

КОЛИЧЕСТВО ПОЯВЛЕНИЙ ЭЛЕМЕНТОВ В ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ ФИЛЬТРУЮЩИХ ГЕНЕРАТОРОВ

О. В. Камловский

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

E-mail: ov-kam@yandex.ru

Получены оценки для числа r -грамм на отрезках выходных последовательностей фильтрующих генераторов над конечными полями. Оцениваются коэффициенты кросс-корреляции рассматриваемых последовательностей и приводятся условия, при которых последовательности, выработанные на различных начальных векторах, не совпадают.

Ключевые слова: *фильтрующие генераторы, конечные поля, линейные рекуррентные последовательности, суммы аддитивных характеров.*

Введение

Пусть $P = \text{GF}(q)$ — конечное поле из q элементов, $F(x)$ — унитарный реверсивный многочлен (старший его коэффициент равен единице, а младший отличен от нуля) степени m над полем P , $f : P^k \rightarrow P$. Рассмотрим выходную последовательность $v = (v(i))_{i=0}^{\infty}$ фильтрующего генератора над полем P , удовлетворяющую соотношению

$$v(i) = f(u(i + t_1), u(i + t_2), \dots, u(i + t_k)), \quad i \geq 0, \quad (1)$$

где $t_1, t_2, \dots, t_k$ — фиксированный набор целых чисел, таких, что $0 \leq t_1 < t_2 < \dots < t_k \leq m - 1$; $u = (u(i))_{i=0}^{\infty}$ — линейная рекуррентная последовательность (ЛРП) порядка m над полем P с характеристическим многочленом $F(x)$ [1–5].

Исследуются частотные характеристики последовательности v . Для каждого элемента $z \in P$ и натурального числа l обозначим через $N_l(z, v)$ количество появлений элемента $z \in P$ среди элементов $v(0), v(1), \dots, v(l - 1)$. В данной работе при некоторых ограничениях на начальный вектор $(u(0), \dots, u(m - 1))$ ЛРП u и набор $t_1, \dots, t_k$ (в частности, если $F(x)$ неприводим над полем P , то требуется лишь условие $(u(0), \dots, u(m - 1)) \neq (0, \dots, 0)$) доказывается, что для всех l , не превосходящих период $T(F)$ многочлена $F(x)$, выполнено неравенство

$$\left| N_l(z, v) - |f^{-1}(z)| \frac{l}{q^k} \right| \leq (q - 1) q^{\frac{k}{2} - 1} C_l(F), \quad (2)$$

где $f^{-1}(z)$ — множество всех прообразов элемента z при действии f , а величина $C_l(F)$ определена равенствами

$$C_l(F) = \begin{cases} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) q^{m/2}, & \text{если } l < T(F), \\ \begin{cases} (3(q^m l - l^2))^{1/3}, & \text{если } l < T(F) \text{ и } F(x) \text{ неприводим над } P, \\ (q^m - T(F))^{1/2}, & \text{если } l = T(F). \end{cases} \end{cases} \quad (3)$$

Оценка (2) нетривиальна (правая часть неравенства меньше l) при выполнении условий

$$\begin{aligned} l &> (q-1) \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) q^{(m+k)/2-1}, \\ l &\geq \sqrt{3} q^{m/2+3k/4}, \\ l = T(F) &\geq (q-1) q^{(m+k)/2-1} \end{aligned}$$

соответственно.

Получено обобщение оценки (2) на случай r -грамм. Ранее аналогичные оценки для случая $q = 2$ и $T(F) = 2^m - 1$ были получены М. В. Левашовым и А. Б. Горчаковым.

Автору не известны другие общие оценки частот $N_l(z, v)$ при $l < T(F)$. В случае, когда $T(F) = 2^m - 1$, u — ЛРП максимального периода над полем $P = \text{GF}(2)$ с характеристическим многочленом $F(x)$, а f задается многочленом от переменных $x_1, \dots, x_k$ степени $\deg f$, набор $(v(0), \dots, v(2^m - 2))$ является кодовым словом кода, эквивалентного коду Рида — Маллера порядка $\deg f$ с выколотой первой координатой [6]. Спектр весов кодов Рида — Маллера известен для значений $\deg f \in \{1, 2\}$, а также в некоторых диапазонах значений частот для произвольной степени f [6, § 15.3]. Из этих результатов следуют оценки частот $N_l(z, v)$ при $l = 2^m - 1$. Другие оценки для данных частот при фиксированном значении $\deg f$ получены в работе [7, теорема 1]. В [8, теоремы 1, 2] получены оценки частот появлений цепочек из подряд идущих нулей и единиц в ситуации, когда $q = 2$, $l = T(F) = 2^m - 1$, $f(x_1, \dots, x_k) = x_1 x_l$, где $l \in \{2, 3, \dots, k\}$.

Методом, применённым для доказательства оценки (2), получены оценки сверху для коэффициентов кросс-корреляции выходных последовательностей фильтрующих генераторов. С использованием этих оценок приводятся условия, при которых не совпадают последовательности, полученные на различных начальных векторах.

1. Условия на числа $t_1, \dots, t_k$ и начальный вектор

Всюду в дальнейшем будем накладывать следующее условие на ЛРП u и набор чисел $t_1, t_2, \dots, t_k$: для всех ненулевых векторов $\bar{a} = (a_1, a_2, \dots, a_k) \in P^k$ последовательность

$$\omega = a_1 x^{t_1} u + a_2 x^{t_2} u + \dots + a_k x^{t_k} u,$$

элементы которой определены соотношением

$$\omega(i) = a_1 u(i + t_1) + a_2 u(i + t_2) + \dots + a_k u(i + t_k), \quad i \geq 0,$$

имеет минимальный многочлен $M_\omega(x)$ равный $F(x)$. Минимальный многочлен последовательности ω связан с минимальным многочленом $M_u(x)$ ЛРП u следующим равенством [2, гл. 25, теорема 5], [9, лемма 1]:

$$M_\omega(x) = \frac{M_u(x)}{(M_u(x), a_1 x^{t_1} + a_2 x^{t_2} + \dots + a_k x^{t_k})}.$$

Таким образом, сформулированное выше условие на ЛРП u и числа $t_1, \dots, t_k$ равносильно следующим равенствам:

$$M_u(x) = F(x), (F(x), a_1 x^{t_1} + a_2 x^{t_2} + \dots + a_k x^{t_k}) = e, \quad (a_1, \dots, a_k) \in P^k \setminus \{\bar{0}\}. \quad (4)$$

Приведём два примера, при которых соотношение (4) имеет место.

Утверждение 1. Пусть $F(x)$ — унитарный реверсивный многочлен степени m над полем P . Тогда

- 1) если $F(x)$ неприводим над полем P , то условие (4) выполнено тогда и только тогда, когда начальный вектор $(u(0), \dots, u(m-1))$ ЛРП u ненулевой;
- 2) если $F(x)$ приводим и m_0 — наименьшая из степеней всех неприводимых делителей многочлена $F(x)$, $M_u(x) = F(x)$, а $t_k \leq m_0 + t_1 - 1$, то условие (4) выполнено.

