Math-Net.Ru

Общероссийский математический портал

О. В. Камловский, Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа, *Матем. сб.*, 2009, том 200, номер 4, 31–52

DOI: <https://doi.org/10.4213/sm4528>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.172.240.79

26 апреля 2023 г., 14:51:36

УДК 519.4

О. В. Камловский

Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа

В работе изучаются частоты появлений элементов в линейных рекуррентных последовательностях векторов над кольцами Галуа. Исследование этих частот сводится к изучению соответствующих тригонометрических сумм над кольцами Галуа. На основании оценок тригонометрических сумм получены нетривиальные оценки частот появления элементов в линейных рекуррентных последовательностях, обобщающие некоторые известные результаты для последовательностей над конечным полем. Эти оценки являются асимптотически неулучшаемыми.

Библиография: 25 названий.

Ключевые слова: линейные рекуррентные последовательности, кольца Галуа, тригонометрические суммы, распределение элементов псевдослучайных последовательностей, оценки тригонометрических сумм.

§ 1. Введение

Последовательность $u = (u(i))_{i=0}^{\infty}$ элементов коммутативного кольца R называется *линейной рекуррентной последовательностью (ЛРП) порядка m над кольцом R* , если для нее выполнены равенства

$$u(i+m) = a_0 u(i) + a_1 u(i+1) + \dots + a_{m-1} u(i+m-1), \quad i \geq 0,$$

где $a_0, a_1, \dots, a_{m-1}$ – фиксированные элементы кольца R (см., например, [1]). При этом многочлен

$$F(x) = x^m - a_{m-1}x^{m-1} - \dots - a_1x - a_0$$

называется *характеристическим многочленом ЛРП u* . ЛРП над конечными полями и кольцами вычетов часто используются при генерации псевдослучайных последовательностей, а также при построении помехоустойчивых кодов. Одним из важных свойств псевдослучайных последовательностей является близость частот появлений элементов на отрезках этих последовательностей к своим “естественным” средним значениям. В настоящей работе изучаются частотные характеристики ЛРП над кольцами Галуа, включающими в себя конечные поля и примарные кольца вычетов.

Рассмотрим ЛРП $u_1, u_2, \dots, u_r$ над кольцом Галуа $R = \text{GR}(q^n, p^n)$, состоящим из $q^n = p^{tn}$ элементов и имеющим характеристику p^n , где p – простое число. Назовем эти последовательности *линейно независимыми над кольцом R* ,

Работа выполнена в рамках Программы поддержки ведущих научных школ РФ (грант № НШ-4.2008.10).

если для всех ненулевых векторов $\bar{c} = (c_1, c_2, \dots, c_r) \in R^r$ последовательность $c_1 u_1 + c_2 u_2 + \dots + c_r u_r$ – ненулевая. Будем считать, что все последовательности $u_1, u_2, \dots, u_r$ имеют один и тот же характеристический многочлен $F(x)$, где $F(x)$ – некоторый унитарный многочлен над кольцом R .

Пусть l – натуральное число, а $\bar{z} = (z_1, z_2, \dots, z_r)$ – упорядоченный набор элементов кольца R . Обозначим через $N_l(\bar{z}, u_1, \dots, u_r)$ количество целых чисел $i \in \{0, \dots, l-1\}$ таких, что

$$\begin{cases} u_1(i) = z_1, \\ u_2(i) = z_2, \\ \dots\dots\dots \\ u_r(i) = z_r. \end{cases}$$

Другими словами, величина $N_l(\bar{z}, u_1, \dots, u_r)$ равна частоте появлений r -граммы $\bar{z} \in R^r$ на начальном отрезке длины l ЛРП векторов, элементы которой имеют вид $(u_1(i), u_2(i), \dots, u_r(i))$, $i \geq 0$. При $r = 1$ рассматриваемая частота равна количеству появлений элемента $z_1 \in R$ на начальном отрезке длины l последовательности u_1 . Если последовательности $u_1, u_2, \dots, u_r$ являются сдвигами одной и той же последовательности u , т.е. $u_1 = x^{s_1}u$, $u_2 = x^{s_2}u$, $\dots$, $u_r = x^{s_r}u$, то величина $N_l(\bar{z}, u_1, \dots, u_r)$ равна частоте появления r -граммы $\bar{z}$ среди наборов $(u(i+s_1), u(i+s_2), \dots, u(i+s_r))$, $0 \leq i < l$. Таким образом, результаты о частотах появления элементов в ЛРП векторов являются обобщениями результатов о частотных характеристиках одной ЛРП u .

Частоты $N_l(\bar{z}, u_1, \dots, u_r)$ хорошо изучены в случае, когда $R = \text{GR}(q, p) = \text{GF}(q)$ – конечное поле из q элементов. Наиболее сильные результаты в этом направлении были получены при использовании метода тригонометрических сумм. Первой работой, в которой аппарат тригонометрических сумм был применен для изучения рассматриваемых частот, является работа [2]. В ней получены оценки частот $N_l(z_1, u_1)$ для ЛРП u_1 над конечным простым полем. Затем эти оценки были существенно обобщены. Так, в работе [3; теорема 1] доказано, что если $u_1, u_2, \dots, u_r$ – линейно независимая система ЛРП над полем $\text{GF}(q)$, многочлен $F(x)$ неприводим над полем $R = \text{GF}(q)$ и имеет период $T(F) > 12$, то справедлива оценка

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{|R|^r} \right| < q^{m/2} \ln T(F), \quad (1)$$

где m – степень многочлена $F(x)$. Величина $l/|R|^r$ представляет собой “естественное” среднее значение частоты появления набора $\bar{z}$ на отрезке длины l ЛРП векторов. В случае, когда $l = T(F)$, множитель $\ln T(F)$ в оценке (1) можно убрать. В работе [4; теорема 2] показано, что правую часть неравенства (1) можно уменьшить примерно в $\pi/2$ раз и, кроме того, оценка (1) асимптотически неулучшаема. Приведенные результаты допускают уточнение лишь в некоторых частных случаях (см. [5]–[7]).

Представляет значительный интерес получение оценок, аналогичных оценке (1) для ЛРП над кольцом Гауа и, в частности, над кольцом $\mathbb{Z}_{p^n}$ вычетов

по модулю p^n . Для применения метода тригонометрических сумм в этом случае оказалось необходимым развить сам аппарат тригонометрических сумм над кольцами Галуа. Так, в [8] была получена оценка для сумм Вейля над кольцами Галуа, обобщающая известные оценки из работ [9], [10]. На основе этой оценки в [11] были получены нетривиальные оценки частот $N_l(\bar{z}, u_1, \dots, u_r)$ в случае, когда $R = \text{GR}(q^n, p^n)$, $l = T(F)$ и последовательности $u_1, u_2, \dots, u_r$ являются линейно независимыми сдвигами одной и той же последовательности. В [12] была получена оценка для так называемых гибридных сумм, представляющих собой суммы Вейля с некоторыми весовыми множителями. В настоящей работе этот результат используется для оценки тригонометрических сумм, возникающих при исследовании частот $N_l(\bar{z}, u_1, \dots, u_r)$, $l \leq T(F)$. Получено обобщение оценки (1) на случай ЛРП над кольцом Галуа. Так же как и в случае конечного поля, показана асимптотическая неупрощаемость этих оценок.

Отметим, что оценки для сумм Вейля и соответствующие оценки гибридных сумм над кольцами Галуа использовались для описания частотных характеристик последовательностей, полученных выделением старшего двоичного разряда из ЛРП максимального периода над кольцом $\mathbb{Z}_{2^n}$ (см. [13]–[15]). Из оценок частот появления элементов в ЛРП над кольцами Галуа следуют оценки для частот появления элементов в последовательностях, полученных выделением в них какого-либо разряда. Поэтому результаты настоящей работы применимы и для описания частотных характеристик координатных последовательностей ЛРП над кольцами Галуа. Однако в случае ЛРП максимального периода над кольцом $\mathbb{Z}_{2^n}$ оценки оказываются менее точными, чем оценки из перечисленных выше работ.

Настоящая работа имеет следующую структуру. В § 2 приведены необходимые сведения из теории колец Галуа и ЛРП над кольцами Галуа. В § 3 рассмотрены некоторые общие результаты о связи тригонометрических сумм и характеристик над кольцами Галуа. В § 4 приведены оценки для тригонометрических сумм, связанных с вычислением частот $N_l(\bar{z}, u_1, \dots, u_r)$. Эти результаты в настоящей работе носят вспомогательный характер, однако они представляют также и самостоятельный интерес. Основные результаты работы получены в § 5, где даны оценки частот $N_l(\bar{z}, u_1, \dots, u_r)$, $l \leq T(F)$. В § 6 показано, что эти оценки являются асимптотически неупрощаемыми. В § 7 оценки частот $N_l(\bar{z}, u_1, \dots, u_r)$ уточнены для случая $l = T(F)$.

