

УДК 519.4

DOI 10.17223/20710410/60/3

ЧИСЛО ПОЯВЛЕНИЙ ЭЛЕМЕНТОВ ИЗ ЗАДАННОГО ПОДМНОЖЕСТВА НА ОТРЕЗКАХ УСЛОЖНЕНИЙ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А. С. Тиссин

ООО «Центр сертификационных исследований», г. Москва, Россия

E-mail: at_science@mail.ru

Пусть v — последовательность, построенная по правилу $v(i) = f(u_1(i), \dots, u_k(i))$, $i \geq 0$, где $u_1, \dots, u_k$ — линейные рекуррентные последовательности над полем P с характеристическим многочленом $F(x)$. Изучается величина $N_l(H, v)$, равная количеству появлений элементов из подмножества $H \subset P$ среди элементов $v(0), v(1), \dots, v(l-1)$; получены её нетривиальные оценки снизу и сверху, вычислены границы для некоторых подмножеств H . Результаты обобщаются на случай r -грамм.

Ключевые слова: конечные поля, фильтрующие генераторы, кривизна дискретной функции, линейные рекуррентные последовательности, характеры абелевых групп.

THE NUMBER OF OCCURRENCES OF ELEMENTS FROM A GIVEN SUBSET ON THE COMPLICATION SEGMENTS OF LINEAR RECURRENCE SEQUENCES

A. S. Tissin

Certification Research Center, LLC, Moscow, Russia

Let v be a sequence constructed by the rule $v(i) = f(u_1(i), \dots, u_k(i))$, $i \geq 0$, where $u_1, \dots, u_k$ are linear recurrence sequences over the field P with characteristic polynomial $F(x)$. We study the value $N_l(H, v)$, which is equal to the number of occurrences of elements from the subset $H \subset P$ among the elements $v(0), v(1), \dots, v(l-1)$. We have obtained non-trivial estimates for the value $N_l(H, v)$ and considered special cases when the set H is a subgroup of the group P^* , H is the set of all primitive elements of the field P . Results are generalized to the case of r -tuples for the value $N_l(H, \mathbf{s}, v) = |\{i \in \{0, \dots, l-1\} : v(i+s_1) \in H, \dots, v(i+s_r) \in H\}|$, where $\mathbf{s} = (s_1, \dots, s_r)$ is a set of non-negative integers.

Keywords: finite fields, filter generators, discrete function curvature, linear recurrence sequences, characters of abelian group.

Введение

Пусть $P = \text{GF}(q)$ — конечное поле из q элементов, где $q = p^t$, p — простое число; $F(x)$ — унитарный реверсивный (старший коэффициент равен e — единице поля P — и $F(0) \neq 0$) многочлен степени m над полем P , $f: P^k \rightarrow P$.

Будем изучать частотные характеристики последовательности v , построенной по правилу

$$v(i) = f(u_1(i), u_2(i), \dots, u_k(i)), \quad i \geq 0, \quad (1)$$

где $u_j = (u_j(i))_{i=0}^{\infty}$ — линейная рекуррентная последовательность (ЛРП) над полем P для всех $j = 1, 2, \dots, k$ с характеристическим многочленом $F(x)$. В случае, когда $u_1, u_2, \dots, u_k$ являются сдвигами одной ЛРП u , v является выходной последовательностью фильтрующего генератора, усложняющего ЛРП u с использованием фильтрующей функции f .

В работе изучается величина $N_l(H, v)$, равная количеству появлений элементов из подмножества $H \subset P$ среди элементов $v(0), v(1), \dots, v(l-1)$. В случае $|H| = 1$ для последовательности v , вырабатываемой фильтрующим генератором, оценки величины $N_l(H, v)$ получены в [1]. В случае $H \subset P$, где H — подгруппа мультипликативной группы P или множество всех примитивных элементов поля P , величины $N_l(H, u)$ для ЛРП u рассмотрены в работах [2–5]. Таким образом, рассматриваемая постановка задачи является обобщением ранее изученных случаев.

Получены нетривиальные оценки частот $N_l(v, H)$ для случаев, когда H — подгруппа группы P^* и H — множество всех примитивных элементов поля P . Приведены обобщения этих результатов для частот появлений r -грамм.

1. Оценки частот появлений элементов на отрезках усложнений ЛРП

Опишем частотные характеристики последовательности v .

Назовём систему ЛРП $u_1, u_2, \dots, u_k$ устойчивой, если для всех $a_1, a_2, \dots, a_k \in P$, которые не все равны нулю, последовательности $a_1 u_1 + a_2 u_2 + \dots + a_k u_k$ имеют один и тот же минимальный многочлен [1].

Для каждого $c \in P$ рассмотрим аддитивный характер поля P

$$\chi_c(x) = e^{2\pi i \operatorname{Tr}_{P_0}^P(cx)/p}, \quad x \in P,$$

где $P_0 = \operatorname{GF}(p)$; $\operatorname{Tr}_{P_0}^P(x) = x + x^p + \dots + x^{p^{t-1}}$.

