Уточнение оценок для числа появлений элементов в линейных рекуррентных последовательностях над кольцами Галуа*

О. В. КАМЛОВСКИЙ
Центр сертификационных исследований
e-mail: ov-kam@yandex.ru

УДК 519.4

Ключевые слова: линейные рекуррентные последовательности, псевдослучайные числа, кольца Галуа, оценки экспоненциальных сумм, распределение элементов в последовательностях.

Аннотация

Рассматривается задача получения оценок для числа появлений элементов на отрезках линейных рекуррентных последовательностей векторов над кольцами Галуа. Для её решения применяется метод тригонометрических сумм. Использование отличного от обычно применяющегося при решении рассматриваемой задачи класса тригонометрических сумм позволяет в некоторых случаях уточнить известные результаты.

Abstract

O. V. Kamlovskii, Improved bounds for the number of occurrences of elements in linear recurrence sequences over Galois rings, Fundamentalnaya i prikladnaya matematika, vol. 17 (2011/2012), no. 7, pp. 97—115.

We establish bounds for the number of occurrences of elements on segments of linear recurrence sequences of vectors over Galois rings. We use the method of exponential sums for this problem. We improve known results with the help of a new class of exponential sums.

1. Введение

Пусть R — коммутативное кольцо с единицей. Последовательность $u = \big(u(i)\big)_{i=0}^{\infty}$ элементов кольца R называется линейной рекуррентной последовательностью порядка m над кольцом R, если для некоторых элементов $a_0, a_1, \ldots, a_{m-1}$ кольца R выполнены равенства

$$u(i+m) = a_0 u(i) + a_1 u(i+1) + \ldots + a_{m-1} u(i+m-1), \quad i \geqslant 0.$$

Многочлен

$$F(x) = x^m - a_{m-1}x^{m-1} - \ldots - a_1 x - a_0$$

*Работа поддержана грантом НШ-4.2010.10 Президента Российской Федерации.

Фундаментальная и прикладная математика, 2011/2012, том 17, № 7, с. 97—115.

называется характеристическим многочленом линейной рекуррентной последовательности u (см., например, [7, 14]). С использованием линейных рекуррентных последовательностей над конечными полями и кольцами вычетов удаётся построить генераторы псевдослучайных чисел, обладающие хорошими свойствами (см., например, [5]). Всюду в данной работе в качестве кольца R рассматривается кольцо Галуа $GR(q^n, p^n)$, состоящее из q^n элементов и имеющее характеристику p^n, где p — простое число, $q = p^t$ для некоторого натурального числа t (см. [9, 15]). Частными случаями кольца Галуа являются конечное поле Галуа $GR(q, p) = GF(q)$ из q элементов и примарное кольцо вычетов $GR(p^n, p^n) = \mathbb{Z}_{p^n}$ по модулю p^n.

Рассмотрим линейные рекуррентные последовательности $u_1, u_2, \ldots, u_r$ над кольцом $R = GR(q^n, p^n)$, имеющие один и тот же характеристический многочлен $F(x)$. Линейной рекуррентной последовательностью векторов будем называть последовательность, элементы которой имеют вид $\big(u_1(i), u_2(i), \ldots, u_r(i)\big)$ для всех $i \geqslant 0$. Для каждого натурального числа l и набора $\bar{z} = (z_1, z_2, \ldots, z_r)$ из множества R^r обозначим $N_l(\bar{z}, u_1, \ldots, u_r)$ количество целых чисел $i \in \overline{0, l-1}$, таких что

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

Другими словами, величина $N_l(\bar{z}, u_1, \ldots, u_r)$ равна числу появлений r-граммы $\bar{z}$ на начальном отрезке длины l рассматриваемой линейной рекуррентной последовательности векторов. Отметим, что если последовательности $u_1, u_2, \ldots, u_r$ являются сдвигами одной линейной рекуррентной последовательности u, т. е. для некоторых целых неотрицательных чисел $s_1, s_2, \ldots, s_r$ выполнены равенства $u_1 = x^{s_1}u$, $u_2 = x^{s_2}u, \ldots, u_r = x^{s_r}u$, то величина $N_l(\bar{z}, u_1, \ldots, u_r)$ равна числу появлений вектора $\bar{z}$ среди векторов $\big(u(i+s_1), u(i+s_2), \ldots, u(i+s_r)\big)$, где $0 \leqslant i \leqslant l-1$.

Пусть $F(x)$ — унитарный многочлен над кольцом $R = GR(q^n, p^n)$. Назовём многочлен $F(x)$ реверсивным многочленом, если элемент $F(0)$ принадлежит мультипликативной группе R^* кольца R. Обозначим $\bar{F}(x)$ образ многочлена $F(x)$ при действии естественного эпиморфизма колец многочленов $R[x] \to \bar{R}[x]$, где $\bar{R} = R/pR$ — фактор-кольцо кольца R по идеалу pR. Многочлен $F(x)$ будем называть многочленом Галуа над кольцом R, если многочлен $\bar{F}(x)$ является неприводимым многочленом над полем $\bar{R} = GF(q)$.

В [3, теорема 3], в частности, было показано, что если $F(x)$ — реверсивный многочлен Галуа степени m над кольцом $R = GR(q^n, p^n)$, имеющий период $T(F) = p^\nu T(\bar{F}) = p^\nu(q^m - 1)$, $u_1, u_2, \ldots, u_r$ — линейно независимая система линейных рекуррентных последовательностей над кольцом R с характеристическим многочленом $F(x)$, $l < q^m - 1$, то имеет место неравенство

$$\left|N_l(\bar{z},u_1,\dots,u_r)-\frac{l}{q^{nr}}\right|\leqslant\sum_{k=0}^{n-1}\frac{(q^r-1)S_{l,k}(F)}{q^{(k+1)r}},\tag{1}$$

где

$$S_{l,k}(F)=\Big(3p^{\nu}l\big(q^m-l+(l-1)(p^{n-k-1}-1)q^{m/2}\big)\Big)^{1/3}.\tag{2}$$

При доказательстве данного результата понадобилось оценить сверху модуль суммы $\sigma_l(u)=\sum\limits_{i=0}^{l-1}\chi\big(u(i)\big)$ значений аддитивного характера χ кольца R от произвольной ненулевой линейной рекуррентной последовательности u над кольцом R с характеристическим многочленом $F(x)$. Ранее в работах [2,4,6,10,12,13,16,17] для получения оценок величины $\sigma_l(u)$ использовался подход И. М. Виноградова и оценки не зависели от длины l отрезка линейной рекуррентной последовательности. При доказательстве неравенства (1) для оценки величины $\sigma_l(u)$ был применён совершенно другой метод, основанный на идеях работы [11]. В [3] показано, что оценка (1) нетривиальна и точнее всех аналогичных известных оценок при $l=O(m^{3/2}q^{m/2})$, $m\to\infty$.

