О. В. Камловский, Коэффициенты кросс-корреляции разрядных последовательностей равномерных линейных рекуррент над примарным кольцом вычетов,
Матем. вопр. криптогр., 2020, том 11, выпуск 1, 47–62

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2020 Т. 11 № 1 С. 47–62

УДК 512.547+512.552 DOI https://doi.org/10.4213/mvk314

Коэффициенты кросс-корреляции разрядных последовательностей равномерных линейных рекуррент над примарным кольцом вычетов

О. В. Камловский

ООО «Центр сертификационных исследований», *Москва*

Получено 29.IV.2019

Аннотация. Изучается класс последовательностей элементов простого поля, полученных в результате выделения старшего p-ичного разряда из линейных рекуррентных последовательностей над кольцом вычетов по модулю p^n. Приводятся абсолютные и неабсолютные оценки сверху для модулей коэффициентов кросс-корреляции рассматриваемых последовательностей. Эти результаты позволяют указать условия, при которых отрезки разрядных последовательностей, полученных из различных исходных последовательностей, также являются различными.

Ключевые слова: равномерные последовательности, линейные рекуррентные последовательности, разрядные последовательности, коэффициенты кросс-корреляции

Cross-correlation coefficients for digit sequences of uniform linear recurrent sequences over the residue ring

O. V. Kamlovskiy

Certification Research Center, *LLC*, *Moscow*

Abstract. We study the class of sequences over the prime field with p elements formed by the most significant p-ary digits of linear recurrent sequences over the residue ring modulo p^n. We obtain absolute and nonabsolute bounds for the cross-correlation coefficients of such sequences. This results lead to some sufficient conditions for segments of digit sequences obtained from different initial sequences to be different.

Keywords: uniform sequences, linear recurrent sequences, digit sequences, cross-correlation coefficients

Citation: Matematicheskie Voprosy Kriptografii, 2020, v. 11, № 1, pp. 47–62 (Russian)

Введение

Линейные рекуррентные последовательности (ЛРП) над кольцами вычетов примарного порядка p^n, где p — простое число, исследовались в ряде работ (см., например, [1,2]). Одной из сложных современных задач является получение точных формул или оценок для частот появлений элементов на отрезках рассматриваемых последовательностей. В то же время важно уметь строить так называемые равномерные ЛРП, в которых на отрезках длины, кратной периоду последовательности, каждый элемент кольца появляется одинаково часто (см. [3–9]). Кроме того, для практических приложений необходимо усложнять исходную последовательность, чтобы получать последовательности с большим рангом (линейной сложностью). Один из таких способов построения равномерных ЛРП был предложен А.С. Кузьминым и А.А. Нечаевым в [1]. Он основан на сложении исходной (основной) ЛРП со счетчиковой последовательностью и последующим выделением старшего p-ичного разряда. Частотные характеристики r-грамм на циклах и отрезках таких последовательностей были изучены в [10, 11]. В частности, были получены оценки для модуля кросс-корреляционной функции, позволяющие гарантировать отсутствие сокращения периода и одинаковых последовательностей при различных начальных векторах ЛРП.

Данная работа продолжает исследования, начатые в [10, 11]. В ней рассматриваются коэффициенты кросс-корреляции, характеризующие «близость» друг к другу отрезков исследуемых последовательностей. Отметим, что детально изучены сложные законы распределения элементов в основных последовательностях и их разрядных последовательностях (см., например, [2, 12–16]). Целью данной работы является получение для коэффициентов кросс-корреляции разрядных последовательностей равномерных ЛРП результатов, аналогичных тем, которые известны для разрядных последовательностей основных ЛРП.

1. Класс исследуемых последовательностей

Пусть $R = \mathbb{Z}_{p^n} = \{0, 1, \ldots, p^n - 1\}$ — примарное кольцо вычетов. Рассмотрим унитарный реверсивный многочлен Галуа $F(x) \in R[x]$ (старший коэффициент многочлена $F(x)$ равен 1, многочлен $\bar{F}(x)$, полученный из $F(x)$ приведением всех его коэффициентов по модулю p, неприводим над полем $P = \mathbb{Z}_p$ и $\bar{F}(x) \neq x$) степени $\deg F(x) = m - 2$. Обозначим через $\oplus$, $\ominus$, $\otimes$ операции сложения, вычитания и умножения в поле P соответственно. Пусть

$$H(x) = (x-1)^2 F(x). \tag{1}$$

Будет рассматривать семейство $L_R(H)$ всех ЛРП над кольцом R с характеристическим многочленом $H(x)$. Всюду далее будет изучаться случай, когда $\bar{F}(x) \neq x \ominus 1$. В этой ситуации (см. [1, 10]) каждая ЛРП $\omega \in L_R(H)$ однозначно представима в виде

$$\omega = v + u, \tag{2}$$

где $v \in L_R((x-1)^2)$, $u \in L_R(F)$, причем существуют такие однозначно определенные элементы a, $b \in R$, что

$$v(i) = ai + b, \quad i \geqslant 0.$$

Последовательность ω является равномерной (см. [1, 10]) тогда и только тогда, когда $a \in R^*$, где R^* — мультипликативная группа кольца R. В этом случае ее период связан с периодом многочлена $\bar{F}(x)$ соотношением

$$T(\omega) = p^n T(\bar{F}) = \frac{p^n(p^{m-2}-1)}{d}, \tag{3}$$

где d — некоторый делитель числа $p^{m-2}-1$.