Известно [6], что группа аддитивных характеров поля P имеет вид $\{\chi_c : c \in P\}$.

Для каждого $\mathbf{c} = (c_1, \dots, c_k) \in P^k$ рассмотрим отображение $\chi_{\mathbf{c}} : P^k \rightarrow \mathbb{C}^*$, действующее по правилу

$$\chi_{\mathbf{c}}(\mathbf{x}) = \chi_{c_1}(x_1) \chi_{c_2}(x_2) \dots \chi_{c_k}(x_k), \quad \text{где } \mathbf{x} = (x_1, \dots, x_k) \in P^k.$$

Тогда группа характеров группы $P^k = \underbrace{P \oplus \dots \oplus P}_k$ имеет вид $\{\chi_{\mathbf{c}} : \mathbf{c} \in P^k\}$ [6].

Определим отображение $\mu_c : P^k \rightarrow \mathbb{C}^*$, где $c \in P$, равенством

$$\mu_c(\mathbf{x}) = \chi_c(f(\mathbf{x})), \quad \mathbf{x} \in P^k. \quad (2)$$

Разложим отображение μ_c по базису характеров группы P^k :

$$\mu_c(\mathbf{x}) = \sum_{\mathbf{c} \in P^k} \nu_{\mu_c}(\mathbf{c}) \chi_{\mathbf{c}}(\mathbf{x}). \quad (3)$$

Известно [7], что

$$\nu_{\mu_c}(\mathbf{c}) = \frac{1}{q^k} \sum_{\mathbf{x} \in P^k} \mu_c(\mathbf{x}) \overline{\chi_{\mathbf{c}}}(\mathbf{x}), \quad (4)$$

где $\overline{\chi_{\mathbf{c}}}$ — характер, сопряжённый характеру $\chi_{\mathbf{c}}$.

Для каждого реверсивного многочлена $F(x)$ степени m и периода $T(F)$ над полем P определим параметр $C_l(F)$ следующими равенствами:

$$C_l(F) = \begin{cases} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) q^{m/2}, & \text{если } l < T(F), \\ (q^m - T(F))^{1/2}, & \text{если } l = T(F). \end{cases}$$

Лемма 1 [1]. Пусть $F(x)$ — реверсивный многочлен над полем P степени m с периодом $T(F)$. Тогда для каждой ЛРП w с минимальным многочленом $F(x)$ и каждого $l \leq T(F)$ выполнено неравенство

$$\left| \sum_{i=0}^{l-1} \chi_c(w(i)) \right| \leq C_l(F),$$

где χ_c — произвольный нетривиальный ($c \neq 0$) аддитивный характер поля P .

Кривизной функции $f : P^k \rightarrow P$ назовём следующую величину [8]:

$$\sigma(f) = \max_{c \in P} \sum_{\mathbf{c} \in P^k} |\nu_{\mu_c}(\mathbf{c})|.$$

Для непустого подмножества H поля P введём обозначение

$$\varkappa(H) = \max_{c \in P^*} \left| \sum_{h \in H} \chi_c(h) \right|.$$

Следующая теорема устанавливает для каждого натурального l оценку величины

$$N_l(H, v) = |\{i \in \{0, \dots, l-1\} : v(i) \in H\}|.$$

Обозначим через $f^{-1}(H)$ полный прообраз множества H при действии отображения f .

Теорема 1. Пусть $F(x)$ — реверсивный многочлен степени m над полем $P = \text{GF}(q)$, $u_1, u_2, \dots, u_k$ — устойчивая система ЛРП с характеристическим многочленом $F(x)$, v — последовательность, определённая по правилу (1). Тогда для любого непустого подмножества $H \subset P$ при $l \leq T(F)$ справедлива оценка

$$\left| N_l(H, v) - |f^{-1}(H)| \frac{l}{q^k} \right| \leq \frac{q-1}{q} \varkappa(H) \sigma(f) C_l(F).$$

Доказательство. Из соотношения ортогональности для характеров [6] получим

$$\frac{1}{q} \sum_{c \in P} \chi_c(x) = \begin{cases} 1, & x = 0, \\ 0, & x \neq 0. \end{cases}$$

Тогда справедливы равенства

$$N_l(H, v) = \sum_{h \in H} \sum_{i=0}^{l-1} \frac{1}{q} \sum_{c \in P} \chi_c(v(i) - h) = \frac{1}{q} \sum_{c \in P} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \chi_c(v(i)).$$

Выделим отдельно слагаемое, соответствующее случаю $c = 0$:

$$N_l(H, v) = \frac{l}{q} |H| + \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \chi_c(v(i)).$$

Так как $v(i) = f(u_1(i), u_2(i), \dots, u_k(i))$, то

$$\begin{aligned} N_l(H, v) - \frac{l}{q} |H| &= \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \chi_c(f(u_1(i), u_2(i), \dots, u_k(i))) = \\ &= \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \mu_c(u_1(i), u_2(i), \dots, u_k(i)) = \\ &= \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \sum_{\mathbf{c} \in P^k} \nu_{\mu_c}(\mathbf{c}) \chi_c(u_1(i), u_2(i), \dots, u_k(i)) = \\ &= \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \sum_{\mathbf{c} \in P^k} \nu_{\mu_c}(\mathbf{c}) \chi(u_{\mathbf{c}}(i)), \end{aligned}$$

где $u_{\mathbf{c}}(i) = c_1 u_1(i) + c_2 u_2(i) + \dots + c_k u_k(i)$, $i \geq 0$; $\chi = \chi_e$ — канонический аддитивный характер поля P .

