Math-Net.Ru

Общероссийский математический портал

В. Л. Куракин, Семейство последовательностей максимального периода над кольцом из 8 элементов с низкой кросс-корреляцией, *Матем. вопр. криптогр.*, 2011, том 2, выпуск 3, 47–73

DOI: <https://doi.org/10.4213/mvk36>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.209.52.79

26 апреля 2023 г., 18:07:03

УДК: 512.53, 519.113.6

Семейство последовательностей максимального периода над кольцом из 8 элементов с низкой кросс-корреляцией

В. Л. Куракин

Российский государственный социальный университет, Москва

Получено 10.V.2011

В работе строится семейство последовательностей периода $2(2^m - 1)$ над кольцом из 8 элементов, кросс-корреляционная функция которых асимптотически оптимальна относительно оценок Сидельникова и Уолша.

Ключевые слова: линейные рекуррентные последовательности над кольцами, линейные рекурренты максимального периода, кросс-корреляционная функция, оценка Сидельникова, оценка Уолша, оптимальная кросс-корреляция, суммы характеров

Family of maximal period sequences with low cross-correlation over an 8-element ring

V. L. Kurakin

Russian State Social University, Moscow

Abstract. A family of sequences over a ring with 8 elements having period $2(2^m - 1)$ and cross-correlation function asymptotically optimal with respect to the Sidelnikov and Welch bounds is constructed.

Key words: linear recurrent sequences over rings, sequences of maximal period, cross-correlation function, Sidelnikov bound, Welch bound, optimal cross-correlation, sums of characters

Citation: *Mathematical Aspects of Cryptography*, 2011, vol. 2, no. 3, pp. 47–73 (Russian).

© 2011 В. Л. Куракин

1. Кросс-корреляционная функция

Пусть A — семейство последовательностей над кольцом вычетов $\mathbb{Z}_m$, период каждой из которых равен T . Через $\omega \in \mathbb{C}$ обозначим первообразный корень степени m из 1 в поле комплексных чисел. Отображение

$$\chi: \mathbb{Z}_m \rightarrow \mathbb{C}^*, \quad \chi(a) = \omega^a, \quad 0 \leq a < m,$$

является характером группы $(\mathbb{Z}_m, +)$, т.е. *аддитивным характером кольца $\mathbb{Z}_m$* . Кросс-корреляционная функция последовательностей $u, v \in A$ определяется равенством

$$C_{u,v}(t) = \sum_{i=0}^{T-1} \chi(u(i) - v(i+t)) = \sum_{i=0}^{T-1} \omega^{u(i)-v(i+t)}, \quad t \geq 0,$$

где разность $u(i) - v(i+t)$ рассматривается как действительное число и суммирование проводится в поле комплексных чисел $\mathbb{C}$. Эта функция периодична: $C_{u,v}(t+T) = C_{u,v}(t)$. Очевидно, $|C_{u,v}(t)| \leq T$. Значение $C_{u,u}(0) = T$ и равные ему значения $C_{u,u}(t)$ при $T \mid t$ называют *фазовыми*. Автокорреляционная функция последовательности u определяется равенством $C_u(t) = C_{u,u}(t)$.

Для последовательностей над полем $P = GF(2)$ кросс-корреляционная функция имеет вид

$$C_{u,v}(t) = \sum_{i=0}^{T-1} (-1)^{u(i)-v(i+t)}, \quad t \geq 0.$$

Сдвиг последовательности u на t шагов влево обозначим $x^t u$, так что

$$x^t u(i) = u(i+t), \quad i \geq 0.$$

Тогда

$$C_{u,v}(t) = T - 2\rho(u, x^t v),$$

где $\rho(u, x^t v) = |\{i: 0 \leq i < T, u(i) \neq v(i+t)\}|$ — расстояние Хэмминга между двоичными векторами длины T . Поэтому кросс-корреляционную функцию можно воспринимать как меру близости между последовательностями u и $x^t v$, которая тем больше по модулю, чем ближе последовательности. Функция $C_{u,v}(t)$ равна 0 тогда и только тогда, когда $u - x^t v$ есть равномерная двоичная последовательность (а значит, T чётно), т.е. содержит одинаковое число 0 и 1 на цикле.

