ограничим върху изследването на един техен период. Практически интерест представляват редици с голям период. В изложението по-долу следваме подхода на Lidl-Niederreiter, който се отличава малко от подхода на Golomb.

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

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

да бъде независимо от $\boldsymbol{b}$ 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 $\boldsymbol{a} = (a_i)$ с нейна шифтвана версия $\boldsymbol{a}' = (a_i + h)$, очакваме приблизително равен брой съвпадения и несъвпадения, тъй като всяка от двойките $(0,0)$, $(),1)$, $(1,0)$, $(1,1)$ трябва да се появява с вероятност приблизително $1/4$. За измерване на степента на различие на една редица $\boldsymbol{a}$ с нейната шифтвана версия въвеждаме функцията *автокорелация* $C_{\boldsymbol{a}}(h)$, която дефинираме чрез

$$c_{\boldsymbol{a}}(h) = \sum_{i=0}^{r} -1(-1)^{a_k - a_{k+h}}. \tag{4.17}$$

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

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

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

$(G3)$ $C_{\boldsymbol{a}}(h) = const$ 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 $\boldsymbol{a} = (a_i)_{i=0}^{N-1}$ 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 $\Lambda_k(\boldsymbol{a})$ линеен регистър с минимална дължина, генериращ редица $\boldsymbol{s}^{(k)}$, която съвпада в първите си k елемента с $\boldsymbol{a}$. Характеристичния полином на $\Lambda_k(\boldsymbol{a})$ ще означаваме с $m_k(\boldsymbol{a})$ като $\deg m_k(\boldsymbol{a}) = L_k(\boldsymbol{a})$. Редицата $\boldsymbol{L} = (L_k(\boldsymbol{a}))$ наричаме *профил на линейната сложност на* $\boldsymbol{a}$. *Линейна сложност* $L(\boldsymbol{a})$ *на редицата* $\boldsymbol{a}$ наричаме машималната стоиност на $L_k(\boldsymbol{a})$, ако редицата $(L_k(\boldsymbol{a})$ е ограничена и ∞ в противен случай. Следователно, $L(\boldsymbol{a}) = \infty$ тогава и само тогава, когато $\boldsymbol{a}$ е безкрайна непериодична редица.[7] Освен това $L(\boldsymbol{a}) = L_N(\boldsymbol{a})$ ако $\boldsymbol{a}$ е крайна с дължина N.

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

$$L_k(\boldsymbol{a}) = \begin{cases} 1 & \text{за } k = 1, \ldots, N-1; \\ N & \text{за } k = N. \end{cases} \tag{4.18}$$

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

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

(*a*) $L_{k-1}(\boldsymbol{a}) \le L_k(\boldsymbol{a}) \le k$ *за всяко* $k \le N$;

(*b*) $L(\boldsymbol{a}) = L_{r+s}(\boldsymbol{a})$ *ако* $\boldsymbol{a}$ *е периодична с период* r *и предпериод* s.

В общият случай е много по-трудно да се пресметне профилът на линейната сложност, отколкото само линейната сложност. В този раздел ще опишем ефективен алгоритъм за решаване на тази задача. Ще започнем с една лема, която представлява и самостоятелен интерес.

Лема 4.28. *Нека* $\boldsymbol{a}$ *и* $\boldsymbol{b}$ *са две редици с дължина* N *над* $\mathbb{F}_q$. *Тогава*

$$L_k(\boldsymbol{a}+\boldsymbol{b}) \le L_k(\boldsymbol{a}) + L_k(\boldsymbol{b}), \tag{4.19}$$

за всяко $k \le N$.