§ 2. ЛРП над кольцами Галуа

Приведем сначала некоторые результаты из теории колец Галуа (см., например, [16], [17]) и теории ЛРП над кольцами Галуа (см., например, [1], [18]). *Кольцом Галуа* называется конечное коммутативное кольцо R с единицей e , в котором множество всех делителей нуля имеет вид pR для некоторого простого числа p . Важными примерами колец Галуа являются примарное кольцо вычетов $\mathbb{Z}_{p^n}$ и конечное поле $\text{GF}(q)$ из q элементов. Произвольное кольцо Галуа R однозначно с точностью до изоморфизма определяется своей характеристикой p^n и числом элементов p^{tn} . Поэтому далее такое кольцо будем

обозначать через $\text{GR}(q^n, p^n)$, где $q = p^t$. Множество всех делителей нуля pR кольца $R = \text{GR}(q^n, p^n)$ образует идеал кольца R , причем факторкольцо $\overline{R}$ кольца R по идеалу pR является полем из q элементов. Множество $\Gamma(R)^*$ всех элементов c кольца R , удовлетворяющих условию $c^{q-1} = e$, является циклической подгруппой порядка $q - 1$ мультипликативной группы R^* кольца R . При этом группа R^* раскладывается в прямое произведение своих подгрупп $\Gamma(R)^*$ и $e + pR$. Каждый элемент c кольца R может быть единственным образом представлен в виде

$$c = c_0 + pc_1 + \dots + p^{n-1}c_{n-1}, \quad (2)$$

где c_i – элемент множества $\Gamma(R) = \Gamma(R)^* \cup \{0\}$, $i = \overline{0, n-1}$. Равенство (2) называется *p-адическим представлением элемента c*.

Пусть $F(x)$ – унитарный многочлен степени m над кольцом R . Многочлен $F(x)$ будем называть *многочленом Галуа над кольцом R*, если образ $\overline{F}(x)$ многочлена $F(x)$ при действии естественного эпиморфизма колец многочленов $R[x] \rightarrow \overline{R}[x]$ является неприводимым многочленом над полем $\overline{R}$. Если $F(x)$ – многочлен Галуа над кольцом R , то факторкольцо $S = R[x]/F(x)$ является кольцом Галуа $\text{GR}(q^{mn}, p^n)$. Кольцо S можно рассматривать как расширение кольца R . Обозначим через $\text{Aut}(S/R)$ множество всех автоморфизмов кольца S , оставляющих на месте каждый элемент кольца R . Группа $\text{Aut}(S/R)$ является циклической группой порядка m , порожденной некоторым автоморфизмом $\varkappa$. Автоморфизм $\varkappa$ действует на каждый элемент s кольца S , имеющий p -адическое представление $s = s_0 + ps_1 + \dots + p^{n-1}s_{n-1}$, следующим образом:

$$\varkappa(s) = s_0^q + ps_1^q + \dots + p^{n-1}s_{n-1}^q.$$

Используя группу автоморфизмов кольца Галуа, можно ввести функцию Tr_R^S , называемую следом. Пусть $R = \text{GR}(q^n, p^n)$, $S = \text{GR}(q^{mn}, p^n)$. Функцию Tr_R^S из кольца S в кольцо R определим на элементах x кольца S равенством

$$\text{Tr}_R^S(x) = \sum_{\tau \in \text{Aut}(S/R)} \tau(x).$$

Функция $\text{Tr}_R^S(x)$ является эпиморфизмом R -модуля S_R на R -модуль R_R .

Пусть $F(x)$ – многочлен Галуа над кольцом $R = \text{GR}(q^n, p^n)$. В работе [19] доказано, что период $T(F)$ многочлена $F(x)$ и период $T(\overline{F})$ многочлена $\overline{F}(x)$ связаны соотношением $T(F) = p^\nu T(\overline{F})$, $0 \leq \nu \leq n-1$. Если m – степень многочлена $F(x)$, то период $T(F)$ многочлена $F(x)$ равен $(q^m - 1)p^\nu/d$, где d – делитель числа $q^m - 1$. Если при этом $d = 1$, $\nu = n-1$, т.е. $T(F) = (q^m - 1)p^{n-1}$, то многочлен $F(x)$ называют *многочленом максимального периода*. Пусть $u = (u(i))_{i=0}^\infty$ – ЛРП над кольцом R с характеристическим многочленом $F(x)$, α – корень многочлена $F(x)$ в кольце $S = \text{GR}(q^{mn}, p^n)$. В [16] доказано, что существует единственный элемент $b \in S$ такой, что для всех $i \geq 0$ справедливо равенство

$$u(i) = \text{Tr}_R^S(b\alpha^i). \quad (3)$$

Обозначим через $L_R(F)$ множество всех ЛРП над кольцом R с характеристическим многочленом $F(x)$, а через $L_R(F)^*$ – множество всех ЛРП u из множества $L_R(F)$ таких, что в представлении (3) элемент b является обратимым

элементом кольца S . Условие обратимости элемента b равносильно наличию в начальном векторе $(u(0), u(1), \dots, u(m-1))$ ЛРП u хотя бы одного обратимого элемента кольца R .

Всюду далее будем считать, что $F(0)$ является обратимым элементом кольца R . В этом случае многочлен Галуа $F(x)$ будем называть *реверсивным многочленом Галуа*. При таком характеристическом многочлене каждая ЛРП $u \in L_R(F)$ – чисто периодическая последовательность, а период $T(u)$ каждой ЛРП $u \in L_R(F)^*$ равен периоду $T(F)$ многочлена $F(x)$. Если $F(x)$ – многочлен максимального периода над кольцом R , то любую ЛРП $u \in L_R(F)^*$ называют *ЛРП максимального периода*.

§ 3. Характеры и тригонометрические суммы

Тригонометрические суммы (см., например, [20], [21]) достаточно хорошо изучены и часто применяются при решении различных теоретико-числовых проблем. Такие суммы можно рассматривать и в кольцах Галуа. При этом используется теория характеров конечных абелевых групп (см. [21]).

Рассмотрим характеры аддитивной группы кольца $R = \text{GR}(q^n, p^n)$. Обозначим через R_0 множество, состоящее из элементов $0, e, 2e, \dots, (p^n - 1)e$, где e – единица кольца R . Множество R_0 является подкольцом кольца R , изоморфным кольцу $\mathbb{Z}_{p^n}$. Для любого элемента c кольца R отображение $\chi_c: R \rightarrow \mathbb{C}^*$, определяемое равенством $\chi_c(x) = \exp\{2\pi i \text{Tr}_{R_0}^R(cx)/p^n\}$ является характером аддитивной группы кольца R , причем если a и b – различные элементы кольца R , то $\chi_a \neq \chi_b$. Других характеров аддитивной группы кольца R нет. Характер χ_e будем обозначать через χ . Укажем некоторые свойства характера χ , которые понадобятся в дальнейшем.

УТВЕРЖДЕНИЕ 1. *Справедливы следующие соотношения:*

$$\sum_{c \in R} \chi(cx) = \begin{cases} |R|, & \text{если } x = 0, \\ 0, & \text{если } x \neq 0; \end{cases} \quad (4)$$

$$\sum_{c \in R^*} \chi(cx) = \begin{cases} |R^*|, & \text{если } x = 0, \\ -|pR|, & \text{если } x \in p^{n-1}R \setminus \{0\}, \\ 0, & \text{если } x \notin p^{n-1}R. \end{cases} \quad (5)$$

ДОКАЗАТЕЛЬСТВО. Используя соотношения ортогональности для характеров, получим равенства

$$\sum_{c \in R} \chi(cx) = \sum_{c \in R} \chi_c(x) = \begin{cases} |R|, & \text{если } x = 0, \\ 0, & \text{если } x \neq 0. \end{cases}$$

Таким образом, соотношение (4) доказано. Докажем теперь равенства (5). Если рассмотреть ограничение характера χ на подгруппу $p^k R$ аддитивной группы кольца R , то получим нетривиальный характер этой подгруппы при всех

$k = \overline{1, n-1}$. Тогда, используя соотношения ортогональности для характеров, получим, что

$$\sum_{c \in p^k R} \chi(c) = 0 \quad (6)$$

для всех $k = \overline{0, n-1}$. Если $x = 0$, то соотношение (5) выполнено. Пусть теперь $x = p^s \tilde{x}$, где $\tilde{x}$ – некоторый обратимый элемент кольца R , а s – целое число из множества $\{0, \dots, n-1\}$. При $s = n-1$ получим следующие равенства:

$$\sum_{c \in R^*} \chi(cx) = \sum_{c \in R} \chi(cx) - \sum_{c \in pR} \chi(cx) = 0 - \sum_{c \in pR} \chi(cx) = - \sum_{c \in pR} \chi(0) = -|pR|.$$

Если же $s < n-1$, то

$$\sum_{c \in R^*} \chi(cx) = \sum_{c \in R} \chi(cx) - \sum_{c \in pR} \chi(cx) = - \sum_{c \in pR} \chi(cx),$$

и, используя представление (2) элементов кольца R и равенство (6), получим

$$\begin{aligned} \sum_{c \in R^*} \chi(cx) &= - \sum_{c_1, \dots, c_{n-1} \in \Gamma(R)} \chi((pc_1 + \dots + p^{n-1}c_{n-1})p^s \tilde{x}) \\ &= |\Gamma(R)|^s \sum_{c_1, \dots, c_{n-s-1} \in \Gamma(R)} \chi((p^{s+1}c_1 + \dots + p^{n-1}c_{n-s-1})\tilde{x}) \\ &= |\Gamma(R)|^s \sum_{c \in p^{s+1}R} \chi(c) = 0. \end{aligned}$$

Таким образом, равенства (5) доказаны.

