Math-Net.Ru

Общероссийский математический портал

О. В. Камловский, Метод В. М. Сидельникова для оценки числа знаков на отрезках линейных рекуррентных последовательностей над кольцами Галуа, *Матем. заметки*, 2012, том 91, выпуск 3, 371–382

DOI: <https://doi.org/10.4213/mzm7836>

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: 52.205.19.152

26 апреля 2023 г., 13:34:12

Метод В. М. Сидельникова для оценки числа знаков на отрезках линейных рекуррентных последовательностей над кольцами Галуа

О. В. Камловский

В. М. Сидельниковым с использованием метода тригонометрических сумм были получены оценки частот появлений элементов на отрезках линейных рекуррентных последовательностей над конечными полями. В данной работе эти результаты обобщаются на случай колец Галуа. Показывается, что полученные оценки в некоторых случаях точнее, чем известные результаты.

Библиография: 14 названий.

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 ее знаков 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]). 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 используются при построении датчиков псевдослучайных чисел (см., например, [2], [3]), а также при создании помехоустойчивых кодов (см., например, [4], [5]). В каждом из этих приложений одними из важных характеристик ЛРП u являются количества появлений элементов кольца R на различных отрезках этой последовательности.

В статье Сидельникова [6] был предложен способ оценки числа знаков в ЛРП над конечными полями, который позволил в ряде случаев уточнить известные результаты. Однако вопрос о возможности применения идей этой работы для получения оценок частот знаков в ЛРП над примарными кольцами вычетов и в более общем случае для ЛРП над кольцами Галуа оставался открытым. В данной работе предлагается один из вариантов решения этой задачи, основанный на применении оценок тригонометрических сумм над кольцами Галуа из работы [7].

Работа выполнена при финансовой поддержке программы “Ведущие научные школы” (грант № НШ-4.2008.10).

Пусть p – простое число, $R = GR(q^n, p^n)$ – кольцо Галуа характеристики p^n , состоящее из q^n элементов. Назовем многочлен $F(x) \in R[x]$ *реверсивным* *многочленом*, если элемент $F(0)$ является обратимым элементом кольца R . Обозначим $\overline{F}(x)$ образ многочлена $F(x)$ при действии естественного эпиморфизма колец многочленов $R[x] \rightarrow \overline{R}[x]$, где $\overline{R} = R/pR$ – фактор-кольцо кольца R по идеалу pR . Многочлен $F(x)$ будем называть *многочленом Галуа над кольцом R* , если многочлен $\overline{F}(x)$ является неприводимым многочленом над полем $\overline{R} = GF(q)$, состоящим из q элементов (см., например, [1]).

Рассмотрим последовательности $u_1, u_2, \dots, u_r$ над кольцом Галуа $R = GR(q^n, p^n)$. Назовем эти последовательности линейно независимыми над кольцом R , если для всех ненулевых векторов $(c_1, c_2, \dots, c_r)$ из множества R^r последовательность $c_1 u_1 + c_2 u_2 + \dots + c_r u_r$ будет ненулевой. Будем считать, что все последовательности $u_1, u_2, \dots, u_r$ являются ЛРП над кольцом R с одним и тем же характеристическим многочленом $F(x)$, где $F(x)$ – некоторый унитарный многочлен над кольцом R . В этом случае последовательность, элементы которой имеют вид $(u_1(i), u_2(i), \dots, u_r(i))$ для всех $i \geq 0$, будем называть ЛРП векторов с характеристическим многочленом $F(x)$.

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

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

Величина $N_l(\bar{z}, u_1, \dots, u_r)$ равна числу появлений r -граммы $\bar{z}$ из множества R^r на начальном отрезке длины l ЛРП векторов. Следует отметить, что результаты о частотах появления элементов в ЛРП векторов являются обобщениями результатов о частотных характеристиках одной ЛРП.

В работе [8; следствие 1] было показано, что если $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = GR(q^n, p^n)$, $u_1, u_2, \dots, u_r$ – линейно независимая система ЛРП над кольцом R с характеристическим многочленом $F(x)$, $T(F) = p^\nu T(\overline{F})$, где $0 \leq \nu \leq n-1$, $l \leq T(F)$, то справедлива оценка

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

В этой оценке величина l/q^{nr} является “естественным” средним значением числа появлений вектора $\bar{z}$ на отрезке длины l в ЛРП векторов. Оценка (1) является обобщением на случай колец Галуа известных результатов Коробова (см. [9]), Нечаева (см. [10]) и Нидеррайтера (см. [11]).