Доказательство. Пункт 1 очевиден. Докажем пункт 2. Пусть $F_1(x), \dots, F_t(x)$ — все различные неприводимые делители многочлена $F(x)$. Тогда для каждого $j \in \{1, 2, \dots, t\}$ в силу реверсивности $F_j(x)$ получим

$$(F_j(x), a_1x^{t_1} + a_2x^{t_2} + \dots + a_kx^{t_k}) = (F_j(x), a_1 + a_2x^{t_2-t_1} + \dots + a_kx^{t_k-t_1}).$$

Так как $t_k - t_1 \leq m_0 - 1 < \deg F_j(x)$, то для всех $(a_1, \dots, a_k) \in P^k \setminus \{\bar{0}\}$ будем иметь $(F_j(x), a_1x^{t_1} + a_2x^{t_2} + \dots + a_kx^{t_k}) = e$. ■

Приведём другие соотношения, эквивалентные равенствам (4), полученные в работе [9, формула (10)]. Введём обозначение

$$V(F) = \{(a_1, \dots, a_k) \in P^k : (F(x), a_1x^{t_1} + a_2x^{t_2} + \dots + a_kx^{t_k}) = e\}.$$

Пусть $F_1(x), \dots, F_t(x)$ — все различные неприводимые делители многочлена $F(x)$. Для каждого $j \in \{1, 2, \dots, t\}$ рассмотрим множество

$$W(F_j) = \{(a_1, \dots, a_k) \in P^k : F_j(x) \mid a_1x^{t_1} + a_2x^{t_2} + \dots + a_kx^{t_k}\}.$$

Оно является линейным пространством над полем P . Для всех целых чисел $i_1, \dots, i_s$, таких, что $1 \leq i_1 < \dots < i_s \leq t$, обозначим через $d(i_1, \dots, i_s)$ размерность линейного пространства $W(F_{i_1}) \cap \dots \cap W(F_{i_s})$. Справедливо равенство

$$V(F) = P^k \setminus (W(F_1) \cup \dots \cup W(F_t)),$$

и с использованием формулы для вычисления мощности объединения множеств будем иметь

$$\begin{aligned} |V(F)| &= q^k + \sum_{s=1}^t (-1)^s \sum_{1 \leq i_1 < \dots < i_s \leq t} |W(F_{i_1}) \cap \dots \cap W(F_{i_s})| = \\ &= q^k + \sum_{s=1}^t (-1)^s \sum_{1 \leq i_1 < \dots < i_s \leq t} q^{d(i_1, \dots, i_s)}. \end{aligned}$$

Таким образом, условие (4) равносильно следующим соотношениям:

$$M_u(x) = F(x) \text{ и } \sum_{s=1}^t (-1)^s \sum_{1 \leq i_1 < \dots < i_s \leq t} q^{d(i_1, \dots, i_s)} = -1.$$

2. Оценки сумм характеров от линейных рекуррент

Рассмотрим χ — канонический аддитивный характер поля $P = \text{GF}(q)$, определённый равенством

$$\chi(x) = e^{2\pi i \text{tr}_P^q(x)/p}, \quad x \in P, \quad (5)$$

где i — мнимая комплексная единица; tr_p^q — функция следа из поля P в простое подполе $P_0 = \text{GF}(p)$. Для каждой последовательности u над полем P и натурального числа l рассмотрим сумму

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

Приведём оценки величины $S_l(u)$.

Теорема 1. Пусть $P = \text{GF}(q)$, $F(x)$ — унитарный реверсивный многочлен степени m над полем P . Тогда для каждой ЛРП u над полем P с минимальным многочленом $F(x)$ при всех $l \leq T(F)$ справедлива оценка

$$|S_l(u)| \leq C_l(F),$$

где величина $C_l(F)$ определена равенством (3).

Доказательство. В работе [5, теорема 8.81] при $l \leq T(F)$ получена оценка

$$|S_l(u)| \leq q^{\frac{m}{2}} \frac{1}{T(F)} \sum_{a=0}^{T(F)-1} \left| \sum_{k=0}^{l-1} e^{2\pi i ak/T(F)} \right|,$$

а как показано в работе [10, теорема 1],

$$\frac{1}{T(F)} \sum_{a=0}^{T(F)-1} \left| \sum_{k=0}^{l-1} e^{2\pi i ak/T(F)} \right| \leq \frac{4}{\pi^2} \ln T(F) + \frac{9}{5}.$$

Таким образом,

$$|S_l(u)| \leq \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) q^{m/2}. \quad (6)$$

Неравенство

$$|S_l(u)| \leq (3(q^m l - l^2))^{1/3} \quad (7)$$

для случая, когда P — простое поле, получено в работе [11, теорема 1]. Несложно заметить, что доказательство из этой работы справедливо для произвольного поля $P = \text{GF}(q)$. При $l = T(F)$ неравенство

$$|S_l(u)| \leq (q^m - T(u))^{1/2} \quad (8)$$

вытекает из доказательства теоремы 8.78 из [5] (см. также упражнение 8.66). ■

Отметим, что оценки (6) и (8) несколько усиливают известные оценки Н. М. Коровова [12, теорема 1]. Оценка (6) является асимптотически неулучшаемой [9, теорема 3]. Оценка (7) нетривиальна (её правая часть меньше l) и точнее оценки (6) при условии

$$\sqrt{3}q^{m/2} \leq l \leq \frac{1}{3} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right)^3 q^{m/2}.$$

3. Спектральные коэффициенты отображений

Пусть χ — канонический аддитивный характер поля P , определённый равенством (5). Через $\bar{\chi}$ обозначим характер, сопряжённый к характеру χ , т. е. $\bar{\chi}(x) = \overline{\chi(x)}$, $x \in P$, где черта означает комплексное сопряжение. Для каждого вектора $\bar{a} = (a_1, \dots, a_k) \in P^k$ рассмотрим отображение $\chi_{\bar{a}}$, осуществляемое по правилу

$$\chi_{\bar{a}}(x_1, \dots, x_k) = \chi(a_1 x_1 + \dots + a_k x_k), \quad x_1, \dots, x_k \in P. \quad (9)$$

Несложно показать, что $\chi_{\bar{a}}$ является характером группы $(P^k, +)$. Обозначим через $\bar{a}\bar{b}$ скалярное произведение векторов $\bar{a}, \bar{b} \in P^k$, т. е.

$$\bar{a}\bar{b} = (a_1, \dots, a_k)(b_1, \dots, b_k) = a_1b_1 + \dots + a_kb_k.$$

В этих обозначениях равенство (9) запишется в виде

$$\chi_{\bar{a}}(\bar{x}) = \chi(\bar{a}\bar{x}), \quad \bar{x} = (x_1, \dots, x_k) \in P^k.$$

Приведём вспомогательный результат из работы [5, соотношение (5.9)].

Лемма 1.

$$\sum_{c \in P} \chi(cx) = \begin{cases} q, & \text{если } x = 0, \\ 0, & \text{если } x \in P \setminus \{0\}. \end{cases}$$

Нам понадобятся следующие свойства спектральных коэффициентов отображений.