Рассмотрим отображение $f : R \to P$, ставящее в соответствие каждому элементу $x \in R$ с p-ичным представлением

$$x = x_0 + px_1 + \ldots + p^{n-1}x_{n-1},$$

где x_0, x_1, …, $x_{n-1} \in P$, его старший разряд x_{n-1}. Обозначим через $\omega' = f(\omega)$ последовательность с элементами $f(\omega(i))$, где $i \geqslant 0$. Учитывая равенство (2), получим

$$\omega'(i) = f(v(i) + u(i)) = f(ai + b + u(i)), \quad i \geqslant 0. \tag{4}$$

Если ω — равномерная последовательность над кольцом R (т. е. $a \in R^*$), то ω' является равномерной последовательностью над полем P. Исследования работ [1, 11] показывают, что последовательности ω' представляют интерес для криптографических приложений.

2. Коэффициенты кросс-корреляции

Пусть ω_1, $\omega_2 \in L_R(H)$ и выполнены равенства

$$\omega_1(i) = a_1 i + b_1 + u_1(i), \quad \omega_2(i) = a_2 i + b_2 + u_2(i), \quad i \geqslant 0, \tag{5}$$

где a_1, a_2, b_1, $b_2 \in R$, u_1, $u_2 \in L_R(F)$. Каждый гомоморфизм ψ группы $(P, \oplus)$ в мультипликативную группу $\mathbb{C}^*$ поля комплексных чисел имеет вид (см. [17])

$$\psi(x) = e^{2\pi i \frac{c \otimes x}{p}}, \quad x \in P, \tag{6}$$

где $c \in P$. Будем использовать обозначение $\psi = \psi_c$. Определим коэффициент кросс-корреляции последовательностей

$$\omega_1' = f(\omega_1), \quad \omega_2' = f(\omega_2) \tag{7}$$

равенством

$$C_{\omega_1',\omega_2'}(\psi, l, t) = \sum_{i=0}^{l-1} \psi(\omega_1'(i) \ominus \omega_2'(i+t)), \tag{8}$$

где $l, t \in \mathbb{N}$. Так как всюду в дальнейшем результаты не будут зависеть от выбора элемента $c \in P$, $c \neq 0$, то для рассматриваемого коэффициента будем использовать обозначение $C_{\omega_1',\omega_2'}(l,t)$. Значение величины $C_{\omega_1',\omega_2'}(l,t)$ тесно связано с близостью между векторами

$$(\omega_1'(0), \ldots, \omega_1'(l-1)), \quad (\omega_2'(t), \ldots, \omega_2'(l+t-1)). \tag{9}$$

Чем меньше величина $|C_{\omega_1',\omega_2'}(l,t)|$, тем заметнее отличаются друг от друга рассматриваемые векторы. В случае $p = 2$ имеет место равенство

$$C_{\omega_1',\omega_2'}(l,t) = \sum_{i=0}^{l-1} (-1)^{\omega_1'(i) \oplus \omega_2'(i+t)},$$

и несложно проверить, что расстояние $\rho_{\omega_1',\omega_2'}(l,t)$ Хэмминга между векторами (9) вычисляется по формуле

$$\rho_{\omega_1',\omega_2'}(l,t) = \frac{l - C_{\omega_1',\omega_2'}(l,t)}{2}.$$

3. Сведение к суммам характеров кольца вычетов

Рассмотрим отображение $g = g_c : R \to \mathbb{C}$, определенное по правилу

$$g_c(x) = \psi(f(x)), \quad x \in R,$$

где f — функция выделения старшего p-ичного разряда, $c \in R$, $c \neq 0$, а $\psi = \psi_c$. Обозначим через L множество всех отображений из R в $\mathbb{C}$. Относительно операций сложения и умножения на комплексные числа L образует линейное пространство со скалярным произведением S, задаваемым для $h_1, h_2 \in L$ по правилу

$$S(h_1, h_2) = \frac{1}{|R|} \sum_{x \in R} h_1(x) \bar{h}_2(x),$$

где черта обозначает комплексное сопряжение. Множество характеров группы $(R,+)$ состоит из характеров χ_a, $a \in R$, определенных равенством (см., например, [17])

$$\chi_a(x) = e^{2\pi i \frac{ax}{p^n}}, \quad x \in R. \tag{10}$$

Система характеров $\{\chi_a, a \in R\}$ образует ортонормированный базис евклидова пространства (L,S), и справедливы равенства

$$g_c(x) = \sum_{d\in R} \nu_{c,d}\chi_d(x), \tag{11}$$

$$\nu_{c,d} = \frac{1}{|R|}\sum_{x\in R} g_c(x)\bar{\chi}_d(x). \tag{12}$$

В дальнейшем нам понадобится оценка величины

$$\sigma(g_c) = \sum_{d\in R} |\nu_{c,d}|. \tag{13}$$

Лемма 1 ([12]). 1) $\nu_{c,d} = 0$ *при всех* $d \in pR$,
2) *при* $n \geqslant 2$

$$\sigma(g_c) < \frac{2(n-1)}{\pi}\ln p + \frac{13}{40}p + \frac{7}{20}.$$

Докажем результаты, позволяющие свести изучение коэффициента $C_{\omega_1',\omega_2'}(l,t)$ к исследованию сумм значений аддитивных характеров кольца R.