В данной работе (см. следствие 2) будет доказано, что при условиях, сформулированных для результата (1), и дополнительных условиях $T(\overline{F}) = q^m - 1$, $l < T(\overline{F})$ справедлива оценка

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{q^{nr} - 1}{q^{nr}} (3p^\nu l (q^m - l + \delta_l))^{1/3}, \quad (2)$$

где

$$\delta_l = (l-1)(p^{n-1} - 1)q^{m/2}.$$

В случае, когда $n = 1$, т.е. $R = GF(q)$, выполнено равенство $\delta_l = 0$ и полученная оценка совпадает с оценкой В. М. Сидельникова (см. [6; следствие 4]).

Показывается, что оценка (2) нетривиальна и точнее оценки (1) при выполнении следующих условий:

$$3(q^{nr} - 1)^3 p^{n+\nu-1} q^{m/2} \leq l \leq \frac{1}{\sqrt{3}} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right)^{3/2} p^{n+\nu-1} q^{m/2}.$$

Рассматривается случай, когда многочлен $\bar{F}(x)$ является произвольным неприводимым многочленом над полем $GF(q)$, и показывается, что в этом случае справедливы оценки, аналогичные оценке (2).

В работах [12]–[14] исследовались частоты появления элементов кольца $\mathbb{Z}_{2^n}$ вычетов по модулю 2^n в координатной последовательности, полученной выделением старшего двоичного разряда из ЛРП u максимального периода над кольцом $\mathbb{Z}_{2^n}$. Из оценок (1) и (2), рассматриваемых при $r = 1$, нетрудно получить оценки числа появлений элементов в координатных последовательностях ЛРП $u = u_1$. При этом оценки, вытекающие из неравенства (1), отличаются от результатов вышеуказанных работ некоторым множителем, не зависящим от параметра m . Таким образом, неравенство (2) при некоторых значениях l позволяет уточнить известные оценки числа появлений элементов в последовательностях, полученных выделением старшего двоичного разряда из ЛРП максимального периода над кольцом $\mathbb{Z}_{2^n}$.

2. Сведение к тригонометрическим суммам. Пусть $R = GR(q^n, p^n)$, R_0 – множество, состоящее из элементов $0, e, 2e, \dots, (p^n - 1)e$, где e – единица кольца R . Множество R_0 образует подкольцо кольца R , изоморфное кольцу $\mathbb{Z}_{p^n}$ вычетов по модулю p^n . Рассмотрим аддитивный характер χ кольца R , определенный на элементах этого кольца равенством

$$\chi(x) = \exp \left\{ \frac{2\pi i \operatorname{Tr}_{R_0}^R(x)}{p^n} \right\}, \quad (3)$$

где $\operatorname{Tr}_{R_0}^R$ – функция “след” из кольца R в кольцо R_0 . Пусть $F(x)$ – унитарный многочлен над кольцом R . Обозначим $L_R(F)$ – множество всех ЛРП над кольцом R с характеристическим многочленом $F(x)$. Последовательность, состоящую только из нулевых элементов кольца R , будем обозначать (0).

Определим для каждого элемента c кольца R его норму $\|c\|$ по правилу $\|c\| = \max\{j \in 0, \dots, n : c \in p^j R\}$. Нормой вектора $\bar{c} = (c_1, c_2, \dots, c_r)$ из множества R^r будем называть величину $\|\bar{c}\|$, определенную по правилу $\|\bar{c}\| = \min\{\|c_k\|, k \in 1, \dots, r\}$. Аналогично нормой последовательности u элементов кольца R назовем величину $\|u\|$, равную минимальному значению норм всех элементов последовательности u .

ЛЕММА 1 [7]. При всех элементах x кольца $R = GR(q^n, p^n)$ имеют место равенства

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

ЛЕММА 2. Система последовательностей $u_1, u_2, \dots, u_r$ кольца $R = GR(q^n, p^n)$ линейно независима над R тогда и только тогда, когда при всех $\bar{c} = (c_1, c_2, \dots, c_r)$

из множества R^r для последовательности $u_{\bar{c}} = c_1 u_1 + c_2 u_2 + \dots + c_r u_r$ выполнено равенство $\|u_{\bar{c}}\| = \|\bar{c}\|$.