Утверждение 2. Пусть ψ — произвольное отображение из P^k в мультипликативную группу поля комплексных чисел. Тогда

1) для всех $x_1, \dots, x_k \in P$ выполнено равенство

$$\psi(x_1, \dots, x_k) = \frac{1}{q^k} \sum_{\bar{a} \in P^k} W_\psi(\bar{a}) \chi_{\bar{a}}(x_1, \dots, x_k), \quad (10)$$

где для всех $\bar{a} \in P^k$ комплексные числа $W_\psi(\bar{a})$ (спектральные коэффициенты) определяются по правилу

$$W_\psi(\bar{a}) = \sum_{\bar{b}=(b_1, \dots, b_k) \in P^k} \psi(\bar{b}) \bar{\chi}(\bar{a}\bar{b}); \quad (11)$$

2) если при этом $|\psi(\bar{x})| = 1$ для всех $\bar{x} \in P^k$, то для чисел, определённых равенством (11), имеет место соотношение

$$\sum_{\bar{a} \in P^k} |W_\psi(\bar{a})|^2 = q^{2k};$$

3) если в условиях п. 2 $M(\psi) = \{\bar{a} \in P^k : W_\psi(\bar{a}) \neq 0\}$, то справедливо неравенство

$$\sum_{\bar{a} \in P^k} |W_\psi(\bar{a})| \leq |M(\psi)|^{1/2} q^k;$$

4) в условиях п. 2 справедливо неравенство

$$\sum_{\bar{a} \in P^k} |W_\psi(\bar{a})| \leq q^{3k/2}.$$

Доказательство.

1) Пусть комплексные числа $W_\psi(\bar{a})$ определены равенством (11). Тогда

$$\frac{1}{q^k} \sum_{\bar{a} \in P^k} W_\psi(\bar{a}) \chi_{\bar{a}}(x_1, \dots, x_k) = \frac{1}{q^k} \sum_{\bar{a} \in P^k} \chi(\bar{a}\bar{x}) \sum_{\bar{b} \in P^k} \psi(\bar{b}) \bar{\chi}(\bar{a}\bar{b}) = \frac{1}{q^k} \sum_{\bar{b} \in P^k} \psi(\bar{b}) \sum_{\bar{a} \in P^k} \chi(\bar{a}(\bar{x} - \bar{b})).$$

С использованием леммы 1 получим

$$\begin{aligned} \sum_{\bar{a} \in P^k} \chi(\bar{a}(\bar{x} - \bar{b})) &= \left(\sum_{a_1 \in P} \chi(a_1(x_1 - b_1)) \right) \dots \left(\sum_{a_k \in P} \chi(a_k(x_k - b_k)) \right) = \\ &= \begin{cases} q^k, & \text{если } \bar{x} = \bar{b}, \\ 0, & \text{если } \bar{x} \neq \bar{b}. \end{cases} \end{aligned} \quad (12)$$

Таким образом,

$$\frac{1}{q^k} \sum_{\bar{a} \in P^k} W_\psi(\bar{a}) \chi_{\bar{a}}(x_1, \dots, x_k) = \psi(\bar{x}) = \psi(x_1, \dots, x_k).$$

2) Из равенства (11) имеем

$$\begin{aligned} \sum_{\bar{a} \in P^k} |W_\psi(\bar{a})|^2 &= \sum_{\bar{a} \in P^k} W_\psi(\bar{a}) \overline{W_\psi(\bar{a})} = \sum_{\bar{a} \in P^k} \left(\sum_{\bar{b} \in P^k} \psi(\bar{b}) \bar{\chi}(\bar{a}\bar{b}) \right) \left(\sum_{\bar{c} \in P^k} \overline{\psi(\bar{c})} \chi(\bar{a}\bar{c}) \right) = \\ &= \sum_{\bar{b} \in P^k} \sum_{\bar{c} \in P^k} \psi(\bar{b}) \overline{\psi(\bar{c})} \sum_{\bar{a} \in P^k} \chi(\bar{a}(\bar{c} - \bar{b})). \end{aligned}$$

Используя соотношение (12), получим

$$\sum_{\bar{a} \in P^k} |W_\psi(\bar{a})|^2 = q^k \sum_{\bar{b} \in P^k} \psi(\bar{b}) \overline{\psi(\bar{b})} = q^k \sum_{\bar{b} \in P^k} |\psi(\bar{b})|^2 = q^{2k}.$$

3) Согласно неравенству Коши и п. 2, будем иметь

$$\sum_{\bar{a} \in P^k} |W_\psi(\bar{a})| = \sum_{\bar{a} \in M(\psi)} |W_\psi(\bar{a})| \leq \left(\sum_{\bar{a} \in M(\psi)} |W_\psi(\bar{a})|^2 \right)^{1/2} \left(\sum_{\bar{a} \in M(\psi)} 1 \right)^{1/2} = q^k |M(\psi)|^{1/2}.$$

4) Непосредственно следует из п. 3. ■

Равенства (10) и (11) являются известными разложениями функций по базису характеров [13, соотношение (12)]. Пункт 2 устанавливает хорошо известное равенство Парсеваля [13, равенство (16)], [14, утверждение 1]. Данные результаты приведены лишь для полноты изложения материала.

4. Оценки числа появлений элементов на отрезках выходных последовательностей

Получим теперь оценки для числа $N_l(z, v)$ появлений элемента $z \in P$ среди элементов $v(0), v(1), \dots, v(l-1)$ последовательности v , построенной по правилу (1).

Теорема 2. Пусть $F(x)$ — унитарный реверсивный многочлен степени m над полем $P = \text{GF}(q)$, u — ЛРП над полем P с характеристическим многочленом $F(x)$ и выполнены условия (4). Тогда для всех $z \in P$ и $l \in \mathbb{N}$, таких, что $l \leq T(F)$, справедлива оценка

$$\left| N_l(z, v) - |f^{-1}(z)| \frac{l}{q^k} \right| \leq (q-1) q^{k/2-1} C_l(F), \quad (13)$$

где $f^{-1}(z) = \{(x_1, \dots, x_k) \in P^k : f(x_1, \dots, x_k) = z\}$.

Доказательство. С использованием леммы 1 получим

$$N_l(z, v) = \frac{1}{q} \sum_{c \in P} \chi(-cz) \sum_{i=0}^{l-1} \chi(cv(i))$$

и, следовательно,

$$N_l(z, v) = \frac{l}{q} + \frac{1}{q} \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{l-1} \chi(cv(i)).$$

Для каждого $c \in P$ рассмотрим отображение ψ_c , осуществляемое по правилу

$$\psi_c(x_1, \dots, x_k) = \chi(cf(x_1, \dots, x_k)) = e^{2\pi i \text{tr}_P^q(cf(x_1, \dots, x_k))/p}, \quad x_1, \dots, x_k \in P. \quad (14)$$

Тогда

$$\psi_c(u(i+t_1), \dots, u(i+t_k)) = \chi(cf(u(i+t_1), \dots, u(i+t_k))) = \chi(cv(i)), \quad i \geq 0,$$

а значит,

$$N_l(z, v) = \frac{l}{q} + \frac{1}{q} \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{l-1} \psi_c(u(i+t_1), \dots, u(i+t_k)).$$