Выделим отдельно слагаемое, соответствующее случаю $\mathbf{c} = \mathbf{0}$:

$$N_l(H, v) - \frac{l|H|}{q} = \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \nu_{\mu_c}(\mathbf{0}) + \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \sum_{\mathbf{c} \neq \mathbf{0}} \nu_{\mu_c}(\mathbf{c}) \chi(u_{\mathbf{c}}(i)).$$

Введём обозначение

$$\delta_l(H) = \frac{l|H|}{q} + \frac{1}{q} \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \nu_{\mu_c}(\mathbf{0}).$$

Изучим отдельно $\delta_l(H)$. В силу того, что $\nu_{\mu_0}(\mathbf{0}) = 1$, получим

$$\delta_l(H) = \frac{1}{q} \sum_{c \in P} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \nu_{\mu_c}(\mathbf{0}).$$

Далее, используя формулу (4), запишем

$$\delta_l(H) = \frac{1}{q} \sum_{c \in P} \sum_{h \in H} \bar{\chi}_c(h) \sum_{i=0}^{l-1} \frac{1}{q^k} \sum_{\mathbf{b} \in P^k} \mu_c(\mathbf{b}).$$

Тогда, согласно (2) и соотношению ортогональности характеров, будем иметь

$$\delta_l(H) = \frac{l}{q^{k+1}} \sum_{c \in P} \sum_{h \in H} \bar{\chi}_c(h) \sum_{\mathbf{b} \in P^k} \chi(cf(\mathbf{b})) = \frac{l}{q^{k+1}} \sum_{c \in P} \sum_{h \in H} \sum_{\mathbf{b} \in P^k} \chi(c(f(\mathbf{b}) - h)) = \frac{l}{q^k} |f^{-1}(H)|.$$

Следовательно,

$$\begin{aligned} \left| N_l(H, v) - \frac{l}{q^k} |f^{-1}(H)| \right| &= \frac{1}{q} \left| \sum_{c \neq 0} \sum_{h \in H} \bar{\chi}_c(h) \sum_{\mathbf{c} \neq \mathbf{0}} \nu_{\mu_c}(\mathbf{c}) \sum_{i=0}^{l-1} \chi(u_{\mathbf{c}}(i)) \right| \leq \\ &\leq \frac{q-1}{q} \max_{c \neq 0} \left| \sum_{h \in H} \bar{\chi}_c(h) \sum_{\mathbf{c} \neq \mathbf{0}} \nu_{\mu_c}(\mathbf{c}) \sum_{i=0}^{l-1} \chi(u_{\mathbf{c}}(i)) \right|. \end{aligned} \quad (5)$$

Введём обозначение

$$R_c = c \neq 0_{h \in H} \bar{\chi}_c(h) c \neq 0_{\mathbf{c} \neq \mathbf{0}} \nu_{\mu_c}(\mathbf{c}) c \neq 0_{i=0}^{l-1} \chi(u_{\mathbf{c}}(i)).$$

Заметим, что для любого $c \in P^*$ верно

$$\begin{aligned} |R_c| &= \left| \sum_{h \in H} \bar{\chi}_c(h) \sum_{\mathbf{c} \neq \mathbf{0}} \nu_{\mu_c}(\mathbf{c}) \sum_{i=0}^{l-1} \chi(u_{\mathbf{c}}(i)) \right| = \left| \sum_{h \in H} \bar{\chi}_c(h) \right| \left| \sum_{\mathbf{c} \neq \mathbf{0}} \nu_{\mu_c}(\mathbf{c}) \sum_{i=0}^{l-1} \chi(u_{\mathbf{c}}(i)) \right| \leq \\ &\leq \kappa(H) \left(\sum_{\mathbf{c} \neq \mathbf{0}} |\nu_{\mu_c}(\mathbf{c})| \right) \max_{\mathbf{c} \neq \mathbf{0}} \left| \sum_{i=0}^{l-1} \chi(u_{\mathbf{c}}(i)) \right| \leq \kappa(H) \sigma(f) \max_{\mathbf{c} \neq \mathbf{0}} \left| \sum_{i=0}^{l-1} \chi(u_{\mathbf{c}}(i)) \right|. \end{aligned}$$

Тогда из устойчивости системы ЛРП $u_1, u_2, \dots, u_k$ и леммы 1 получим, что

$$|R_c| \leq \kappa(H) \sigma(f) \max_{\mathbf{c} \neq \mathbf{0}} \left| \sum_{i=0}^{l-1} \chi(u_{\mathbf{c}}(i)) \right| \leq \kappa(H) \sigma(f) \cdot C_l(F).$$

Таким образом, согласно (5), будем иметь

$$\left| N_l(H, v) - \frac{l}{q^k} |f^{-1}(H)| \right| \leq \frac{q-1}{q} \kappa(H) \sigma(f) C_l(F).$$

Теорема 1 доказана. ■

Замечание 1. Из теоремы 1 при $|H| = 1$ получим оценку из работы [1].