ДОКАЗАТЕЛЬСТВО. Если при всех векторах $\bar{c}$ выполнено равенство $\|u_{\bar{c}}\| = \|\bar{c}\|$, то равенство $u_{\bar{c}} = (0)$ имеет место только при $\bar{c} = \bar{0}$, а значит система $u_1, u_2, \dots, u_r$ линейно независима над кольцом R . Покажем, что из линейной независимости системы $u_1, u_2, \dots, u_r$ следует, что при всех $\bar{c} \in R^r$ выполнено равенство $\|u_{\bar{c}}\| = \|\bar{c}\|$. Неравенство $\|u_{\bar{c}}\| \geq \|\bar{c}\|$ очевидно. Допустим, что $\|u_{\bar{c}}\| > \|\bar{c}\| = k$. Пусть $c_i = p^k c'_i$, где $c'_i \in R$ для всех $i \in 1, \dots, r$. Из условия $\|\bar{c}\| = k$ следует, что хотя бы один из элементов c'_i обратим в кольце R . В силу того, что $\|u_{\bar{c}}\| > k$, последовательность $c'_1 u_1 + c'_2 u_2 + \dots + c'_r u_r$ состоит только из элементов кольца pR , а значит имеет место равенство

$$p^{n-1} c'_1 u_1 + p^{n-1} c'_2 u_2 + \dots + p^{n-1} c'_r u_r = (0),$$

что противоречит линейной независимости рассматриваемой системы ЛРП.

УТВЕРЖДЕНИЕ 1. Пусть $F(x)$ – унитарный многочлен над кольцом $R = GR(q^n, p^n)$, $u_1, u_2, \dots, u_r$ – линейно независимая система ЛРП из множества $L_R(F)$, l – натуральное число. Тогда справедливо следующее соотношение:

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \sum_{k=0}^{n-1} \frac{q^r - 1}{q^{(k+1)r}} \max_{u \in L_R(F), \|u\|=k} |\sigma_l(u)|,$$

где

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

ДОКАЗАТЕЛЬСТВО. С использованием леммы 1 получим

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

где $\bar{z} = (z_1, z_2, \dots, z_r)$. Тогда справедливо соотношение

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

Пусть $\bar{c} = (c_1, c_2, \dots, c_r)$, $u_{\bar{c}} = c_1 u_1 + c_2 u_2 + \dots + c_r u_r$. Введем обозначение

$$\bar{c}\bar{z} = (c_1, \dots, c_r)(z_1, \dots, z_r) = c_1 z_1 + \dots + c_r z_r.$$

Выделяя отдельно слагаемое, соответствующее нулевому набору $(c_1, c_2, \dots, c_r)$, и изменяя порядок суммирования, получим соотношение

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

Из этого соотношения и равенства $|\chi(x)| = 1$, справедливого для всех элементов x кольца R , будет следовать неравенство

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{1}{q^{nr}} \sum_{\bar{c} \in R^r \setminus \{\bar{0}\}} \left| \sum_{i=0}^{l-1} \chi(u_{\bar{c}}(i)) \right|. \quad (4)$$

Векторы $\bar{c} \in R^r$, имеющие норму k , принадлежат множеству $(p^k R)^r \setminus (p^{k+1} R)^r$ и их число равно $|p^k R|^r - |p^{k+1} R|^r = q^{(n-k-1)r}(q^r - 1)$. Тогда с использованием неравенства (4) получим

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \sum_{k=0}^{n-1} \frac{q^r - 1}{q^{(k+1)r}} \max_{\bar{c} \in R^r, \|\bar{c}\|=k} |\sigma_l(u_{\bar{c}})|.$$

Для завершения доказательства остается воспользоваться леммой 2 и заметить, что в условиях утверждения при всех $\bar{c} \in R^r$ последовательность $u_{\bar{c}}$ является ЛРП с характеристическим многочленом $F(x)$.

Таким образом, для оценки сверху величины $|N_l(\bar{z}, u_1, \dots, u_r) - l/q^{nr}|$ достаточно оценить модуль тригонометрической суммы $\sigma_l(u)$, где последовательность u также как и последовательности $u_1, u_2, \dots, u_r$ принадлежит множеству $L_R(F)$. В дальнейшем будем исследовать тригонометрическую сумму $\sigma_l(u)$.