В данной работе будет показано, что при некоторых ограничениях на длину l исследуемого отрезка линейной рекуррентной последовательности оценка (1) допускает существенное уточнение. Так, в условиях, сформулированных для оценки (1), при дополнительных соотношениях $l<q^m/2$ и $m\geqslant 2(1+(n-1)\log_q p)$ справедливо неравенство

$$\left|N_l(\bar{z},u_1,\dots,u_r)-\frac{l}{q^{nr}}\right|\leqslant\left(\frac{q}{2(q-1)}\right)^{1/3}S_l(F),$$

где $S_l(F)$ — правая часть неравенства (1). Кроме того, показано, что при $\bar{z}=\bar{0}$, $l<q^{m/2}/\big(2(q-1)\big)$ и $m\geqslant 2(n-1)\log_q p$ справедливо соотношение

$$\left|N_l(\bar{z},u_1,\dots,u_r)-\frac{l}{q^{nr}}\right|\leqslant\left(\frac{q}{2(q-1)^2}\right)^{1/3}S_l(F).$$

Доказательство результатов основано на сведении изучения частоты $N_l(\bar{z},u_1,\dots,u_r)$ к исследованию суммы

$$\tau_l(z,u)=\sum_{a\in R^*}\chi(-az)\sum_{i=0}^{l-1}\chi(au(i))$$

для всех элементов z кольца R и ненулевых линейных рекуррентных последовательностей u над кольцом R с характеристическим многочленом $F(x)$. Для оценки суммы $\tau_l(z,u)$ применён метод, аналогичный тому, который использовался в работе [3].

2. Сведение к оценке тригонометрических сумм

Пусть $R = GR(q^n, p^n)$, $F(x)$ — унитарный многочлен над кольцом R, $u_1, u_2, \ldots, u_r$ — линейная рекуррентная последовательность над кольцом R с характеристическим многочленом $F(x)$. Назовём систему этих последовательностей линейно независимой над кольцом R, если при всех векторах $\bar{c} = (c_1, c_2, \ldots, c_r)$ из множества R^r, последовательность $u_{\bar{c}} = c_1u_1 + c_2u_2 + \ldots + c_ru_r$ ненулевая. Заметим, что при всех $\bar{c} \in R^r$ последовательность $u_{\bar{c}}$ принадлежит множеству $L_R(F)$ всех линейных рекуррентных последовательностей над кольцом R с характеристическим многочленом $F(x)$. Определим норму $\|c\|$ элемента c кольца R, норму $\|\bar{c}\|$ вектора $\bar{c} = (c_1, c_2, \ldots, c_r)$, принадлежащего множеству R^r, и норму $\|u\|$ последовательности $u = \big(u(i)\big)_{i=0}^{\infty}$ над кольцом R по следующим правилам:

$$\|c\| = \max\big\{j \in \overline{0,n} \colon c \in p^jR\big\},$$
$$\|\bar{c}\| = \min\big\{\|c_j\| \colon j \in \overline{1,r}\big\},$$
$$\|u\| = \min\{\|u(j)\| \colon j \geqslant 0\}.$$

В дальнейшем нам понадобится следующий вспомогательный результат.

Лемма 1 [3]. *Система последовательностей $u_1, u_2, \ldots, u_r$ линейно независима над кольцом R тогда и только тогда, когда при всех $\bar{c} \in R^r$ выполнено равенство $\|u_{\bar{c}}\| = \|\bar{c}\|$.*

Пусть χ — аддитивный характер кольца R, определённый на элементах этого кольца равенством

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

где $R_0 = \{0, e, 2e, \ldots, (p^n - 1)e\}$ — подкольцо кольца R, порождённое единицей e кольца R и изоморфное кольцу $\mathbb{Z}_{p^n}$, $\mathrm{Tr}_{R_0}^R$ — функция следа из кольца R в кольцо R_0 (см. [9]).

Утверждение 1. *Для каждой линейно независимой системы последовательностей $u_1, u_2, \ldots, u_r$ из множества $L_R(F)$ имеет место неравенство*

$$\left|N_l(\bar{z}, u_1, \ldots, u_r) - \frac{l}{q^{nr}}\right| \leqslant \frac{1}{|R^*|}\sum_{k=0}^{n-1}\frac{q^r - 1}{q^{(k+1)r}}\max_{z \in R,\, \|z\| \geqslant k}\ \max_{u \in L_R(F),\, \|u\| = k}|\tau_l(z,u)|,$$

где

$$\tau_l(z,u) = \sum_{a \in R^*}\chi(-az)\sum_{i=0}^{l-1}\chi\big(au(i)\big). \tag{4}$$

Доказательство. Используя соотношения ортогональности для характеров (см., например, [2]), получаем

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

где $\bar{z} = (z_1, z_2, \ldots, z_r)$. Преобразовав это соотношение, будем иметь

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

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

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

где

$$\bar{c}\cdot\bar{z} = (c_1, c_2, \ldots, c_r)\cdot(z_1, z_2, \ldots, z_r) = c_1z_1 + c_2z_2 + \ldots + c_rz_r.$$

Заметим, что если a — фиксированный элемент из множества R^*, а вектор $\bar{c}$ пробегает всё множество $R^r \setminus \{\bar{0}\}$, то вектор $a\bar{c}$ также пробегает всё множество $R^r \setminus \{\bar{0}\}$. Используя равенства $(a\bar{c})\cdot\bar{z} = a(\bar{c}\cdot\bar{z})$, $au_{\bar{c}} = u_{a\bar{c}}$, получаем

$$N_l(\bar{z}, u_1, \ldots, u_r) - \frac{l}{q^{nr}} = \frac{1}{q^{nr}|R^*|} \sum_{a\in R^*} \sum_{\bar{c}\in R^r\setminus\{\bar{0}\}} \chi\big(-a(\bar{c}\cdot\bar{z})\big) \sum_{i=0}^{l-1} \chi\big(au_{\bar{c}}(i)\big).$$

Изменив порядок суммирования, будем иметь

$$N_l(\bar{z}, u_1, \ldots, u_r) - \frac{l}{q^{nr}} = \frac{1}{q^{nr}|R^*|} \sum_{k=0}^{n-1} \sum_{\bar{c}\in R^r\setminus\{\bar{0}\},\, \|\bar{c}\|=k} \tau_l(\bar{c}\cdot\bar{z}, u_{\bar{c}}).$$

Количество векторов $\bar{c}\in R^r$, имеющих норму k, равно $q^{(n-k-1)r}(q^r-1)$ для всех $k \in \{0, 1, \ldots, n-1\}$. Тогда

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

Для завершения доказательства остаётся воспользоваться леммой 1 и заметить, что в условиях утверждения при всех $\bar{c}\in R^r$ последовательность $u_{\bar{c}}$ является линейной рекуррентной последовательностью с характеристическим многочленом $F(x)$ и выполнено неравенство $\|\bar{c}\cdot\bar{z}\| \geqslant \|\bar{c}\|$. □

В дальнейшем будем исследовать тригонометрическую сумму $\tau_l(z, u)$, где u — последовательность из множества $L_R(F)$.

