

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/19/1

УДК 621.391.1:004.7

ОЦЕНКИ ЧИСЛА ПОЯВЛЕНИЙ ЭЛЕМЕНТОВ НА ОТРЕЗКАХ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

И. Б. Биляк

*г. Москва, Россия***E-mail:** bil-ib@mail.ru

Рассмотрен некоторый класс тригонометрических сумм от линейных рекуррентных последовательностей. Эти суммы исследуются с использованием метода В. М. Сидельникова. Получены оценки числа появлений элементов на отрезках линейных рекуррент, которые в некоторых случаях уточняют ранее известные результаты.

Ключевые слова: *тригонометрические суммы, линейные рекуррентные последовательности, число появлений элементов.*

Введение

Изучение числа появлений элементов в линейных рекуррентных последовательностях (ЛРП) над кольцами является одной из важных математических задач. Интерес к этой задаче связан прежде всего с построением на основе ЛРП генераторов псевдослучайных чисел, использующих различные способы усложнения аналитического строения линейных рекуррент (см., например, [1]).

Пусть $\text{GF}(q)$ — конечное поле из q элементов, $f(x) = x^m - a_{m-1}x^{m-1} - \dots - a_1x - a_0$ — реверсивный ($a_0 \neq 0$) неприводимый многочлен степени m над этим полем. Линейной рекуррентной последовательностью над полем $\text{GF}(q)$ с характеристическим многочленом $f(x)$ будем называть последовательность $u = u(0)u(1)u(2) \dots$ элементов этого поля, удовлетворяющую соотношению

$$u(i+m) = a_0u(i) + a_1u(i+1) + \dots + a_{m-1}u(i+m-1), \quad i \geq 0.$$

Каждая такая ненулевая ЛРП u является чисто периодической последовательностью, при этом её период $T(u)$ равен периоду $T(f)$ многочлена $f(x)$ и делит $q^m - 1$ (см., например, [2]).

Рассмотрим линейные рекуррентные последовательности $u_1, u_2, \dots, u_r$ с характеристическим многочленом $f(x)$. Назовём эти последовательности линейно независимыми над полем $\text{GF}(q)$, если для всех ненулевых векторов $\bar{c} = (c_1, c_2, \dots, c_r) \in \text{GF}(q)^r$ последовательность $c_1u_1 + c_2u_2 + \dots + c_ru_r$ является ненулевой. Обозначим через $N_l(\bar{z}, u_1, \dots, u_r)$ количество целых чисел $i \in \{0, 1, \dots, l-1\}$, удовлетворяющих условиям $u_1(i) = z_1, u_2(i) = z_2, \dots, u_r(i) = z_r$, где $\bar{z} = (z_1, z_2, \dots, z_r) \in \text{GF}(q)^r$. Таким образом, величина $N_l(\bar{z}, u_1, \dots, u_r)$ равна количеству появлений r -граммы $\bar{z}$ на отрезке длины l последовательности векторов, элементы которой имеют вид $(u_1(i), u_2(i), \dots, u_r(i))$ для всех $i \geq 0$.

Всюду в дальнейшем будем считать, что $u_1, u_2, \dots, u_r$ — линейно независимая система ЛРП над полем $\text{GF}(q)$ с реверсивным неприводимым характеристическим многочленом $f(x)$. В работах В. И. Нечаева [3] и И. Е. Шпарлинского [4] доказано, что для произвольной r -граммы $\bar{z} \in \text{GF}(q)^r$ при всех l , не превосходящих период $T = T(f)$ многочлена $f(x)$, справедлива следующая оценка:

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

Величина l/q^r представляет собой «естественное» среднее значение для количества появлений r -граммы на отрезке длины l в последовательности векторов. Таким образом, неравенство (1) можно рассматривать как верхнюю оценку модуля отклонения количества появлений r -граммы на отрезке ЛРП векторов от средней величины. Из этого неравенства следуют верхняя и нижняя оценки числа $N_l(\bar{z}, u_1, \dots, u_r)$. При условии $l \geq q^{m/2+r} \ln T$ нижняя оценка рассматриваемой величины больше нуля, а верхняя — меньше l , т. е. оценка (1) нетривиальна. Впервые она была получена Н. М. Коробовым в [5] для простого поля и случая, когда ЛРП $u_1, u_2, \dots, u_r$ — сдвиги одной последовательности. В этой работе впервые был применен аппарат тригонометрических сумм для получения оценок количества появлений элементов в ЛРП.