Утверждение 1. *Пусть* $n \geqslant 2$, *тогда*

$$|C_{\omega_1',\omega_2'}(l,t)| < \left(\frac{2(n-1)}{\pi}\ln p + \frac{13}{40}p + \frac{7}{20}\right)^2 \max_{d,r\in R^*}\left|\sum_{i=0}^{l-1}\chi(d\omega_1(i)+r\omega_2(i+t))\right|,$$

где $\chi = \chi_1$.

Доказательство. С использованием (8) и (11) получим

$$C_{\omega_1',\omega_2'}(l,t) = \sum_{i=0}^{l-1}\psi_c(\omega_1'(i))\psi_{p\ominus c}(\omega_2'(i+t))$$

$$= \sum_{i=0}^{l-1}\psi_c(f(\omega_1(i)))\psi_{p\ominus c}(f(\omega_2(i+t))) = \sum_{i=0}^{l-1} g_c(\omega_1(i))g_{p\ominus c}(\omega_2(i+t))$$

$$= \sum_{i=0}^{l-1} \sum_{d \in R} \nu_{c,d} \chi_d(\omega_1(i)) \sum_{r \in R} \nu_{p \ominus c,r} \chi_r(\omega_2(i+t))$$

$$= \sum_{d,r \in R} \nu_{c,d} \nu_{p \ominus c,r} \sum_{i=0}^{l-1} \chi_d(\omega_1(i)) \chi_r(\omega_2(i+t)).$$

Согласно лемме 1 в этой формуле достаточно ограничиться суммированием по всем d, r из множества $R \backslash pR = R^*$, поэтому

$$C_{\omega_1', \omega_2'}(l,t) = \sum_{d,r \in R^*} \nu_{c,d} \nu_{p \ominus c,r} \sum_{i=0}^{l-1} \chi(d\omega_1(i) + r\omega_2(i+t))$$

и, переходя к абсолютным величинам, получим

$$|C_{\omega_1', \omega_2'}(l,t)| \leqslant \left(\sum_{d \in R^*} |\nu_{c,d}| \right) \left(\sum_{r \in R^*} |\nu_{p \ominus c,r}| \right) \max_{d,r \in R^*} \left| \sum_{i=0}^{l-1} \chi(d\omega_1(i) + r\omega_2(i+t)) \right|.$$

Для завершения доказательства утверждения 1 остается воспользоваться оценкой величины $\sigma(g_c)$ из леммы 1. □

4. Абсолютная оценка

Получим оценку коэффициента кросс-корреляции (8), которая не будет зависеть от длины l рассматриваемых отрезков ЛРП. Назовем такую оценку абсолютной.

Нам понадобится следующий вспомогательный результат.

Лемма 2 ([10]). *Если $F(x)$ — реверсивный многочлен Галуа степени $m-2$ над кольцом $R = \mathbb{Z}_{p^n}$, $\bar{F}(x) \neq x \ominus 1$, то для каждой ЛРП $\omega \in L_R(H) \backslash L_R(x-1)$ и любого такого $l \in \mathbb{N}$, что $l \leqslant p^n T(\bar{F})$,*

$$\left| \sum_{i=0}^{l-1} \chi(\omega(i)) \right| < \left(\frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5} \right) p^{\frac{m}{2}+2n-2}.$$

На множестве всех векторов-строк фиксированной длины над кольцом R зададим бинарное отношение $\sim$, положив $\vec{\alpha} \sim \vec{\beta}$, если существует такой элемент $c \in R^*$, что $\vec{\beta} = c\vec{\alpha}$.