С использованием равенства (10) будем иметь

$$N_l(z, v) = \frac{l}{q} + \frac{1}{q} \sum_{c \in P^*} \chi(-cz) \sum_{i=0}^{l-1} \frac{1}{q^k} \sum_{\bar{a} \in P^k} W_{\psi_c}(\bar{a}) \chi_{\bar{a}}(u(i+t_1), \dots, u(i+t_k)).$$

Изменив порядок суммирования, получим

$$N_l(z, v) = \frac{l}{q} + \frac{1}{q^{k+1}} \sum_{c \in P^*} \chi(-cz) \sum_{\bar{a} \in P^k} W_{\psi_c}(\bar{a}) \sum_{i=0}^{l-1} \chi_{\bar{a}}(u(i+t_1), \dots, u(i+t_k)).$$

Выделяя отдельно слагаемое, соответствующее $\bar{a} = \bar{0}$, будем иметь

$$N_l(z, v) = \frac{l}{q} + \frac{l}{q^{k+1}} \sum_{c \in P^*} \chi(-cz) W_{\psi_c}(\bar{0}) + \frac{1}{q^{k+1}} \sum_{c \in P^*} \chi(-cz) \sum_{\bar{a} \in P^k \setminus \{\bar{0}\}} W_{\psi_c}(\bar{a}) \sum_{i=0}^{l-1} \chi(u_{\bar{a}}(i)), \quad (15)$$

где для каждого $\bar{a} = (a_1, \dots, a_k) \in P^k$ через $u_{\bar{a}}$ обозначена последовательность над полем P с элементами $u_{\bar{a}}(i) = a_1 u(i+t_1) + \dots + a_k u(i+t_k)$, $i \geq 0$.

Из равенств (11), (14), леммы 1 и соотношения $W_{\psi_0}(\bar{0}) = q^k$ следует, что

$$\begin{aligned} \frac{l}{q} + \frac{l}{q^{k+1}} \sum_{c \in P^*} \chi(-cz) W_{\psi_c}(\bar{0}) &= \frac{l}{q^{k+1}} \sum_{c \in P} \chi(-cz) \sum_{b_1, \dots, b_k \in P} \psi_c(b_1, \dots, b_k) = \\ &= \frac{l}{q^{k+1}} \sum_{c \in P} \chi(-cz) \sum_{b_1, \dots, b_k \in P} \chi(cf(b_1, \dots, b_k)) = \\ &= \frac{l}{q^{k+1}} \sum_{b_1, \dots, b_k \in P} \sum_{c \in P} \chi(c(f(b_1, \dots, b_k) - z)) = \frac{l}{q^k} |f^{-1}(z)|. \end{aligned}$$

Тогда из равенства (15) получим

$$\left| N_l(z, v) - |f^{-1}(z)| \frac{l}{q^k} \right| \leq \frac{1}{q^{k+1}} \sum_{c \in P^*} \sum_{\bar{a} \in P^k \setminus \{\bar{0}\}} |W_{\psi_c}(\bar{a})| \max_{\bar{a} \in P^k \setminus \{\bar{0}\}} \left| \sum_{i=0}^{l-1} \chi(u_{\bar{a}}(i)) \right|.$$

Заметим, что по условию (4) для всех $\bar{a} \in P^k \setminus \{\bar{0}\}$ ЛРП $u_{\bar{a}}$ имеет минимальный член $F(x)$, поэтому согласно теореме 1

$$\left| N_l(z, v) - |f^{-1}(z)| \frac{l}{q^k} \right| \leq \frac{C_l(F)}{q^{k+1}} \sum_{c \in P^*} \sum_{\bar{a} \in P^k \setminus \{\bar{0}\}} |W_{\psi_c}(\bar{a})|. \quad (16)$$

Остаётся воспользоваться п. 4 утверждения 2. ■

Отметим, что если f — сбалансированное отображение, т. е. $|f^{-1}(z)| = q^{k-1}$ для всех $z \in P$, то величина $|f^{-1}(z)| l / q^k$ равна «естественному» среднему значению для числа появлений элемента z на отрезке длины l последовательности v .

Правая часть оценки из теоремы 2 при $l = T(F)$ будет меньше периода $T(F)$ многочлена $F(x)$ при условии $(q-1)q^{k/2-1}(q^m - T(F))^{1/2} < T(F)$, которое заведомо выполнено при $T(F) \geq (q-1)q^{(m+k)/2-1}$.

При $l < T(F)$ правая часть оценки из теоремы 2 меньше l тогда и только тогда, когда

$$l > (q-1) \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) q^{(m+k)/2-1} \text{ и } l > (q-1) (3(q^m l - l^2))^{1/3} q^{k/2-1}$$

соответственно. Второе из этих неравенств заведомо выполнено, если $l \geq (3q^m l)^{1/3} q^{k/2}$, т. е. при $l \geq \sqrt{3} q^{m/2+3k/4}$.

В случае, когда для отображений ψ_c , $c \in P^*$, сопоставленных функции f по правилу (14), известны коэффициенты $W_{\psi_c}(\bar{a})$, $\bar{a} \in P^k$, оценку из теоремы 2 можно уточнить, воспользовавшись неравенством (16). Отсюда с использованием п. 3 утверждения 2 получим также неравенство

$$\left| N_l(z, v) - |f^{-1}(z)| \frac{l}{q^k} \right| \leq \frac{(q-1)C_l(F)}{q} \max_{c \in P^*} |M(\psi_c)|^{1/2}. \quad (17)$$

Для случая $q = 2$ в оценках (16) и (17) рассматривается только значение $c = e$, и в этой ситуации коэффициенты $W_{\psi_c}(\bar{a})$ совпадают с коэффициентами Уолша — Адамара булевой функции $f(x_1, \dots, x_k)$ [15, с. 77]. Если f является бент-функцией, то оценки (13), (16) и (17) совпадают. В случае, когда f имеет нечётный вес, выполнено равенство $M(\psi_e) = P^k$ и оценка (13) совпадает с оценкой (17). Если f — платовидная функция порядка $2t$ [15, § 6.5], то $W_{\psi_e}(\bar{a}) \in \{0, \pm 2^{k-t}\}$ для всех $\bar{a} \in P^k$, $|M(\psi_e)| = 2^{2t}$, а значит, оценки (16) и (17) совпадают, причём они точнее оценки (13).

Как показано в работе [16, теорема 2], при случайном равновероятном выборе булевой функции $f(x_1, \dots, x_k)$ с чётным весом случайная величина η_k , равная числу нулевых коэффициентов Уолша — Адамара, имеет математическое ожидание, удовлетворяющее при $k \rightarrow \infty$ условию $E\eta_k \sim (2^{k+3}/\pi)^{1/2}$. Таким образом, при больших k для почти всех булевых функций f чётного веса правая часть неравенства (17) равна

$$C_l(F) \left(2^{k-2} - \left(\frac{2^{k-1}}{\pi} \right)^{1/2} \right)^{1/2},$$

и при $k \rightarrow \infty$ она эквивалентна правой части неравенства (13).