3. Семейство сдвигов последовательности

Пусть u — чисто периодическая последовательность, состоящая из элементов кольца $R = GR(q^n, p^n)$, т. е. при некотором натуральном числе T выполнены равенства $u(i+T) = u(i)$ для всех $i \geqslant 0$. Назовём сдвигом последовательности u последовательность $x^j u$, где j — целое неотрицательное число. Обозначим $P(u)$ — множество всех сдвигов последовательности u. Если $T = T(u)$ —

период последовательности u, то $P(u) = \{u, xu, x^2u, \dots, x^{T-1}u\}$. Отметим, что если $F(x)$ — реверсивный многочлен Галуа над кольцом R, то каждая линейная рекуррентная последовательность из множества $L_R(F)$ является чисто периодической последовательностью.

В дальнейшем понадобятся следующие леммы.

Лемма 2 [2]. *Для характера χ кольца $R = GR(q^n, p^n)$, определённого равенством* (3)*, справедливы соотношения*

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

Лемма 3. *Пусть u — чисто периодическая последовательность из элементов кольца $R = GR(q^n, p^n)$, $z \in R$, $T = T(u)$. Тогда при всех $j \in \{0, 1, \dots, T-1\}$ для значений суммы $\tau_l(z, u)$, определённой равенством* (4)*, справедливы соотношения*

$$|\tau_l(z,u) - \tau_l(z, x^j u)| \leqslant q^n j, \quad |\tau_l(z,u) - \tau_l(z, x^{T-j}u)| \leqslant q^n j.$$

Доказательство. Используя лемму 2, получаем, что для каждой последовательности v над кольцом R выполнены равенства

$$\tau_l(z,v) = \sum_{i=0}^{l-1} \sum_{a \in R^*} \chi\big(a(v(i) - z)\big) = N_l(z,v)|R^*| - D_l(z,v)|pR|, \tag{5}$$

где $N_l(z,v)$ — количество появлений элемента z среди элементов $v(0), v(1), \dots, v(l-1)$, а $D_l(z,v)$ — количество элементов вида $z + p^{n-1}c$, $c \in R$, $p^{n-1}c \neq 0$ среди элементов $v(0), v(1), \dots, v(l-1)$. Используя равенство (5) и учитывая, что векторы $\big(u(0), u(1), \dots, u(l-1)\big)$, $\big(u(j), u(j+1), \dots, u(j+l-1)\big)$, а также векторы $\big(u(0), u(1), \dots, u(l-1)\big)$, $\big(u(T-j), u(T-j+1), \dots, u(T-j+l-1)\big)$ содержат по меньшей мере $l - j$ равных элементов, получаем

$$\begin{aligned} |\tau_l(z,u) - \tau_l(z, x^j u)| &\leqslant \\ &\leqslant |N_l(z,u) - N_l(z, x^j u)|\,|R^*| + |D_l(z,u) - D_l(z, x^j u)|\,|pR| \leqslant j|R| \end{aligned}$$

и аналогично

$$|\tau_l(z,u) - \tau_l(z, x^{T-j}u)| \leqslant j|R|. \qquad \square$$

Лемма 4 [1]. *Для всех неотрицательных действительных чисел x и натуральных чисел s имеет место неравенство*

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

где $[x/s]$ — целая часть числа x/s.

Теорема 1. *Пусть u — чисто периодическая последовательность из элементов кольца $R = GR(q^n, p^n)$, $z \in R$, $T = T(u)$, $l \leqslant T/2$. Тогда имеет место неравенство*

$$|\tau_l(z,u)| \leqslant \left(\frac{3q^n}{2} \sum_{v \in P(u)} |\tau_l(z,v)|^2\right)^{1/3}.$$

Доказательство. Выберем последовательность ω, имеющую максимальное значение величины $|\tau_l(z,v)|$ среди всех линейных рекуррентных последовательностей v из множества $P(u)$. Пусть $\tau = |\tau_l(z,\omega)|$. Для доказательства теоремы достаточно показать, что

$$\tau \leqslant \left(\frac{3q^n}{2} \sum_{v \in P(u)} |\tau_l(z,v)|^2\right)^{1/3}.$$

Для всех чисел $s \in \{0,1,\ldots,T-1\}$ положим $\omega_s = x^s\omega$, $\omega_{-s} = x^{T-s}\omega$. Из равенства (5) следует, что $\tau = |\tau_l(z,\omega)| \leqslant l|R^*|$, а значит, $[\tau/q^n] < l \leqslant T/2$. Это неравенство гарантирует, что все последовательности

$$\omega_{-[\tau/q^n]}, \ldots, \omega_{-1}, \omega_0, \omega_1, \ldots, \omega_{[\tau/q^n]}$$

являются попарно различными. Согласно лемме 3 для всех $j \in \{0,1,\ldots,T-1\}$ выполнены неравенства

$$|\tau_l(z,\omega_j)| \geqslant \tau - q^n j, \quad |\tau_l(z,\omega_{-j})| \geqslant \tau - q^n j,$$

а тогда, используя лемму 4, получаем

$$\sum_{v \in P(u)} |\tau_l(z,v)|^2 = \sum_{v \in P(\omega)} |\tau_l(z,v)|^2 \geqslant \tau^2 + 2\sum_{j=1}^{[\tau/q^n]} (\tau - q^n j)^2 \geqslant \frac{2\tau^3}{3q^n}. \qquad \square$$

4. Уточнение оценок с использованием мультипликаторов многочленов

Пусть $F(x)$ — реверсивный многочлена Галуа над кольцом $R = GR(q^n, p^n)$, имеющий степень m. Известно (см. [9,15]), что в расширении $S = GR(q^{mn}, p^n)$ кольца R содержится корень α многочлена $F(x)$, причём $\alpha \in S^*$. Группа S^* является прямым произведением своих подгрупп $\Gamma(S) = \{x \in S\colon x^{q^m-1} = e\}$ и $e + pS$, причём группа $\Gamma(S)$ является циклической подгруппой порядка $q^m - 1$. Пусть $\alpha = \alpha_0\beta$, где $\alpha_0 \in \Gamma(S)$, $\beta \in e + pS$. Рассмотрим период $T(F)$ многочлена $F(x)$. Справедливы равенства $T(F) = p^\nu T(\bar{F}) = p^\nu(q^m-1)/d$, где $0 \leqslant \nu \leqslant n-1$, а d — делитель числа $q^m - 1$. Кроме того, мультипликативные порядки $\operatorname{ord}\alpha_0$ и $\operatorname{ord}\beta$ элементов α_0 и β соответственно удовлетворяют равенствам $\operatorname{ord}\alpha_0 = T(\bar{F})$, $\operatorname{ord}\beta = p^\nu$.

В дальнейшем нам понадобится понятие мультипликатора многочлена. По аналогии с [8] назовём абсолютным мультипликатором многочлена $F(x)$ над

кольцом R множество

$$M_R(F) = \{a \in \Gamma(R)\colon F(x) \mid x^j - a \text{ при некотором } j \geqslant 0\}.$$

Опишем свойства множества $\mathrm{M}_R(F)$.