Перейдем теперь к изучению тригонометрических сумм, связанных с соответствующими частотами появлений элементов в ЛРП.

§ 4. Оценки тригонометрических сумм

Рассмотрим многочлен $f(x)$ над кольцом Галуа $R = \text{GR}(q^n, p^n)$. Будем называть многочлен $f(x)$ *невырожденным*, если все его коэффициенты при мономах x^k , где k делится на p , равны нулю.

Используя p -адическое представление (2) элементов кольца R , многочлен $f(x)$ запишем в следующем виде:

$$f(x) = f_0(x) + pf_1(x) + \dots + p^{n-1}f_{n-1}(x),$$

где $f_i(x)$, $i = \overline{0, n-1}$, – многочлены с коэффициентами из множества $\Gamma(R)$. Пусть каждый из многочленов $f_i(x)$ имеет степень m_i . Назовем число

$$D = \max\{p^{n-1}m_0, p^{n-2}m_1, \dots, pm_{n-2}, m_{n-1}\}$$

взвешенной степенью многочлена $f(x)$.

Обозначим через χ характер аддитивной группы кольца R , определенный на элементах этого кольца равенством

$$\chi(x) = \exp\left\{2\pi i \frac{\text{Tr}_{R_0}^R(x)}{p^n}\right\}, \quad (7)$$

где $R_0 = \{0, e, 2e, \dots, (p^n - 1)e\}$. Пусть γ – произвольный образующий элемент группы $(\Gamma(R)^*, \cdot)$. Рассмотрим отображение ψ из кольца R в поле $\mathbb{C}$, задаваемое при всех $j = \overline{0, q-2}$ равенством

$$\psi(\gamma^j) = \exp\left\{2\pi i \frac{j}{q-1}\right\}. \quad (8)$$

УТВЕРЖДЕНИЕ 2 (см. [12]). Пусть $f(x)$ – невырожденный многочлен над кольцом $R = \text{GR}(q^n, p^n)$, имеющий взвешенную степень D , а отображения χ и ψ определены равенствами (7) и (8) соответственно. Тогда

$$\left| \sum_{x \in \Gamma(R)^*} \chi(f(x))(\psi(x))^a \right| \leq D\sqrt{q}, \quad a = \overline{0, q-2}.$$

Пусть $S = \text{GR}(q^{mn}, p^n)$ – расширение степени m кольца $R = \text{GR}(q^n, p^n)$. Группа S^* всех обратимых элементов кольца S раскладывается в прямое произведение своих подгрупп: $S^* = \Gamma(S)^*(e + pS)$. Каждый элемент α этой группы имеет порядок $\text{ord } \alpha$, причем $\text{ord } \alpha = p^\nu(q^m - 1)/d$, где d – некоторый делитель числа $q^m - 1$, $0 \leq \nu \leq n-1$. Для произвольного элемента b кольца S обозначим через $\|b\|$ наибольшее число $j \in \{0, \dots, n\}$ такое, что $b \in p^j S$. Величину $\|b\|$ будем называть *нормой элемента b* . Обозначим через χ' характер аддитивной группы кольца S , определенный на элементах этого кольца равенством

$$\chi'(y) = \chi(\text{Tr}_R^S(y)) = \exp\left\{2\pi i \frac{\text{Tr}_{R_0}^S(y)}{p^n}\right\}. \quad (9)$$

Характер χ' называют *поднятием характера χ на кольцо S* . Для каждого элемента a кольца $\mathbb{Z}_{\text{ord } \alpha}$ рассмотрим также отображение φ_a из кольца $\mathbb{Z}_{\text{ord } \alpha}$ в поле $\mathbb{C}$, определенное для всех $x \in \mathbb{Z}_{\text{ord } \alpha}$ равенством

$$\varphi_a(x) = \exp\left\{2\pi i \frac{ax}{\text{ord } \alpha}\right\}. \quad (10)$$

Каждое отображение φ_a является характером группы $(\mathbb{Z}_{\text{ord } \alpha}, +)$.

УТВЕРЖДЕНИЕ 3. Пусть α, b – элементы из кольца $S = \text{GR}(q^{mn}, p^n)$, $\alpha \in S^*$, $\text{ord } \alpha = p^\nu(q^m - 1)/d$, $b \neq 0$, $a = \overline{0, \text{ord } \alpha - 1}$. Тогда

$$\left| \sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j)\varphi_a(j) \right| \leq p^{n+\nu-\|b\|-1} q^{m/2}.$$

ДОКАЗАТЕЛЬСТВО. Разобьем множество $\{0, \dots, \text{ord } \alpha - 1\}$ на p^ν подмножеств следующего вида: $M_k = \{k + p^\nu s : s = \overline{0, (q^m - 1)/d - 1}\}$, $k = \overline{0, p^\nu - 1}$. Тогда

$$\sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j)\varphi_a(j) = \sum_{k=0}^{p^\nu - 1} \sum_{j \in M_k} \chi'(b\alpha^j)\varphi_a(j)$$

и, следовательно, справедливо неравенство

$$\left| \sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j) \varphi_a(j) \right| \leq p^\nu \max_{k=0, p^\nu-1} \left| \sum_{j \in M_k} \chi'(b\alpha^j) \varphi_a(j) \right|. \quad (11)$$

Оценим каждую из сумм

$$S_k = \sum_{j \in M_k} \chi'(b\alpha^j) \varphi_a(j), \quad k = \overline{0, p^\nu - 1}.$$

Представим элемент α в виде $\alpha = \alpha_1 \alpha_2$, где $\alpha_1 \in \Gamma(S)^*$, $\alpha_2 \in e + pS$. Тогда справедливы равенства

$$\begin{aligned} S_k &= \sum_{s=0}^{(q^m-1)/d-1} \chi'(b\alpha^{k+p^\nu s}) \varphi_a(k+p^\nu s) \\ &= \sum_{s=0}^{(q^m-1)/d-1} \chi'(b\alpha_1^{k+p^\nu s} \alpha_2^{k+p^\nu s}) \varphi_a(p^\nu s) \varphi_a(k). \end{aligned}$$

Учитывая, что $\text{ord } \alpha_1 = (q^m - 1)/d$, $\text{ord } \alpha_2 = p^\nu$ и $|\varphi_a(k)| = 1$, получим

$$|S_k| = \left| \sum_{s=0}^{(q^m-1)/d-1} \chi'(b\alpha^k (\alpha_1)^{p^\nu s}) \varphi_a(p^\nu s) \right|.$$

Пусть $\beta = \alpha_1^{p^\nu}$. В силу того, что $\text{ord } \beta = (q^m - 1)/d$, справедливо соотношение

$$|S_k| = \left| \sum_{s=0}^{\text{ord } \beta - 1} \chi'(b\alpha^k \beta^s) \exp\left\{ \frac{2\pi i a s}{\text{ord } \beta} \right\} \right|. \quad (12)$$

Обозначим через γ образующий элемент группы $(\Gamma(S)^*, \cdot)$. Так как $\text{ord } \gamma^d = \text{ord } \beta$, то найдется число $t \in \{0, \dots, \text{ord } \beta - 1\}$ такое, что $\beta^t = \gamma^d$, причем числа t и $\text{ord } \beta$ взаимно простые. Тогда $\{ts \pmod{\text{ord } \beta} : s \in \{0, \dots, \text{ord } \beta - 1\}\} = \{0, \dots, \text{ord } \beta - 1\}$. Учитывая этот факт и используя равенство (12), получим

$$|S_k| = \left| \sum_{s=0}^{\text{ord } \beta - 1} \chi'(b\alpha^k \beta^{ts}) \exp\left\{ \frac{2\pi i a t s}{\text{ord } \beta} \right\} \right| = \left| \sum_{s=0}^{\text{ord } \beta - 1} \chi'(b\alpha^k (\gamma^d)^s) \exp\left\{ \frac{2\pi i a t s}{\text{ord } \beta} \right\} \right|.$$

Пусть s' – произвольное число из множества $\{0, \dots, q^m - 2\}$, сравнимое с числом $s \in \{0, \dots, \text{ord } \beta - 1\}$ по модулю $\text{ord } \beta = \text{ord } \gamma^d$. Тогда

$$\chi'(b\alpha^k (\gamma^d)^{s'}) \exp\left\{ \frac{2\pi i a t s'}{\text{ord } \beta} \right\} = \chi'(b\alpha^k (\gamma^d)^s) \exp\left\{ \frac{2\pi i a t s}{\text{ord } \beta} \right\}$$

и, следовательно, справедливы следующие равенства:

$$\begin{aligned} |S_k| &= \left| \sum_{s=0}^{\text{ord } \beta - 1} \chi'(b\alpha^k (\gamma^d)^s) \exp\left\{ \frac{2\pi i a t s}{\text{ord } \beta} \right\} \right| \\ &= \frac{1}{d} \left| \sum_{s'=0}^{q^m-2} \chi'(b\alpha^k (\gamma^{s'})^d) \exp\left\{ \frac{2\pi i a t s'}{\text{ord } \beta} \right\} \right|. \end{aligned} \quad (13)$$