5. Коэффициенты кросс-корреляции

Пусть $P = \text{GF}(q)$, $F(x)$ — унитарный реверсивный многочлен степени m над полем P , u_1, u_2 — ЛРП над полем P с характеристическим многочленом $F(x)$, $f_1 : P^k \rightarrow P$, $f_2 : P^s \rightarrow P$. Рассмотрим последовательности v_1 и v_2 , полученные по правилу

$$v_1(i) = f_1(u_1(i+t_1), \dots, u_1(i+t_k)), \quad v_2(i) = f_2(u_2(i+l_1), \dots, u_2(i+l_s)), \quad i \geq 0,$$

где $t_1, \dots, t_k, l_1, \dots, l_s$ — некоторые целые неотрицательные числа.

Определим коэффициент кросс-корреляции $C_{v_1, v_2}(l, t)$ последовательностей v_1 и v_2 равенством

$$C_{v_1, v_2}(l, t) = \sum_{i=0}^{l-1} \chi(v_1(i) - v_2(i+t)), \quad t = 0, 1, \dots, T(F) - 1,$$

где χ — аддитивный характер поля P , заданный равенством (5). В случае $l = T(F)$ функция $C_{v_1, v_2}(l, t)$ от переменной t называется кросс-корреляционной функцией [5, с. 579]. Величина $|C_{v_1, v_2}(l, t)|$ характеризует близость начальных отрезков длины l последовательностей v_1 и $x^t v_2$.

Будем говорить, что система ЛРП $\omega_1, \dots, \omega_n$ над полем P с характеристическим многочленом $F(x) \in P[x]$ *сильно линейно независима*, если для всех $(c_1, \dots, c_n) \in P^n \setminus \{\bar{0}\}$ последовательность $c_1 \omega_1 + \dots + c_n \omega_n$ имеет минимальный многочлен $F(x)$. Если $\Phi_1(x), \dots, \Phi_n(x)$ — генераторы ЛРП $\omega_1, \dots, \omega_n$ [2, глава 25, § 2] относительно характеристического многочлена $F(x)$ соответственно, то сильная линейная независимость равносильна соотношениям

$$(c_1 \Phi_1(x) + \dots + c_n \Phi_n(x), F(x)) = e \text{ для всех } \bar{c} = (c_1, \dots, c_n) \in P^n \setminus \{\bar{0}\}.$$

Определим отображения ψ_1 и ψ_2 равенствами

$$\begin{aligned} \psi_1(x_1, \dots, x_k) &= \chi(f_1(x_1, \dots, x_k)), \quad x_1, \dots, x_k \in P, \\ \psi_2(y_1, \dots, y_s) &= \chi(-f_2(y_1, \dots, y_s)), \quad y_1, \dots, y_s \in P. \end{aligned}$$

Теорема 3. Пусть система

$$x^{t_1} u_1, x^{t_2} u_1, \dots, x^{t_k} u_1, x^{l_1+t} u_2, x^{l_2+t} u_2, \dots, x^{l_s+t} u_2$$

сильно линейно независима над полем P . Тогда для всех $l \leq T(F)$

$$\left| C_{v_1, v_2}(l, t) - \frac{l}{q^{k+s}} W_{\psi_1}(\bar{0}) W_{\psi_2}(\bar{0}) \right| \leq q^{\frac{k+s}{2}} C_l(F),$$

где

$$W_{\psi_1}(\bar{0}) = \sum_{(a_1, \dots, a_k) \in P^k} \chi(f_1(a_1, \dots, a_k)), \quad W_{\psi_2}(\bar{0}) = \sum_{(b_1, \dots, b_s) \in P^s} \chi(-f_2(b_1, \dots, b_s)),$$

а величина $C_l(F)$ определена соотношениями (3).

Доказательство. Из равенства

$$C_{v_1, v_2}(l, t) = \sum_{i=0}^{l-1} \psi_1(u_1(i+t_1), \dots, u_1(i+t_k)) \psi_2(u_2(i+l_1+t), \dots, u_2(i+l_s+t))$$

с использованием формулы (10) будем иметь

$$C_{v_1, v_2}(l, t) = \frac{1}{q^{k+s}} \sum_{\bar{a} \in P^k, \bar{b} \in P^s} W_{\psi_1}(\bar{a}) W_{\psi_2}(\bar{b}) \sum_{i=0}^{l-1} \chi(w_{\bar{a}, \bar{b}}(i)),$$

где $w_{\bar{a}, \bar{b}}$ — последовательность, определённая для всех $\bar{a} = (a_1, \dots, a_k)$, $\bar{b} = (b_1, \dots, b_s)$ равенством

$$w_{\bar{a}, \bar{b}}(i) = a_1 u_1(i+t_1) + \dots + a_k u_1(i+t_k) + b_1 u_2(i+l_1+t) + \dots + b_s u_2(i+l_s+t), \quad i \geq 0.$$

Поэтому

$$C_{v_1, v_2}(l, t) - \frac{l}{q^{k+s}} W_{\psi_1}(\bar{0}) W_{\psi_2}(\bar{0}) = \frac{1}{q^{k+s}} \sum_{(\bar{a}, \bar{b}) \neq (\bar{0}, \bar{0})} W_{\psi_1}(\bar{a}) W_{\psi_2}(\bar{b}) \sum_{i=0}^{l-1} \chi(w_{\bar{a}, \bar{b}}(i)),$$

где суммирование осуществляется по всем наборам $(\bar{a}, \bar{b}) \in P^k \times P^s$, для которых $\bar{a} \neq \bar{0}$ или $\bar{b} \neq \bar{0}$. Учитывая, что для всех рассматриваемых наборов минимальный многочлен последовательности $w_{\bar{a}, \bar{b}}$ равен $F(x)$, с использованием теоремы 1 и п. 4 утверждения 2 будем иметь

$$\left| C_{v_1, v_2}(l, t) - \frac{l}{q^{k+s}} W_{\psi_1}(\bar{0}) W_{\psi_2}(\bar{0}) \right| \leq \frac{1}{q^{k+s}} \left(\sum_{\bar{a} \in P^k} |W_{\psi_1}(\bar{a})| \right) \left(\sum_{\bar{b} \in P^s} |W_{\psi_2}(\bar{b})| \right) C_l(F) \leq q^{(k+s)/2} C_l(F).$$

Теорема доказана. ■

Следствие 1. Пусть в условиях теоремы 3 хотя бы одно из отображений f_1 или f_2 сбалансировано. Тогда

$$|C_{v_1, v_2}(l, t)| \leq q^{(k+s)/2} C_l(F).$$

Доказательство. Пусть отображение f_1 сбалансировано. Согласно равенству (11) и лемме 1,

$$W_{\psi_1}(\bar{0}) = \sum_{a_1, \dots, a_k \in P} \chi(f_1(a_1, \dots, a_k)) = q^{k-1} \left(\sum_{a \in P} \chi(a) \right) = 0.$$

Аналогично, если f_2 сбалансировано, то $W_{\psi_2}(\bar{0}) = 0$. ■

Следствие 2. Пусть система

$$x^{t_1} u_1, x^{t_2} u_1, \dots, x^{t_k} u_1, x^{l_1} u_2, x^{l_2} u_2, \dots, x^{l_s} u_2$$

сильно линейно независима над полем P и хотя бы одно из отображений f_1, f_2 сбалансировано. Тогда при выполнении каждого из двух условий

$$1) T(F) \geq q^{(m+k+s)/2},$$

$$2) F(x) \text{ — многочлен максимального периода и } k + s < 2m$$

последовательности v_1 и v_2 различны.