Значение функции кросс-корреляции в системах связи объяснено в [5]. Основным параметром, по которому оцениваются кросс-корреляционные свойства семейства A над кольцом $\mathbb{Z}_m$, является число

$$C_{\max} = C_{\max}(A) = \max\{|C_{u,v}(t)| : u, v \in A, 0 \leq t < T, (u, t) \neq (v, 0)\}.$$

В некоторых приложениях последовательность из A считается неотличимой от ее циклического сдвига. Поэтому семейство A выбирается замкнутым относительно сдвигов и наряду с ним, в качестве основного рассматривают семейство $\tilde{A}$, состоящее из каким-то образом выбранных представителей всех циклов семейства A . При этом $|\tilde{A}| = |A|/T$.

Представляют интерес семейства над кольцом $\mathbb{Z}_m$ с возможно меньшим значением параметра $C_{\max}$. Существуют теоретические нижние оценки для этого параметра, наиболее известные из которых — оценки Сидельникова и Уолша. Согласно оценке Сидельникова [8] для семейства из $|A| = T + 1$ последовательностей периода T параметр $C_{\max}$ при больших T ограничен снизу:

$$C_{\max} \geq \sqrt{\alpha T}, \quad (1)$$

где $\alpha = 2$ для двоичных и $\alpha = 1$ для недвоичных последовательностей. Первое семейство p -ичных последовательностей ($p \geq 3$ простое), для которых достигается эта оценка, было построено В.М.Сидельниковым. Из оценки (1) видно, что в недвоичном случае теоретически возможно строить семейства последовательностей, для которых параметр $C_{\max}$ будет в $\sqrt{2}$ раз меньше, чем в двоичном случае. Это объясняет интерес к недвоичным последовательностям.

Оценка Уолша [12] (в одной из ее формулировок) утверждает, что для семейства из $|A| = M$ последовательностей периода T над кольцом $\mathbb{Z}_m$ верно неравенство

$$C_{\max}^2 \geq \frac{T^2(M-1)}{MT-1} = T \left(1 - \frac{T-1}{MT-1} \right). \quad (2)$$

Эта оценка показывает, что при $M, T \rightarrow \infty$ асимптотически $C_{\max}$ не меньше $\sqrt{T}$. Семейства, удовлетворяющие этому условию, называют асимптотически оптимальными относительно оценки Уолша.

2. Оптимальные семейства последовательностей над кольцом $\mathbb{Z}_4$

В настоящее время найдено множество семейств последовательностей, асимптотически оптимальных относительно оценок Сидельникова и Уолша.

Рассмотрим семейства из работы [9], поскольку семейство, которое строится в данной работе, является их обобщением.

В дальнейшем через $GR(q^n, p^n)$ будем обозначать кольцо Галуа характеристики p^n , состоящее из q^n элементов [6, 10, 11]. Пусть $R = \mathbb{Z}_4$ — кольцо вычетов по модулю 4 и $R' = GR(4^m, 4)$ — его расширение Галуа степени m . Обозначим через

$$\Gamma(R') = \{b \in R' : b^{2^m} = b\}$$

2-адическое координатное множество кольца R' . Это множество состоит из 2^m элементов, попарно различных по модулю радикала $2R'$ кольца R' , и замкнуто относительно умножения. Любой элемент $a \in R'$ однозначно представляется в виде

$$a = a_0 + 2a_1, \quad \text{где } a_0 = \gamma_0(a), a_1 = \gamma_1(a) \in \Gamma(R'), \quad (3)$$

называемым *2-адическим разложением* элемента a . Относительно операций сложения $a \oplus b = \gamma_0(a + b)$, $a, b \in \Gamma(R')$, и умножения кольца R' множество $\Gamma(R')$ образует поле $GF(2^m)$.