Доказателство. Нека $\Lambda_k(\boldsymbol{a})$ и $\Lambda_k(\boldsymbol{b})$ са два линейни шифт-регистъра, които пораждат редици, съвпадащи съответно с $\boldsymbol{a}$ и $\boldsymbol{b}$ в първите им k елемента. Нека $f_{\boldsymbol{a}}(x)$ и $f_{\boldsymbol{b}}(x)$ са съответните характеристични полиноми. Означаваме с Нека $s_{\boldsymbol{a}}^{(k)}$ и $s_{\boldsymbol{b}}^{(k)}$ редиците, породени съответно от регистрите $\Lambda_k(\boldsymbol{a})$ и $\Lambda_k(\boldsymbol{b})$. Съгласно Теорема 4.1 съществуват полиноми $g_{\boldsymbol{a}}(x)$ и $g_{\boldsymbol{b}}(x)$, удовлетворяващи

$$\begin{aligned} s_{\boldsymbol{a}}(x) &= \frac{g_{\boldsymbol{a}}(x)}{f_{\boldsymbol{a}}^*(x)}, \quad \deg g_{\boldsymbol{a}}(x) < L_k(\boldsymbol{a}), \\ s_{\boldsymbol{b}}(x) &= \frac{g_{\boldsymbol{b}}(x)}{f_{\boldsymbol{b}}^*(x)}, \quad \deg g_{\boldsymbol{b}}(x) < L_k(\boldsymbol{b}), \end{aligned} \tag{4.20}$$

където $s_{\boldsymbol{a}}(x)$ и $s_{\boldsymbol{b}}(x)$ са формалните степенни редове, асоциирани с редиците $s_{\boldsymbol{a}}^{(k)}$ и $s_{\boldsymbol{b}}^{(k)}$. Очевидно имаме

$$\begin{gathered} s_{\boldsymbol{a}}(x) + s_{\boldsymbol{b}}(x) = \frac{g_{\boldsymbol{a}}(x) f_{\boldsymbol{b}}^*(x) + g_{\boldsymbol{b}}(x) f_{\boldsymbol{a}}^*(x)}{f_{\boldsymbol{a}}^*(x) f_{\boldsymbol{b}}^*(x)} \\ \deg\left(g_{\boldsymbol{a}}(x) f_{\boldsymbol{b}}^*(x) + g_{\boldsymbol{b}}(x) f_{\boldsymbol{a}}^*(x)\right) < \deg\left(f_{\boldsymbol{a}}^*(x) f_{\boldsymbol{b}}^*(x)\right). \end{gathered} \tag{4.21}$$

Редицата $s_{\boldsymbol{a}}^{(k)} + s_{\boldsymbol{b}}^{(k)}$ съвпада в първите си k компоненти с $\boldsymbol{a}+\boldsymbol{b}$ и може да бъде получена от линеен регистър с характеристичен полином $f_{\boldsymbol{a}}(x) f_{\boldsymbol{b}}(x)$. Това доказва твърдението, тъй като $\deg f_{\boldsymbol{a}} f_{\boldsymbol{b}} = L_k(\boldsymbol{a}) + L_k(\boldsymbol{b})$. □

Алгоритъмът на Berlekamp–Massey почива на следния фундаментален резултат.

Теорема 4.29. *Нека* $\boldsymbol{a}$ *е редица с дължина* N *над* $\mathbb{F}_q$, *а* k – *естествено число, за което* $k+1 \le N$. *Нека по-нататък* $\boldsymbol{s} = \boldsymbol{s}^{(k)}$ *е редица, която съвпада с* $\boldsymbol{a}$ *в първите* k *елемента* $a_0, a_1, \ldots, a_{k-1}$ *и която е генерирана от линеен шифт-регистър* $\Lambda_k(\boldsymbol{a})$ *с дължина* $L_k(\boldsymbol{a})$. *Тогава*

$$L_{k+1}(\boldsymbol{a}) = \begin{cases} L_k(\boldsymbol{a}) & \text{ако } s_k = a_k; \\ \max\{L_k(\boldsymbol{a}), k+1-L_k(\boldsymbol{a})\} & \text{ако } s_k \ne a_k. \end{cases} \tag{4.22}$$

Доказателство. Съгласно Лема 4.28 $L_{k+1}(\boldsymbol{a}) \ge L_k(\boldsymbol{a})$ и първата част на теоремата е очевидна.