2. Приложения результатов для некоторых подмножеств H

Приведём известные оценки величин $\kappa(H)$, справедливые при определённом выборе H и уточняющие тривиальную оценку $\kappa(H) \leq |H|$.

Лемма 2 [4]. Пусть d — делитель $q - 1$, H — множество всех элементов вида a^d , где $a \in P$. Тогда для величины $\kappa(H)$ справедлива оценка

$$\kappa(H) \leq \frac{d-1}{d}(\sqrt{q} + 1).$$

Непосредственно из леммы 2 и теоремы 1 получим следующий результат.

Следствие 1. Пусть d делит $q - 1$ и H — множество всех элементов вида a^d , где $a \in P$, тогда в условиях теоремы 1 выполнено

$$\left| N_l(H, v) - |f^{-1}(H)| \frac{l}{q^k} \right| \leq \frac{(d-1)(\sqrt{q} + 1)}{d} \frac{q-1}{q} C_l(F) \sigma(f).$$

Лемма 3 [4]. Пусть d делит $q - 1$ и H — подгруппа группы P^* , имеющая порядок $(q - 1)/d$, тогда

$$\kappa(H) \leq \frac{(d-1)\sqrt{q} + 1}{d}.$$

Из леммы 3 и теоремы 1 вытекает

Следствие 2. Пусть d делит $q - 1$ и H — подгруппа группы P^* , имеющая порядок $(q - 1)/d$, тогда в условиях теоремы 1 выполнено

$$\left| N_l(H, v) - |f^{-1}(H)| \frac{l}{q^k} \right| \leq \frac{(d-1)\sqrt{q} + 1}{d} \frac{q-1}{q} C_l(F) \sigma(f).$$

Далее рассмотрим задачу о количестве примитивных элементов на отрезках последовательности v . Для этого понадобятся некоторые вспомогательные свойства функции Мёбиуса μ [3].

Лемма 4 [3]. Для всех $n \in \mathbb{N}$ верно равенство

$$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n},$$

где φ — функция Эйлера.

Лемма 5 [3]. Для всех $n \in \mathbb{N}$ справедливо равенство

$$\sum_{d|n} |\mu(d)| = 2^s,$$

где s — количество различных простых чисел в каноническом разложении числа n .

Теорема 2. Пусть в условиях теоремы 1 H — множество всех примитивных элементов поля P и f — сбалансированное отображение, тогда

$$\left| N_l(H, v) - \frac{l\varphi(q-1)}{q} \right| \leq \frac{q-1}{\sqrt{q}} 2^s C_l(F) \sigma(f),$$

где s — количество различных простых делителей числа $q - 1$.

Доказательство. Для каждого делителя n числа $q - 1$ обозначим через $M_l(n)$ количество элементов $c \in P^*$ среди знаков $v(0), v(1), \dots, v(l-1)$, имеющих мультипликативный порядок $\text{ord } c = n$. Рассмотрим число

$$\sum_{d|n} M_l(d).$$

Оно равно количеству элементов $c \in P^*$, таких, что $c^n = e$ в группе P^* , т.е. элементов из группы $\langle \gamma^{(q-1)/n} \rangle$, где γ — примитивный элемент поля P . Отсюда получим

$$\sum_{d|n} M_l(d) = V_l((q-1)/n),$$

где $V_l((q-1)/n)$ — количество элементов $c \in P^*$ среди $v(0), v(1), \dots, v(l-1)$, имеющих вид $a^{(q-1)/n}$, $a \in P^*$. Применив формулу обращения Мёбиуса, получим

$$M_l(n) = \sum_{d|n} \mu(d) V_l((q-1)d/n).$$

В частности,

$$N_l(H, v) = M_l(q-1) = \sum_{d|(q-1)} \mu(d) V_l(d).$$

Пусть H_d — множество всех элементов вида a^d , $a \in P^*$. Тогда, согласно следствию 2,

$$V_l(d) = |f^{-1}(H_d)| \frac{l}{q^k} + \theta_d \frac{q-1}{q} C_l(F) \sigma(f),$$

где θ_d — некоторое действительное число $|\theta_d| \leq \sqrt{q}$. Тогда получим

$$N_l(H, v) = \frac{l}{q^k} \sum_{d|(q-1)} |f^{-1}(H_d)| \mu(d) + \frac{q-1}{q} C_l(F) \sigma(f) \sum_{d|(q-1)} \mu(d) \theta_d.$$