Рассмотрим многочлен $f(x) = b\alpha^k x^d$ над кольцом $S = \text{GR}(q^{mn}, p^n)$. Так как $\|b\alpha^k\| = \|b\|$, то взвешенная степень D многочлена $f(x)$ равна $dp^{n-\|b\| - 1}$. Кроме того, многочлен $f(x)$ является невырожденным. Определим отображение ψ' из множества $\Gamma(S)^*$ в поле $\mathbb{C}$ следующим равенством:

$$\psi'(\gamma^{s'}) = \exp\left\{2\pi i \frac{s'}{q^m - 1}\right\}, \quad s' = \overline{0, q^m - 2}.$$

Пусть $a' = atd \pmod{q^m - 1}$. Тогда, используя равенства (13) и утверждение 2, примененное к характеристам кольца S , получим

$$|S_k| = \frac{1}{d} \left| \sum_{x \in \Gamma(S)^*} \chi'(f(x)) (\psi'(x))^{a'} \right| \leq \frac{1}{d} dp^{n-\|b\| - 1} q^{m/2} = p^{n-\|b\| - 1} q^{m/2}.$$

В итоге, используя неравенства (11), имеем

$$\left| \sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j) \varphi_a(j) \right| \leq p^{n+\nu-\|b\| - 1} q^{m/2}.$$

ТЕОРЕМА 1. Пусть α, b – элементы кольца $S = \text{GR}(q^{mn}, p^n)$, $\alpha \in S^*$, $b \neq 0$, $\text{ord } \alpha = p^\nu(q^m - 1)/d$, $l \geq 0$ – целое число, $l \leq \text{ord } \alpha$, χ' – характер аддитивной группы кольца S , определенный равенством (9). Тогда

$$\left| \sum_{j=0}^{l-1} \chi'(b\alpha^j) \right| \leq p^{n+\nu-\|b\| - 1} \left(\frac{2}{\pi} \ln(\text{ord } \alpha) + \frac{7}{5} \right) q^{m/2}.$$

ДОКАЗАТЕЛЬСТВО. Пусть отображения φ_a определены равенством (10). Используя соотношения ортогональности для характеров, получим, что для всех $j, k \in \{0, \dots, \text{ord } \alpha - 1\}$ справедливы равенства

$$\sum_{a=0}^{\text{ord } \alpha - 1} \varphi_a(j - k) = \begin{cases} \text{ord } \alpha, & \text{если } j = k, \\ 0, & \text{если } j \neq k. \end{cases}$$

Используя эти равенства, получим соотношение

$$\sum_{i=0}^{l-1} \chi'(b\alpha^i) = \frac{1}{\text{ord } \alpha} \sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j) \sum_{k=0}^{l-1} \sum_{a=0}^{\text{ord } \alpha - 1} \varphi_a(j - k).$$

Изменяя в этом соотношении порядок суммирования и учитывая равенство $\varphi_a(j - k) = \varphi_a(j)\varphi_a(-k)$, получим

$$\sum_{j=0}^{l-1} \chi'(b\alpha^j) = \frac{1}{\text{ord } \alpha} \sum_{a=0}^{\text{ord } \alpha - 1} \left(\sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j) \varphi_a(j) \right) \left(\sum_{k=0}^{l-1} \varphi_a(-k) \right).$$

Отсюда легко следует, что

$$\left| \sum_{j=0}^{l-1} \chi'(b\alpha^j) \right| \leq \frac{1}{\text{ord } \alpha} \sum_{a=0}^{\text{ord } \alpha - 1} \left| \sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j) \varphi_a(j) \right| \left| \sum_{k=0}^{l-1} \varphi_a(-k) \right|.$$

Согласно утверждению 3 справедливо соотношение

$$\left| \sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j) \varphi_a(j) \right| \leq p^{n+\nu-\|b\|-1} q^{m/2},$$

а в силу неравенства (8.35) из работы [21] верна оценка

$$\sum_{a=0}^{\text{ord } \alpha - 1} \left| \sum_{k=0}^{l-1} \varphi_a(-k) \right| \leq \left(\frac{2}{\pi} \ln(\text{ord } \alpha) + \frac{7}{5} \right) \text{ord } \alpha.$$

Таким образом, имеет место неравенство

$$\left| \sum_{j=0}^{l-1} \chi'(b\alpha^j) \right| \leq p^{n+\nu-\|b\|-1} \left(\frac{2}{\pi} \ln(\text{ord } \alpha) + \frac{7}{5} \right) q^{m/2}.$$

Оценка из теоремы 1 может быть уточнена в случае, когда значение l совпадает с числом $\text{ord } \alpha$, а именно, имеет место следующая

ТЕОРЕМА 2 (см. [11; теорема 2.1]). Пусть α , b – элементы кольца $S = \text{GR}(q^{mn}, p^n)$, $\alpha \in S^*$, $b \neq 0$, $\text{ord } \alpha = p^\nu(q^m - 1)/d$, $0 \leq \nu \leq n - 1$, а d – делитель числа $q^m - 1$. Тогда

$$\left| \sum_{j=0}^{\text{ord } \alpha - 1} \chi'(b\alpha^j) + \frac{p^\nu}{d} \right| \leq \frac{p^\nu(dp^{n-\|b\|-1} - 1)}{d} q^{m/2}.$$

Заметим, что ранее в [11] в формулировке этой теоремы было указано условие $m > 1$, которое не использовалось в соответствующем доказательстве. В этом доказательстве использовалось лишь то, что α является обратимым элементом, поэтому приведенная оценка остается справедливой и при $m = 1$.

§ 5. Оценки числа появлений наборов на отрезках ЛРП векторов

Рассмотрим произвольные последовательности $u_1, u_2, \dots, u_r$ над кольцом $R = \text{GR}(q^n, p^n)$. Напомним, что эти последовательности называются *линейно независимыми над кольцом R* , если для всех ненулевых векторов $\bar{c} = (c_1, c_2, \dots, c_r) \in R^r$ последовательность $c_1 u_1 + c_2 u_2 + \dots + c_r u_r$ является ненулевой. Рассмотрим естественный эпиморфизм φ из кольца R в факторкольцо $R/pR = \text{GF}(q)$. Для произвольной последовательности u элементов кольца R обозначим через $\bar{u}$ последовательность над полем $\text{GF}(q)$, элементы которой определены равенствами $\bar{u}(i) = \varphi(u(i))$, $i \geq 0$. Несложно проверить, что последовательности $u_1, u_2, \dots, u_r$ линейно независимы над кольцом R только тогда, когда последовательности $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_r$ линейно независимы над полем $\text{GF}(q)$. Кроме того, если u – ЛРП над кольцом R с характеристическим многочленом $F(x)$, то последовательность $\bar{u}$ является ЛРП над полем $\bar{R}$ с характеристическим многочленом $\bar{F}(x)$, который есть образ многочлена $F(x)$ при действии естественного эпиморфизма из кольца $R[x]$ в кольцо $\bar{R}[x]$. В случае, когда

$u_1, u_2, \dots, u_r$ – линейно независимая система ЛРП над кольцом R , получим, что $r \leq m$, где m – степень многочлена $F(x)$. Более того, все рассматриваемые последовательности будут принадлежать множеству $L_R(F)^*$, состоящему из всех ЛРП над кольцом R с характеристическим многочленом $F(x)$, у которых в начальном векторе есть хотя бы один обратимый элемент кольца R .

Перейдем к оценкам частот $N_l(\bar{z}, u_1, \dots, u_r)$ появления набора $\bar{z} = (z_1, z_2, \dots, z_r) \in R^r$ среди векторов $(u_1(i), u_2(i), \dots, u_r(i))$, $i = \overline{0, l-1}$.

ТЕОРЕМА 3. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, $T(F) = p^\nu T(\bar{F})$, $u_1, u_2, \dots, u_r$ – линейно независимая система ЛРП над кольцом R с характеристическим многочленом $F(x)$. Тогда для всех $\bar{z} \in R^r$ и всех $l \in \mathbb{N}$ таких, что $l \leq T(F)$, справедлива оценка

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{p^\nu (p^n q^{rn} - 1)(q^r - 1)}{(pq^r - 1)q^{nr}} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right) q^{m/2}. \quad (14)$$

ДОКАЗАТЕЛЬСТВО. Используя равенства (4), величину $N_l(\bar{z}, u_1, \dots, u_r)$ представим в виде

$$N_l(\bar{z}, u_1, \dots, u_r) = \sum_{i=0}^{l-1} \prod_{j=1}^r \frac{1}{q^n} \sum_{c_j \in R} \chi(c_j(u_j(i) - z_j)),$$

где $\chi = \chi_e$. Тогда справедливо соотношение

$$N_l(\bar{z}, u_1, \dots, u_r) = \frac{1}{q^{nr}} \sum_{i=0}^{l-1} \sum_{(c_1, c_2, \dots, c_r) \in R^r} \chi\left(-\sum_{j=1}^r c_j z_j\right) \chi\left(\sum_{j=1}^r c_j u_j(i)\right). \quad (15)$$