Утверждение 2. *Пусть $F(x)$ — реверсивный многочлен Галуа над кольцом $R = GR(q^n, p^n)$, $t = (T(\bar{F}), q-1)$. Справедливы следующие утверждения*:

1) $M_R(F) = \langle\alpha\rangle \cap \Gamma(R)$, *где $\langle\alpha\rangle$ — группа, порождённая элементом α,*
2) *для каждой ненулевой последовательности $u \in L_R(F)$ и элемента $a \in M_R(F)$ выполнено включение $au \in P(u)$, причём если $au = x^j u$ для некоторого числа $j \in \mathbb{N}_0$, то $T(\bar{F})/t$ делит j,*
3) $|M_R(F)| = t$.

Доказательство. Для доказательства утверждения 1) достаточно заметить, что многочлен $F(x)$ делит многочлен $x^j - a$ для некоторого целого неотрицательного числа j тогда и только тогда, когда $\alpha^j = a$.

Докажем утверждение 2). Представим линейную рекуррентную последовательность u, используя функцию следа:

$$u(i) = \mathrm{Tr}_R^S(b\alpha^i), \quad i \geqslant 0, \tag{6}$$

где b — однозначно определённый ненулевой элемент кольца S (см. [9, теорема 8]). Если $a \in M_R(F)$, то $a = \alpha^j$ для некоторого числа $j \geqslant 0$, и для последовательности $v = au$ справедливы равенства

$$v(i) = a\,\mathrm{Tr}_R^S(b\alpha^i) = \mathrm{Tr}_R^S(ab\alpha^i) = \mathrm{Tr}_R^S(b\alpha^{i+j}) = u(i+j).$$

Значит, $v = x^j u$ и $v \in P(u)$. Из равенства $au = x^j u$ и соотношения (6) следует, что элемент $\alpha^j - a$ принадлежит множеству pS. Обозначим $\bar{\alpha}$ образ элемента α при действии естественного эпиморфизма из кольца S в поле $S/pS = GF(q^m)$. Тогда элемент $\bar{\alpha}^j$ будет принадлежать полю $GF(q)$. Это возможно тогда и только тогда, когда $\mathrm{ord}\,\bar{\alpha} = T(\bar{F})$ делит $j(q-1)$, т. е. когда $T(\bar{F})/t$ делит j.

Докажем утверждение 3). Используя утверждение 1) и равенство $R^* = \Gamma(R)\dot{\times}(e + pR)$, получаем

$$|M_R(F)| = |\{j \in \overline{0, T(F)-1}\colon \alpha_0^j \in \Gamma(R),\ \beta^j = e\}|. \tag{7}$$

Элемент α_0^j принадлежит $\Gamma(R)$ тогда и только тогда, когда $\alpha_0^{j(q-1)} = e$. Это условие равносильно тому, что $T(\bar{F})/t$ делит j. Так как $\mathrm{ord}\,\beta = p^\nu$, равенство $\beta^j = e$ выполнено тогда и только тогда, когда p^ν делит j. В итоге, используя равенство (7), получаем $|M_R(F)| = t$. □

Следующий результат при некоторых более сильных ограничениях на l существенно уточняет теорему 1 в случае, когда $z = 0$.

Теорема 2. *Пусть $F(x)$ — реверсивный многочлен Галуа над кольцом $R = GR(q^n, p^n)$, u — ненулевая линейная рекуррентная последовательность из*

множества $L_R(F)$, $t = (T(\bar{F}), q-1)$. *Тогда при* $l \leqslant T(\bar{F})/(2t)$ *справедливо неравенство*

$$|\tau_l(0,u)| \leqslant \left(\frac{3q^n}{2t}\sum_{v\in P(u)}|\tau_l(0,v)|^2\right)^{1/3}.$$

Доказательство. Зададим на множестве $P(u)$ бинарное отношение $\sim$, положив для всех $v, v' \in P(u)$ $v \sim v'$ тогда и только тогда, когда найдётся элемент $a \in \mathrm{M}_R(F)$, такой что $v = av'$. Отношение $\sim$ является отношением эквивалентности на множестве $P(u)$. Кроме того, если $v \sim v'$, то $\tau_l(0,v) = \tau_l(0,v')$. Обозначим $\{v\}$ класс эквивалентности относительно рассматриваемого отношения $\sim$, содержащий представитель v. Пусть ω — линейная рекуррентная последовательность из множества $P(u)$, имеющая максимальное значение величины $|\tau_l(0,v)|$ среди всех линейных рекуррентных последовательностей v из множества $P(u)$, и пусть $\tau_0 = |\tau_l(0,\omega)|$. По доказанному в теореме 1 справедливо неравенство $[\tau_0/q^n] < l$, а значит, $[\tau_0/q^n] < T(\bar{F})/(2t) \leqslant T(u)/(2t)$. Тогда, определив для всех чисел $s \in \{0,1,\ldots,T(u)-1\}$ последовательности $\omega_s = x^s\omega$, $\omega_{-s} = x^{T(u)-s}\omega$, рассмотрим следующие классы:

$$\{\omega_{-[\tau_0/q^n]}\},\ldots,\{\omega_{-1}\},\{\omega_0\},\{\omega_1\},\ldots,\{\omega_{[\tau_0/q^n]}\}.$$

Согласно пункту 2) утверждения 2 эти классы являются попарно различными, причём по пункту 3) утверждения 2 каждый из рассматриваемых классов имеет мощность $t = |M_R(F)|$. В итоге, используя леммы 3 и 4, получаем

$$\sum_{v\in P(u)}|\tau_l(0,v)|^2 \geqslant t\left(\tau_0^2 + 2\sum_{j=1}^{[\tau_0/q^n]}(\tau_0 - q^n j)^2\right) \geqslant \frac{2t\tau_0^3}{3q^n}. \qquad \square$$

5. Оценки тригонометрических сумм

Получим оценки для тригонометрической суммы $\sum\limits_{v\in P(u)}|\tau_l(z,v)|^2$, где сумма $\tau_l(z,v)$ определена равенством (4).

Нам понадобятся следующие леммы.

Лемма 5. *Пусть* χ — *аддитивный характер кольца* $R = GR(q^n,p^n)$, *определённый равенством* (3), $f = |R^*| = q^{n-1}(q-1)$, $z \in R$, $\|z\| \geqslant k$, *где* $0 \leqslant k \leqslant n-1$. *Тогда справедливы равенства*

$$\sum_{c\in R^*}\sum_{a\in c+p^{n-k}R}\chi\big((c-a)z\big) = q^k f,$$

$$\sum_{c\in R^*}\sum_{a\in R^*\setminus c+p^{n-k}R}\chi\big((c-a)z\big) = \begin{cases} f^2 - q^k f, & \text{если } \|z\| = n,\\ q^{2(n-1)} - q^k f, & \text{если } \|z\| = n-1,\\ -q^k f, & \text{если } \|z\| < n-1. \end{cases}$$

Доказательство. Первое равенство следует из равенств

$$\sum_{c\in R^*}\sum_{a\in c+p^{n-k}R}\chi\big((c-a)z\big)= \\ =\sum_{c\in R^*}\sum_{d\in p^{n-k}R}\chi(dz)=\sum_{c\in R^*}\sum_{d\in p^{n-k}R}\chi(0)=|R^*|\,|p^{n-k}R|.$$