Доказательство. Допустим $v_1 = v_2$, тогда, согласно следствию 1, $T(F) = |C_{v_1, v_2}(T(F), 0)| \leq q^{(k+s)/2} (q^m - T(F))^{1/2}$, что противоречит условию 1. Если $F(x)$ — многочлен максимального периода, то по следствию 1 получим $T(F) = q^m - 1 = |C_{v_1, v_2}(T(F), 0)| \leq q^{(k+s)/2}$, что противоречит условию 2. ■

6. Обобщения на случай r -грамм

Пусть всюду далее $F(x)$ — унитарный реверсивный многочлен степени m над полем $P = \text{GF}(q)$, v — выходная последовательность фильтрующего генератора, удовлетворяющая равенству (1), $l \in \mathbb{N}$. Для набора $\bar{s} = (s_1, \dots, s_r)$ целых неотрицательных чисел и r -граммы $\bar{z} = (z_1, \dots, z_r) \in P^r$ обозначим через $N_l(\bar{z}, \bar{s}, v)$ количество чисел $i \in \{0, 1, \dots, l-1\}$, таких, что

$$\begin{cases} v(i + s_1) = z_1, \\ v(i + s_2) = z_2, \\ \dots \\ v(i + s_r) = z_r, \end{cases}$$

т.е. $N_l(\bar{z}, \bar{s}, v)$ — число появлений $\bar{z}$ среди r -грамм $(v(i + s_1), \dots, v(i + s_r))$, где $i \in \{0, 1, \dots, l-1\}$. Потребуем, чтобы числа $t_1, \dots, t_k$ и $s_1, \dots, s_r$ были выбраны так, что система

$$x^{s_1+t_1} u, \dots, x^{s_1+t_k} u, x^{s_2+t_1} u, \dots, x^{s_2+t_k} u, \dots, x^{s_r+t_1} u, \dots, x^{s_r+t_k} u \quad (18)$$

сильно линейно независима над полем P . Данное требование равносильно тому, что $M_u(x) = F(x)$ и для всех элементов $a_1^{(1)}, \dots, a_k^{(1)}, \dots, a_1^{(r)}, \dots, a_k^{(r)} \in P$, не равных нулю одновременно, выполнено соотношение

$$(a_1^{(1)}x^{s_1+t_1} + \dots + a_k^{(1)}x^{s_1+t_k} + \dots + a_1^{(r)}x^{s_r+t_1} + \dots + a_k^{(r)}x^{s_r+t_k}, F(x)) = e.$$

В частности, условие сильной линейной независимости системы (18) означает, что числа $s_1+t_1, \dots, s_1+t_k, s_2+t_1, \dots, s_2+t_k, \dots, s_r+t_1, \dots, s_r+t_k$ попарно различны и $rk \leq m$. В случае, когда $s_1 = 0, s_2 = 1, \dots, s_r = r-1$, попарное различие рассматриваемых чисел имеет место тогда и только тогда, когда

$$t_2 \geq t_1 + r, t_3 \geq t_2 + r, \dots, t_k \geq t_{k-1} + r.$$

Лемма 2. Пусть χ — канонический аддитивный характер поля $P = \text{GF}(q)$, задаваемый равенством (5), а ψ_c — отображение, определённое соотношением (14), где $c \in P$. Тогда

$$\frac{l}{q^{(k+1)r}} \sum_{c_1, \dots, c_r \in P} \chi(-c_1 z_1 - \dots - c_r z_r) W_{\psi_{c_1}}(\bar{0}) \cdots W_{\psi_{c_r}}(\bar{0}) = \frac{l}{q^{kr}} |f^{-1}(z_1)| \cdots |f^{-1}(z_r)|.$$

Доказательство. С использованием равенства (11) получим

$$\begin{aligned} & \frac{l}{q^{(k+1)r}} \sum_{c_1, \dots, c_r \in P} \chi(-c_1 z_1 - \dots - c_r z_r) W_{\psi_{c_1}}(\bar{0}) \cdots W_{\psi_{c_r}}(\bar{0}) = \\ & = \frac{l}{q^{(k+1)r}} \sum_{c_1, \dots, c_r \in P} \chi(-c_1 z_1 - \dots - c_r z_r) \times \\ & \times \left(\sum_{b_1^{(1)}, \dots, b_k^{(1)} \in P} \chi(c_1 f(b_1^{(1)}, \dots, b_k^{(1)})) \right) \cdots \left(\sum_{b_1^{(r)}, \dots, b_k^{(r)} \in P} \chi(c_r f(b_1^{(r)}, \dots, b_k^{(r)})) \right) = \\ & = \frac{l}{q^{(k+1)r}} \left(\sum_{b_1^{(1)}, \dots, b_k^{(1)} \in P} \sum_{c_1 \in P} \chi(c_1 (f(b_1^{(1)}, \dots, b_k^{(1)}) - z_1)) \right) \cdots \\ & \cdots \left(\sum_{b_1^{(r)}, \dots, b_k^{(r)} \in P} \sum_{c_r \in P} \chi(c_r (f(b_1^{(r)}, \dots, b_k^{(r)}) - z_r)) \right). \end{aligned}$$

Для завершения доказательства остаётся воспользоваться леммой 1. ■

Теорема 4. Пусть $F(x)$ — унитарный реверсивный многочлен степени m над полем $P = \text{GF}(q)$, v — последовательность, удовлетворяющая равенству (1). Тогда если система ЛРП (18) сильно линейно независима над полем P , то для всех $l \leq T(F)$ и $\bar{z} \in P^r$ справедлива оценка

$$\left| N_l(\bar{z}, \bar{s}, v) - |f^{-1}(z_1)| \cdots |f^{-1}(z_r)| \frac{l}{q^{kr}} \right| \leq \frac{((q-1)q^{k/2} + 1)^r - 1}{q^r} C_l(F),$$

где $C_l(F)$ — величина, определённая равенством (3).

Доказательство. С использованием леммы 1 получим

$$N_l(\bar{z}, \bar{s}, v) = \sum_{i=0}^{l-1} \left(\frac{1}{q} \sum_{c_1 \in P} \chi(c_1 (v(i+s_1) - z_1)) \right) \cdots \left(\frac{1}{q} \sum_{c_r \in P} \chi(c_r (v(i+s_r) - z_r)) \right).$$

Отсюда будем иметь

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

где $\bar{c}\bar{z} = (c_1, \dots, c_r)(z_1, \dots, z_r) = c_1 z_1 + \dots + c_r z_r$. Выделяя слагаемое, соответствующее случаю $(c_1, \dots, c_r) = (0, \dots, 0) = \bar{0}$, получим

$$N_l(\bar{z}, \bar{s}, v) - \frac{l}{q^r} = \frac{1}{q^r} \sum_{\bar{c} \in P^r \setminus \{\bar{0}\}} \chi(-\bar{c}\bar{z}) D_l(\bar{c}), \quad (19)$$