Пусть $F(x) \in R[x]$ — унитарный многочлен степени m , образ $\bar{F}(x)$ которого над полем вычетов $\bar{R} = R/2R = GF(2)$ неприводим над полем $\bar{R}$. Такой многочлен называется *многочленом Галуа*. В дальнейшем предполагается, что период $T(\bar{F})$ многочлена $\bar{F}(x)$ равен $T(\bar{F}) = 2^m - 1$, т. е. $\bar{F}(x)$ есть многочлен максимального периода над полем вычетов $\bar{R}$. Тогда период $T(F)$ многочлена $F(x)$ над кольцом R может быть равен $2^m - 1$ или $2(2^m - 1)$. В первом случае многочлен $F(x)$ называется *отмеченным*, во втором — *многочленом максимального периода* (ММП) над кольцом R [1]. В кольце Галуа $R' = GR(4^m, 4)$ многочлен $F(x)$ имеет корень α . Многочлен $F(x)$ является отмеченным тогда и только тогда, когда $\alpha \in \Gamma(R')$, т. е. $\alpha = \gamma_0(\alpha)$.

Обозначим через $L_R(F)$ множество всех линейных рекуррентных последовательностей (ЛРП) над кольцом R с характеристическим многочленом $F(x)$. Пусть

$$L_R^*(F) = \{u \in L_R(F) : \bar{u} \neq 0\} = L_R(F) \setminus 2L_R(F)$$

есть множество последовательностей из $L_R(F)$, у которых начальный вектор не равен нулевому вектору по модулю 2.

В [9] рассматриваются два семейства последовательностей над кольцом $R = \mathbb{Z}_4$, которые мы будем обозначать A_0 и B_0 (в [9] они обозначаются A и B):

$$A_0 = L_R(F) \setminus 0, \quad \text{где } F(x) \text{ — отмеченный многочлен,}$$

$$B_0 = L_R^*(F), \quad \text{где } F(x) \text{ — ММП,}$$

причем во втором случае на корень α многочлена $F(x)$ накладываются условия, формулируемые в терминах p -адического разложения (3) следующим образом: если

$$\alpha = \alpha_0 + 2\alpha_1 = \alpha_0(1 + 2\delta), \quad \text{где } \delta = \alpha_0^{-1}\alpha_1, \quad (4)$$

то

$$\delta \neq 1, \quad \text{tr}_1^m(\bar{\delta}) = 1. \quad (5)$$

Здесь

$$\text{tr} = \text{tr}_1^m = \text{tr}_{GF(2)}^{GF(2^m)} = \text{tr}_{\Gamma(R)}^{\Gamma(R')}$$

— след из поля $\Gamma(R') = GF(2^m)$ в поле $\Gamma(R) = GF(2)$, определяемый равенством

$$\text{tr}(x) = x \oplus x^2 \oplus \dots \oplus x^{2^{m-1}}.$$

В следующей таблице перечислены параметры семейств A_0 и B_0 : число последовательностей M , период последовательностей T , число циклов M/T и верхняя оценка на кросс-корреляцию последовательностей $C_{\max}$, доказанная в [9].

	M	T	M/T	$C_{\max} \leq$
A_0	$2^{2m} - 1$	$2^m - 1$	$2^m + 1 = T + 2$	$1 + \sqrt{T + 1}$
B_0	$2^{2m} - 2^m$	$2(2^m - 1)$	$2^{m-1} = \frac{T+2}{4}$	$2 + \sqrt{T + 2}$

Таким образом, эти семейства асимптотически оптимальны относительно оценок Сидельникова и Уолша.

Последовательности семейств A_0 и B_0 имеют представление функцией след. Напомним, что функция след из кольца Галуа R' в кольцо R определяется равенством

$$\text{Tr}(a) = \text{Tr}_R^{R'}(a) = \sum_{\varphi \in \text{Aut}(R'/R)} \varphi(a), \quad a \in R'. \quad (6)$$

Каждая последовательность $u \in A_0$ представляется в виде

$$u(i) = \text{Tr}_R^{R'}(c\alpha^i), \quad c \neq 0, \quad \text{где } \alpha = \alpha_0 \in \Gamma(R'),$$

а каждая последовательность $v \in B_0$ — в виде

$$v(i) = \text{Tr}_R^{R'}(c\alpha^i), \quad c \notin 2R', \quad \alpha = \alpha_0(1 + 2\delta),$$

где δ удовлетворяет условиям (5). В [5] построено семейство A последовательностей над кольцом из 8-ми элементов, которое является аналогом семейства A_0 . В данной работе строится семейство B над кольцом из 8-ми элементов, являющееся аналогом семейства B_0 .