Покажем, что справедливо второе равенство. Используя лемму 2, получаем

$$\sum_{c,a\in R^*}\chi\big((c-a)z\big)=\Big|\sum_{d\in R^*}\chi(dz)\Big|^2=\begin{cases}f^2, & \text{если } \|z\|=n,\\ q^{2(n-1)}, & \text{если } \|z\|=n-1,\\ 0, & \text{если } \|z\|<n-1.\end{cases}$$

Теперь для завершения доказательства остаётся заметить, что $c+p^{n-k}R\subset R^*$ при всех $c\in R^*$ и $k\in\{0,1,\dots,n-1\}$, что приводит к равенству

$$\sum_{c\in R^*}\sum_{a\in R^*\setminus c+p^{n-k}R}\chi\big((c-a)z\big)=\sum_{c,a\in R^*}\chi\big((c-a)z\big)-\sum_{c\in R^*}\sum_{a\in c+p^{n-k}R}\chi\big((c-a)z\big).\ \square$$

Лемма 6 [2]. *Пусть $F(x)$ — реверсивный многочлен Галуа степени m над кольцом $R=GR(q^n,p^n)$, $T(F)=p^\nu T(\bar F)=p^\nu(q^m-1)/d$, где $0\leqslant\nu\leqslant n-1$, а d — делитель числа q^m-1. Тогда для каждой ненулевой линейной рекуррентной последовательности $u\in L_R(F)$ выполнено неравенство*

$$\Big|\sum_{s=0}^{T(F)-1}\chi\big(u(s)\big)+\frac{p^\nu}{d}\Big|\leqslant\frac{p^\nu(dp^{n-\|u\|-1}-1)}{d}q^{m/2}.$$

Теорема 3. *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 линейная рекуррентная последовательность из множества $L_R(F)$, $\|u\|=k$, $f=q^{n-1}(q-1)$, $t=(T(\bar F),q-1)$, $z\in R$, $\|z\|\geqslant k$, $l\leqslant T(\bar F)/t$. Тогда*

$$\sum_{v\in P(u)}|\tau_l(z,v)|^2\leqslant\frac{T(u)lf}{q^m-1}\big(q^{m+k}-\delta_k(z)l+(lf-q^k)(dp^{n-k-1}-1)q^{m/2}\big),$$

где

$$\delta_k(z)=\begin{cases}f, & \text{если } z=0,\\ \dfrac{q^{2(n-1)}}{f}, & \text{если } z\neq0,\ k=n-1,\\ 0, & \text{если } z\neq0,\ k<n-1.\end{cases}$$

Доказательство. Так как $F(x)$ — реверсивный многочлен, то u — чисто периодическая последовательность и $P(u)=\{v_0,v_1,\dots,v_{T(u)-1}\}$, где $v_k=x^ku$ для всех $k\geqslant0$. Число $T(u)$ делит число $T(F)$, поэтому справедливо соотношение

$$\sum_{v\in P(u)}|\tau_l(z,v)|^2=\frac{T(u)}{T(F)}\sum_{s=0}^{T(F)-1}|\tau_l(z,v_s)|^2.$$

Имеет место равенство

$$\sum_{s=0}^{T(F)-1} |\tau_l(z,v_s)|^2 = \sum_{s=0}^{T(F)-1} \tau_l(z,v_s)\overline{\tau_l(z,v_s)},$$

где черта означает комплексное сопряжение. Тогда

$$\sum_{v\in P(u)} |\tau_l(z,v)|^2 = \frac{T(u)}{T(F)} \sum_{s=0}^{T(F)-1} \sum_{a,c\in R^*} \chi\big((c-a)z\big) \sum_{i,j=0}^{l-1} \chi\big(av_s(i) - cv_s(j)\big). \quad (8)$$

Разобьём правую часть равенства (8) на две суммы, рассмотрев отдельно случаи, когда $i = j$ и $i \neq j$:

$$\sum_{v\in P(u)} |\tau_l(z,v)|^2 = S_1 + S_2, \quad (9)$$

где

$$S_1 = \frac{T(u)}{T(F)} \sum_{s=0}^{T(F)-1} \sum_{a,c\in R^*} \chi\big((c-a)z\big) \sum_{i=0}^{l-1} \chi\big((a-c)v_s(i)\big),$$

$$S_2 = \frac{T(u)}{T(F)} \sum_{s=0}^{T(F)-1} \sum_{a,c\in R^*} \chi\big((c-a)z\big) \sum_{i\neq j} \chi\big(av_s(i) - cv_s(j)\big).$$

Рассмотрим величину S_1. Заметим, что при фиксированном $i\in\{0,1,\ldots,l-1\}$ если s пробегает всё множество $\{0,1,\ldots,T(F)-1\}$, то величина $v_s(i)$ пробегает все значения $u(0), u(1), \ldots, u(T(F)-1)$, значит,

$$S_1 = \frac{T(u)l}{T(F)} \sum_{a,c\in R^*} \chi\big((c-a)z\big) \sum_{s=0}^{T(F)-1} \chi\big((a-c)u(s)\big).$$

При $a, c \in R^*$ обозначим $u_{a,c}$ последовательность, элементы которой определены равенствами

$$u_{a,c}(i) = (a-c)u(i), \quad i \geqslant 0.$$

Выясним, в каких случаях последовательность $u_{a,c}$ является нулевой. Так как $\|u\| = k$, то $\|u_{a,c}\| = \|a-c\| + k$. Отсюда получаем, что $u_{a,c}$ — нулевая последовательность тогда и только тогда, когда $a - c \in p^{n-k}R$. Другими словами, при каждом фиксированном $c \in R^*$, элемент a должен принадлежать множеству $c + p^{n-k}R$. Тогда верно равенство

$$S_1 = T(u)l \sum_{c\in R^*} \sum_{a\in c+p^{n-k}R} \chi\big((c-a)z\big) + \\ + \frac{T(u)l}{T(F)} \sum_{c\in R^*} \sum_{a\in R^*\setminus c+p^{n-k}R} \chi\big((c-a)z\big) \sum_{s=0}^{T(F)-1} \chi\big(u_{a,c}(s)\big).$$

Изменив порядок суммирования и добавив в последнюю сумму слагаемое p^ν/d, получим

$$S_1 = S_1' + \frac{T(u)l}{T(F)} \sum_{c\in R^*} \sum_{a\in R^*\setminus c+p^{n-k}R} \chi\big((c-a)z\big)\Big(\sum_{s=0}^{T(F)-1} \chi\big(u_{a,c}(s)\big) + \frac{p^\nu}{d}\Big), \quad (10)$$

где

$$S_1' = T(u)l \sum_{c\in R^*}\Big(\sum_{a\in c+p^{n-k}R} \chi\big((c-a)z\big) - \frac{1}{q^m-1} \sum_{a\in R^*\setminus c+p^{n-k}R} \chi\big((c-a)z\big)\Big).$$

Рассмотрим величину S_2. Изменив порядок суммирования в выражении, будем иметь

$$S_2 = \frac{T(u)}{T(F)} \sum_{a,c\in R^*} \chi\big((c-a)z\big) \sum_{i\neq j} \sum_{s=0}^{T(F)-1} \chi\big(u_{a,c,i,j}(s)\big),$$