Да допуснем, че $s_k \neq a_k$ и да положим $\lambda = s_k - a_k \neq 0$. Нека $\boldsymbol{b}$ е редицата $(\underbrace{0,0,\ldots,0}_{k},\lambda)$. Тя съвпада в първите $k+1$ позиции с редицата $\boldsymbol{s}-\boldsymbol{a}$. От Лема 4.28 и Пример 4.26, получаваме

$$k+1 = L_{k+1}(\boldsymbol{b}) = L_{k+1}(\boldsymbol{s}-\boldsymbol{a}) \leq L_{k+1}(\boldsymbol{s}) + L_{k+1}(-\boldsymbol{a}) = L_k(\boldsymbol{a}) + L_{k+1}(\boldsymbol{a}).$$

Тук негласно използвахме факта, че редиците $\boldsymbol{a}$ и $-\boldsymbol{a}$ имат един и същ профил на линейната сложност. Следователно, $L_{k+1}(\boldsymbol{a}) \geq k+1-L_k(\boldsymbol{a})$, откъдето

$$L_{k+1}(\boldsymbol{a}) \geq \max\left\{L_k(\boldsymbol{a}), k+1-L_k(\boldsymbol{a})\right\}. \tag{4.23}$$

Остава да покажем, че неравенството в (4.23) се достига равенство. Достатъчно е да построим линеен шифт-регистър $\Lambda_{k+1}(\boldsymbol{a})$ с дължина $\max\left\{L_k(\boldsymbol{a}), k+1-L_k(\boldsymbol{a})\right\}$, който генерира първите $k+1$ елемента на $\boldsymbol{a}$.

Да предположим, че сме конструирали линейни регистри $\Lambda_i(\boldsymbol{a})$ с дължини $L_i(\boldsymbol{a})$, генериращи първите i елемента на $\boldsymbol{a}$ за $i = 1,2,\ldots,k$. Ще считаме, че за тези регистри е изпълнено

$$L_{i+1}(\boldsymbol{a}) = \max\left\{L_i(\boldsymbol{a}), i+1-L_i(\boldsymbol{a})\right\}$$

за всички $i \leq k-1$, за които $\Lambda_i(\boldsymbol{a}) \neq \Lambda_{i+1}(\boldsymbol{a})$. Да означим характеристичния полином на $\Lambda_i(\boldsymbol{a})$ с

$$f_i(x) = x^{L_i(\boldsymbol{a})} - c^{(i)}_{L_i(\boldsymbol{a})-1}x^{L_i(\boldsymbol{a})-1} - \ldots - c^{(i)}_1 x - c^{(i)}_0. \tag{4.24}$$

Този полином се строи тривиално за $i=1$ като положим $L_0(\boldsymbol{a}) = 0$, $L_1(\boldsymbol{a}) = 1$ и $f_1(x) = x-1$.

Нека $k \geq 1$ и да означим с m най-големия индекс $i \leq k-1$, за който $L_i(\boldsymbol{a}) < L_{i+1}(\boldsymbol{a})$. Полагаме

$$n = L_{m+1}(\boldsymbol{a}), \quad r = L_m(\boldsymbol{a}),$$

т.е.

$$n = L_k(\boldsymbol{a}) = L_{k-1}(\boldsymbol{a}) = \ldots = L_{m+1}(\boldsymbol{a}) > L_m(\boldsymbol{a}) = r$$

и

$$n = \max\{r, m+1-r\} = m+1-r \quad (\text{понеже } n \neq r).$$

По дефиниция,

$$\sum_{i=0}^{n-1} c_i^{(k)} a_{i+j} = \begin{cases} a_{n+j} & \text{за } j = 0,1,\ldots,k-n-1, \\ s_k & \text{за } j = k-n, \end{cases} \tag{4.25}$$

и

$$\sum_{i=0}^{r-1} c_i^{(m)} a_{i+j} = \begin{cases} a_{r+j} & \text{за } j = 0,1,\ldots,m-r-1, \\ t_m & \text{за } j = m-r, \end{cases} \tag{4.26}$$