Теорема 1. *Пусть последовательности ω_1, ω_2 определены равенством (5), ω_1', ω_2' заданы соотношением (7), $F(x)$ — реверсивный*

многочлен Галуа степени $m-2$ *над кольцом* R, $\bar{F}(x) \neq x \ominus 1$ *и* $(u_1(0),\dots,u_1(m-3),a_1) \not\sim (u_2(t),\dots,u_2(t+m-3),a_2)$, $n \geqslant 2$. *Тогда при всех* $l \leqslant p^n T(\bar{F})$ *для коэффициента кросс-корреляции* (8) *справедлива оценка*

$$|C_{\omega_1',\omega_2'}(l,t)| < \left(\frac{2(n-1)}{\pi}\ln p + \frac{13}{40}p + \frac{7}{20}\right)^2 \left(\frac{4}{\pi^2}\ln T(\bar{F}) + \frac{9}{5}\right) p^{\frac{m}{2}+2n-2}.$$

Доказательство. Покажем, что при условии

$$(u_1(0),\dots,u_1(m-3),a_1) \not\sim (u_2(t),\dots,u_2(t+m-3),a_2)$$

последовательность с элементами $d\omega_1(i) + r\omega_2(i+t)$, где $i \geqslant 0$, не принадлежит множеству $L_R(x-1)$ при всех $d, r \in R^*$. Действительно, согласно (5) $d\omega_1(i) + r\omega_2(i+t) = const$ для всех $i \geqslant 0$ только если $(da_1 + ra_2)i + du_1(i) + ru_2(i+t) = const$ для всех $i \geqslant 0$. В силу единственности представления (2) это равносильно тому, что $da_1 + ra_2 = 0$ и $du_1(i) + ru_2(i+t) = 0$ для всех $i \geqslant 0$, т. е. условию

$$d(u_1(0),\dots,u_1(m-3),a_1) + r(u_2(t),\dots,u_2(t+m-3),a_2) = (0,\dots,0).$$

Для завершения доказательства остается воспользоваться леммой 2 и утверждением 1. □

5. Сравнение с основными ЛРП

Пусть $G(x)$ — унитарный реверсивный многочлен Галуа степени m над кольцом $R = \mathbb{Z}_{p^n}$, $\delta_1, \delta_2 \in L_R(G)$ — ЛРП и $\delta_1' = f(\delta_1)$, $\delta_2' = f(\delta_2)$ — их p-ичные разрядные последовательности. Последовательности δ_1' и δ_2' зачастую рассматриваются как усложнения последовательностей δ_1 и δ_2 соответственно (см. [1, 2]). Оценим коэффициент кросс-корреляции

$$C_{\delta_1',\delta_2'}(l,t) = \sum_{i=0}^{l-1} \psi(\delta_1'(i) \ominus \delta_2'(i+t)).$$

Теорема 2. *Пусть* δ_1, $\delta_2 \in L_R(G)$, $G(x)$ — *реверсивный многочлен Галуа степени* m *над кольцом* R, $\delta_1' = f(\delta_1)$, $\delta_2' = f(\delta_2)$, $(\delta_1(0),\dots,\delta_1(m-1)) \not\sim (\delta_2(t),\dots,\delta_2(t+m-1))$, $n \geqslant 2$. *Тогда при всех* $l \leqslant T(G)$

$$|C_{\delta_1',\delta_2'}(l,t)| < \left(\frac{2(n-1)}{\pi}\ln p + \frac{13}{40}p + \frac{7}{20}\right)^2 \left(\frac{4}{\pi^2}\ln T(\bar{G}) + \frac{9}{5}\right) p^{\frac{m}{2}+2n-2}.$$

Доказательство проводится аналогично доказательству теоремы 1 с использованием оценки (см. [12]).

$$\left|\sum_{i=0}^{l-1}\chi(\delta(i))\right| < \left(\frac{4}{\pi^2}\ln T(\bar{G}) + \frac{9}{5}\right)p^{\frac{m}{2}+2n-2},$$

справедливой для всех $l \leqslant T(G)$ и каждой ненулевой ЛРП $\delta \in L_R(G)$. □

Теорема 2 обобщает на случай произвольного значения p результаты работ [13, 14, 16]. Кроме того, при $p = 2$ теорема 2 устанавливает несколько более точные оценки, чем результаты, приведенные в указанных статьях.

Отметим, что при фиксированных значениях n, p и $m \to \infty$ правые части оценок из теорем 1 и 2 имеют вид $O(mp^{\frac{m}{2}})$.

Рассмотрим оценки из теорем 1 и 2 в наиболее интересном частном случае, когда $F(x)$ и $G(x)$ — многочлены максимальных периодов: $T(F) = p^{n-1}(p^{m-2}-1)$, $T(G) = p^{n-1}(p^m-1)$. В этом случае для равномерных ЛРП ω_1', ω_2' удается гарантировать несколько более точные оценки, чем для ЛРП δ_1', δ_2'. Отметим, что в общем случае нельзя добиться равномерности последовательностей δ_1' и δ_2', в то время как равномерность последовательностей ω_1' и ω_2' достигается выбором обратимых элементов a_1 и a_2 в равенстве (5). Таким образом, разрядные последовательности равномерных ЛРП ω_1, ω_2 с точки зрения обоснованности свойств распределений элементов на отрезках более интересны, чем разрядные последовательности основных ЛРП δ_1, δ_2.