где для всех $a, c \in R^*$, $i, j \in \{0, 1, \ldots, l-1\}$ последовательность $u_{a,c,i,j}$ определена равенствами

$$u_{a,c,i,j}(s) = av_s(i) - cv_s(j) = au(i+s) - cu(j+s), \quad s \geqslant 0.$$

Представим линейную рекуррентную последовательность u, используя функцию следа:

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

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

$$u_{a,c,i,j}(s) = \mathrm{Tr}_R^S(ab\alpha^{i+s} - cb\alpha^{j+s}) = \mathrm{Tr}_R^S\big((a\alpha^i - c\alpha^j)b\alpha^s\big), \quad s \geqslant 0.$$

Покажем, что элемент $a\alpha^i - c\alpha^j$ является обратимым элементом кольца S. Допустим противное: $a\alpha^i - c\alpha^j \in pS$. Тогда для образа $\bar\alpha$ элемента α при действии естественного эпиморфизма колец $S \to S/pS$ получим $\bar\alpha^{i-j} \in GF(q)$. Данное включение возможно тогда и только тогда, когда $T(\bar F)/t$ делит $i-j$, что невозможно при различных i, j из множества $\{0, 1, \ldots, l-1\}$, где $l \leqslant T(\bar F)/t$. Таким образом, последовательность $u_{a,c,i,j}$ является ненулевой линейной рекуррентной последовательностью с характеристическим многочленом $F(x)$, причём $\|u_{a,c,i,j}\| = \|b\| = \|u\| = k$. Возвращаясь к сумме S_2, имеем

$$S_2 = S_2' + \frac{T(u)}{T(F)} \sum_{a,c\in R^*} \chi\big((c-a)z\big) \sum_{i\neq j}\Big(\sum_{s=0}^{T(F)-1} \chi\big(u_{a,c,i,j}(s)\big) + \frac{p^\nu}{d}\Big), \quad (11)$$

где

$$S_2' = -\frac{T(u)l(l-1)}{q^m-1} \sum_{a,c\in R^*} \chi\big((c-a)z\big) =$$

$$= -\frac{T(u)l(l-1)}{q^m-1} \sum_{c\in R^*}\Big(\sum_{a\in c+p^{n-k}R} \chi\big((c-a)z\big) + \sum_{a\in R^*\setminus c+p^{n-k}R} \chi\big((c-a)z\big)\Big).$$

Используя равенства (9)—(11), получаем

$$\sum_{v\in P(u)}|\tau_l(z,v)|^2 = D_1 + D_2, \tag{12}$$

где

$$D_1 = S_1' + S_2' =$$
$$= \frac{T(u)l}{q^m-1}\sum_{c\in R^*}\Biggl((q^m-l)\sum_{a\in c+p^{n-k}R}\chi\bigl((c-a)z\bigr) - l\sum_{a\in R^*\setminus c+p^{n-k}R}\chi\bigl((c-a)z\bigr)\Biggr),$$

$$D_2 = \frac{T(u)}{T(F)}\Biggl(l\sum_{(a,c)\in M_1}\chi\bigl((c-a)z\bigr)\Biggl(\sum_{s=0}^{T(F)-1}\chi\bigl(u_{a,c}(s)\bigr)+\frac{p^\nu}{d}\Biggr)+$$

$$+\sum_{(a,c)\in M_2}\chi\bigl((c-a)z\bigr)\sum_{i\neq j}\Biggl(\sum_{s=0}^{T(F)-1}\chi\bigl(u_{a,c,i,j}(s)\bigr)+\frac{p^\nu}{d}\Biggr)\Biggr),$$

множество M_1 состоит из всех пар (a,c), в которых $c\in R^*$, $a\in R^*\setminus c+p^{n-k}R$, $M_2 = R^*\times R^*$. Используя лемму 5, получаем

$$D_1 = \begin{cases} h(q^{m+k}f - lf^2), & \text{если } \|z\| = n,\\ h(q^{m+k}f - lq^{2(n-1)}), & \text{если } \|z\| = n-1,\\ hq^{m+k}f, & \text{если } \|z\| < n-1,\end{cases}$$

где $h = T(u)l/(q^m-1)$. Таким образом, справедлива оценка

$$D_1 \leqslant \frac{T(u)lf}{q^m-1}(q^{m+k} - \delta_k(z)l). \tag{13}$$

Применяя лемму 6 и соотношения $\|u_{a,c}\|\geqslant k$ для всех $(a,c)\in M_1$, $\|u_{a,c,i,j}\| = k$ для всех $(a,c)\in M_2$, получаем неравенство

$$D_2 \leqslant \frac{T(u)}{T(F)}\left(lf(f-q^k)\frac{p^\nu}{d}(dp^{n-k-1}-1)q^{m/2} + f^2l(l-1)\frac{p^\nu}{d}(dp^{n-k-1}-1)q^{m/2}\right),$$

равносильное неравенству

$$D_2 \leqslant \frac{T(u)lf}{q^m-1}(lf-q^k)(dp^{n-k-1}-1)q^{m/2}. \tag{14}$$

Используя соотношения (12)—(14), получаем

$$\sum_{v\in P(u)}|\tau_l(z,v)|^2 \leqslant \frac{T(u)lf}{q^m-1}(q^{m+k} - \delta_k(z)l + (lf-q^k)(dp^{n-k-1}-1)q^{m/2}). \qquad \square$$

Непосредственно из теорем 1 и 3 выводится важное следствие.

Следствие 1. *Пусть в условиях теоремы* 3 $l\leqslant T(u)/2$. *Тогда при всех* $z\in R$ *имеет место оценка*

$$|\tau_l(z,u)| \leqslant \left(\frac{3T(u)q^nlf}{2(q^m-1)}\bigl(q^{m+k} - \delta_k(z)l + (lf-q^k)(dp^{n-k-1}-1)q^{m/2}\bigr)\right)^{1/3}.$$

В случае $z = 0$ оценку из следствия 1 уточняет следующее следствие теорем 2 и 3.

Следствие 2. *Пусть в условиях теоремы* 3 $l \leqslant T(\bar{F})/(2t)$. *Тогда*

$$|\tau_l(0,u)| \leqslant \left(\frac{3T(u)q^n lf}{2(q^m-1)t}\big(q^{m+k} - lf + (lf - q^k)(dp^{n-k-1}-1)q^{m/2}\big)\right)^{1/3}.$$

6. Оценки числа появлений наборов в линейных рекуррентных последовательностях векторов

Перейдём к исследованию частотных характеристик линейных рекуррентных последовательностей векторов. Получим оценки числа $N_l(\bar{z}, u_1, \ldots, u_r)$ появлений набора $\bar{z} = (z_1, z_2, \ldots, z_r) \in R^r$ среди векторов $\big(u_1(i), u_2(i), \ldots, u_r(i)\big)$, где $i = 0, 1, \ldots, l-1$.