Функцию след над кольцом Галуа можно записать в явном виде, используя p -адическое разложение элементов. Если $a \in \Gamma(R')$, то

$$\mathrm{Tr}_R^{R'}(a) = \sum_{r=0}^{m-1} a^{2^r}, \quad a \in \Gamma(R'). \quad (7)$$

Поэтому для произвольного элемента $a \in R'$ с p -адическим разложением $a = a_0 + 2a_1$ справедливо равенство [6]

$$\mathrm{Tr}_R^{R'}(a) = \mathrm{Tr}(a_0) + 2 \mathrm{Tr}(a_1) = \sum_{r=0}^{m-1} (a_0^{2^r} + 2a_1^{2^r}), \quad a \in R'.$$

3. Последовательности над кольцом S из 8 элементов

Пусть $R = \mathbb{Z}_4$. Рассмотрим кольцо $S = R[x]/(x^2, 2x)$, состоящее из 8-ми элементов. Согласно [7], S является наименьшим неквазифробениусовым кольцом. Последовательности над кольцом S , их представление функцией след, ранги координатных последовательностей и частотные характеристики рассматривались в [2–4]. В [5] построено семейство отмеченных последовательностей периода $2^m - 1$ над кольцом S , кросс-корреляционная функция которого асимптотически оптимальна относительно оценок Сидельникова и Уоллаша. В этой работе строится аналогичное семейство последовательностей максимального периода над кольцом S .

Перечислим свойства кольца S , указанные в [2]. Пусть $\theta \in S$ — образ элемента x при естественном эпиморфизме $R[x] \rightarrow S$ с ядром $(x^2, 2x)$. Тогда $\theta^2 = 2\theta = 0$ и

$$S = R[\theta] = \{a + b\theta : a \in R, b \in \{0, 1\}\} = \{0, 1, 2, 3, \theta, 1 + \theta, 2 + \theta, 3 + \theta\}. \quad (8)$$

Кольцо S локально, его максимальный идеал, совпадающий с радикалом, равен

$$J = J(S) = (2, \theta) = \{0, 2, \theta, 2 + \theta\},$$

поле вычетов есть $\bar{S} = S/J(S) = GF(2)$ и $J^2 = 0$. Если $a \in S$, $F(x) \in S[x]$, $u \in S^\infty$ — элемент, многочлен и последовательность над кольцом S , то через

$\bar{a}$, $\bar{F}(x)$, $\bar{u}$ будем обозначать их образы при естественном эпиморфизме $S \rightarrow \bar{S}$. Унитарный многочлен $F(x) \in S[x]$ будем называть *многочленом Галуа* над кольцом S , если многочлен $\bar{F}(x)$ неприводим над полем $\bar{S}$.

Как видно из (8), аддитивная группа $(S, +)$ кольца S есть прямая сумма

$$(S, +) = \langle 1 \rangle \dot{+} \langle \theta \rangle \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2.$$

Соответственно, группа $S^\wedge$ аддитивных характеров кольца S имеет вид

$$(S^\wedge, \cdot) = \langle \chi_1 \rangle \dot{+} \langle \chi_2 \rangle,$$

где характеры $\chi_1, \chi_2: S \rightarrow \mathbb{C}$ определяются равенствами

$$\chi_1(a + b\theta) = \omega^a, \quad \chi_2(a + b\theta) = (-1)^b, \quad \omega = \sqrt{-1}.$$

Здесь $a \in R = \{0, 1, 2, 3\}$, $b \in \{0, 1\}$. Рассмотрим характер $\chi = \chi_1\chi_2$, тогда

$$\chi(a + b\theta) = \omega^a(-1)^b. \quad (9)$$

Легко проверить, что выполняются равенства

$$\chi(a + b\theta) = \chi(a + 2b), \quad \chi(c(a + b\theta)) = \chi(c(a + 2b)), \quad c \in S. \quad (10)$$

Пусть u, v — две последовательности периода T над кольцом S . *Кросс-корреляционную функцию* последовательностей u, v определим равенством

$$C_{u,v}(t) = \sum_{i=0}^{T-1} \chi(u(i) - v(i+t)), \quad t \geq 0.$$

Очевидно, $|C_{u,v}(t)| \leq T$ и $C_{u,u}(0) = T$.