где

$$D_l(\bar{c}) = \sum_{i=0}^{l-1} \chi(c_1 v(i + s_1)) \cdots \chi(c_r v(i + s_r)). \quad (20)$$

Обозначим через $|\bar{c}|$ вес (количество ненулевых координат) вектора $\bar{c} \in P^r$. Тогда равенство (19) запишется в виде

$$N_l(\bar{z}, \bar{s}, v) - \frac{l}{q^r} = \frac{1}{q^r} \sum_{d=1}^r \sum_{\substack{\bar{c} \in P^r, \\ |\bar{c}|=d}} \chi(-\bar{c}\bar{z}) D_l(\bar{c}). \quad (21)$$

Пусть вектор $\bar{c} = (c_1, \dots, c_r) \in P^r$ имеет вес d , ненулевые элементы в нём стоят на местах $j_1, \dots, j_d$ и выполнено равенство $c_{j_1} = h_1, \dots, c_{j_d} = h_d$. Тогда с использованием равенств (14) и (20) получим

$$D_l(\bar{c}) = \sum_{i=0}^{l-1} \psi_{h_1}(u(i + s_{j_1} + t_1), \dots, u(i + s_{j_1} + t_k)) \cdots \psi_{h_d}(u(i + s_{j_d} + t_1), \dots, u(i + s_{j_d} + t_k)).$$

Используя равенство (10), $D_l(\bar{c})$ запишем следующим образом:

$$\begin{aligned} D_l(\bar{c}) &= \sum_{i=0}^{l-1} \left(\frac{1}{q^k} \sum_{\bar{a}_1 \in P^k} W_{\psi_{h_1}}(\bar{a}_1) \chi_{\bar{a}_1}(u(i + s_{j_1} + t_1), \dots, u(i + s_{j_1} + t_k)) \right) \cdots \\ &\cdots \left(\frac{1}{q^k} \sum_{\bar{a}_d \in P^k} W_{\psi_{h_d}}(\bar{a}_d) \chi_{\bar{a}_d}(u(i + s_{j_d} + t_1), \dots, u(i + s_{j_d} + t_k)) \right). \end{aligned}$$

Значит,

$$D_l(\bar{c}) = \frac{1}{q^{kd}} \sum_{\bar{a}_1, \dots, \bar{a}_d \in P^k} W_{\psi_{h_1}}(\bar{a}_1) \cdots W_{\psi_{h_d}}(\bar{a}_d) \sum_{i=0}^{l-1} \chi(\omega_{\bar{a}_1, \dots, \bar{a}_d}(i)), \quad (22)$$

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

$$\begin{aligned} \omega_{\bar{a}_1, \dots, \bar{a}_d}(i) &= a_1^{(1)} u(i + s_{j_1} + t_1) + \dots + a_k^{(1)} u(i + s_{j_1} + t_k) + \dots \\ &\dots + a_1^{(d)} u(i + s_{j_d} + t_1) + \dots + a_k^{(d)} u(i + s_{j_d} + t_k), \quad i \geq 0. \end{aligned}$$

Так как система (18) сильно линейно независима над полем P , то минимальный многочлен последовательности $\omega_{\bar{a}_1, \dots, \bar{a}_d}$ равен $F(x)$, за исключением случая, когда $\bar{a}_1 = \dots = \bar{a}_d = \bar{0}$. Выделив отдельно в равенстве (22) слагаемое, соответствующее этому случаю, будем иметь

$$D_l(\bar{c}) = \frac{l}{q^{kd}} W_{\psi_{h_1}}(\bar{0}) \cdots W_{\psi_{h_d}}(\bar{0}) + D_l^*(\bar{c}), \quad (23)$$

где

$$D_l^*(\bar{c}) = \frac{1}{q^{kd}} \sum_{\bar{a}_1, \dots, \bar{a}_d \in P^k \setminus \{(\bar{0}, \dots, \bar{0})\}} W_{\psi_{h_1}}(\bar{a}_1) \cdots W_{\psi_{h_d}}(\bar{a}_d) \sum_{i=0}^{l-1} \chi(\omega_{\bar{a}_1, \dots, \bar{a}_d}(i)). \quad (24)$$

Подставив равенство (23) в соотношение (21), получим

$$N_l(\bar{z}, \bar{s}, v) - \delta_l(\bar{z}) = \frac{1}{q^r} \sum_{d=1}^r \sum_{\substack{\bar{c} \in P^r, \\ |\bar{c}|=d}} \chi(-\bar{c}\bar{z}) D_l^*(\bar{c}), \quad (25)$$

где $\delta_l(\bar{z}) = \frac{l}{q^r} + \frac{1}{q^r} \sum_{d=1}^r \sum_{\substack{\bar{c} \in P^r, \\ |\bar{c}|=d}} \chi(-\bar{c}\bar{z}) \frac{l}{q^{kd}} W_{\psi_{h_1}}(\bar{0}) \cdots W_{\psi_{h_d}}(\bar{0})$.

Для вычисления $\delta_l(\bar{z})$ воспользуемся леммой 2 и равенством $W_{\psi_0}(\bar{0}) = q^k$:

$$\begin{aligned} \delta_l(\bar{z}) &= \frac{l}{q^{(k+1)r}} \underbrace{W_{\psi_0}(\bar{0}) \cdots W_{\psi_0}(\bar{0})}_r + \frac{l}{q^{(k+1)r}} \sum_{\bar{c} \in P^r \setminus \{\bar{0}\}} \chi(-\bar{c}\bar{z}) W_{\psi_{c_1}}(\bar{0}) \cdots W_{\psi_{c_r}}(\bar{0}) = \\ &= \frac{l}{q^{(k+1)r}} \sum_{\bar{c} \in P^r} \chi(-\bar{c}\bar{z}) W_{\psi_{c_1}}(\bar{0}) \cdots W_{\psi_{c_r}}(\bar{0}) = \frac{l}{q^{kr}} |f^{-1}(z_1)| \cdots |f^{-1}(z_r)|. \end{aligned}$$

Подставим найденное значение в равенство (25) и перейдём к исследованию абсолютных величин, в результате будем иметь

$$\left| N_l(\bar{z}, \bar{s}, v) - |f^{-1}(z_1)| \cdots |f^{-1}(z_r)| \frac{l}{q^{kr}} \right| \leq \frac{1}{q^r} \sum_{d=1}^r \sum_{\substack{\bar{c} \in P^r, \\ |\bar{c}|=d}} |D_l^*(\bar{c})|. \quad (26)$$

Из равенства (24), теоремы 1 и п. 4 утверждения 2 получим

$$\begin{aligned} |D_l^*(\bar{c})| &\leq \frac{C_l(F)}{q^{kd}} \sum_{\bar{a}_1, \dots, \bar{a}_d \in P^k \setminus \{(\bar{0}, \dots, \bar{0})\}} |W_{\psi_{h_1}}(\bar{a}_1)| \cdots |W_{\psi_{h_d}}(\bar{a}_d)| \leq \\ &\leq \frac{C_l(F)}{q^{kd}} \left(\sum_{\bar{a}_1 \in P^k} |W_{\psi_{h_1}}(\bar{a}_1)| \right) \cdots \left(\sum_{\bar{a}_d \in P^k} |W_{\psi_{h_d}}(\bar{a}_d)| \right) \leq C_l(F) q^{kd/2}. \end{aligned} \quad (27)$$

Тогда с использованием неравенства (26) можно записать

$$\begin{aligned} \left| N_l(\bar{z}, \bar{s}, v) - |f^{-1}(z_1)| \cdots |f^{-1}(z_r)| \frac{l}{q^{kr}} \right| &\leq \frac{1}{q^r} \sum_{d=1}^r \binom{r}{d} (q-1)^d C_l(F) q^{kd/2} = \\ &= \frac{C_l(F)}{q^r} (((q-1)q^{k/2} + 1)^r - 1). \end{aligned}$$

Теорема доказана. ■

Отметим, что при $r = 1$ оценка из теоремы 4 совпадает с оценкой из теоремы 2. Таким образом, теорема 4 обобщает теорему 2 на случай r -грамм.