Для каждого вектора $\bar{c} = (c_1, c_2, \dots, c_r)$ обозначим через $u_{\bar{c}}$ последовательность элементов кольца R , определенную равенством

$$u_{\bar{c}}(i) = \sum_{j=1}^r c_j u_j(i), \quad i \geq 0, \quad (16)$$

а также введем обозначение $\bar{c}\bar{z} = (c_1, \dots, c_r)(z_1, \dots, z_r) = c_1 z_1 + \dots + c_r z_r$. В равенстве (15) выделим отдельно слагаемое, соответствующее нулевому набору $(c_1, c_2, \dots, c_r)$, и поменяем порядок суммирования. Тогда получим следующее соотношение:

$$N_l(\bar{z}, u_1, \dots, u_r) = \frac{l}{q^{nr}} + \frac{1}{q^{nr}} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \sum_{i=0}^{l-1} \chi(-\bar{c}\bar{z}) \chi(u_{\bar{c}}(i)). \quad (17)$$

Из этого соотношения и равенства $|\chi(x)| = 1$, справедливого для всех $x \in R$, следует неравенство

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{1}{q^{nr}} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \left| \sum_{i=0}^{l-1} \chi(u_{\bar{c}}(i)) \right|. \quad (18)$$

Представим ЛРП u_k , используя функцию след из кольца $S = \text{GR}(q^{mn}, p^n)$ в кольцо R , следующим образом:

$$u_k(i) = \text{Tr}_R^S(b_k \alpha^i), \quad i \geq 0,$$

где b_k , $k = \overline{1, r}$, – обратимый элемент кольца S , а α – корень многочлена $F(x)$ в кольце S . Тогда представление ЛРП $u_{\bar{c}}$ будет иметь следующий вид:

$$u_{\bar{c}}(i) = \text{Tr}_R^S((c_1 b_1 + \dots + c_r b_r) \alpha^i), \quad i \geq 0. \quad (19)$$

Напомним, что *нормой* $\|c\|$ элемента $c \in R$ называется наибольшее число i из множества $\{0, \dots, n\}$ такое, что $c \in p^i R$. Определим норму $\|\bar{c}\|$ вектора $\bar{c} = (c_1, \dots, c_r) \in R^r$ по правилу $\|\bar{c}\| = \min_{i=\overline{1, r}} \|c_i\|$. Покажем, что при условиях доказываемой теоремы для всех $\bar{c} \in R^r$ справедливо равенство $\|c_1 b_1 + \dots + c_r b_r\| = \|\bar{c}\|$. Ясно, что $\|c_1 b_1 + \dots + c_r b_r\| \geq \|\bar{c}\|$. Так как система $u_1, u_2, \dots, u_r$ линейно независима над кольцом R , то, учитывая равенство (19), получим, что система $b_1, b_2, \dots, b_r$ элементов кольца S линейно независима над кольцом R . Допустим, что $\|c_1 b_1 + \dots + c_r b_r\| > \|\bar{c}\|$. Тогда $\|\bar{c}\| = t$, $0 \leq t \leq n-1$. Представим элемент c_k в виде $c_k = p^t \tilde{c}_k$, $1 \leq k \leq r$. Так как $\|\bar{c}\| = t$, то найдется число $j \in \{1, \dots, r\}$ такое, что элемент $\tilde{c}_j$ обратим в кольце R . Тогда получим соотношения $\|c_1 b_1 + \dots + c_r b_r\| = t + \|\tilde{c}_1 b_1 + \dots + \tilde{c}_r b_r\| > t$. Следовательно, элемент $\tilde{c}_1 b_1 + \dots + \tilde{c}_r b_r$ принадлежит множеству pS . Тогда справедливо равенство $p^{n-1} \tilde{c}_1 b_1 + \dots + p^{n-1} \tilde{c}_r b_r = 0$, причем $p^{n-1} \tilde{c}_j \neq 0$. Это противоречит линейной независимости системы $b_1, \dots, b_r$. В итоге при всех $\bar{c} \in R^r$ справедливо равенство $\|c_1 b_1 + \dots + c_r b_r\| = \|\bar{c}\|$. Используя (18), получим

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{1}{q^{nr}} \sum_{t=0}^{n-1} \sum_{\bar{c} \in R^r, \|\bar{c}\|=t} \left| \sum_{i=0}^{l-1} \chi'((b_1 c_1 + \dots + b_r c_r) \alpha^i) \right|,$$

где χ' – характер аддитивной группы кольца S , определенный на элементах этого кольца равенством (9). В силу реверсивности многочлена $F(x)$ корень α этого многочлена обратим в кольце S , а так как $F(x)$ – многочлен Галуа, то $\text{ord } \alpha = T(F)$. Применяя далее теорему 1, получим

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{1}{q^{nr}} \sum_{t=0}^{n-1} \sum_{\bar{c} \in R^r, \|\bar{c}\|=t} p^{n+\nu-t-1} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right) q^{m/2}. \quad (20)$$

Вектор $\bar{c} \in R^r$ имеет норму t только тогда, когда он принадлежит множеству $(p^t R)^r \setminus (p^{t+1} R)^r$. Число таких векторов равно $|p^t R|^r - |p^{t+1} R|^r = q^{(n-t-1)r} (q^r - 1)$. Используя неравенство (20), получим

$$\begin{aligned} & \left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \\ & \leq \frac{1}{q^{nr}} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right) q^{m/2 + (n-1)r} p^{n+\nu-1} (q^r - 1) \sum_{t=0}^{n-1} q^{-tr} p^{-t}. \end{aligned}$$

Таким образом, доказана справедливость оценки

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{p^\nu (p^n q^{rn} - 1)(q^r - 1)}{(pq^r - 1)q^{nr}} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right) q^{m/2}.$$

Отметим, что в случае $n = 1$, т.е. когда кольцо R является полем $\text{GF}(q)$, оценка из теоремы 3 совпадает с оценкой, полученной в теореме 2 работы [4]. Таким образом, оценка из теоремы 3 обобщает указанный результат на случай произвольного кольца Галуа R . Величина l/q^{nr} представляет собой “естественное” среднее значение для числа появлений вектора $\bar{z}$ на отрезке длины l последовательности векторов. Таким образом, теорема 3 устанавливает верхнюю оценку отклонения частоты $N_l(\bar{z}, u_1, \dots, u_r)$ от “естественного” среднего значения. Приведем более простую, но менее точную оценку.

СЛЕДСТВИЕ 1. Пусть выполнены условия теоремы 3. Тогда

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right) q^{m/2}. \quad (21)$$

ДОКАЗАТЕЛЬСТВО. Достаточно воспользоваться неравенством (18) и оценкой

$$\left| \sum_{i=0}^{l-1} \chi(u_{\bar{c}}(i)) \right| = \left| \sum_{i=0}^{l-1} \chi'((c_1 b_1 + \dots + c_r b_r) \alpha^i) \right| \leq p^{n+\nu-1} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right) q^{m/2},$$

которая согласно теореме 1 справедлива для всех векторов $(c_1, \dots, c_r) \in R^r \setminus \{\bar{0}\}$.

Приведем теперь условие, при котором на отрезках ЛРП векторов появится любой набор из множества R^r .

СЛЕДСТВИЕ 2. Пусть выполнены условия теоремы 3 и число l удовлетворяет неравенству

$$l > (q^{nr} - 1) p^{n+\nu-1} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right) q^{m/2}. \quad (22)$$

Тогда среди наборов $(u_1(i), u_2(i), \dots, u_r(i))$, $i = \overline{0, l-1}$, появятся все векторы $\bar{z} \in R^r$.

ДОКАЗАТЕЛЬСТВО. Согласно следствию 1 выполнено следующее соотношение:

$$N_l(\bar{z}, u_1, \dots, u_r) \geq \frac{l}{q^{nr}} - \frac{q^{nr} - 1}{q^{nr}} p^{n+\nu-1} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right) q^{m/2}.$$

При условии

$$l > (q^{nr} - 1) p^{n+\nu-1} \left(\left(\frac{2}{\pi} \right) \ln T(F) + \frac{7}{5} \right) q^{m/2}$$

правая часть этого неравенства больше нуля и, следовательно, набор $\bar{z}$ появится в ЛРП векторов среди первых ее l элементов.

Из неравенства (21) можно получить верхнюю и нижнюю оценки частоты $N_l(\bar{z}, u_1, \dots, u_r)$. Как показано в следствии 2, при выполнении условия (22) нижняя оценка будет нетривиальной. Несложно проверить, что при этом условии верхняя оценка также является нетривиальной, т.е. меньше l . Таким образом, условие (22) гарантирует нетривиальность оценки (21) и, следовательно, и более точной оценки (14). В § 6 будет доказано, что эти оценки являются асимптотически неулучшаемыми.

§ 6. Нижняя оценка отклонения частот появления элементов от среднего значения

Пусть $F(x)$ – реверсивный многочлен Галуа над кольцом $R = \text{GR}(q^n, p^n)$, u – ЛРП над кольцом R с характеристическим многочленом $F(x)$, $\bar{s} = (s_1, s_2, \dots, s_r)$ – упорядоченный набор целых неотрицательных чисел. Рассмотрим величину $N_l(\bar{z}, \bar{s}, u) = N_l(\bar{z}, x^{s_1}u, \dots, x^{s_r}u)$, которая равна количеству появлений набора $\bar{z} \in R^r$ среди векторов вида $(u(i + s_1), \dots, u(i + s_r))$, $i = \overline{0, l-1}$. Пусть α – корень многочлена $F(x)$ в кольце $S = \text{GR}(q^{mn}, q^n)$. Будем считать, что набор $\bar{s}$ подобран так, что система $\alpha^{s_1}, \dots, \alpha^{s_r}$ линейно независима над кольцом R . В этом случае система последовательностей $x^{s_1}u, \dots, x^{s_r}u$ линейно независима над кольцом R и для частоты $N_l(\bar{z}, \bar{s}, u)$ справедливы оценки, полученные в теореме 3 и следствии 1.