В. М. Сидельниковым в работе [6] в случае, когда q — простое число, доказано неравенство

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} \right| \leq \frac{q^r - 1}{q^r} (3(q^m l - l^2))^{\frac{1}{3}}. \quad (2)$$

Оценка (2) является нетривиальной и улучшает оценку (1) при

$$\sqrt{3}q^{(m+3r)/2} \leq l \leq \frac{1}{24}((m+3r) \ln q)^3 q^{m/2}.$$

В данной работе доказано, что в условиях, сформулированных для результата (1), и при дополнительном условии $l \leq \min\{T/2, T/(T, q-1)\}$ справедлива следующая оценка:

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} \right| \leq \frac{q^r - 1}{q^r(q-1)} \left(\frac{3q}{2} ((q-1)q^m l - l^2) \right)^{\frac{1}{3}}. \quad (3)$$

Оценка (3) является нетривиальной и улучшает оценку (1) при значениях l , удовлетворяющих условию

$$\frac{\sqrt{3}q^{\frac{m+3r}{2}}}{\sqrt{h(q)}} \leq l \leq \frac{h(q)}{3} q^{\frac{m}{2}} \ln^3 T,$$

где $h(q) = 2(q-1)^2/q$. Правые части неравенств (2) и (3) совпадают, если $q = 2$. Оценка (3) улучшает также оценку (2) при $q \geq 3$ и

$$\frac{\sqrt{3}q^{\frac{m+3r}{2}}}{\sqrt{h(q)}} \leq l \leq \frac{10}{13} q^m.$$

Кроме того, при $q \geq 3$ правая часть неравенства (3) меньше правой части неравенства (2) в $\sqrt[3]{2(q-1)/q}$ раз.

1. Оценка тригонометрической суммы

Для изучения количества появлений элементов на отрезках ЛРП докажем вспомогательные результаты о тригонометрических суммах. Обозначим через χ аддитивный характер поля $\text{GF}(q)$, определённый на элементах поля равенством $\chi(x) = \exp\{\text{tr}_p^q(x)2\pi i/p\}$, где p — характеристика поля $\text{GF}(q)$; $\text{tr}_p^q(x)$ — функция следа из поля $\text{GF}(q)$ в поле $\text{GF}(p)$; i — мнимая единица. Пусть $L(f(x))$ — множество всех ЛРП над полем $\text{GF}(q)$ с характеристическим многочленом $f(x)$, а $L(f(x))^*$ — множество всех ненулевых ЛРП из множества $L(f(x))$. Период каждой ЛРП из множества $L(f(x))^*$ равен периоду T многочлена $f(x)$ и порядку корня α многочлена $f(x)$ в мультипликативной группе поля $\text{GF}(q^m)$ (см., например, [2]). Определим величину $\nu_l(z, u)$ следующим равенством:

$$\nu_l(z, u) = \sum_{c \in \text{GF}(q)^*} \chi(-cz) \sum_{i=0}^{l-1} \chi(cu(i)),$$

где $\text{GF}(q)^*$ — мультипликативная группа поля $\text{GF}(q)$, а z — произвольный элемент этого поля. Сформулируем и докажем некоторые свойства этой величины.

Лемма 1. Пусть $f(x)$ — реверсивный неприводимый многочлен степени m над полем $\text{GF}(q)$, T — его период, а l — натуральное число, не превосходящее величину $T/(T, q-1)$. Тогда для любого элемента z поля $\text{GF}(q)$ справедливо соотношение

$$\sum_{u \in L(f(x))^*} |\nu_l(z, u)|^2 = \begin{cases} (q-1)q^m l - l^2, & \text{если } z \neq 0, \\ (q-1)(q^m l - (q-1)l^2), & \text{если } z = 0. \end{cases} \quad (4)$$

Доказательство. Левую часть (4) можно представить в виде

$$\sum_{u \in L(f(x))^*} \sum_{b, c \in \text{GF}(q)^*} \chi(-cz) \overline{\chi(-bz)} \sum_{i, j=0}^{l-1} \chi(cu(i)) \overline{\chi(bu(j))}, \quad (5)$$