Если f — сбалансированное отображение, то

$$|f^{-1}(z_1)| \cdots |f^{-1}(z_r)| \frac{l}{q^{kr}} = \frac{l}{q^r},$$

и теорема 4 устанавливает оценку отклонения частоты $N_l(\bar{z}, \bar{s}, v)$ от «естественного» среднего значения l/q^r .

Приведём условия, при которых применима оценка из теоремы 4. Как отмечалось ранее, на длину r набора $\bar{z}$ накладывается условие $r \leq m/k$, где m — степень многочлена $F(x)$, а k — число переменных функции f . Укажем условия, при которых оценка из теоремы 4 нетривиальна (правая часть неравенства меньше l). С использованием неравенств (26) и (27) получим, что справедлива менее точная оценка

$$\left| N_l(\bar{z}, \bar{s}, v) - |f^{-1}(z_1)| \cdots |f^{-1}(z_r)| \frac{l}{q^{kr}} \right| \leq \frac{(q^r - 1)C_l(F)}{q^r} q^{kr/2}. \quad (28)$$

Если $l = T(F)$, то данная оценка нетривиальна при условии $T(F) \geq q^{(m+kr)/2}$. Если $l < T(F)$, то оценка (28) нетривиальна при условиях

$$l > \frac{q^r - 1}{q^r} \left(\frac{4}{\pi^2} \ln T(F) + \frac{9}{5} \right) q^{(m+kr)/2} \text{ и } l > \frac{q^r - 1}{q^r} (3(q^m l - l^2))^{1/3} q^{kr/2}$$

соответственно. Второе из этих неравенств заведомо выполнено, если $l \geq \sqrt{3} q^{m/2+3kr/4}$.

Согласно соотношению (27), $|D_l^*(\bar{c})| \leq \frac{C_l(F)}{q^{kd}} \left(\max_{c \in P^*} \sum_{\bar{a} \in P^k} |W_{\psi_c}(\bar{a})| \right)^d$, поэтому в условиях теоремы 4 справедлива оценка

$$\left| N_l(\bar{z}, \bar{s}, v) - |f^{-1}(z_1)| \cdots |f^{-1}(z_r)| \frac{l}{q^{kr}} \right| \leq \frac{C_l(F)}{q^r} \left(\left(\frac{q-1}{q^k} \left(\max_{c \in P^*} \sum_{\bar{a} \in P^k} |W_{\psi_c}(\bar{a})| \right) + 1 \right)^r - 1 \right).$$

Отсюда с использованием п. 3 утверждения 2 получим

$$\left| N_l(\bar{z}, \bar{s}, v) - |f^{-1}(z_1)| \cdots |f^{-1}(z_r)| \frac{l}{q^{kr}} \right| \leq \frac{C_l(F)}{q^r} \left(\left((q-1) \max_{c \in P^*} |M(\psi_c)|^{1/2} + 1 \right)^r - 1 \right).$$

Пусть $P = \text{GF}(q)$, $f(x_1, \dots, x_k) = c_1 x_1 + \dots + c_k x_k$ для некоторых не всех равных нулю элементов $c_1, \dots, c_k \in P$. Тогда $|M(\psi_c)| = 1$ для всех $c \in P$, последовательность v , удовлетворяющая равенству (2), является ЛРП с характеристическим многочленом $F(x)$, и для неё из последнего неравенства получим известные оценки (см. [9, теорема 2], [11, теорема 3], [17, теорема 1])

$$\left| N_l(\bar{z}, \bar{s}, v) - \frac{l}{q^r} \right| \leq \frac{q^r - 1}{q^r} C_l(F).$$

При этом из доказательства теоремы 4 следует, что вместо сильной линейной независимости системы (18) достаточно потребовать сильную линейную независимость системы $x^{s_1}v, \dots, x^{s_r}v$.

ЛИТЕРАТУРА

1. Алферов А. П., Zubov А. Ю., Кузьмин А. С., Черемушкин А. С. Основы криптографии. М.: Гелиос АРВ, 2001. 480 с.
2. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра: учебник. Т. 2. М.: Гелиос АРВ, 2003. 416 с.
3. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., and Nechaev A. A. Linear recurring sequences over rings and modules // J. Math. Sci. 1995. V. 76. No. 6. P. 2793–2915.
4. Лаксов Д. Линейные рекуррентные последовательности над конечными полями // Математика: сб. переводов. 1967. Т. 11. № 6. С. 145–158.

5. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. Т. 1, 2. 822 с.
6. Мак-Вильямс Ф. Д., Слоэн Н. Д. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
7. Dai Z. D., Feng X. N., Liu M. L., and Wan Z. X. Some statistical properties of feedforward sequences (I) // Science in China (Ser. A). 1994. V. 37. No. 1. P. 34–41.
8. Dai Z. D., Feng X. N., Liu M. L., and Wan Z. X. Some statistical properties of feedforward sequences (II) // Science in China (Ser. A). 1994. V. 37. No. 2. P. 129–136.
9. Niederreiter H. Distribution properties of feedback shift register sequences // Probl. Control and Inform. Theory. 1986. V. 15. No. 1. P. 19–34.
10. Cochran T. On a trigonometric inequality of Vinogradov // J. Number Theory. 1987. V. 27. No. 1. P. 9–16.
11. Сидельников В. М. Оценки для числа появлений знаков на отрезках рекуррентной последовательности над конечным полем // Дискретная математика. 1991. Т. 3. № 2. С. 87–95.
12. Коробов Н. М. Распределение невычетов и первообразных корней в рекуррентных рядах // Докл. Акад. наук СССР. 1953. Т. 88. № 4. С. 603–606.
13. Солодовников В. И. Бент-функции из конечной абелевой группы в конечную абелеву группу // Дискретная математика. 2002. Т. 14. № 1. С. 99–113.
14. Амбросимов А. С. Свойства бент-функций q -значной логики над конечными полями // Дискретная математика. 1994. Т. 6. № 3. С. 50–60.
15. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
16. Рязанов Б. В. О распределении спектральной сложности булевых функций // Дискретная математика. 1994. Т. 6. № 2. С. 111–119.
17. Нечаев В. И. Распределение знаков в последовательности прямоугольных матриц над конечным полем // Труды математического института им. В. А. Стеклова. 1997. Т. 218. С. 335–342.