6. Неабсолютная оценка

Получим верхнюю оценку модуля коэффициента кросс-корреляции (8), которая зависит от длины l рассматриваемых отрезков ЛРП. Для этого понадобится соответствующая оценка суммы

$$\sigma_l(\omega) = \sum_{i=0}^{l-1}\chi(\omega(i)).$$

Утверждение 2. *Если $F(x)$ — реверсивный многочлен Галуа степени $m-2$ над кольцом $R = \mathbb{Z}_{p^n}$, $\bar{F}(x) \neq x \ominus 1$, $T(F) = p^{\nu}(p^{m-2}-1)/d$, $T(\bar{F}) \geqslant p^{2n}/3$, то для каждой ЛРП $\omega \in L_R(H)\backslash L_R(x-1)$ и любого*

такого $l \in \mathbb{N}$, *что* $l < T(\bar{F})$, *выполнено неравенство*

$$|\sigma_l(\omega)| \leqslant \left(\frac{3p^n l}{d} \left(p^{m-2} + (l-1)(dp^{n-1} - 1) p^{\frac{m}{2}-1} \right) \right)^{\frac{1}{3}}.$$

Доказательство. Пусть последовательность ω удовлетворяет соотношению (2). По условию либо $a \neq 0$, либо u — ненулевая последовательность. Если u — нулевая последовательность, то согласно [10, теорема 1] $|\sigma_l(\omega)| < p^n$. В этом случае доказываемое неравенство имеет место, так как $3T(\bar{F}) \geqslant p^{2n}$. Пусть теперь u — ненулевая ЛРП. Так как $F(x)$ — реверсивный многочлен, то ω является чисто периодической последовательностью и $T(\omega) \geqslant T(u) \geqslant T(\bar{F})$. Пусть $v_k = x^k\omega$, $k \geqslant 0$, — сдвиг последовательности ω на k шагов влево. Тогда множество $P(\omega)$ всех сдвигов ЛРП ω имеет вид $P(\omega) = \{v_0, v_1, \ldots, v_{T(\omega)-1}\}$. Согласно [18, теорема 1] будет выполнено неравенство

$$|\sigma_l(\omega)| \leqslant \left(3 \sum_{v \in P(\omega)} |\sigma_l(v)|^2 \right)^{\frac{1}{3}}. \tag{14}$$

Период $T(\omega)$ является делителем числа $p^n T(\bar{F})$, поэтому справедливо соотношение

$$\sum_{v \in P(\omega)} |\sigma_l(v)|^2 = \frac{T(\omega)}{p^n T(\bar{F})} \sum_{k=0}^{p^n T(\bar{F})-1} |\sigma_l(v_k)|^2. \tag{15}$$

Оценим сверху величину

$$R(\omega) = \sum_{k=0}^{p^n T(\bar{F})-1} |\sigma_l(v_k)|^2.$$

Имеет место равенство

$$R(\omega) = \sum_{k=0}^{p^n T(\bar{F})-1} \sigma_l(v_k)\overline{\sigma_l(v_k)},$$

где $\overline{\sigma_l(v_k)}$ — число, комплексно сопряженное к числу $\sigma_l(v_k)$. Тогда

$$R(\omega) = \sum_{k=0}^{p^n T(\bar{F})-1} \sum_{i=0}^{l-1} \chi(v_k(i)) \sum_{j=0}^{l-1} \chi(-v_k(j)). \tag{16}$$

Из (16) следует, что

$$R(\omega) = \sum_{k=0}^{p^n T(\bar{F})-1} \sum_{i,j=0}^{l-1} \chi(v_k(i) - v_k(j))$$
$$= \sum_{k=0}^{p^n T(\bar{F})-1} \sum_{i,j=0}^{l-1} \chi(ai - aj + u(k+i) - u(k+j)).$$

Представим ЛРП u с использованием функции «след» (см., например, [1]):

$$u(i) = \mathrm{Tr}_R^S(b\alpha^i),\ i \geqslant 0,$$

где $S = GR(p^{(m-2)n}, p^n)$ — кольцо Галуа характеристики p^n, состоящее из $p^{(m-2)n}$ элементов, α — корень многочлена $F(x)$ в кольце S, а b — ненулевой элемент кольца S. Тогда

$$R(\omega) = \sum_{i,j=0}^{l-1} \chi(a(i-j)) \sum_{k=0}^{p^n T(\bar{F})-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k),$$

где χ' — аддитивный характер кольца S, определенный равенством $\chi'(y) = \chi(\mathrm{Tr}_R^S(y))$. Выделив отдельно слагаемое, соответствующее случаю $i = j$, получим

$$R(\omega) = p^n T(\bar{F}) l + p^{n-\nu} \sum_{i \neq j} \chi(a(i-j)) \sum_{k=0}^{p^\nu T(\bar{F})-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k).$$

Значит,

$$R(\omega) = p^n T(\bar{F}) l$$
$$+p^{n-\nu} \sum_{i \neq j} \chi(a(i-j)) \left(\sum_{k=0}^{p^\nu T(\bar{F})-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k) + \frac{p^\nu}{d} \right) - \frac{p^n}{d} \sum_{i \neq j} \chi(a(i-j)).$$