Теорема 4. *Пусть $F(x)$ — реверсивный многочлен Галуа степени m над кольцом $R = GR(q^n, p^n)$, $T(F) = p^\nu T(\bar{F}) = p^\nu(q^m-1)/d$, $u_1, u_2, \ldots, u_r$ — линейно независимая система линейных рекуррентных последовательностей из множества $L_R(F)$, $f = q^{n-1}(q-1)$, $t = (T(\bar{F}), q-1)$. Тогда для всех $\bar{z} \in R^r$ и всех $l \in \mathbb{N}$, таких что $l \leqslant \min\{T(\bar{F})/2, T(\bar{F})/t\}$, справедлива оценка*

$$\left|N_l(\bar{z}, u_1, \ldots, u_r) - \frac{l}{q^{nr}}\right| \leqslant \sum_{k=0}^{n-1} \frac{(q^r-1)G_{l,k}(F)}{q^{(k+1)r}}, \tag{15}$$

где

$$G_{l,k}(F) = \left(\frac{3p^\nu lq}{2(q-1)df}\big(q^{m+k} - \delta_k l + (lf - q^k)(dp^{n-k-1}-1)q^{m/2}\big)\right)^{1/3},$$

$$\delta_k = \begin{cases} 0, & \text{если } k < n-1, \\ \dfrac{q^{n-1}}{q-1}, & \text{если } k = n-1. \end{cases}$$

Доказательство. Достаточно воспользоваться утверждением 1, следствием 1 и неравенствами

$$T(\bar{F}) \leqslant T(u), \quad \frac{T(u)}{q^m-1} \leqslant \frac{p^\nu}{d},$$

справедливыми для каждой ненулевой линейной рекуррентной последовательности u с характеристическим многочленом $F(x)$. □

Следствие 3. *Пусть в условиях теоремы* 4 *дополнительно выполнены соотношения*

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

где $\varkappa(q) = q/\big(2(q-1)\big)$. *Тогда среди векторов* $\big(u_1(i), u_2(i), \ldots, u_r(i)\big)$, $i = 0, 1, \ldots, l-1$, *появятся все векторы из множества* R^r.

Доказательство. Обозначим G правую часть неравенства (15). Из неравенства (15) выводим, что $l/q^{nr} - G \leqslant N_l(\bar{z}, u_1, \ldots, u_r)$. Тогда если $l/q^{nr} - G > 0$, то вектор $\bar{z}$ появляется среди первых l элементов линейной рекуррентной последовательности векторов. Это неравенство выполнено при условии

$$l \geqslant (q^{nr}-1)\left(\frac{3p^{\nu}l\varkappa(q)}{f}\big(q^{m+n-1} + lf(p^{n-1}-1)q^{m/2}\big)\right)^{1/3}.$$

Это соотношение при $l \geqslant q^{m/2}$ имеет место, если

$$l \geqslant (q^{nr}-1)\left(\frac{3p^{\nu}l\varkappa(q)}{f}\big(q^{m/2+n-1}l + lf(p^{n-1}-1)q^{m/2}\big)\right)^{1/3}.$$

Последнее неравенство равносильно тому, что

$$l \geqslant 3\varkappa(q)(q^{nr}-1)^3 p^{\nu} q^{m/2}\left(\frac{1}{q-1} + p^{n-1} - 1\right). \qquad \square$$

В частности, из доказательства следствия 3 следует, что при выполнении условия

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

оценка (15), рассматриваемая в случае, когда $d = 1$, является нетривиальной.

Следствие 4. *Пусть в условиях теоремы* 4 *дополнительно выполнены соотношения* $T(\bar{F}) = q^m - 1$, $q \geqslant 3$. *Тогда при* $m \geqslant 2(1 + (n-1)\log_q p)$ *имеют место неравенства*

$$\left|N_l(\bar{z}, u_1, \ldots, u_r) - \frac{l}{q^{nr}}\right| \leqslant G_l(F) \leqslant \varkappa(q)^{1/3} S_l(F),$$

где $S_l(F)$ *и* $G_l(F)$ *— правые части неравенств* (1) *и* (15) *соответственно.*

Доказательство. Достаточно доказать, что при всех $k \in \{0, 1, \ldots, n-1\}$ имеет место неравенство

$$G_{l,k}(F) \leqslant \varkappa(q)^{1/3} S_{l,k}(F),$$

где величина $S_{l,k}(F)$ определена равенством (2). Необходимо проверить, что для всех $k \in \{0, 1, \ldots, n-1\}$ справедливо неравенство

$$\frac{1}{f}\big(q^{m+k} + (lf - q^k)(p^{n-k-1}-1)q^{m/2}\big) \leqslant q^m - l + (l-1)(p^{n-k-1}-1)q^{m/2}.$$

Это соотношение выполнено, когда

$$l \leqslant \frac{1}{f}(f - q^k)\big(q^m - (p^{n-k-1}-1)q^{m/2}\big). \tag{16}$$

При $k = n-1$ неравенство (16) имеет вид

$$l \leqslant \frac{q-2}{q-1}q^m$$

и справедливо при всех $l \leqslant T(\bar{F})/2$. При $k \leqslant n-2$ неравенство (16) выполнено при

$$l \leqslant \left(1 - \frac{1}{q(q-1)}\right)\left(q^m - (p^{n-1}-1)q^{m/2}\right).$$

Так как при $q \geqslant 3$ величина $1 - 1/\big(q(q-1)\big)$ не меньше $5/6$, то для выполнения неравенства (16) достаточно выполнения неравенства

$$l \leqslant \frac{5}{6}\left(q^m - (p^{n-1}-1)q^{m/2}\right),$$

и оно справедливо при всех $l \leqslant T(\bar{F})/2$, где $m \geqslant 2(1 + (n-1)\log_q p)$. □

Из следствия 4 вытекает, что при $d = 1$, $q \geqslant 3$ и некоторых ограничениях на m оценка (15) точнее оценки (1), причём оценка (15) отличается от оценки (1) мультипликативным множителем

$$\varkappa(q)^{1/3} = \left(\frac{q}{2(q-1)}\right)^{1/3}.$$

Этот множитель монотонно уменьшается с ростом q и стремится к величине $1/\sqrt[3]{2} = 0{,}7937\ldots$ Приведём таблицу некоторых начальных значений величины $\varkappa(q)^{1/3}$ с точностью до четырёх знаков после запятой.

q	3	4	5	7	8	9	11	13	16
$\varkappa(q)^{1/3}$	0,9086	0,8736	0,8549	0,8356	0,8298	0,8255	0,8193	0,8151	0,8109

Сравним оценки (1) и (15) в случае, когда $d = 1$ и $q = 2$. Несложно проверить, что при $n = 1$, т. е. когда $R = GF(2)$, рассматриваемые оценки совпадают. Если же $n > 1$, то, рассуждая аналогично доказательству следствия 4, нетрудно показать, что оценка (15) точнее оценки (1) при $l < (2^m - (2^{n-1}-1)2^{m/2})/2$.

7. Оценки для количества нулей в линейной рекуррентной последовательности векторов

Уточним оценки из предыдущего раздела для числа $N_l(\bar{0}, u_1, \ldots, u_r)$ появлений набора $\bar{0} = (0, 0, \ldots, 0) \in R^r$ среди векторов $\big(u_1(i), u_2(i), \ldots, u_r(i)\big)$, $i = 0, 1, \ldots, l-1$. Непосредственно из утверждения 1 и следствия 2 получим следующий результат.