где черта обозначает комплексное сопряжение. Очевидно, что $\overline{\chi(x)} = \chi^{-1}(x) = \chi(-x)$. Воспользуемся этим в (5) и получим

$$\sum_{u \in L(f(x))^*} |\nu_l(z, u)|^2 = \sum_{u \in L(f(x))^*} \sum_{b, c \in \text{GF}(q)^*} \chi(-cz + bz) \sum_{i, j=0}^{l-1} \chi(cu(i) - bu(j)). \quad (6)$$

Для нулевой последовательности u из определения величины $\nu_l(z, u)$ следует, что при $z \neq 0$ она принимает значение $-l$, а при $z = 0$ — значение $(q-1)l$. Таким образом, получим

$$\sum_{u \in L(f(x))^*} |\nu_l(z, u)|^2 = \begin{cases} \sum_{u \in L(f(x))} |\nu_l(z, u)|^2 - l^2, & \text{если } z \neq 0, \\ \sum_{u \in L(f(x))} |\nu_l(z, u)|^2 - (q-1)^2 l^2, & \text{если } z = 0. \end{cases} \quad (7)$$

Для любой ЛРП из множества $L(f(x))$ найдётся единственный элемент γ из поля $\text{GF}(q^m)$, такой, что

$$u(i) = \text{tr}_q^{q^m}(\gamma \alpha^i) \text{ для всех } i \geq 0,$$

где $\text{tr}_q^{q^m}(x)$ — функция следа из поля $\text{GF}(q^m)$ в поле $\text{GF}(q)$ (см. [2, Теорема 8.24]). Далее, с использованием этого представления знаков ЛРП, из выражения (6) получим

$$\sum_{u \in L(f(x))} |\nu_l(z, u)|^2 = \sum_{b, c \in \text{GF}(q)^*} \chi(-cz + bz) \sum_{i, j=0}^{l-1} \sum_{\gamma \in \text{GF}(q^m)} \chi_m(\gamma(c\alpha^i - b\alpha^j)). \quad (8)$$

где χ_m — аддитивный характер поля $\text{GF}(q^m)$, определённый на элементах этого поля равенством $\chi_m(x) = \chi(\text{tr}_q^m(x))$. Воспользуемся соотношением ортогональности для характеров и получим

$$\sum_{\gamma \in \text{GF}(q^m)} \chi_m(\gamma(c\alpha^i - b\alpha^j)) = \begin{cases} q^m, & \text{если } c\alpha^i = b\alpha^j, \\ 0, & \text{если } c\alpha^i \neq b\alpha^j. \end{cases} \quad (9)$$

Если для некоторых элементов b и c поля $\text{GF}(q)$ выполняется соотношение $c\alpha^i = b\alpha^j$, то элемент α^{i-j} является элементом поля $\text{GF}(q)$. Далее получим $\alpha^{(i-j)(q-1)} = e$ и, следовательно, $T(f) = \text{ord } \alpha | (j-i)(q-1)$, $T(f)/(T(f), q-1) | (j-i)$. Элементы i и j всегда меньше $T(f)/(T(f), q-1)$, значит, соотношение $c\alpha^i = b\alpha^j$ выполняется тогда и только тогда, когда $i = j$ и $b = c$, откуда, используя (8) и (9), получим

$$\sum_{u \in L(f(x))} |\nu_l(z, u)|^2 = \sum_{c \in \text{GF}(q)^*} \sum_{i=0}^{l-1} q^m = (q-1)q^m l. \quad (10)$$

Для завершения доказательства остаётся подставить равенство (10) в равенство (7). ■

Лемма 2. Пусть u — ЛРП периода T над полем $\text{GF}(q)$, j — целое число из отрезка $[-T, T]$, z — произвольный элемент поля $\text{GF}(q)$. Тогда

$$|\nu_l(z, x^T u) - \nu_l(z, x^{T+j} u)| \leq q|j|.$$

Доказательство. Пусть $\chi(x) = \exp\{\text{tr}_p^q(x)2\pi i/p\}$ для всех элементов x поля $\text{GF}(q)$. Воспользуемся соотношением ортогональности для характеров

$$\sum_{i=0}^{l-1} \sum_{c \in \text{GF}(q)} \chi(c(u(i) - z)) = qN_l(z, u),$$

где $N_l(z, u)$ — число появлений z среди элементов $u(0), u(1), \dots, u(l-1)$. Так как $|N_l(z, x^T u) - N_l(z, x^{T+j} u)| \leq |j|$ для всех $j \in [-T, T]$, то $|\nu_l(z, x^T u) - \nu_l(z, x^{T+j} u)| = q|N_l(z, x^T u) - N_l(z, x^{T+j} u)| \leq q|j|$. ■