Если $a = 0$, то

$$\sum_{i \neq j} \chi(a(i-j)) = l(l-1).$$

Если $a \neq 0$, то

$$\sum_{i \neq j} \chi(a(i-j)) = -l + \sum_{i,j=0}^{l-1} \chi(a(i-j)) = -l + \left| \sum_{i=0}^{l-1} \chi(ai) \right|^2.$$

Переходя к рассмотрению абсолютных величин, получим

$$|R(\omega)| \leqslant p^n T(\bar{F}) l + \frac{lp^n}{d} + p^{n-\nu} l(l-1) \max_{i \neq j} \left| \sum_{k=0}^{p^\nu T(\bar{F})-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k) + \frac{p^\nu}{d} \right|$$

$$= \frac{lp^{m+n-2}}{d} + p^{n-\nu} l(l-1) \max_{i \neq j} \left| \sum_{k=0}^{p^\nu T(\bar{F})-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k) + \frac{p^\nu}{d} \right|.$$

Заметим, что образ элемента $\alpha^i - \alpha^j$ при действии естественного эпиморфизма колец $S \to S/pS$ равен $\bar{\alpha}^i - \bar{\alpha}^j$, где $\bar{\alpha}$ — корень многочлена $\bar{F}(x)$ в поле $GF(q^{m-2})$. Тогда при всех различных $i, j \in \overline{0, l-1}$ и $l \leqslant T(\bar{F})$ элемент $\bar{\alpha}^i - \bar{\alpha}^j$ ненулевой, а значит, элемент $\alpha^i - \alpha^j$ — обратимый элемент кольца S. С использованием оценки из [19] получим

$$\left| \sum_{k=0}^{p^\nu T(\bar{F})-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k) + \frac{p^\nu}{d} \right| \leqslant \frac{dp^{n-1} - 1}{d} p^{\frac{m}{2}+\nu-1}.$$

Таким образом,

$$|R(\omega)| \leqslant \frac{lp^n}{d} \left(p^{m-2} + (l-1)(dp^{n-1} - 1) p^{\frac{m}{2}-1} \right),$$

а значит, согласно равенству (15)

$$\sum_{v \in P(\omega)} |\sigma_l(v)|^2 \leqslant \frac{lp^n}{d} \left(p^{m-2} + (l-1)(dp^{n-1} - 1) p^{\frac{m}{2}-1} \right).$$

Для завершения доказательства остается воспользоваться неравенством (14). □

Основным результатом этого раздела является следующая неабсолютная оценка модуля коэффициента кросс-корреляции.

Теорема 3. *Пусть в условиях теоремы 1 дополнительно выполнены соотношения* $T(\bar{F}) \geqslant p^{2n}/3$, $l < T(\bar{F})$, *тогда*

$$|C_{\omega_1', \omega_2'}(l, t)| < C(n, p)^2 \left(\frac{3p^n l}{d} \left(p^{m-2} + (l-1)(dp^{n-1} - 1) p^{\frac{m}{2}-1} \right) \right)^{\frac{1}{3}},$$

где

$$C(n, p) = \frac{2(n-1)}{\pi} \ln p + \frac{13}{40} p + \frac{7}{20}.$$

Доказательство. проводится аналогично доказательству теоремы 1 с использованием утверждений 1 и 2. □

Покажем, что полученная неабсолютная оценка точнее абсолютной оценки из теоремы 1 при всех l, удовлетворяющих условиям

$$p^{\frac{m}{2}-1} \leqslant l \leqslant \frac{1}{\sqrt{3}} C(F)^{\frac{3}{2}} p^{\frac{m}{2}+2n-2}, \tag{17}$$

где

$$C(F) = \frac{4}{\pi^2} \ln T(\bar{F}) + \frac{9}{5}.$$

Действительно, это так при условии

$$\frac{3p^n l}{d}(p^{m-2} + (l-1)(dp^{n-1}-1)p^{\frac{m}{2}-1}) < C(F)^3 p^{\frac{3m}{2}+6n-6}.$$

Последнее неравенство заведомо выполнено, если

$$\frac{l}{d}\left(p^{m-2} + l(dp^{n-1}-1)p^{\frac{m}{2}-1}\right) \leqslant \frac{1}{3} C(F)^3 p^{\frac{3m}{2}+5n-6}. \tag{18}$$

Так как $l \geqslant p^{m/2-1}$, то неравенство (18) выполняется при условии

$$\frac{l}{d}\left(p^{\frac{m}{2}-1} l + l(dp^{n-1}-1)p^{\frac{m}{2}-1}\right) \leqslant \frac{1}{3} C(F)^3 p^{\frac{3m}{2}+5n-6},$$

что равносильно

$$l^2 \leqslant \frac{1}{3} C(F)^3 p^{m+4n-4}.$$

7. Различные отрезки последовательностей

Рассмотрим вопрос о значении длины l, при которой отрезки (9) являются различными.