Найдем среднее значение величины $|N_l(\bar{z}, \bar{s}, u) - l/q^{nr}|^2$ в случае, когда u пробегает все множество $L_R(F)^*$ линейных рекуррентных последовательностей над кольцом R с характеристическим многочленом $F(x)$, у которых в начальном векторе есть хотя бы один обратимый элемент кольца R , а $\bar{z} \in R^r$.

ТЕОРЕМА 4. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, α – корень многочлена $F(x)$ в кольце $S = \text{GR}(q^{mn}, q^n)$ и набор $\bar{s} = (s_1, s_2, \dots, s_r) \in \mathbb{N}_0^r$ подобран так, что система $\alpha^{s_1}, \dots, \alpha^{s_r}$ линейно независима над кольцом R . Тогда при каждом натуральном числе $l \leq T(\bar{F})$ справедливо равенство

$$\begin{aligned} & \frac{1}{|R|^r |L_R(F)^*|} \sum_{\bar{z} \in R^r} \sum_{u \in L_R(F)^*} \left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right|^2 \\ &= l \frac{(q^{nr} - 1)(q^m - 1) - (q^r - 1)(l - 1)}{q^{2nr}(q^m - 1)}. \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Введем обозначение

$$S_l(\bar{z}, \bar{s}, u) = \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \chi(-\bar{c}\bar{z}) \sum_{i=0}^{l-1} \chi(u_{\bar{c}}(i)),$$

где $\bar{c}\bar{z} = (c_1, \dots, c_r)(z_1, \dots, z_r) = c_1 z_1 + \dots + c_r z_r$, χ – характер аддитивной группы кольца R , определенный в (7), а последовательность $u_{\bar{c}}$ определена равенством

$$u_{\bar{c}}(i) = \sum_{j=1}^r c_j u(i + s_j), \quad i \geq 0.$$

Согласно (17) справедливо соотношение

$$\left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right| = \frac{1}{q^{nr}} |S_l(\bar{z}, \bar{s}, u)|.$$

Найдем сумму

$$\Delta = \sum_{\bar{z} \in R^r} \sum_{u \in L_R(F)^*} |S_l(\bar{z}, \bar{s}, u)|^2 = \sum_{\bar{z} \in R} \sum_{u \in L_R(F)^*} S_l(\bar{z}, \bar{s}, u) \overline{S_l(\bar{z}, \bar{s}, u)}, \quad (23)$$

где величина $\overline{S_l(\bar{z}, \bar{s}, u)}$ является комплексно сопряженной к величине $S_l(\bar{z}, \bar{s}, u)$. Тогда

$$\frac{1}{|R|^r |L_R(F)^*|} \sum_{\bar{z} \in R^r} \sum_{u \in L_R(F)^*} \left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right|^2 = \frac{\Delta}{q^{2nr} |R|^r |L_R(F)^*|}. \quad (24)$$

Используя соотношение (23) и равенство $\overline{\chi(x)} = \chi(-x)$, справедливое для всех $x \in R$, имеем

$$\Delta = \sum_{\bar{z} \in R^r} \sum_{u \in L_R(F)^*} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \sum_{\bar{d} \in R^r \setminus \{\bar{0}\}} \chi(-\bar{c}\bar{z}) \chi(\bar{d}\bar{z}) \sum_{i,j=0}^{l-1} \chi(u_{\bar{c}}(i)) \chi(-u_{\bar{d}}(j)).$$

Следовательно, изменив порядок суммирования и воспользовавшись свойствами характеров, получим

$$\Delta = \sum_{u \in L_R(F)^*} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \sum_{\bar{d} \in R^r \setminus \{\bar{0}\}} \sum_{i,j=0}^{l-1} \chi(u_{\bar{c}}(i) - u_{\bar{d}}(j)) \sum_{\bar{z} \in R^r} \chi((\bar{d} - \bar{c})\bar{z}).$$

Пусть $\bar{d} - \bar{c} = \bar{a} = (a_1, \dots, a_r)$, $\bar{z} = (z_1, \dots, z_r)$. Используя равенства (4), заключаем, что

$$\begin{aligned} \sum_{\bar{z} \in R^r} \chi((\bar{d} - \bar{c})\bar{z}) &= \sum_{\bar{z} \in R^r} \chi(\bar{a}\bar{z}) = \sum_{z_1 \in R} \chi(a_1 z_1) \cdots \sum_{z_r \in R} \chi(a_r z_r) \\ &= \begin{cases} |R|^r, & \text{если } \bar{d} = \bar{c}, \\ 0, & \text{если } \bar{d} \neq \bar{c}. \end{cases} \end{aligned}$$

Тогда

$$\Delta = q^{nr} \sum_{u \in L_R(F)^*} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \sum_{i,j=0}^{l-1} \chi(u_{\bar{c}}(i) - u_{\bar{c}}(j)). \quad (25)$$

Для каждой ЛРП $u \in L_R(F)^*$ найдется однозначно определенный элемент $b \in S^*$ такой, что имеет место равенство (3). Тогда в силу линейности функции Tr_R^S получим

$$\chi(u_{\bar{c}}(i) - u_{\bar{c}}(j)) = \chi(\text{Tr}_R^S(b(c_1 \alpha^{s_1} + \cdots + c_r \alpha^{s_r})(\alpha^i - \alpha^j))),$$

где α – корень многочлена $F(x)$ в кольце $S = \text{GR}(q^{mn}, q^n)$. Пусть χ' – аддитивный характер кольца S , определенный равенством $\chi'(y) = \chi(\text{Tr}_R^S(y))$. Так

как между ЛРП из множества $L_R(F)^*$ и обратимыми элементами кольца S существует взаимно однозначное соответствие, то из (25) имеем

$$\Delta = q^{nr} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \sum_{i,j=0}^{l-1} \sum_{b \in S^*} \chi'(b(c_1 \alpha^{s_1} + \dots + c_r \alpha^{s_r})(\alpha^i - \alpha^j)). \quad (26)$$

Заметим, что при всех различных числах i, j из множества $\{0, \dots, T(\bar{F}) - 1\}$ элемент $\alpha^i - \alpha^j$ является обратимым элементом кольца S . При доказательстве теоремы 3 было показано, что в силу линейной независимости системы $\alpha^{s_1}, \dots, \alpha^{s_r}$ над кольцом R для всех векторов $\bar{c} = (c_1, \dots, c_r) \in R^r$ справедливы равенства

$$\|\bar{c}\| = \|c_1 \alpha^{s_1} + \dots + c_r \alpha^{s_r}\| = \|b(c_1 \alpha^{s_1} + \dots + c_r \alpha^{s_r})(\alpha^i - \alpha^j)\|.$$

В силу соотношения (5) имеем

$$\sum_{b \in S^*} \chi'(b(c_1 \alpha^{s_1} + \dots + c_r \alpha^{s_r})(\alpha^i - \alpha^j)) = \begin{cases} |S^*|, & \text{если } i = j, \\ -|pS|, & \text{если } i \neq j, \|\bar{c}\| = n - 1, \\ 0, & \text{если } i \neq j, \|\bar{c}\| < n - 1. \end{cases}$$

Используя равенство (26) и тот факт, что количество векторов $\bar{c} \in R^r$, имеющих норму $n - 1$, равно $q^r - 1$, получим

$$\begin{aligned} \Delta &= q^{nr} \sum_{\bar{c} \neq \bar{0}} \sum_{i=0}^{l-1} |S^*| + q^{nr} \sum_{\|\bar{c}\|=n-1} \sum_{i \neq j} (-|pS|) \\ &= q^{nr} (q^{nr} - 1)l|S^*| - q^{nr} (q^r - 1)l(l-1)|pS|. \end{aligned}$$

Так как $|S^*| = q^{m(n-1)}(q^m - 1)$, а $|pS| = q^{m(n-1)}$, то

$$\Delta = q^{nr} l q^{m(n-1)} ((q^{nr} - 1)(q^m - 1) - (q^r - 1)(l - 1)).$$

Воспользовавшись равенством (24) и соотношением $|L_R(F)^*| = |S^*|$, окончательно получим

$$\begin{aligned} &\frac{1}{|R|^r |L_R(F)^*|} \sum_{\bar{z} \in R^r} \sum_{u \in L_R(F)^*} \left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right|^2 \\ &= l \frac{(q^{nr} - 1)(q^m - 1) - (q^r - 1)(l - 1)}{q^{2nr}(q^m - 1)}. \end{aligned}$$

Выведем теперь нижнюю оценку модуля отклонения числа появлений наборов в ЛРП векторов от “естественного” среднего значения.