Так как f — сбалансированное отображение, для любого d получим

$$|f^{-1}(H_d)| = q^{k-1} |H_d| = q^{k-1} \frac{q-1}{d}.$$

Отсюда, используя сбалансированность f и результаты лемм 4 и 5, имеем

$$\begin{aligned} \left| N_l(H, v) - \frac{l \varphi(q-1)}{q} \right| &\leq \frac{q-1}{q} C_l(F) \sigma(f) \sum_{d|(q-1)} |\mu(d)| |\theta_d| \leq \\ &\leq C_l(F) \sigma(f) \frac{(q-1) \sqrt{q}}{q} \sum_{d|(q-1)} |\mu(d)| = \frac{q-1}{\sqrt{q}} 2^s C_l(F) \sigma(f). \end{aligned}$$

Теорема 2 доказана. ■

Полученные в п. 2 оценки частот $N_l(H, v)$ обобщают соответствующие результаты работ [1, 2, 7, 9, 10].

3. Обобщение на случай r -грамм

Для набора $\mathbf{s} = (s_1, \dots, s_r)$ целых неотрицательных чисел и непустого подмножества $H \subset P$ для каждого натурального l рассмотрим величину

$$N_l(H, \mathbf{s}, v) = |\{i \in \{0, \dots, l-1\} : v(i+s_1) \in H, \dots, v(i+s_r) \in H\}|.$$

Пусть w — последовательность над полем P и $k \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Обозначим через $x^k w$ сдвиг последовательности w на k шагов влево, т. е.

$$x^k w = (w(k), w(k+1), \dots).$$

В дальнейшем будем рассматривать ситуацию, когда набор $\mathbf{s} = (s_1, s_2, \dots, s_r)$ удовлетворяет условию, что система ЛРП

$$x^{s_1} u_1, \dots, x^{s_r} u_1, x^{s_1} u_2, \dots, x^{s_r} u_2, \dots, x^{s_1} u_k, \dots, x^{s_r} u_k \quad (6)$$

устойчива.

Лемма 6 [1]. Пусть χ — канонический аддитивный характер поля $P = \text{GF}(q)$, $z_1, \dots, z_r \in P$, μ_c — отображение, определённое соотношением (2), где $c \in P$. Тогда

$$\frac{1}{q^{(k-1)r}} |f^{-1}(z_1)| \cdots |f^{-1}(z_r)| = \sum_{\mathbf{c}=(c_1, \dots, c_r) \in P^r} \chi(-c_1 z_1 - \dots - c_r z_r) \nu_{\mu_{c_1}}(\mathbf{0}) \cdots \nu_{\mu_{c_r}}(\mathbf{0}).$$

Непосредственно из леммы 6 следует

Лемма 7. В условиях леммы 6 для любого непустого подмножества $H \subset P$ справедливо равенство

$$\frac{1}{q^{(k-1)r}} |f^{-1}(H)|^r = \sum_{h_1, \dots, h_r \in P} \sum_{c_1, \dots, c_r \in P} \chi(-c_1 h_1 - \dots - c_r h_r) \nu_{\mu_{c_1}}(\mathbf{0}) \cdots \nu_{\mu_{c_r}}(\mathbf{0}).$$

Теорема 3. Пусть $F(x)$ — унитарный реверсивный многочлен степени m над полем $P = \text{GF}(q)$, v — последовательность, удовлетворяющая равенству (1). Тогда если набор $\mathbf{s}$ выбран так, что система (6) устойчива, то для всех $l \leq T(F)$ справедлива оценка

$$\left| N_l(H, \mathbf{s}, v) - |f^{-1}(H)|^r \frac{l}{q^{kr}} \right| \leq C_l(F) \frac{(\chi(H)\sigma(f)(q-1)+1)^r - 1}{q^r}.$$

Доказательство. Справедливо равенство

$$N_l(H, \mathbf{s}, v) = \sum_{i=0}^{l-1} \left(\frac{1}{q} \sum_{c_1 \in P} \sum_{h_1 \in H} \chi(c_1(v(i+s_1) - h_1)) \right) \cdots \left(\frac{1}{q} \sum_{c_r \in P} \sum_{h_r \in H} \chi(c_r(v(i+s_r) - h_r)) \right).$$

Отсюда будем иметь

$$N_l(H, \mathbf{s}, v) = \frac{1}{q^r} \sum_{\mathbf{c}=(c_1, \dots, c_r) \in P^r} \sum_{\mathbf{h}=(h_1, \dots, h_r) \in H^r} \chi(-\mathbf{c}\mathbf{h}) \sum_{i=0}^{l-1} \chi(c_1 v(i+s_1)) \cdots \chi(c_r v(i+s_r)),$$