Теорема 4. *Пусть последовательности* ω_1, ω_2 *определены равенством* (5), *последовательности* ω_1', ω_2' *заданы соотношением* (7), $F(x)$ — *реверсивный многочлен Галуа степени* $m-2$ *над кольцом* R, $m \geqslant 4$, $n \geqslant 2$, $\bar{F}(x) \neq x \ominus 1$, $(u_1(0), \ldots, u_1(m-3), a_1) \not\sim (u_2(t), \ldots, u_2(t+m-3), a_2)$,

$$l_0 = \left\lceil 3C(n,p)^6 p^{\frac{m}{2}+2n-2} \right\rceil.$$

Тогда если $l_0 < T(\bar{F})$, *то*

$$(\omega_1'(0), \ldots, \omega_1'(l_0-1)) \neq (\omega_2'(t), \ldots, \omega_2'(t+l_0-1)).$$

Доказательство. Допустим, что рассматриваемые отрезки последовательностей равны. Тогда $|C_{\omega_1',\omega_2'}(l_0,t)| = l_0$. Так как $C(n,p) \geqslant 1$, $m \geqslant 4$, то из условия $T(\bar{F}) > l_0$ следует, что $3T(\bar{F}) \geqslant p^{2n}$. Тогда по теореме 3

$$l_0 = |C_{\omega_1',\omega_2'}(l_0,t)| < C(n,p)^2 \left(\frac{3p^n l_0}{d} \left(p^{m-2} + (l_0-1)(dp^{n-1}-1)p^{\frac{m}{2}-1} \right) \right)^{\frac{1}{3}}. \tag{19}$$

Покажем, что при всех

$$l \geqslant 3C(n,p)^6 p^{\frac{m}{2}+2n-2}$$

будет выполнено соотношение

$$C(n,p)^2 \left(\frac{3p^n l}{d} \left(p^{m-2} + (l-1)(dp^{n-1}-1)p^{\frac{m}{2}-1} \right) \right)^{\frac{1}{3}} \leqslant l, \tag{20}$$

которое будет противоречить соотношению (19) при подстановке значения $l = l_0$. Неравенство (20) имеет место, если

$$\frac{3p^n C(n,p)^6}{d}(p^{m-2} + l(dp^{n-1}-1)p^{\frac{m}{2}-1}) \leqslant l^2.$$

Так как рассматривается случай $l \geqslant p^{m/2-1}$, то полученное неравенство заведомо выполнено при условии

$$\frac{3p^n C(n,p)^6}{d}(lp^{\frac{m}{2}-1} + l(dp^{n-1}-1)p^{\frac{m}{2}-1}) \leqslant l^2,$$

т. е. при

$$l \geqslant 3C(n,p)^6 p^{\frac{m}{2}+2n-2}.$$

□

Теорема 4 показывает, что если p, n фиксированы, а $m \to \infty$, то векторы (9) различаются при длине $l = O(p^{\frac{m}{2}})$.

8. Неабсолютная оценка для больших длин отрезков

Оценка из теоремы 3 справедлива при $l < T(\bar{F})$, в то время как оценка из теоремы 1 имеет место при $l \leqslant p^n T(\bar{F})$. Предложим подход, позволяющий получить неабсолютные оценки на длине $l \leqslant p^n(T(\bar{F}) - 1)$.

Теорема 5. *Пусть в условиях теоремы 1 дополнительно выполнено соотношение* $l \leqslant p^n(T(\bar{F}) - 1)$, *тогда*

$$|C_{\omega_1',\omega_2'}(l,t)| < p^n C(n,p)^2 \left(\frac{3l_1}{d}(p^{m-2} - l_1 + (l_1-1)(dp^{n-1}-1)p^{\frac{m}{2}-1})\right)^{\frac{1}{3}},$$

где $l_1 = \left\lfloor \frac{l-1}{p^n} \right\rfloor + 1$.

Доказательство. Из утверждения 1 следует, что

$$|C_{\omega_1',\omega_2'}(l,t)| < C(n,p)^2 \max_{\omega \in L_R(H)\setminus L_R(x-1)} \left|\sum_{i=0}^{l-1} \omega(i)\right|. \tag{21}$$

Согласно [10] если ω имеет вид (2), где u — нулевая последовательность, то

$$\left|\sum_{i=0}^{l-1} \omega(i)\right| < p^n,$$

а если u — ненулевая последовательность, то

$$\left|\sum_{i=0}^{l-1} \omega(i)\right| \leqslant \sum_{j=1}^{p^n} \left|\sum_{k=0}^{l_j-1} v_j(k)\right|,$$

где $l_j = \left\lfloor \frac{l-j}{p^n} \right\rfloor + 1$, а $v_j(k) = u(j-1+kp^n)$, $k \geqslant 0$. При этом последовательность v_j является ненулевой ЛРП, характеристический многочлен которой — реверсивный многочлен Галуа степени $m-2$ и периода $(p^{m-2}-1)/d$. Из [18, следствие 1] следует, что при $l_j < T(\bar{F})$ справедлива оценка

$$\left|\sum_{k=0}^{l_j-1} v_j(k)\right| \leqslant \left(\frac{3l_j}{d}(p^{m-2} - l_j + (l_j-1)(dp^{n-1}-1)p^{\frac{m}{2}-1})\right)^{\frac{1}{3}}.$$