3. Обобщение метода В. М. Сидельникова. Пусть R – конечное кольцо, χ – произвольный аддитивный характер кольца R , u – чисто периодическая последовательность элементов кольца R , т.е. для некоторого натурального числа T выполнены равенства $u(i+T) = u(i)$ для всех $i \geq 0$. Рассмотрим сумму $\sigma_l(u)$ значений характера χ от ЛРП u :

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

Для целого неотрицательного числа j обозначим v_j последовательность над кольцом R , элементы которой задаются равенствами

$$v_j(i) = u(i+j), \quad i \geq 0.$$

Последовательность v_j будем называть *сдвигом* последовательности u . Обозначим $P(u)$ – множество всех сдвигов последовательности u . Если $T = T(u)$ – период последовательности u , то множество $P(u)$ имеет мощность T и имеет вид: $P(u) = \{v_0, v_1, \dots, v_{T-1}\}$, причем $v_0 = u$. В дальнейшем понадобится следующая лемма.

ЛЕММА 3 [6]. Для всех неотрицательных действительных чисел x имеет место неравенство

$$x^2 + 2 \sum_{j=1}^{[x/2]} (x-2j)^2 \geq \frac{x^3}{3},$$

где $[x/2]$ – целая часть числа $x/2$.

ТЕОРЕМА 1. При всех натуральных числах l таких, что $l < T$, имеет место неравенство

$$|\sigma_l(u)| \leq \left(3 \sum_{v \in P(u)} |\sigma_l(v)|^2 \right)^{1/3}.$$

ДОКАЗАТЕЛЬСТВО. Обозначим ω – ЛРП из множества $P(u)$, имеющую максимальное значение величины $|\sigma_l(v)|$ среди всех ЛРП v из множества $P(u)$. Пусть $\sigma = |\sigma_l(\omega)|$. Для доказательства теоремы достаточно показать, что

$$\sigma \leq \left(3 \sum_{v \in P(u)} |\sigma_l(v)|^2 \right)^{1/3}.$$

Так как значениями характера χ являются комплексные корни некоторой степени из единицы, то $\sigma = |\sigma_l(\omega)| \leq l < T$. Для всех чисел j из множества $-\lceil \sigma/2 \rceil, \dots, \lceil \sigma/2 \rceil$ обозначим ω_j последовательность над кольцом R , элементы $\omega_j(i)$ которой определены при всех $i \geq 0$ равенствами:

$$\omega_j(i) = \begin{cases} \omega(i+j), & \text{если } j \geq 0, \\ \omega(i+T+j), & \text{если } j < 0. \end{cases}$$

В частности, $\omega_0 = \omega$. Так как $\lceil \sigma/2 \rceil < T/2$, то последовательности ω_j являются различными последовательностями из множества $P(\omega) = P(u)$ для всех $j \in -\lceil \sigma/2 \rceil, \dots, \lceil \sigma/2 \rceil$. Заметим, что при всех $j \in 1, \dots, \lceil \sigma/2 \rceil$ наборы $(\omega_0(0), \dots, \omega_0(l-1))$ и $(\omega_j(0), \dots, \omega_j(l-1))$ содержат по крайней мере $l-j$ одинаковых элементов, а при всех $j \in -\lceil \sigma/2 \rceil, \dots, -1$ наборы $(\omega_0(0), \dots, \omega_0(l-1))$ и $(\omega_j(0), \dots, \omega_j(l-1))$ содержат по крайней мере $l-|j|$ одинаковых элементов. Тогда суммы $\sigma_l(\omega_j)$ и $\sigma_l(\omega_0)$ содержат не менее $l-|j|$ равных слагаемых, а значит $|\sigma_l(\omega_j) - \sigma_l(\omega_0)| \leq 2|j|$, и имеет место неравенство $|\sigma_l(\omega_j)| \geq \sigma_l(\omega_0) - 2|j| = \sigma - 2|j|$ для всех $j \in -\lceil \sigma/2 \rceil, \dots, \lceil \sigma/2 \rceil$. В итоге, с использованием леммы 3, получим соотношения

$$\sum_{v \in P(u)} |\sigma_l(v)|^2 \geq \sum_{j=-\lceil \sigma/2 \rceil}^{\lceil \sigma/2 \rceil} |\sigma_l(\omega_j)|^2 \geq \sigma^2 + 2 \sum_{j=1}^{\lceil \sigma/2 \rceil} (\sigma - 2j)^2 \geq \frac{\sigma^3}{3}.$$

Теорема 1 сводит получение верхних оценок величины $|\sigma_l(u)|$ к получению верхних оценок величины $\sum_{v \in P(u)} |\sigma_l(v)|^2$.