Лемма 3 [7]. Пусть q — натуральное число, тогда для всех действительных чисел $\nu \geq 0$ справедливо неравенство

$$\nu^2 + 2 \sum_{j=1}^{\lfloor \nu/q \rfloor} (\nu - qj)^2 \geq \frac{2\nu^3}{3q}.$$

Теорема 1. Пусть $f(x)$ — реверсивный неприводимый многочлен степени m над полем $\text{GF}(q)$, T — его период, u — ненулевая ЛРП над полем $\text{GF}(q)$ с характеристическим многочленом $f(x)$, z — элемент поля $\text{GF}(q)$, а l — натуральное число. Тогда при $l \leq \min\{T/2, T/(T, q-1)\}$ справедлива оценка

$$|\nu_l(z, u)| \leq \left(\frac{3q}{2} ((q-1)q^m l - l^2) \right)^{\frac{1}{3}}.$$

Доказательство. Рассмотрим в множестве $L(f(x))^*$ ЛРП u_0 , для которой величина $\nu = |\nu_l(z, u_0)|$ равна максимально возможному значению. Пусть j — произвольное целое число из интервала $[-\lfloor \nu/q \rfloor, \lfloor \nu/q \rfloor]$. Через u_j обозначим ЛРП, определённую равенством

$$u_j(i) = u_0(i + T + j) \text{ для всех } i \geq 0.$$

Покажем, что среди u_j , где $j \in \overline{[-\nu/q], [\nu/q]}$, нет одинаковых. Если найдутся целые числа j_1 и j_2 , такие, что $u_{j_1} = u_{j_2}$, то для корня α многочлена $f(x)$ будет справедливо соотношение $\alpha^{j_1-j_2} = e$. Это равенство может выполняться лишь при условии, что T делит $j_1 - j_2$. Как показано при доказательстве леммы 2, справедливо соотношение $\nu = |qN_l(z, u_0) - l|$, поэтому $\nu < ql$ и в условиях теоремы справедливы неравенства

$$|j_1 - j_2| \leq 2[\nu/q] < 2l \leq T.$$

Значит, $u_{j_1} = u_{j_2}$ тогда и только тогда, когда $j_1 = j_2$. Теперь с использованием лемм 1–3 имеем

$$(q-1)q^{ml} - l^2 \geq \sum_{j=-[\nu/q]}^{[\nu/q]} |\nu_l(z, u_j)|^2 \geq \nu^2 + 2 \sum_{j=1}^{[\nu/q]} (\nu - qj)^2 \geq \frac{2\nu^3}{3q}.$$

Окончательно получим

$$|\nu_l(z, u)| \leq \nu \leq \left(\frac{3q}{2} ((q-1)q^{ml} - l^2) \right)^{\frac{1}{3}}.$$

Теорема доказана. ■

Заметим, что полученная оценка справедлива для произвольного $z \in \text{GF}(q)$. Далее сформулируем результат, доказанный О. В. Камловским для случая $z = 0$.

Теорема 2 [7]. Пусть $f(x)$ — реверсивный неприводимый многочлен степени m над полем $\text{GF}(q)$, T — его период, u — ненулевая ЛРП над полем $\text{GF}(q)$ с характеристическим многочленом $f(x)$, а l — натуральное число. Тогда при условии $l \leq t/2$, где $t = T/(T, q-1)$, справедлива оценка

$$|\nu_l(0, u)| \leq \left(\frac{3q}{2} (q^{ml} - (q-1)l^2) \right)^{\frac{1}{3}}.$$

2. Оценка числа появлений r -грамм в ЛРП векторов

Сформулируем и докажем основной результат работы.