СЛЕДСТВИЕ 3. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, α – корень многочлена $F(x)$ в кольце $S = \text{GR}(q^{mn}, p^n)$, набор $\bar{s} = (s_1, s_2, \dots, s_r) \in \mathbb{N}_0^r$ подобран так, что система $\alpha^{s_1}, \dots, \alpha^{s_r}$ линейно независима над кольцом R . Тогда при любом фиксированном значении $l \leq T(\bar{F})$ найдутся ЛРП $u \in L_R(F)^*$ и набор $\bar{z} \in R^r$ такие, что

$$\left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right| \geq l^{1/2} \left(\frac{(1 - q^{-nr})(q^m - l)}{q^{nr}(q^m - 1)} \right)^{1/2}. \quad (27)$$

ДОКАЗАТЕЛЬСТВО. Заметим, что

$$(q^{nr} - 1)(q^m - 1) - (q^r - 1)(l - 1) \geq (q^{nr} - 1)(q^m - l).$$

Тогда согласно теореме 4 получим неравенство

$$\frac{1}{|R|^r |L_R(F)^*|} \sum_{\bar{z} \in R^r} \sum_{u \in L_R(F)^*} \left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right|^2 \geq l \frac{(q^{nr} - 1)(q^m - l)}{q^{2nr}(q^m - 1)}.$$

Следовательно, найдутся ЛРП $u \in L_R(F)^*$ и набор $\bar{z} \in R^r$ такие, что

$$\left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right|^2 \geq l \frac{(q^{nr} - 1)(q^m - l)}{q^{2nr}(q^m - 1)}.$$

Извлекая квадратный корень из обеих частей этого неравенства, получим

$$\left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right| \geq l^{1/2} \left(\frac{(1 - q^{-nr})(q^m - l)}{q^{nr}(q^m - 1)} \right)^{1/2}.$$

Пусть выполнены условия следствия 3. Рассмотрим многочлен $F(x)$, имеющий период $T(F) = p^\nu(q^m - 1)$, и отрезок длины $l = [(q^m + 1)/2]$. Тогда, используя оценку (27), получим, что найдутся ЛРП $u \in L_R(F)^*$ и набор $\bar{z} \in R^r$, удовлетворяющие соотношению

$$\left| N_l(\bar{z}, \bar{s}, u) - \frac{l}{q^{nr}} \right| > \left(\frac{q^m}{2} \right)^{1/2} \left(\frac{(1 - q^{-nr})(q^m - 1)/2}{q^{nr}(q^m - 1)} \right)^{1/2} = \frac{(q^{nr} - 1)^{1/2}}{2q^{nr}} q^{m/2}.$$

Это неравенство показывает, что оценки (14) и (21), рассматриваемые для модуля отклонения частоты $N_l(\bar{z}, \bar{s}, u)$ от “естественной” средней величины, являются асимптотически неулучшаемыми. В этих оценках сомножитель $q^{m/2}$ нельзя заменить на показательную функцию (от переменной m) с меньшим основанием степени.

§ 7. Уточнение оценок в случае частот появлений наборов на циклах ЛРП векторов

Уточним теперь оценки величины $N_l(\bar{z}, u_1, \dots, u_r)$ для случая, когда длина l отрезка равна периоду последовательностей. Рассмотрим реверсивный многочлен Галуа $F(x)$ степени m над кольцом $R = \text{GR}(q^n, p^n)$. Пусть ЛРП $u_1, u_2, \dots, u_r$ выбраны из множества $L_R(F)^*$ всех ЛРП над кольцом R с характеристическим многочленом $F(x)$, у которых в начальном векторе есть хотя бы один обратимый элемент кольца R . В этом случае $u_1, u_2, \dots, u_r$ будут чисто периодическими последовательностями с одинаковым периодом T , который совпадает с периодом $T(F)$ многочлена $F(x)$, причем $T(F) = p^\nu(q^m - 1)/d$, $\nu = \overline{0, n-1}$, а d – делитель числа $q^m - 1$. Обозначим через $N(\bar{z}, u_1, \dots, u_r)$ величину $N_T(\bar{z}, u_1, \dots, u_r)$, равную количеству появлений r -граммы $\bar{z} \in R^r$ среди r -грамм $(u_1(i), u_2(i), \dots, u_r(i))$, $i = \overline{0, T-1}$.

Рассмотрим величину $\omega(\bar{z})$, определенную так:

$$\omega(\bar{z}) = \begin{cases} \frac{q^{m-nr} - 1}{q^m - 1} T, & \text{если } \bar{z} = \bar{0}, \\ \frac{q^{m-nr}}{q^m - 1} T, & \text{если } \bar{z} \neq \bar{0}. \end{cases}$$

Эта величина близка к “естественному” среднему значению T/q^{nr} для частоты $N(\bar{z}, u_1, \dots, u_r)$ (точнее, при всех наборах $\bar{z}$ справедливо неравенство $|T/q^{nr} - \omega(\bar{z})| < p^\nu/d$). Оценка отклонения числа появлений элементов в ЛРП векторов от величины $\omega(\bar{z})$ приведена в следующей теореме.

ТЕОРЕМА 5. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = \text{GR}(q^n, p^n)$, имеющий период $T = p^\nu(q^m - 1)/d$, $u_1, u_2, \dots, u_r$ – линейно независимая система ЛРП над кольцом R с характеристическим многочленом $F(x)$. Тогда для всех наборов $\bar{z} \in R^r$ справедливо неравенство

$$|N(\bar{z}, u_1, \dots, u_r) - \omega(\bar{z})| \leq \frac{p^\nu((q^{nr}p^n - 1)(q^r - 1)d - (q^r p - 1)(q^{nr} - 1))}{q^{nr}d(q^r p - 1)} q^{m/2}. \quad (28)$$

ДОКАЗАТЕЛЬСТВО. Используя равенства (17), величину $N(\bar{z}, u_1, \dots, u_r)$ представим в виде

$$N(\bar{z}, u_1, \dots, u_r) = \frac{T}{q^{nr}} + \frac{1}{q^{nr}} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \chi(-\bar{c}\bar{z}) \sum_{i=0}^{T-1} \chi(u_{\bar{c}}(i)).$$

Пусть

$$\sigma(u_{\bar{c}}) = \sum_{i=0}^{T-1} \chi(u_{\bar{c}}(i)).$$

Тогда

$$N(\bar{z}, u_1, \dots, u_r) - \frac{T}{q^{nr}} = \frac{1}{q^{nr}} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \chi(-\bar{c}\bar{z}) \sigma(u_{\bar{c}}). \quad (29)$$

Прибавим к обеим частям равенства (29) величину

$$\delta(\bar{z}) = \frac{p^\nu}{q^{nr}d} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \chi(-\bar{c}\bar{z}).$$

Тогда получим, что

$$N(\bar{z}, u_1, \dots, u_r) - \frac{T}{q^{nr}} + \delta(\bar{z}) = \frac{1}{q^{nr}} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \chi(-\bar{c}\bar{z}) \left(\sigma(u_{\bar{c}}) + \frac{p^\nu}{d} \right).$$

Из соотношения (4) имеем

$$\delta(\bar{z}) = \frac{p^\nu}{q^{nr}d} \left(\prod_{j=1}^r \sum_{c_j \in R} \chi(c_j z_j) - 1 \right) = \begin{cases} \frac{(q^{nr} - 1)p^\nu}{q^{nr}d}, & \text{если } \bar{z} = \bar{0}, \\ -\frac{p^\nu}{q^{nr}d}, & \text{если } \bar{z} \neq \bar{0}. \end{cases}$$

Отсюда и из равенства $T = T(F) = (q^m - 1)p^\nu/d$ получаем, что $T/q^{nr} - \delta(\bar{z}) = \omega(\bar{z})$. Таким образом, справедливо неравенство

$$|N(\bar{z}, u_1, \dots, u_r) - \omega(\bar{z})| \leq \frac{1}{q^{nr}} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \left| \sigma(u_{\bar{c}}) + \frac{p^\nu}{d} \right|. \quad (30)$$

Как показано в доказательстве теоремы 3, последовательность $u_{\bar{c}}$ имеет следующее представление:

$$u_{\bar{c}}(i) = \text{Tr}_R^S((c_1 b_1 + \dots + c_r b_r) \alpha^i), \quad i \geq 0.$$

Тогда, используя соотношения (30), получим

$$|N(\bar{z}, u_1, \dots, u_r) - \omega(\bar{z})| \leq \frac{1}{q^{nr}} \sum_{t=0}^{n-1} \sum_{\bar{c} \in R^r, \|\bar{c}\|=t} \left| \sum_{i=0}^{T-1} \chi'((c_1 b_1 + \dots + c_r b_r) \alpha^i) + \frac{p^\nu}{d} \right|.$$

В силу линейной независимости системы $u_1, \dots, u_r$ над кольцом R для всех векторов $\bar{c} \in R^r$ справедливо равенство $\|\bar{c}\| = \|c_1 b_1 + \dots + c_r b_r\|$. В силу теоремы 2 имеем

$$|N(\bar{z}, u_1, \dots, u_r) - \omega(\bar{z})| \leq \frac{1}{q^{nr}} \sum_{t=0}^{n-1} \sum_{\bar{c} \in R^r, \|\bar{c}\|=t} \frac{p^\nu (dp^{n-t-1} - 1)}{d} q^{m/2}.$$

Остается заметить, что правая часть этого неравенства равна

$$\frac{p^\nu ((q^{nr} p^n - 1)(q^r - 1)d - (q^r p - 1)(q^{nr} - 1))}{q^{nr} d (q^r p - 1)} q^{m/2}.$$

Ранее в [11] результат теоремы 5 был получен лишь для случая, когда последовательности $u_1, u_2, \dots, u_r$ являются сдвигами одной и той же ЛРП. Похожие оценки были получены в [22], где исследовались частотные характеристики некоторых последовательностей матриц над кольцами Галуа.