4. Оценка тригонометрической суммы. Пусть $R = GR(q^n, p^n)$, u – ЛРП над кольцом R , χ – характер, определенный равенством (3),

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

Получим оценку сверху величины

$$\sum_{v \in P(u)} |\sigma_l(v)|^2.$$

Пусть $S = GR(q^{mn}, p^n)$ – расширение степени m кольца R . Обозначим χ' аддитивный характер кольца S , являющийся поднятием характера χ , т.е. он определен на элементах этого кольца равенством

$$\chi'(y) = \chi(\text{Tr}_R^S(y)), \quad (5)$$

где Tr_R^S – функция “след” из кольца S в кольцо R .

Нам понадобится следующая лемма.

ЛЕММА 4 [7], [8]. Пусть $S = GR(q^{mn}, p^n)$, α – обратимый элемент кольца S , имеющий мультипликативный порядок $\text{ord } \alpha = p^\nu(q^m - 1)/d$, где $0 \leq \nu \leq n - 1$, а d – делитель числа $q^m - 1$. Тогда для каждого ненулевого элемента b кольца S имеет место неравенство

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

где $\|b\| = \max\{j \in \{0, \dots, n\} : b \in p^j S\}$ – норма элемента b .

ТЕОРЕМА 2. Пусть $F(x)$ – реверсивный многочлен Галуа степени m над кольцом $R = GR(q^n, p^n)$, $T(F) = p^\nu T(\bar{F}) = p^\nu(q^m - 1)/d$, u – ненулевая ЛРП из множества $L_R(F)$, l – натуральное число, $l \leq T(\bar{F})$. Тогда

$$\sum_{v \in P(u)} |\sigma_l(v)|^2 \leq \frac{T(u)l}{q^m - 1} (q^m - l + (l - 1)(dp^{n-\|u\|} - 1)q^{m/2}),$$

где $\|u\| = \min\{\|u(j)\| : j \geq 0\}$.

ДОКАЗАТЕЛЬСТВО. Так как $F(x)$ – реверсивный многочлен, то u является чисто периодической последовательностью и $P(u) = \{v_0, v_1, \dots, v_{T(u)-1}\}$, где $v_k = x^k u$ для всех $k \geq 0$. Период $T(u)$ ЛРП u является делителем числа $T(F)$, поэтому справедливо соотношение

$$\sum_{v \in P(u)} |\sigma_l(v)|^2 = \frac{T(u)}{T(F)} \sum_{k=0}^{T(F)-1} |\sigma_l(v_k)|^2. \quad (6)$$

Имеет место равенство

$$\sum_{k=0}^{T(F)-1} |\sigma_l(v_k)|^2 = \sum_{k=0}^{T(F)-1} \sigma_l(v_k) \overline{\sigma_l(v_k)},$$

где $\overline{\sigma_l(v_k)}$ – комплексно сопряженное число к числу $\sigma_l(v_k)$. Тогда с использованием равенства $\chi(x) = \chi(-x)$ получим

$$\sum_{k=0}^{T(F)-1} |\sigma_l(v_k)|^2 = \sum_{k=0}^{T(F)-1} \sum_{i=0}^{l-1} \chi(v_k(i)) \sum_{j=0}^{l-1} \chi(-v_k(j)). \quad (7)$$

С использованием соотношений (6) и (7) будем иметь

$$\begin{aligned} \sum_{v \in P(u)} |\sigma_l(v)|^2 &= \frac{T(u)}{T(F)} \sum_{k=0}^{T(F)-1} \sum_{i,j=0}^{l-1} \chi(v_k(i) - v_k(j)) \\ &= \frac{T(u)}{T(F)} \sum_{k=0}^{T(F)-1} \sum_{i,j=0}^{l-1} \chi(u(k+i) - u(k+j)). \end{aligned}$$

Представим ЛРП u с использованием функции “след”:

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

где $S = GR(q^{mn}, p^n)$, α – корень многочлена $F(x)$ в кольце S , а b – ненулевой элемент кольца S . Тогда

$$\begin{aligned} \sum_{v \in P(u)} |\sigma_l(v)|^2 &= \frac{T(u)}{T(F)} \sum_{k=0}^{T(F)-1} \sum_{i,j=0}^{l-1} \chi'(b\alpha^{k+i} - b\alpha^{k+j}) \\ &= \frac{T(u)}{T(F)} \sum_{k=0}^{T(F)-1} \sum_{i,j=0}^{l-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k), \end{aligned}$$

где χ' – аддитивный характер кольца S , определенный равенством (5). Выделив отдельно слагаемое, соответствующее случаю $i = j$, получим

$$\sum_{v \in P(u)} |\sigma_l(v)|^2 = \frac{T(u)}{T(F)} \left(\sum_{i \neq j} \sum_{k=0}^{T(F)-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k) + T(F)l \right).$$