где $\mathbf{c}\mathbf{h} = (c_1, \dots, c_r)(h_1, \dots, h_r) = c_1 h_1 + \dots + c_r h_r$. Выделяя слагаемое, соответствующее случаю $(c_1, \dots, c_r) = (0, \dots, 0) = \mathbf{0}$, получим

$$N_l(H, \mathbf{s}, v) - |H|^r \frac{l}{q^r} = \frac{1}{q^r} \sum_{\mathbf{c} \in P^r \setminus \{\mathbf{0}\}} \sum_{\mathbf{h} \in H^r} \chi(-\mathbf{c}\mathbf{h}) D_l(\mathbf{c}),$$

где

$$D_l(\mathbf{c}) = \sum_{i=0}^{l-1} \chi(c_1 v(i + s_1)) \dots \chi(c_r v(i + s_r)).$$

Обозначим через $\|\mathbf{c}\|$ вес (количество ненулевых координат) вектора $\mathbf{c} \in P^r$. Тогда

$$N_l(H, \mathbf{s}, v) - |H|^r \frac{l}{q^r} = \frac{1}{q^r} \sum_{d=1}^r \sum_{\mathbf{h} \in H^r} \sum_{\mathbf{c} \in P^r \setminus \{\mathbf{0}\}, \|\mathbf{c}\|=d} \chi(-\mathbf{c}\mathbf{h}) D_l(\mathbf{c}). \quad (7)$$

Пусть вектор $\mathbf{c} = (c_1, \dots, c_r) \in P^r$ имеет вес d , ненулевые элементы в нём стоят на местах $j_1, \dots, j_d$ и выполнено равенство $c_{j_1} = \gamma_1, \dots, c_{j_d} = \gamma_d$. Тогда для $D_l(\mathbf{c})$, используя равенство (2), получим

$$D_l(\mathbf{c}) = \sum_{i=0}^{l-1} \mu_{\gamma_1}(u_1(i + s_1), \dots, u_k(i + s_1)) \dots \mu_{\gamma_d}(u_1(i + s_d), \dots, u_k(i + s_d)).$$

С учётом (3) запишем

$$\begin{aligned} D_l(\mathbf{c}) &= \sum_{i=0}^{l-1} \left(\sum_{\mathbf{a}_1 \in P^k} \nu_{\mu_{\gamma_1}}(\mathbf{a}_1) \chi_{\mathbf{a}_1}(u_1(i + s_1), \dots, u_k(i + s_1)) \right) \dots \\ &\dots \left(\sum_{\mathbf{a}_d \in P^k} \nu_{\mu_{\gamma_d}}(\mathbf{a}_d) \chi_{\mathbf{a}_d}(u_1(i + s_d), \dots, u_k(i + s_d)) \right). \end{aligned}$$

Тогда

$$D_l(\mathbf{c}) = \sum_{\mathbf{a}_1, \dots, \mathbf{a}_d \in P^k} \nu_{\mu_{\gamma_1}}(\mathbf{a}_1) \dots \nu_{\mu_{\gamma_d}}(\mathbf{a}_d) \sum_{i=0}^{l-1} \chi(\omega_{\mathbf{a}_1, \dots, \mathbf{a}_d}(i)),$$

где $\omega_{\mathbf{a}_1, \dots, \mathbf{a}_d}$ — последовательность над полем P , элементы которой определены для всех векторов $\mathbf{a}_1 = (a_1^{(1)}, \dots, a_k^{(1)})$, $\dots$, $\mathbf{a}_d = (a_1^{(d)}, \dots, a_k^{(d)})$ равенством

$$\begin{aligned} \omega_{\mathbf{a}_1, \dots, \mathbf{a}_d}(i) &= a_1^{(1)} u_1(i + s_1) + \dots + a_k^{(1)} u_k(i + s_1) + \dots \\ &\dots + a_1^{(d)} u_1(i + s_d) + \dots + a_k^{(d)} u_k(i + s_d), \quad i \geq 0. \end{aligned}$$

Так как система (6) устойчива над полем P , то минимальный многочлен последовательности $\omega_{\mathbf{a}_1, \dots, \mathbf{a}_d}$ равен $F(x)$, кроме случая, когда $\mathbf{a}_1 = \dots = \mathbf{a}_d = \mathbf{0}$. Выделив отдельно этот случай, получим

$$D_l(\mathbf{c}) = l \cdot \nu_{\mu_{\gamma_1}}(\mathbf{0}) \dots \nu_{\mu_{\gamma_d}}(\mathbf{0}) + D_l^*(\mathbf{c}),$$

где

$$D_l^*(\mathbf{c}) = \sum_{(\mathbf{a}_1, \dots, \mathbf{a}_d) \neq \mathbf{0}} \nu_{\mu_{\gamma_1}}(\mathbf{a}_1) \dots \nu_{\mu_{\gamma_d}}(\mathbf{a}_d) \sum_{i=0}^{l-1} \chi(\omega_{\mathbf{a}_1, \dots, \mathbf{a}_d}(i)),$$

где суммирование производится по всем наборам $(\mathbf{a}_1, \dots, \mathbf{a}_d)$, в которых хотя бы один из векторов $\mathbf{a}_1, \dots, \mathbf{a}_d$ ненулевой.