Теорема 3. Пусть $f(x)$ — реверсивный неприводимый многочлен степени m над полем $\text{GF}(q)$, T — его период, $u_1, u_2, \dots, u_r$ — линейно независимая система ЛРП над полем $\text{GF}(q)$ с характеристическим многочленом $f(x)$, l — натуральное число, не превосходящее значения $\min\{T/2, T/(T, q-1)\}$, $\bar{z}$ — произвольный элемент множества $\text{GF}(q)^r$. Тогда справедлива следующая оценка:

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} \right| \leq \frac{q^r - 1}{q^r(q-1)} \left(\frac{3q}{2} ((q-1)q^{ml} - l^2) \right)^{\frac{1}{3}}.$$

Доказательство. Пусть $\chi(x) = \exp\{\text{tr}_p^q(x)2\pi i/p\}$ — аддитивный характер поля $\text{GF}(q)$, где p — характеристика поля. Используя соотношения ортогональности для характеров, представим $N_l(\bar{z}, u_1, \dots, u_r)$ в виде

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

Тогда справедливо соотношение

$$N_l(\bar{z}, u_1, \dots, u_r) = \frac{1}{q^r} \sum_{i=0}^{l-1} \sum_{(c_1, c_2, \dots, c_r) \in \text{GF}(q)^r} \chi \left(\sum_{j=1}^r c_j(u_j(i) - z_j) \right). \quad (11)$$

1) Пусть $\bar{z} = \bar{0}$. Тогда воспользуемся результатом теоремы 2:

$$\left| N_l(\bar{0}, u_1, \dots, u_r) - \frac{l}{q^r} \right| \leq \frac{q^r - 1}{q^r(q-1)} \left(\frac{3q}{2} (q^m l - (q-1)l^2) \right)^{\frac{1}{3}}.$$

2) Пусть далее $\bar{z} \neq \bar{0}$. Для каждого вектора $\bar{c} = (c_1, c_2, \dots, c_r)$ через $u_{\bar{c}}$ обозначим такую последовательность, элементы которой определены равенствами

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

и обозначим

$$z_{\bar{c}} = \sum_{j=1}^r c_j z_j.$$

Последовательность $u_{\bar{c}}$ — ЛРП с характеристическим многочленом $f(x)$, причём из условия линейной независимости системы $u_1, u_2, \dots, u_r$ следует, что для всех $\bar{c} \neq \bar{0}$ ЛРП $u_{\bar{c}}$ является ненулевой. В равенстве (11) выделим слагаемое, соответствующее нулевому набору $(c_1, c_2, \dots, c_r)$, тогда получим соотношение

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

Для любого $a \in \text{GF}(q)^*$ справедливо соотношение $au_{\bar{c}} = u_{a\bar{c}}$, $az_{\bar{c}} = z_{a\bar{c}}$, следовательно, получим

$$N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} = \frac{1}{q^r} \frac{1}{q-1} \sum_{a \in \text{GF}(q)^*} \sum_{i=0}^{l-1} \sum_{\bar{c} \in \text{GF}(q)^r \setminus \{\bar{0}\}} \chi(au_{\bar{c}}(i) - az_{\bar{c}}),$$

а значит,

$$N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} = \frac{1}{q^r(q-1)} \sum_{\bar{c} \in \text{GF}(q)^r \setminus \{\bar{0}\}} \nu_l(z_{\bar{c}}, u_{\bar{c}}). \quad (12)$$

Из соотношения (12) следует неравенство

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} \right| \leq \frac{q^r - 1}{q^r(q-1)} \max_{\bar{c} \neq \bar{0}} |\nu_l(z_{\bar{c}}, u_{\bar{c}})|.$$

Используя теоремы 1 и 2, получим

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} \right| \leq \frac{q^r - 1}{q^r(q-1)} \left(\frac{3q}{2} (q^m l(q-1) - l^2) \right)^{\frac{1}{3}}. \quad (13)$$

В силу того, что при $\bar{z} = \bar{0}$ оценка является более точной, можем применить оценку (13) для любого z . ■

Если ограничиться случаем $\bar{z} \neq \bar{0}$, то при некоторых ограничениях на l возможно доказать более сильную оценку, чем в теореме 3.