където $t_m \neq a_m$, тъй като $\Lambda_{m+1}(\boldsymbol{a}) \neq \lambda_m(\boldsymbol{a})$. Да положим $\mu = t_m - a_m$ и да положим

$$f_{k+1}(x) = x^{M-n}f_k(x) - \lambda\mu^{-1}x^{M-k+m-r}f_m(x), \tag{4.27}$$

където $M = \max\{n, k-m+r\} = \max\{n, (k+1)-(m+1-r)\} = \max\{n, k+1-n\}$. Полиномът $f_{k+1}(x)$ се разписва във вида

$$f_{k+1}(x) = x^M - c_{n-1}^{(k)} x^{M_1} - \ldots - c_1^{(k)} x^{M-n+1} - c_0^{(k)} x^{M-n} \\ - \lambda\mu^{-1}(x^{M-k+m} - c_{r-1}^{(m)} x^{M-k+m-1} - \ldots - c_1^{(m)} x^{M-k+m-r+1} + c_0^{(m)} x^{M-k+m-r}). \quad (4.28)$$

Чрез директно проесмятане можем да проверим, че линеен регистър с характеристичен полином $f_{k+1}(x)$ и начално състояние $(a_0, a_1, \ldots, a_{M-1})$ поражда първите $k+1$ елемента на $\boldsymbol{a}$. Линеен регистър с дължина M, характеристичен полином $\lambda\mu^{-1}x^{M-k+m-r}f_m(x)$ и начално състояние $(a_0, a_1, \ldots, a_{M-1})$ генерира редицата

$$b_j = \lambda\mu^{-1}\left(-a_{M-k+m+j} + \sum_{i=0}^{r-1} c_i^{(m)} a_{M-k+m-r+i+j}\right),$$

Очевидно,

$$b_j = \begin{cases} 0 & \text{за } j = 0, 1, \ldots, k-M-1, \\ \lambda & \text{за } j = k-M, \end{cases}$$

докато $x^{M-n}f_k(x)$ поражда редицата

$$u_j = \sum_{i=0}^{n-1} c_i^k a_{M+j-n+i} = \begin{cases} a_{M+j} & \text{за } j = 0, 1, \ldots, k-M-1, \\ s_k & \text{за } j = k-M. \end{cases}$$

Лесно се проверява, че $\Lambda_{k+1}(\boldsymbol{a})$ с характеристичен полином $f_{k+1}(x)$ генерира първите $k+1$ елемента на $\boldsymbol{a}$.

Теорема 4.29 представлява теоретична основа за алгоритъма на Berlekemp-Massey. Този алгоритъм определя линеен регистър $\Lambda_N(\boldsymbol{a})$ от минимална възможна дължина, който генерира зададена крайна редица $\boldsymbol{a}$ над $\mathbb{F}_q$ с дължина N.

Алгоритъм на Berlekamp-Massey

Нека $\boldsymbol{a} = (a_i)_{i=0}^{N-1}$ е редица с дължина N над $\mathbb{F}_q$. Следният алгоритъм пресмята целите числа $L_k(\boldsymbol{a})$ и полиномите

$$f_k(x) = x^{L_k(\boldsymbol{a})} - c_{L_k(\boldsymbol{a})-1}^{(k)} x^{L_k(\boldsymbol{a})-1} - \ldots - c_1^{(k)} x - c_0^{(k)},$$

за всяко $k \le N$. Ако редицата започва със s нули, началните условия са

$$L_s = 0,\ L_{s+1} = 1,\ f_s = 1,\ f_{s+1} = x - 1.$$

for $k = 1$ *to* N
  $\delta_k = -a_k + \sum_{i=0}^{L_k-1} c_i^{(k)} a_{k-L_k+i}$
  if $\delta_k = 0$
  then $f_{k+1} = f_k; L_{k+1} = L_k$
  else $m = \max\{i \mid L_i < L_{i+1}\}$
    $L_{k+1} = \max\{L_k, k+1-L_k\}$
    $f_{k+1} = x^{L_{k+1}-L_k} f_k(x) - \delta_k \delta_m^{-1} x^{L_{k+1}-k+m-L_m} f_m(x)$
  end{*if*}
end{*for*}