Заметим, что если $u_1, u_2, \dots, u_r$ – ЛРП максимального периода над полем $R = \text{GF}(q)$, то правая часть неравенства (28) обращается в нуль и мы получаем известные точные значения частот появления r -грамм на цикле ЛРП векторов. Как следует из результатов работ [23]–[25], при $r = 1$ оценка (28) достижима для ЛРП над кольцом $R = \mathbb{Z}_4$ при всех четных значениях m .

Более простая оценка исследуемого отклонения приведена в следствии 4.

СЛЕДСТВИЕ 4. Пусть выполнены условия теоремы 5. Тогда

$$|N(\bar{z}, u_1, \dots, u_r) - \omega(\bar{z})| \leq \frac{p^\nu (q^{nr} - 1)(dp^{n-1} - 1)}{q^{nr} d} q^{m/2}. \quad (31)$$

ДОКАЗАТЕЛЬСТВО. Достаточно воспользоваться неравенством (30) и оценкой

$$\left| \sigma(u_{\bar{c}}) + \frac{p^\nu}{d} \right| \leq \frac{p^\nu (dp^{n-1} - 1)}{d} q^{m/2},$$

которая согласно теореме 2 справедлива для всех векторов $(c_1, \dots, c_r) \in R^r \setminus \{\bar{0}\}$.

Приведем теперь условие, при котором в ЛРП векторов появится любой набор из множества R^r .

СЛЕДСТВИЕ 5. Пусть выполнены условия теоремы 5, а также следующее неравенство:

$$T(\overline{F}) \geq p^{n-1}(q^{nr} - 1)q^{m/2}.$$

Тогда среди r -грамм $(u_1(i), u_2(i), \dots, u_r(i))$, $i = \overline{0, T-1}$, появятся все r -граммы из множества R^r .

ДОКАЗАТЕЛЬСТВО. Так как

$$\omega(\bar{z}) \geq \frac{(q^{m-nr} - 1)T(u)}{q^m - 1},$$

то, используя соотношение (31), получим, что для любой r -граммы $\bar{z} \in R^r$ справедливо неравенство

$$N(\bar{z}, u_1, \dots, u_r) \geq \frac{q^{m-nr} - 1}{q^m - 1} T(u) - \frac{p^\nu(q^{nr} - 1)(dp^{n-1} - 1)}{q^{nr}d} q^{m/2}. \quad (32)$$

Для завершения доказательства остается заметить, что при условии $T(\overline{F}) \geq p^{n-1}(q^{nr} - 1)q^{m/2}$ правая часть неравенства (32) больше нуля.

Из формул (28) и (31) следуют верхняя и нижняя оценки частот $N(\bar{z}, u_1, \dots, u_r)$. Эти оценки существенно уточняют оценки, полученные в предыдущих параграфах для части периода последовательности. В силу следствия 5 при условии $T(\overline{F}) \geq p^{n-1}(q^{nr} - 1)q^{m/2}$ соответствующие нижние оценки рассматриваемой частоты будут больше нуля для всех r -грамм $\bar{z} \in R^r$. Нетрудно проверить, что при этом условии соответствующие верхние оценки частоты $N(\bar{z}, u_1, \dots, u_r)$ будут меньше периода T ЛРП векторов.

Список литературы

- [1] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, A. A. Nechaev, "Linear recurring sequences over rings and modules", *J. Math. Sci.*, **76**:6 (1995), 2793–2915.
- [2] Н. М. Коробов, "Распределение невычетов и первообразных корней в рекуррентных рядах", *Докл. АН СССР*, **88**:4 (1953), 603–606.
- [3] В. И. Нечаев, "Распределение знаков в последовательности прямоугольных матриц над конечным полем", *Аналитическая теория чисел и ее приложения*, Тр. МИАН, **218**, Наука, М., 1997, 335–342; англ. пер.: V. I. Nechaev, "Distribution of signs in a sequence of rectangular matrices over a finite field", *Proc. Steklov Inst. Math.*, **218**:3 (1997), 332–339.
- [4] H. Niederreiter, "Distribution properties of feedback shift register sequences", *Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform.*, **15**:1 (1986), 19–34.
- [5] И. Е. Шпарлинский, "О распределении значений рекуррентных последовательностей", *Пробл. передачи информ.*, **25**:2 (1989), 46–53; англ. пер.: I. E. Shparlinskij, "On distribution of values of recurrence sequences", *Problems Inform. Transmission*, **25**:2 (1989), 120–125.

- [6] В. М. Сидельников, “Оценки для числа появлений знаков на отрезке рекуррентной последовательности над конечным полем”, *Дискрет. матем.*, **3**:2 (1991), 87–95; англ. пер.: V. M. Sidel’nikov, “Estimates for the number of appearances of signs on a segment of a recurrence sequence over a finite field”, *Discrete Math. Appl.*, **2**:5 (1992), 473–481.
- [7] О. В. Камловский, “Оценки частот появления нулей в линейных рекуррентных последовательностях векторов”, *Чебышёвский сборник*, **6**:1 (2005), 135–145.
- [8] P. V. Kumar, T. Hellesteth, A. R. Calderbank, “An upper bound for Weil exponential sums over Galois rings and applications”, *IEEE Trans. Inform. Theory*, **41**:2 (1995), 456–468.
- [9] A. Weil, “On some exponential sums”, *Proc. Nat. Acad. Sci. U.S.A.*, **34**:5 (1948), 204–207.
- [10] L. Carlitz, S. Uchiyama, “Bounds for exponential sums”, *Duke Math. J.*, **24**:1 (1957), 37–41.
- [11] О. В. Камловский, А. С. Кузьмин, “Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа”, *Фундамент. и прикл. матем.*, **6**:4 (2000), 1083–1094.
- [12] A. G. Shanbhag, P. V. Kumar, T. Hellesteth, “Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation of some q -ary sequences sequences”, *IEEE Trans. Inform. Theory*, **42**:1 (1996), 250–254.
- [13] P. Solé, D. Zinoviev, “The most significant bit of maximum-length sequences over $\mathbb{Z}_2$: autocorrelation and imbalance”, *IEEE Trans. Inf. Theory*, **50**:8 (2006), 1844–1846.
- [14] S. Fan, W. Han, “Random properties of the highest level sequences of primitive sequences over $\mathbb{Z}_2$ ”, *IEEE Trans. Inf. Theory*, **49**:6 (2003), 1553–1557.
- [15] H. Hu, D. Feng, W. Wu, “Incomplete exponential sums over galois rings with applications to some binary sequences derived from $\mathbb{Z}_2$ ”, *IEEE Trans. Inf. Theory*, **52**:5 (2006), 2260–2265.
- [16] А. А. Нечаев, “Код Кердока в циклической форме”, *Дискрет. матем.*, **1**:4 (1989), 123–139; англ. пер.: A. A. Nechaev, “Kerdock code in a cyclic form”, *Discrete Math. Appl.*, **1**:4 (1989), 365–384.
- [17] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics, **28**, Dekker, New York, 1974.
- [18] А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев, “Псевдослучайные и полилинейные последовательности”, *Труды по дискретной математике*. Т. 1, Изд-во ТВП, М., 1997, 139–202.
- [19] А. А. Нечаев, “Цикловые типы линейных подстановок над конечными коммутативными кольцами”, *Матем. сб.*, **184**:3 (1993), 21–56; англ. пер.: A. A. Nechaev, “Cycle types of linear substitutions over finite commutative rings”, *Russian Acad. Sci. Sb. Math.*, **78**:2 (1994), 283–311.
- [20] Н. М. Коробов, *Теоретико-числовые методы в приближенном анализе*, МЦНМО, М., 2004.
- [21] Р. Лидл, Г. Нидеррайтер, *Конечные поля*, Мир, М., 1988; пер. с англ.: R. Lidl, H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl., **20**, Addison-Wesley, Reading, MA; Cambridge Univ. Press, Cambridge, 1983.
- [22] В. Н. Цыпышев, “Матричный линейный конгруэнтный генератор над кольцом Галуа нечетной характеристики”, *Тезисы докладов V международной конференции “Алгебра и теория чисел: Современные проблемы и приложения”* (Тула, 2003), Изд-во Тул. ГПУ, Тула, 2003, 233–237.
- [23] S. Boztas, R. Hammous, P. V. Kumar, “4-phase sequences with near-optimum correlation properties”, *IEEE Trans. Inform. Theory*, **38**:3 (1992), 1101–1113.

- [24] А. С. Кузьмин, “Распределение элементов на циклах линейных рекуррент над кольцами вычетов”, *УМН*, **47**:6 (1992), 213–214; англ. пер.: A. S. Kuz'min, “The distribution of elements on cycles of linear recurrences over rings of residues”, *Russian Math. Surveys*, **47**:6 (1992), 219–221.
- [25] A. Kuzmin, A. Nechaev, “Complete weight enumerators of generalized Kerdock code and related linear codes over Galois ring”, *Discrete Appl. Math.*, **111**:1–2 (2001), 117–137.

О. В. Камловский (O. V. Kamlovskii)

E-mail: ov-kam@yandex.ru

Поступила в редакцию

28.02.2008 и 23.12.2008