Заметим, что правая часть последнего неравенства возрастает с ростом l_j и всегда больше либо равна 1. Кроме того, по условию

$$l_1 = \left\lfloor \frac{l-1}{p^n} \right\rfloor + 1 = \frac{l-a}{p^n} + 1 < \frac{l}{p^n} + 1 \leqslant T(\bar{F}),$$

где $a \in \{1, \ldots, p^n\}$ выбрано так, что p^n делит $l-a$. Таким образом,

$$\left|\sum_{i=0}^{l-1}\omega(i)\right| \leqslant p^n\left(\frac{3l_1}{d}\left(p^{m-2}-l_1+(l_1-1)(dp^{n-1}-1)p^{\frac{m}{2}-1}\right)\right)^{\frac{1}{3}},$$

и остается воспользоваться неравенством (21). □

Оценка из теоремы 5 оказывается несколько менее точной, чем оценка из теоремы 3, однако она представляет интерес, если длина отрезков $l \geqslant T(\bar{F})$, так как в этом случае теорема 3 неприменима. По аналогии с вышеприведенными рассуждениями можно показать, что оценка теоремы 5 заведомо точнее абсолютной оценки из теоремы 1, если

$$p^{\frac{m}{2}-1} \leqslant l_1 \leqslant \frac{1}{\sqrt{3}}C(F)^{\frac{3}{2}}p^{\frac{m}{2}+2n-2}.$$

Результаты работы показывают, что разрядные последовательности равномерных ЛРП являются усложнениями исходных ЛРП и могут быть использованы при построении псевдослучайных чисел.

Список литературы

[1] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., "Linear recurring sequences over rings and modules", *J. Math. Sci.*, **76**:6 (1995), 2793–2915.

[2] Кузьмин А.С., Куракин В.Л., Нечаев А.А., "Псевдослучайные и полилинейные последовательности", *Труды по дискретной математике*, **1** (1997), 139–202.

[3] Кейперс Л., Нидеррайтер Г., *Равномерное распределение последовательностей*, М.: Наука, 1985, 408 с.

[4] Ларин М.В., "Транзитивные полиномиальные преобразования колец вычетов", *Дискретная математика*, **14**:2 (2002), 20–32.

[5] Анашин В.С., "Равномерно распределенные последовательности целых p-адических чисел", *Дискретная математика*, **14**:4 (2002), 3–64.

[6] Herendi T., "Uniform distribution of linear recurring sequences modulo prime powers", *Finite Fields and Appl.*, **10**:1 (2004), 1–23.

[7] Knight M.J., Webb W.A., "Uniform distribution of third order linear recurrence sequences", *Acta Arith*, **36** (1980), 7–20.

[8] Narkiewicz W., "Uniform distribution of sequences of integers in residue classes", Lect. Notes Math., **1087**, 1984, 140 pp.

[9] Turnwald G., "Uniform distribution of second-order linear recurring sequences", *Proc. Amer. Math. Soc.*, **96** (1986), 189–198.

[10] Камловский О.В., "Распределение r-грамм в одном классе равномерных последовательностей над кольцами вычетов", *Проблемы передачи информации*, **50**:1 (2014), 98–115.

[11] Камловский О.В., "Равномерные последовательности над простыми полями, построенные из одного класса линейных рекуррент над кольцами вычетов", *Проблемы передачи информации*, **50**:2 (2014), 60–76.

[12] Камловский О.В., "Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа", *Изв. РАН. Сер. матем.*, **77**:6 (2013), 71–96.

[13] Sole P., Zinoviev D., “Distribution of r-patterns in the most significant bit of a maximum length sequence over $\mathbb{Z}_{2^l}$”, *Lect. Notes Comput. Sci.*, **3486** (2005), 275–281.

[14] Sole P., Zinoviev D., “The most significant bit of maximum-length sequences over $\mathbb{Z}_{2^l}$: autocorrelation and imbalance”, *IEEE Trans. Inf. Theory*, **50**:8 (2006), 1844–1846.

[15] Qi W., Zhou J., “Distribution of 0 and 1 in the highest level of primitive sequences over $\mathbb{Z}_{2^e}$”, *Science in China* (*Ser. A*), **40**:6 (1997), 606–611.

[16] Hu H., Feng D., Wu W., “Incomplete exponential sums over Galois rings with applications to some binary sequences derived from $\mathbb{Z}_{2^l}$”, *IEEE Trans. Inf. Theory*, **52**:5 (2006), 2260–2265.

[17] Лидл Р., Нидеррайтер Г., *Конечные поля*, **1, 2**, М.: Мир, 1988, 822 с.

[18] Камловский О.В., “Метод В.М. Сидельникова для оценки числа знаков на отрезках линейных рекуррентных последовательностей над кольцами Галуа”, *Матем. заметки*, **91**:3 (2012), 371–382.

[19] Камловский О.В., Кузьмин А.С., “Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа”, *Фундам. и прикл. математика*, **6**:4 (2000), 1083–1094.