Теорема 5. *Пусть $F(x)$ — реверсивный многочлен Галуа степени m над кольцом $R = GR(q^n, p^n)$, $T(F) = p^\nu T(\bar{F}) = p^\nu(q^m-1)/d$, $u_1, u_2, \ldots, u_r$ — линейно независимая система линейных рекуррентных последовательностей из множества $L_R(F)$, $t = (T(\bar{F}), q-1)$, $f = q^{n-1}(q-1)$. Тогда для всех $l \in \mathbb{N}$, таких что*

$l \leqslant T(\bar{F})/(2t)$, справедлива оценка

$$\left| N_l(\bar{0}, u_1, \ldots, u_r) - \frac{l}{q^{nr}} \right| \leqslant \sum_{k=0}^{n-1} \frac{(q^r-1)H_{l,k}(F)}{q^{(k+1)r}}, \tag{17}$$

где

$$H_{l,k}(F) = \left(\frac{3p^\nu lq}{2(q-1)dft} \big(q^{m+k} - lf + (lf - q^k)(dp^{n-k-1} - 1)q^{m/2}\big) \right)^{1/3}.$$

Аналогично доказательству следствия 3 несложно получить следующее утверждение, вытекающее из теоремы 5 и утверждения 2, описывающего свойства абсолютного мультипликатора $M_R(F)$ многочлена $F(x)$.

Следствие 5. *Пусть в условиях теоремы* 5 *дополнительно выполнены соотношения*

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

где $h(q) = q/(2(q-1)^2)$. Тогда среди векторов $\big(u_1(i), u_2(i), \ldots, u_r(i)\big)$, где $i = 0, 1, \ldots, l-1$, появится вектор $\bar{0} \in R^r$.

Следствие 5, в частности, показывает, что при выполнении условия

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

оценка (17), рассматриваемая в случае, когда $d = 1$, нетривиальна.

Сравним при $d = 1$ оценки (1) и (17). По аналогии с доказательством следствия 4 несложно доказать следующий результат.

Следствие 6. *Пусть в условиях теоремы* 5 *дополнительно выполнено соотношение $T(\bar{F}) = q^m - 1$. Тогда при $m \geqslant 2(n-1)\log_q p$ имеют место неравенства*

$$\left| N_l(\bar{0}, u_1, \ldots, u_r) - \frac{l}{q^{nr}} \right| \leqslant H_l(F) \leqslant h(q)^{1/3} S_l(F),$$

где $S_l(F)$, $H_l(F)$ — правые части неравенств (1) *и* (17) *соответственно.*

Из следствия 6 следует, что при некоторых ограничениях на m оценка (17) отличается от оценки (1) мультипликативным множителем

$$h(q)^{1/3} = \left(\frac{q}{2(q-1)^2} \right)^{1/3}.$$

Этот множитель при $q \geqslant 3$ меньше 1 и монотонно стремится к нулю с ростом q. Таким образом, оценка (17) качественно лучше оценки (1). Приведём таблицу некоторых начальных значений величины $h(q)^{1/3}$ с точностью до четырёх знаков после запятой.

q	3	4	5	7	8	9	11	13	16
$h(q)^{1/3}$	0,7211	0,6057	0,5386	0,4598	0,4337	0,4127	0,3802	0,356	0,3288

Несложно проверить, что в случае $q = 2$, $d = 1$, $n = 1$ оценки (17) и (1) совпадают, а в случае $q = 2$, $d = 1$, $n > 1$ оценка (17) точнее оценки (1) при $m \geqslant 2(n-1)$.

В заключение заметим, что в случае, когда $F(x)$ — многочлен максимального периода $T(F) = p^{n-1}(q^m - 1)$ над кольцом $R = GR(q^n, p^n)$, каждая ненулевая линейная рекуррентная последовательность u над кольцом R с характеристическим многочленом $F(x)$ имеет период $T(u) = p^{n-k-1}(q^m - 1)$, где $\|u\| = k$ (см. [7, теорема 4.6]). Подставив такое значение $T(u)$ в оценку из следствия 1 и воспользовавшись утверждением 1, получим уточнение оценки (15). Аналогично можно несколько улучшить оценку (17).

Литература

[1] Камловский О. В. Оценки частот появления нулей в линейных рекуррентных последовательностях векторов // Чебышёвский сб. — 2005. — Т. 6, вып. 1. — С. 135—146.

[2] Камловский О. В. Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа // Мат. сб. — 2009. — Т. 200, № 4. — С. 31—52.

[3] Камловский О. В. Метод Сидельникова для оценки числа знаков на отрезках линейных рекуррентных последовательностей над кольцами Галуа // Мат. заметки. — 2012. — Т. 91, № 3. — С. 371—382.

[4] Камловский О. В., Кузьмин А. С. Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа // Фундамент. и прикл. мат. — 2000. — Т. 6, вып. 4. — С. 1083—1094.

[5] Кнут Д. Э. Искусство программирования. Т. 2. — М.: Вильямс, 2000.

[6] Коробов Н. М. Распределение невычетов и первообразных корней в рекуррентных рядах // ДАН СССР. — 1953. — Т. 88, № 4. — С. 603—606.

[7] Кузьмин А. С., Куракин В. Л., Нечаев А. А. Псевдослучайные и полилинейные последовательности // Труды по дискретной математике. Т. 1. — М.: ТВП, 1997. — С. 139—202.

[8] Михайлов Д. А. Унитарные полилинейные регистры и их периоды // Дискрет. мат. — 2002. — Т. 14, № 1. — С. 30—59.

[9] Нечаев А. А. Код Кердока в циклической форме // Дискрет. мат. — 1989. — Т. 1, № 4. — С. 123—139.

[10] Нечаев В. И. Распределение знаков в последовательности прямоугольных матриц над конечным полем // Тр. Мат. ин-та им. В. А. Стеклова. — 1997. — Т. 218. — С. 335—342.

[11] Сидельников В. М. Оценки для числа r-грамм на отрезке линейной рекуррентной последовательности // Дискрет. мат. — 1991. — Т. 3, № 2. — С. 87—95.

[12] Шпарлинский И. Е. О распределении значений рекуррентных последовательностей // Проблемы передачи информации. — 1989. — Т. 25, № 2. — С. 46—53.

[13] 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. Inform. Theory. — 2006. — Vol. 52, no. 5. — P. 2260—2265.

[14] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules // J. Math. Sci. — 1995. — Vol. 76, no. 6. — P. 2793—2915.

[15] McDonald B. R. Finite Rings with Identity. — New York: Marcel Dekker, 1974.

[16] Niederreiter H. Distribution properties of feedback shift register sequences // Probl. Control Inform. Theory. — 1986. — Vol. 15, no. 1. — P. 19—34.

[17] Shanbhag A. G., Kumar P. V., Helleseth T. Upper bound for a hybrid sum over Galois rings with applications to aperiodic correlation of some q-ary sequences // IEEE Trans. Inform. Theory. — 1996. — Vol. 42, no. 1. — P. 250—254.