Значит, будет справедливо равенство

$$\sum_{v \in P(u)} |\sigma_l(v)|^2 = \frac{T(u)}{T(F)} \left(\sum_{i \neq j} \left(\sum_{k=0}^{T(F)-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k) + \frac{p^\nu}{d} \right) + T(F)l - \frac{p^\nu}{d} l(l-1) \right).$$

Переходя к рассмотрению абсолютных величин, получим

$$\sum_{v \in P(u)} |\sigma_l(v)|^2 \leq \frac{T(u)}{T(F)} \left(\sum_{i \neq j} \left| \sum_{k=0}^{T(F)-1} \chi'(b(\alpha^i - \alpha^j)\alpha^k) + \frac{p^\nu}{d} \right| + \frac{p^\nu}{d} l(q^m - l) \right).$$

Заметим, что образ элемента $\alpha^i - \alpha^j$ при действии естественного эпиморфизма колец $S \rightarrow S/pS$ будет равен $\bar{\alpha}^i - \bar{\alpha}^j$, где $\bar{\alpha}$ – корень многочлена $\bar{F}(x)$ в поле $GF(q^m)$. Тогда при всех различных $i, j \in 0, \dots, l-1$ и $l \leq T(\bar{F})$ элемент $\bar{\alpha}^i - \bar{\alpha}^j$ будет ненулевым, а значит элемент $\alpha^i - \alpha^j$ будет обратимым элементом кольца S . С использованием леммы 4 и равенств $\|u\| = \|b\| = \|b(\alpha^i - \alpha^j)\|$, $\text{ord } \alpha = T(F)$, получим

$$\sum_{v \in P(u)} |\sigma_l(v)|^2 \leq \frac{T(u)p^\nu l}{T(F)d} (q^m - l + \delta_l(u)) = \frac{T(u)l}{q^m - 1} (q^m - l + \delta_l(u)),$$

где $\delta_l(u) = (l-1)(dp^{n-\|u\|-1} - 1)q^{m/2}$.

Непосредственно из теорем 1 и 2 получим следующее следствие.

СЛЕДСТВИЕ 1. Пусть в условиях теоремы 2 $l < T(u)$. Тогда имеет место оценка

$$|\sigma_l(u)| \leq \left(\frac{3T(u)l}{q^m - 1} (q^m - l + (l-1)(dp^{n-\|u\|-1} - 1)q^{m/2}) \right)^{1/3}.$$

Перейдем к описанию частотных характеристик ЛРП векторов.

5. Оценки числа появлений наборов в ЛРП векторов. Рассмотрим произвольные последовательности $u_1, u_2, \dots, u_r$ над кольцом $R = GR(q^n, p^n)$. Напомним, что эти последовательности называются *линейно независимыми* над кольцом R , если для всех ненулевых векторов $\bar{c} = (c_1, c_2, \dots, c_r) \in \mathbb{R}^r$ последовательность $c_1 u_1 + c_2 u_2 + \dots + c_r u_r$ является ненулевой. Оценим число $N_l(\bar{z}, u_1, \dots, u_r)$ появлений набора $\bar{z} = (z_1, z_2, \dots, z_r) \in \mathbb{R}^r$ среди векторов $(u_1(i), u_2(i), \dots, u_r(i))$, где $i \in 0, \dots, l-1$.

ТЕОРЕМА 3. Пусть $F(x)$ – реверсивный многочлен Галуа степени t над кольцом $R = GR(q^n, p^n)$, $T(F) = p^\nu T(\bar{F}) = p^\nu(q^m - 1)/d$, $u_1, u_2, \dots, u_r$ – линейно независимая система ЛРП над кольцом R с характеристическим многочленом $F(x)$. Тогда для всех $\bar{z} \in R^r$ и всех $l \in \mathbb{N}$ таких, что $l < T(\bar{F})$, справедлива оценка

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \sum_{k=0}^{n-1} \frac{q^r - 1}{q^{(n-k)r}} \left(\frac{3p^\nu l}{d} (q^m - l + (l-1)(dp^k - 1)q^{m/2}) \right)^{1/3}. \quad (8)$$

ДОКАЗАТЕЛЬСТВО. Достаточно воспользоваться утверждением 1, следствием 1 и неравенством $T(u) \leq T(F)$, справедливым для каждой ЛРП u с характеристическим многочленом $F(x)$.