Для произвольного унитарного *реверсивного* (т. е. $F(0) \in S^*$) многочлена $F(x) \in S[x]$ степени m и ЛРП $u \in L_S(F)$ верны оценки $T(u) \leq T(F) \leq \leq 2(2^m - 1)$. Если $T(F) = 2(2^m - 1)$, то многочлен $F(x)$ назовем *многочленом максимального периода над кольцом S* , а ЛРП u ранга m и периода $2(2^m - 1)$ назовем *линейной рекуррентной последовательностью максимального периода* (ЛРП МП) *над кольцом S* . Если $T(\bar{F}) = T(F) = 2^m - 1$, то многочлен $F(x)$ назовем *отмеченным многочленом над кольцом S* .

Если $F(x)$ — отмеченный многочлен, то все ненулевые последовательности из $L_S(F)$ имеют период $2^m - 1$. Пусть $F(x)$ — многочлен максимального периода. Обозначим

$$L_S^*(F) = \{u \in L_S(F) : \bar{u} \neq 0\} = L_S(F) \setminus (2L_S(F) + \theta L_S(F)).$$

Тогда все последовательности из $L_S^*(F)$ имеют период $2(2^m - 1)$, а остальные ненулевые последовательности из $L_S(F)$ — период $2^m - 1$ (см. [2, утверждение 3.13]).

Над кольцом S определим семейства последовательностей, аналогичные семействам A_0, B_0 из [9]. Пусть $F(x) \in S[x]$ — такой многочлен Галуа степени $m \geq 1$, что $\overline{F}(x)$ — многочлен максимального периода над полем $\overline{S}$. Тогда $F(x)$ либо отмеченный многочлен, либо многочлен максимального периода. Если многочлен $F(x)$ отмеченный, то рассмотрим семейство

$$A = L_S(F) \setminus 0.$$

Это семейство состоит из $|S|^m - 1 = 2^{3m} - 1$ последовательностей периода $2^m - 1$ каждая. Если $F(x)$ — многочлен максимального периода, то рассмотрим семейство

$$B = L_S^*(F).$$

Оно состоит из $2^{3m} - 2^{2m}$ последовательностей периода $2(2^m - 1)$.

Многочлен $F(x) \in S[x]$ можно выбрать так, чтобы выполнялось включение $F(x) \in R[x]$. В этом случае семейства A_0, B_0 будут подмножествами в A и B . В общем случае это не так.

В работе [5] изучалось семейство A . В данной работе изучается семейство B . В следующей таблице для сравнения перечислены параметры семейств A_0, B_0, A и B : мощность алфавита $r = |R|$ или $r = |S|$, число последовательностей M , период последовательностей T , число циклов M/T и верхняя оценка кросс-корреляции $C_{\max}$, которая для семейства B будет доказана ниже. Информация о семействах A_0 и B_0 из [9] приведена в таблице для удобства их сравнения с семействами A и B .

	r	M	T	M/T	$C_{\max} \leq$
A_0	4	$2^{2m} - 1$	$2^m - 1$	$2^m + 1$	$1 + \sqrt{T + 1}$
B_0	4	$2^{2m} - 2^m$	$2(2^m - 1)$	2^{m-1}	$2 + \sqrt{T + 2}$
A	8	$2^{3m} - 1$	$2^m - 1$	$2^{2m} + 2^m + 1$	$1 + \sqrt{T + 1}$
B	8	$2^{3m} - 2^{2m}$	$2(2^m - 1)$	2^{2m-1}	$2 + \sqrt{T + 2}$

Из таблицы видно, что семейства A и B асимптотически оптимальны относительно оценок Сидельникова и Уолша. По сравнению с семейством B_0 последовательности из B имеют те же периоды и оценки кросс-корреляции, но число последовательностей в семействе B больше, чем в B_0 . Здесь следует учитывать изменение размера алфавита: последовательности в семействах A_0 и B_0 четверичные, а в семействах A и B — восьмеричные. Именно за счет

этого и происходит существенное увеличение числа последовательностей в семействах A и B .

4. Функция след над кольцом S

Следующие результаты доказаны в [2].