Пример 4.30. Ще демонстрираме алгоритъма в случая, когато $q = 2$. Сега не е нужно да различаваме знаците + и −; освен това $\delta_k = 0$ или 1 и дефиницията на f_{k+1} по-горе се упростява до

$$f_{k+1}(x) = f_k(x) + x^{k-m} f_m(x).$$

Да разгледаме редицата $\boldsymbol{a} = (1\,1\,0\,1\,0\,1\,1\,1\,0\,1)$. Алгоритъмът изпълнява следните стъпки.

$$\begin{array}{ll}
 & L_0 = 0, f_0 = 1 \\
 & L_1 = 1, f_1 = x + 1 \\
k = 1 & \delta_1 = a_1 + \sum_{i=0}^{0} 1 \cdot 1 = 1 + 1 = 0 \\
 & L_2 = 1, f_2 = f_1 = x + 1 \\
k = 2 & \delta_2 = a_2 + \sum_{i=0}^{0} 1 \cdot 1 = 0 + 1 = 1 \neq 0 \\
 & m = \max\{i \colon L_i < L_{i+1}\} = 0 \\
 & L_3 = \max\{L_2, 3 - L_2\} = 2 \\
 & M = \max\{L_2, 2 - 0 + 0\} = 2 \\
 & f_3 = x \cdot f_2 + f_0 = x(x+1) + 1 = x^2 + x + 1
\end{array}$$

$k=3$ $\delta_3 = a_3 + \sum_{i=0}^{1} c_i^{(3)} \cdot a_{1+i} = 1 + 1\cdot 1 + 1\cdot 0 = 0$
$L_4 = 2, f_4 = f_3 = x^2x + 1$

$k=4$ $\delta_4 = 0 + 1\cdot 1 + 1\cdot 0 = 1 \neq 0$
$m = \max\{i\colon L_i < L_{i+1}\} = 2$
$L_5 = \max\{L_4, 5 - L_4\} = 3$
$M = \max\{L_4, 4 - 2 + 1\} = \max\{2, 3, \} = 3$
$f_5 = x\cdot f_4 + f_2 = x(x^2 + x + 1) + x + 1 = x^3 + x^2 + 1$

$k=5$ $\delta_5 = 0 + 1\cdot 0 + 0\cdot 1 + 1\cdot 0 = 1 \neq 0$
$m = 4$
$L_6 = \max\{L_5, 6 - L_5\} = 3$
$M = \max\{3, 3\} = 3$
$f_6 = f_5 + f_4 = (x^3 + x^2 + 1) + (x^2 + x + 1) = x^3 + x$

$k=6$ $\delta_5 = 0 + 0\cdot 1 + 1\cdot 0 + 0\cdot 1 = 1 \neq 0$
$m = 4$
$L_7 = \max\{L_6, 7 - L_6\} = 4$
$M = \max\{3, 4\} = 4$
$f_7 = xf_6 + f_4 = x(x^3 + x) + (x^2 + x + 1) = x^4 + x + 1$

$k=7$ $\delta_7 = 0$
$L_8 = L_7 = 4$
$f_8 = f_7 = x^4 + x + 1$

$k=8$ $\delta_8 \neq 0$
$m = 6$
$L_9 = \max\{4, 9 - 4\} = 5$
$M = \max\{4, 5\} = 5$
$f_9 = xF_8 + f_6 = x(x^4 + x + 1) + x^3 + x = x^5 + x^3 + x^2$

$k=9$ $\delta_9 = 1 \neq 0$
$m = 8 (L_8 = 4)$
$L_{10} = \max\{L_9, 10 - L_9\} = 5$
$M = \max\{5, 9 - 8 + 4\} = 5$
$f_{10} = f_9 + f_8 = (x^5 + x^3 + x^2) + (x^4 + x + 1) = x^5 + x^4 + x^3 + x^2 + x + 1$

□

Задача. Да се построи линеен регистър с минимална дължина, генериращ крайната редица $(a_i)_{i=0}^{9} = (0110000111)$.

4.6 Поточни шифри