Рассмотрим оценку (8) применительно к случаю, когда $n = 1$, т.е. когда кольцо R является конечным полем $GF(q)$. В этом случае $\nu = 0$, $T(F) = T(\bar{F}) = (q^m - 1)/d$. При $d = 1$ правая часть неравенства (8) имеет вид

$$\frac{q^r - 1}{q^r} (3l(q^m - l))^{1/3} \quad (9)$$

и совпадает с оценкой Сидельникова (см. [6]), которая имеет такой вид при всех значениях d . При $d > 1$, т.е., когда многочлен $\bar{F}(x)$ неприводим над полем $GF(q)$ и не является многочленом максимального периода, правая часть неравенства (8) принимает вид

$$\frac{q^r - 1}{q^r} \left(\frac{3l}{d} (q^m - l + (l-1)(d-1)q^{m/2}) \right)^{1/3}. \quad (10)$$

Несложно показать, что величина (10) меньше величины (9) тогда и только тогда, когда $l < (q^{m/2})/2$.

Приведем более простую, но менее точную оценку, чем оценка (8).

СЛЕДСТВИЕ 2. В условиях теоремы 3 имеет место неравенство

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \frac{q^{nr} - 1}{q^{nr}} \left(\frac{3p^\nu l}{d} (q^m - l + (l-1)(dp^{n-1} - 1)q^{m/2}) \right)^{1/3}. \quad (11)$$

СЛЕДСТВИЕ 3. Пусть в условиях теоремы 3 дополнительно выполнены соотношения

$$T(\bar{F}) = q^m - 1, \quad l \geq 3(q^{nr} - 1)^3 p^{n+\nu-1} q^{m/2}.$$

Тогда среди векторов $(u_1(i), u_2(i), \dots, u_r(i))$, где $i \in 0, \dots, l-1$, появятся все векторы из множества R^r .

ДОКАЗАТЕЛЬСТВО. Обозначим G правую часть неравенства (11). Из неравенства (11) получим $l/q^{nr} - G \leq N_l(\bar{z}, u_1, \dots, u_r)$. Тогда если $l/q^{nr} - G > 0$, то вектор $\bar{z}$ появляется среди первых l элементов ЛРП векторов. Это неравенство равносильно условию

$$l > (q^{nr} - 1)(3p^\nu l(q^m - l + (l - 1)(p^{n-1} - 1)q^{m/2}))^{1/3}.$$

Если дополнительно учесть, что $l > q^{m/2}$, то полученное неравенство справедливо при условии, что

$$l \geq (q^{nr} - 1)(3p^\nu l(q^{m/2}l + l(p^{n-1} - 1)q^{m/2}))^{1/3},$$

а это равносильно неравенству

$$l \geq 3(q^{nr} - 1)^3 p^{n+\nu-1} q^{m/2}.$$

Определим условия, при которых оценка из следствия 2, рассматриваемая применительно к наиболее интересному случаю, когда $d = 1$, является нетривиальной. Из неравенства (11) получим

$$\frac{l}{q^{nr}} - G \leq N_l(\bar{z}, u_1, \dots, u_r) \leq \frac{l}{q^{nr}} + G.$$

Оценку (11) будем считать нетривиальной, если $l/q^{nr} - G > 0$ и $l/q^{nr} + G < l$. Оба этих условия будут выполненными тогда и только тогда, когда $l > q^{nr}G$. Как показано при доказательстве следствия 3, для этого достаточно выполнения неравенства

$$l \geq 3(q^{nr} - 1)^3 p^{n+\nu-1} q^{m/2}.$$

Таким образом, выполнение этого неравенства гарантирует нетривиальность оценки (11), рассматриваемой в случае, когда $d = 1$.

Сравним при $d = 1$ оценку (1) и оценку (11). Правая часть неравенства (1) больше правой части неравенства (11) при условии

$$3p^\nu l(q^m + q^{m/2}l(p^{n-1} - 1)) \leq p^{3(n+\nu-1)} C^3 q^{3m/2},$$

где $C = (2/\pi) \ln T(F) + 7/5$. При дополнительном условии $l \geq q^{m/2}$ это неравенство будет иметь место, когда

$$3p^\nu l(q^{m/2}l + q^{m/2}l(p^{n-1} - 1)) \leq p^{3(n+\nu-1)} C^3 q^{3m/2},$$

т.е. при условии $l \leq (1/\sqrt{3})p^{n+\nu-1} C^{3/2} q^{m/2}$. Таким образом, при $d = 1$ оценка (11) точнее оценки (1) при выполнении соотношений

$$q^{m/2} \leq l \leq \frac{1}{\sqrt{3}} \left(\frac{2}{\pi} \ln T(F) + \frac{7}{5} \right)^{3/2} p^{n+\nu-1} q^{m/2}.$$

Заметим, что при рассуждениях использовалось существенное огрубление оценки (11), поэтому на самом деле диапазон значений l , при которых эта оценка является нетривиальной и точнее оценки (1), может быть гораздо большим.

