z_{\mathbf{a}}(\mathbf{b}')| \leq 1 \text{ за всеки две двоични } m\text{-орки } \mathbf{b} \text{ и } \mathbf{b}', \text{ с дължина } 2 \leq m \leq \log_2 r;$$

$$(G3) \quad C_{\mathbf{a}}(h) = \text{const за всяко } h \not\equiv 0 \pmod{r}.$$

Ще докажем, че PN -редиците над $\mathbb{F}_2$ удовлетворяват постулатите $(G1)$ – $(G3)$.

4.5 Алгоритъм на BERLEKEMP-MASSEY

Нека $\mathbf{a} = (a_i)_{i=0}^{N-1}$ е крайна редица с дължина N или безкрайна редица (в такъв случай пишем $N = \infty$) над $\mathbb{F}_q$. За всяко естествено число $k \leq N$ означаваме с $L_k(\mathbf{a})$ линеен регистър с минимална дължина, генериращ редица $\mathbf{s}^{(k)}$, която съвпада в първите си k елемента с $\mathbf{a}$. Характеристичния полином на $L_k(\mathbf{a})$ ще означаваме с $m_k(\mathbf{a})$ като $\deg m_k(\mathbf{a}) = L_k(\mathbf{a})$. Редицата $\mathbf{L} = (L_k(\mathbf{a}))$ наричаме *профил на линейната сложност на $\mathbf{a}$* . *Линейна сложност $L(\mathbf{a})$ на редицата $\mathbf{a}$* наричаме максималната стойност на $L_k(\mathbf{a})$, ако редицата $(L_k(\mathbf{a}))$ е ограничена и ∞ в противен случай. Следователно, $L(\mathbf{a}) = \infty$ тогава и само тогава, когато $\mathbf{a}$ е безкрайна непериодична редица.⁷ Освен това $L(\mathbf{a}) = L_N(\mathbf{a})$ ако $\mathbf{a}$ е крайна с дължина N .

Пример 4.26. Нека $\mathbf{a} = (0, 0, \dots, 0, \lambda)$, $\lambda \neq 0$, е редица с крайна дължина N над $\mathbb{F}_q$. Тогава

$$L_k(\mathbf{a}) = \begin{cases} 1 & \text{за } k = 1, \dots, N-1; \\ N & \text{за } k = N. \end{cases} \quad (4.18)$$

Лема 4.27. Нека $\mathbf{a}$ е редица с дължина N над $\mathbb{F}_q$. Тогава

⁷ Линейна сложност може да бъде дефинирана и като степента на минималния полином на $\mathbf{a}$.