Подставив $D_l(\mathbf{c})$ в соотношение (7), можем записать

$$N_l(H, \mathbf{s}, v) - \delta_l(H) = \frac{1}{q^r} \sum_{d=1}^r \sum_{\substack{\mathbf{c} \in P^r, \\ \|\mathbf{c}\|=d}} \sum_{\mathbf{h} \in H^r} \chi(-\mathbf{c}\mathbf{h}) D_l^*(\mathbf{c}), \quad (8)$$

где

$$\delta_l(H) = |H|^r \frac{l}{q^r} + \frac{l}{q^r} \sum_{d=1}^r \sum_{\substack{\mathbf{c} \in P^r \\ \|\mathbf{c}\|=d}} \sum_{\mathbf{h} \in H^r} \chi(-\mathbf{ch}) \nu_{\mu_{\gamma_1}}(\mathbf{0}) \dots \nu_{\mu_{\gamma_d}}(\mathbf{0}).$$

Для вычисления $\delta_l(H)$ воспользуемся леммой 7 и равенством $\nu_{\mu_0}(\mathbf{0}) = 1$:

$$\begin{aligned} \delta_l(H) &= |H|^r \frac{l}{q^r} \underbrace{\nu_{\mu_0}(\mathbf{0}) \dots \nu_{\mu_0}(\mathbf{0})}_r + \frac{l}{q^r} \sum_{\mathbf{h} \in H^r} \sum_{\mathbf{c} \in P^r \setminus \{\mathbf{0}\}} \chi(-\mathbf{ch}) \nu_{\mu_{c_1}}(\mathbf{0}) \dots \nu_{\mu_{c_r}}(\mathbf{0}) = \\ &= \frac{l}{q^r} \sum_{\mathbf{h} \in H^r} \sum_{\mathbf{c} \in P^r} \chi(-\mathbf{ch}) \nu_{\mu_{c_1}}(\mathbf{0}) \dots \nu_{\mu_{c_r}}(\mathbf{0}) = \frac{l}{q^{kr}} |f^{-1}(H)|^r. \end{aligned} \quad (9)$$

Из леммы 1 для $D_l^*(\mathbf{c})$ получим

$$\begin{aligned} |D_l^*(\mathbf{c})| &\leq C_l(F) \sum_{(\mathbf{a}_1, \dots, \mathbf{a}_d) \neq \mathbf{0}} |\nu_{\mu_{\gamma_1}}(\mathbf{a}_d)| \dots |\nu_{\mu_{\gamma_d}}(\mathbf{a}_d)| \leq \\ &\leq C_l(F) \left(\sum_{\mathbf{a}_1 \in P^k} |\nu_{\mu_{\gamma_1}}(\mathbf{a}_1)| \right) \dots \left(\sum_{\mathbf{a}_d \in P^k} |\nu_{\mu_{\gamma_d}}(\mathbf{a}_d)| \right) \leq C_l(F) \sigma(f)^d. \end{aligned} \quad (10)$$

Тогда, используя соотношения (8), (9) и оценку (10), будем иметь

$$\left| N_l(H, \mathbf{s}, v) - \frac{l}{q^{kr}} |f^{-1}(H)|^r \right| \leq \frac{1}{q^r} \sum_{d=1}^r \sum_{\substack{\mathbf{c} \in P^r \\ \|\mathbf{c}\|=d}} \left| \sum_{\mathbf{h} \in H^r} \chi(-\mathbf{ch}) \right| C_l(F) \sigma(f)^d. \quad (11)$$

Пусть $\mathbf{c} = (c_1, \dots, c_r) \in P^r$, $\|\mathbf{c}\| = d$ и $c_{\gamma_1} \neq 0, \dots, c_{\gamma_d} \neq 0$, тогда

$$\begin{aligned} \left| \sum_{\mathbf{h} \in H^r} \chi(-\mathbf{ch}) \right| &= \left| \sum_{h_{\gamma_1} \in H} \chi(-c_{\gamma_1} h_{\gamma_1}) \dots \sum_{h_{\gamma_d} \in H} \chi(-c_{\gamma_d} h_{\gamma_d}) \right| \leq \\ &\leq \left| \sum_{h_{\gamma_1} \in H} \chi(-c_{\gamma_1} h_{\gamma_1}) \right| \dots \left| \sum_{h_{\gamma_d} \in H} \chi(-c_{\gamma_d} h_{\gamma_d}) \right| \leq \varkappa(H)^d. \end{aligned}$$

Учитывая, что количество векторов $\mathbf{c} \in P^r$, таких, что $\|\mathbf{c}\| = d$, равно $\binom{r}{d} (q-1)^d$, из неравенства (11) получим

$$\begin{aligned} \left| N_l(H, \mathbf{s}, v) - \frac{l}{q^{kr}} |f^{-1}(H)|^r \right| &\leq \frac{1}{q^r} \sum_{d=1}^r \binom{r}{d} (q-1)^d \varkappa(H)^d C_l(F) \sigma(f)^d = \\ &= C_l(F) \frac{(\varkappa(H) \sigma(f) (q-1) + 1)^r - 1}{q^r}. \end{aligned}$$

Теорема 3 доказана. ■

Отметим, что при $r = 1$ оценка теоремы 3 совпадает с оценкой из теоремы 1. Таким образом, получено обобщение теоремы 1 на случай r -грамм.