Теорема 4. Пусть дополнительно, в условиях теоремы 3, $l \leq \frac{T}{2(T, q-1)}$ и $\bar{z} \neq \bar{0}$. Тогда справедлива следующая оценка:

$$\begin{aligned} \left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} \right| &\leq \frac{q^r - q^{r-1}}{q^r(q-1)} \left(\frac{3q}{2} ((q-1)q^m l - l^2) \right)^{\frac{1}{3}} + \\ &+ \frac{q^{r-1} - 1}{q^r(q-1)} \left(\frac{3q}{2} (q^m l - (q-1)l^2) \right)^{\frac{1}{3}}. \end{aligned}$$

Доказательство. Разобьем правую часть равенства (12) на две суммы:

$$N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} = \frac{1}{q^r(q-1)} \sum_{\bar{c} \in \{\text{GF}(q)^r \setminus \bar{0} : z_{\bar{c}} \neq 0\}} \nu_l(z_{\bar{c}}, u_{\bar{c}}) + \frac{1}{q^r(q-1)} \sum_{\bar{c} \in \{\text{GF}(q)^r \setminus \bar{0} : z_{\bar{c}} = 0\}} \nu_l(z_{\bar{c}}, u_{\bar{c}}).$$

Очевидно, что

$$\begin{aligned} |\{\bar{c} \in \text{GF}(q)^r \setminus \bar{0} : z_{\bar{c}} \neq 0\}| &= q^r - q^{r-1}, \\ |\{\bar{c} \in \text{GF}(q)^r \setminus \bar{0} : z_{\bar{c}} = 0\}| &= q^{r-1} - 1. \end{aligned}$$

Отсюда получим

$$\left| N_l(\bar{z}, u_1, \dots, u_r) - \frac{l}{q^r} \right| \leq \frac{q^r - q^{r-1}}{q^r(q-1)} \max_{\bar{c} \neq \bar{0}, z_{\bar{c}} \neq 0} |\nu_l(z_{\bar{c}}, u_{\bar{c}})| + \frac{q^{r-1} - 1}{q^r(q-1)} \max_{\bar{c} \neq \bar{0}} |\nu_l(0, u_{\bar{c}})|.$$

Применив теоремы 1 и 2, получим необходимый результат. ■

Сформулируем и докажем утверждение, вытекающее из теоремы 3.

Утверждение 1. Пусть выполнено условие теоремы 3. Тогда среди элементов

$$u(0), u(1), \dots, u\left(\left\lceil \sqrt{3}q^{\frac{m+3r}{2}} / \sqrt{h(q)} \right\rceil\right),$$

где $h(q) = 2(q-1)^2/q$, появляются все r -граммы.

Доказательство. Для произвольного $\bar{z} \in \text{GF}(q)^r$ справедливо соотношение

$$\frac{l}{q^r} - \frac{q^r - 1}{q^r(q-1)} \left(\frac{3q}{2} (q^m l (q-1) - l^2) \right)^{\frac{1}{3}} \leq N_l(\bar{z}, u_1, \dots, u_r).$$

Если левая часть больше нуля, то появятся все r -граммы. Рассмотрим неравенство

$$\frac{l}{q^r} - \frac{q^r - 1}{q^r(q-1)} \left(\frac{3q}{2} (q^m l (q-1) - l^2) \right)^{\frac{1}{3}} > 0.$$

Оно равносильно

$$l^3 > \frac{(q^r - 1)^3}{(q-1)^3} \left(\frac{3q}{2} (q^m l (q-1) - l^2) \right).$$

Это неравенство заведомо выполнено при условии

$$l^3 \geq \frac{(q^r)^3}{(q-1)^3} \left(\frac{3q}{2} (q^m l (q-1)) \right),$$

то есть при

$$l \geq \frac{\sqrt{3}q^{\frac{m+3r}{2}}}{\sqrt{h(q)}},$$

где $h(q) = 2(q-1)^2/q$. ■

Будем говорить, что оценка $|N_l(\bar{z}, u_1, \dots, u_r) - l/q^r| \leq S$ является нетривиальной, если в неравенстве $l/q^r - S \leq N_l(\bar{z}, u_1, \dots, u_r) \leq -l/q^r + S$ левая часть больше нуля, а правая часть меньше l . Ясно, что это равносильно условию $l/q^r - S > 0$.

Следствие 1. Оценка (3) является нетривиальной при $l > \sqrt{3}q^{\frac{m+3r}{2}} / \sqrt{h(q)}$.

Доказательство. Условие нетривиальности доказано в утверждении 1. ■

Сравним оценку (3) и оценку (2). Заметим, что при $q = 2$ оценки совпадают.