Пусть $R' = GR(4^m, 4)$ — расширение Галуа степени m (см. [6, 10, 11]) кольца Галуа $R = \mathbb{Z}_4 = GR(4, 4)$. Рассмотрим расширение $S' = R'[\theta]$ кольца R' определенным выше элементом $\theta \in S$. Так как θ удовлетворяет условиям $\theta^2 = 2\theta = 0$, то формально S' можно определить как $S' = R'[x]/(x^2, 2x)$, при этом $\theta \in S'$ является образом элемента x при естественном эпиморфизме $R'[x] \rightarrow S'$ с ядром $(x^2, 2x)$. Справедливы включения

$$R \subset S \subset S', \quad R \subset R' \subset S'.$$

Кольцо S' локально, его максимальный идеал, совпадающий с радикалом, равен

$$J' = J(S') = (2, \theta) = \{2a + b\theta : a, b \in R'\}$$

и имеет индекс нильпотентности 2. Порядки и поля вычетов рассматриваемых колец следующие:

$$|R| = 4, \quad |S| = 8, \quad |R'| = 4^m, \quad |S'| = 8^m,$$

$$\bar{R} = R/2R \cong \bar{S} = S/J = GF(2), \quad \bar{R}' = R'/2R' \cong \bar{S}' = S'/J' = GF(2^m).$$

В дальнейшем через $\bar{a}$, $\bar{F}(x)$ и $\bar{u}$ будем обозначать образы элемента $a \in S'$, многочлена $F(x) \in S'[x]$ и последовательности $u \in (S')^\infty$ под действием естественных эпиморфизмов $S' \rightarrow \bar{S}'$, $S'[x] \rightarrow \bar{S}'[x]$ и $(S')^\infty \rightarrow (\bar{S}')^\infty$ соответственно. Элементы кольца S имеют вид

$$S' = \{a + b\theta : a, b \in R'\}, \tag{11}$$

причем $a + b\theta = c + d\theta$, $a, b, c, d \in R'$, тогда и только тогда, когда $a = c$, $\bar{b} = \bar{d}$.

Функция след из кольца S' в S определяется равенством

$$\text{Tr}(a) = \text{Tr}_S^{S'}(a) = \sum_{\varphi \in \text{Aut}(S'/S)} \varphi(a), \quad a \in S'.$$

Аutomорфизмы кольца S' над S , а значит, и функцию след, можно описать явно, для этого требуется ввести 2-адическое разложение для элементов кольца S' .

Множество $\Gamma(S') = \{b \in S' : b^{2^m} = b\}$ назовем *2-адическим координатным множеством кольца S'* . Справедливо равенство $\Gamma(S') = \Gamma(R')$. В частности, при $m = 1$ получаем $\Gamma(S) = \Gamma(R) = \{0, 1\}$.

Каждый элемент $a \in S'$ однозначно представляется в виде

$$a = a_0 + 2a_1 + \theta a_\theta, \quad a_0, a_1, a_\theta \in \Gamma(S'). \quad (12)$$

Элементы a_0, a_1, a_θ назовем *2-адическими координатами элемента a* и будем обозначать следующим образом:

$$a_0 = \gamma_0(a), \quad a_1 = \gamma_1(a), \quad a_\theta = \gamma_\theta(a), \quad a \in S'. \quad (13)$$

Координату a_0 будем называть *нулевой*, или *младшей*, а координаты a_1, a_θ — *первыми*, или *старшими*. Легко увидеть, что алгебра $(\Gamma(S'), \oplus, \cdot)$, где $a \oplus b = \gamma_0(a + b)$, $a, b \in S'$, есть поле, изоморфное полю $\overline{S'} = GF(2^m)$. Изоморфизм $\Gamma(S') \rightarrow \overline{S'}$ задается соотношениями $a \rightarrow \overline{a}$, $a \in \Gamma(S')$. Для произвольного элемента $a \in S'$ выполняется равенство $\gamma_0(a) = a^{2^m}$.