Уточним оценку из теоремы 3 в случае, когда многочлен $F(x)$ имеет максимальный период.

ТЕОРЕМА 4. Пусть в условиях теоремы 3 выполнено равенство $T(F) = p^{n-1} \times (q^m - 1)$. Тогда справедлива оценка

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \sum_{k=0}^{n-1} \frac{q^r - 1}{q^{(n-k)r}} (3p^k l (q^m - l + (l-1)(p^k - 1)q^{m/2}))^{1/3}. \quad (12)$$

ДОКАЗАТЕЛЬСТВО. Заметим, что если u – ненулевая ЛРП над кольцом R с характеристическим многочленом $F(x)$ и $\|u\| = k$, то $T(u) = p^{n-k-1}(q^m - 1)$ (см., например, [1; теорема 4.6]). Тогда согласно следствию 1 будет иметь место неравенство

$$|\sigma_l(u)| \leq (3p^{n-k-1}l(q^m - l + (l-1)(p^{n-k-1} - 1)q^{m/2}))^{1/3}.$$

Таким образом, с использованием утверждения 1 получим

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^{nr}} \right| \leq \sum_{k=0}^{n-1} \frac{q^r - 1}{q^{(n-k)r}} (3p^k l (q^m - l + (l-1)(p^k - 1)q^{m/2}))^{1/3}.$$

Оценка (12) совпадает с оценкой (8) (рассматриваемой в случае, когда $F(x)$ – многочлен максимального периода) тогда и только тогда, когда $n = 1$, т.е., когда кольцо R является полем. Во всех остальных случаях оценка (12) является точнее оценки (8).

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев, “Псевдослучайные и полилинейные последовательности”, *Тр. по дискр. матем.*, **1**, ТВП, М., 1997, 139–202.
- [2] А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин, *Основы криптографии*, Учебное пособие, Гелиос АРВ, М., 2001.
- [3] Д. Кнут, *Искусство программирования. Т. 2. Получисленные алгоритмы*, Мир, М., 2000.
- [4] 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.
- [5] R. J. McEliece, “Irreducible cyclic codes and Gauss sums”, *Combinatorics. Part 1: Theory of Designs, Finite Geometry and Coding Theory*, Math. Centre Tracts, **55**, Math. Centrum, Amsterdam, 1974, 179–196.
- [6] В. М. Сидельников, “Оценки для числа появлений знаков на отрезке рекуррентной последовательности над конечным полем”, *Дискрет. матем.*, **3**:2 (1991), 87–95.
- [7] О. В. Камловский, А. С. Кузьмин, “Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Гауа”, *Фундамент. и прикл. матем.*, **6**:4 (2000), 1083–1094.
- [8] О. В. Камловский, “Частотные характеристики линейных рекуррентных последовательностей над кольцами Гауа”, *Матем. сб.*, **200**:4 (2009), 31–52.
- [9] Н. М. Коробов, “Распределение невычетов и первообразных корней в рекуррентных рядах”, *Докл. АН СССР*, **88**:4 (1953), 603–606.
- [10] В. И. Нечаев, “Распределение знаков в последовательности прямоугольных матриц над конечным полем”, *Аналитическая теория чисел и приложения*, Сборник статей. К 60-летию со дня рождения профессора Анатолия Алексеевича Карацубы, Тр. МИАН, **218**, Наука, М., 1997, 335–342.

- [11] H. Niederreiter, “Distribution properties of feedback shift register sequences”, *Problems Control Inform. Theory*, **15**:1 (1986), 19–34.
- [12] P. Solé, D. Zinoviev, “The most significant bit of maximum-length sequences over $\mathbb{Z}_2$: autocorrelation and imbalance”, *IEEE Trans. Inform. Theory*, **50**:8 (2004), 1844–1846.
- [13] S. Fan, W. Han, “Random properties of the highest level sequences of primitive sequences over $\mathbb{Z}_2$ ”, *IEEE Trans. Inform. Theory*, **49**:6 (2003), 1553–1557.
- [14] 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. Inform. Theory*, **52**:5 (2006), 2260–2265.

О. В. Камловский

E-mail: ov-kam@yandex.ru

Поступило

03.03.2009