Утверждение 2. Пусть $q \geq 3$. Тогда оценка (3) улучшает оценку (2) при

$$l \leq \frac{10}{13}q^m.$$

Доказательство. Выпишем необходимое условие:

$$\frac{q^r - 1}{(q - 1)q^r} \left(\frac{3q}{2} (q^m l (q - 1) - l^2) \right)^{\frac{1}{3}} \leq \frac{q^r - 1}{q^r} (3 (q^m l - l^2))^{\frac{1}{3}}.$$

Это неравенство равносильно соотношению

$$\frac{1}{(q - 1)^3} \left(\frac{q}{2} (q^m (q - 1) - l) \right) \leq q^m - l,$$

которое выполняется при условии

$$\left(1 - \frac{q/2}{(q - 1)^3} \right) l \leq q^m \left(1 - \frac{q}{2(q - 1)^2} \right).$$

Выделив l , получим

$$l \leq q^m \left(\frac{(q - 1)^3 - q(q - 1)/2}{(q - 1)^3 - q/2} \right) = q^m \left(1 + \frac{q/2 - q(q - 1)/2}{(q - 1)^3 - q/2} \right).$$

Таким образом,

$$l \leq q^m \left(1 - \frac{q}{1 + 2q(q - 1)} \right). \quad (14)$$

Возьмём производную функции $g(q) = \left(1 - \frac{q}{1 + 2q(q - 1)} \right)$:

$$g'(q) = \frac{2q^2 - 1}{(1 + 2q(q - 1))^2} > 0, \quad q \in \mathbb{N}.$$

Это означает, что если $l \leq q^m g(3) = \frac{10}{13}q^m$, то для любого $q \geq 3$ выполняется неравенство (14). ■

Используя рассуждения, аналогичные доказательству утверждения 2, несложно показать, что при $q \geq 3$ и $l \leq (q - 1)q^{m-1}$ правая часть неравенства (3) меньше правой части неравенства (2) в $\sqrt[3]{2(q - 1)/q}$ раз.

Далее сравним полученную оценку (3) с оценкой (1).

Утверждение 3. Оценка (3) улучшает оценку Н. М. Коробова (1) при

$$l \leq \frac{h(q)}{3} q^{\frac{m}{2}} \ln^3 T.$$

Доказательство. Выпишем необходимое условие:

$$\frac{q^r - 1}{(q - 1)q^r} \left(\frac{3q}{2} (q^m l(q - 1) - l^2) \right)^{\frac{1}{3}} < \frac{q^r - 1}{q^r} q^{\frac{m}{2}} \ln T.$$

Оно равносильно соотношению

$$\frac{3}{2} \frac{q}{(q - 1)^3} (q^m l(q - 1) - l^2) < q^{\frac{3m}{2}} \ln^3 T.$$

Это неравенство выполнено, когда $\frac{3}{2} \frac{q}{(q - 1)^2} l \leq q^{\frac{m}{2}} \ln^3 T$, что равносильно тому, что $l \leq \frac{h(q)}{3} q^{\frac{m}{2}} (\ln T(u))^3$. ■

Таким образом, из утверждений 2 и 3 следует, что полученная оценка при некоторых ограничениях на l уточняет известные результаты.

ЛИТЕРАТУРА

1. Алферов А. П., Zubov A. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: учеб. пособие. М.: Гелиос АРВ, 2001. 480 с.
2. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988. 824 с.
3. Нечаев В. И. Распределение знаков в последовательности прямоугольных матриц над конечным полем // Труды матем. института им. В. А. Стеклова. 1997. Т. 218. С. 335–342.
4. Шпарлинский И. Е. О распределении значений рекуррентных последовательностей // Проблемы передачи информации. 1989. Т. 25. № 2. С. 46–53.
5. Коробов Н. М. Распределение невычетов и первообразных корней в рекуррентных рядах // Докл. Акад. наук СССР. 1953. Т. 88. № 4. С. 603–606.
6. Сидельников В. М. Оценки для числа появлений знаков на отрезке рекуррентной последовательности над конечным полем // Дискретная математика. 1991. Т. 3. № 2. С. 87–95.
7. Камловский О. В. Оценки частот появления нулей в линейных рекуррентных последовательностях векторов // Чебышевский сборник. 2005. Т. 6. № 1. С. 135–144.