ЛИТЕРАТУРА

1. Камловский О. В. Количество появлений элементов в выходных последовательностях фильтрующих генераторов // Прикладная дискретная математика. 2013. № 3(21). С. 11–25.
2. Коробов Н. М. Распределение невычетов и первообразных корней в рекуррентных рядах // Доклады АН СССР. 1953. Т. 88. № 4. С. 603–606.

3. Виноградов И. М. Основы теории чисел. М.: Наука, 1972. 168 с.
4. Камловский О. В. Неабсолютные оценки для неполных тригонометрических сумм от линейных рекуррент и их приложения // Матем. вопр. криптогр. 2014. Т. 65. № 3. С. 17–34.
5. Нечаев В. И., Степанова Л. Л. Распределение невычетов и первообразных корней в рекуррентных последовательностях над полем алгебраических чисел // Успехи матем. наук. 1965. Т. 20. № 3. С. 197–203.
6. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 822 с.
7. Сидельников В. М. Оценки для числа появлений знаков на отрезках рекуррентной последовательности над конечным полем // Дискретная математика. 1991. Т. 3. № 2. С. 87–95.
8. Логачев О. А., Федоров С. Н., Яценко В. В. Булевы функции как точки на гиперсфере в евклидовом пространстве // Дискретная математика. 2018. Т. 30. № 1. С. 39–55.
9. Шпарлинский И. Е. Распределение невычетов и первообразных корней в рекуррентных последовательностях // Матем. заметки. 1978. Т. 24. № 5. С. 603–613.
10. Шпарлинский И. Е. О распределении значений рекуррентных последовательностей // Проблемы передачи информации. 1989. Т. 25. № 2. С. 46–53.

REFERENCES

1. Kamlovskiy O. V. Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 11–25. (in Russian)
2. Korobov N. M. Raspredelenie nevychetov i pervoobraznykh korney v rekurrentnykh ryadakh [Distribution of non-decomposable and first-order roots in recurrence series]. Dokl. AS USSR, 1953, vol. 88, no. 4, pp. 603–606. (in Russian)
3. Vinogradov I. M. Osnovy teorii chisel [Fundamentals of Number Theory]. Moscow, Nauka Publ., 1972. 168 p. (in Russian)
4. Kamlovskiy O. V. Neabsolyutnye otsenki dlya nepolnykh trigonometricheskikh summ ot lineynykh rekurrent i ikh prilozheniya [Non-absolute estimates for incomplete trigonometric sums from linear recurrences and their applications]. Matem. Vopr. Kriptogr., 2014, vol. 65, no. 3, pp. 17–34. (in Russian)
5. Nechaev V. I. and Stepanova L. L. Raspredelenie nevychetov i pervoobraznykh korney v rekurrentnykh posledovatel'nostyakh nad polem algebraicheskikh chisel [Distribution of non-decomposables and first-order roots in recurrence sequences over a field of algebraic numbers]. Uspekhi Matem. Nauk, 1965, vol. 20, no. 3, pp. 197–203. (in Russian)
6. Lidl R. and Niderrayter G. Konechnye polya [Finite Fields]. Moscow, Mir Publ., 1988. 822 p. (in Russian)
7. Sidel'nikov V. M. Otsenki dlya chisla poyavleniy znakov na otrezkakh rekurrentnoy posledovatel'nosti nad konechnym polem [Estimates for the number of occurrences of signs in recurrence sequence segments over a finite field]. Diskretnaya Matematika, 1991, vol. 3, no. 2, pp. 87–95. (in Russian)
8. Logachev O. A., Fedorov S. N., and Yashchenko V. V. Bulevy funktsii kak tochki na gipersfere v evklidovom prostranstve [Boolean functions as points on a hypersphere in Euclidean space]. Diskretnaya Matematika, 2018, vol. 30, no. 1, pp. 39–55. (in Russian)
9. Shparlinskiy I. E. Raspredelenie nevychetov i pervoobraznykh korney v rekurrentnykh posledovatel'nostyakh [Distribution of non-decomposable and first-order roots in recurrence sequences]. Matem. Zametki, 1978, vol. 24, no. 5, pp. 603–613. (in Russian)
10. Shparlinskiy I. E. O raspredelenii znacheniy rekurrentnykh posledovatel'nostey [On the distribution of values of recurrent sequences]. Problemy Peredachi Informatsii, 1989, vol. 25, no. 2, pp. 46–53. (in Russian)