Группа автоморфизмов $\text{Aut}(S'/S)$ кольца S' над S является циклической группой порядка m и порождается автоморфизмом Фробениуса ρ , действующим по правилу

$$\rho(a) = \gamma_0(a)^2 + 2\gamma_1(a)^2 + \theta\gamma_\theta(a)^2.$$

Отсюда, а также из соотношения (7), вытекает следующее явное описание функции след с использованием p -адического разложения элементов кольца S' :

$$\begin{aligned} \text{Tr}_S^{S'}(a) &= \text{Tr}(a_0) + 2\text{Tr}(a_1) + \theta\text{Tr}(a_\theta) = \\ &= \sum_{r=0}^{m-1} \left(a_0^{2^r} + 2a_1^{2^r} + \theta a_\theta^{2^r} \right), \quad a \in S'. \end{aligned} \quad (14)$$

Отображение $\text{Tr}_S^{S'}$ является сюръективным отображением множества S' на S , линейным над S , и его ограничение на множество R' совпадает с функцией след $\text{Tr}_R^{R'}$.

Опишем представление последовательностей семейств A и B с помощью функции след.

Пусть $F(x) \in S[x]$ — реверсивный многочлен Галуа степени m . В кольце S' многочлен $F(x)$ имеет корень α , и все его корни в S' есть $\alpha, \rho(\alpha), \dots$,

$\rho^{m-1}(\alpha)$. Если к тому же $T(\overline{F}) = 2^m - 1$, то многочлен $F(x)$ является отмеченным тогда и только тогда, когда $\alpha = \gamma_0(\alpha)$, т. е. $\alpha \in \Gamma(S')$. В противном случае, т. е. при $\alpha \neq \gamma_0(\alpha)$, $F(x)$ есть многочлен максимального периода.

Для любой ЛРП $u \in L_S(F)$ существует единственный элемент $c \in S'$, удовлетворяющий условию

$$u(i) = \text{Tr}_S^{S'}(c\alpha^i), \quad i \geq 0. \quad (15)$$

В частности, такое представление имеют последовательности семейств A и B , причем включения $u \in A$, $u \in B$ равносильны условиям $c \neq 0$ и $\overline{c} \neq 0$ соответственно.

Как известно, функция след $\text{tr} = \text{tr}_q^{q^m}$ над полем удовлетворяет соотношениям ортогональности

$$\sum_{x \in GF(q^m)} (-1)^{\text{tr}(x)} = 0, \quad \sum_{x \in GF(q^m)^*} (-1)^{\text{tr}(x)} = -1. \quad (16)$$

Аналогичные соотношения для функции след над кольцом Галуа приведены в [9, с. 1104]. Следующие соотношения ортогональности для функции след над кольцом S доказаны в [5].

Лемма 1. Пусть $\text{Tr} = \text{Tr}_S^{S'}$ и χ — характер кольца S , определенный в (9). Тогда:

- (а) $\sum_{x \in S'} \chi(\text{Tr}(x)) = 0$;
- (б) $\sum_{x \in J(S')} \chi(\text{Tr}(x)) = 0$;
- (в) $\sum_{x \in (S')^*} \chi(\text{Tr}(x)) = 0$;
- (г) $\sum_{x \in (R')^*} \chi(\text{Tr}(cx)) = 0$ для любого $c \in (S')^*$.

5. Вычисление тригонометрической суммы для семейства B

В [9] для кольца $\mathbb{Z}_4$ и затем в [5] для кольца S исследование кросс-корреляционной функции семейства A сводилось к изучению тригонометрической суммы над кольцом S вида

$$\zeta(\gamma) = \sum_{x \in \Gamma(S')^*} \chi(\text{Tr}(\gamma x)), \quad \gamma \in S', \quad (17)$$

где $\chi: S \rightarrow \mathbb{C}$ — характер, определенный в (9), и $\text{Tr} = \text{Tr}_{S'}^{S'}$. В этом параграфе рассматривается аналогичная тригонометрическая сумма $\eta(\gamma)$ для семейства B .

Пусть $F(x) \in S[x]$ — многочлен максимального периода степени m , $\alpha \in S'$ — его корень, являющийся элементом порядка $2(2^m - 1)$. Напомним, что семейство $B = L_S^*(F)$ состоит из $2^{3m} - 2^{2m}$ последовательностей периода $T = 2(2^m - 1)$.

Пусть $u, u' \in B$ — две последовательности, представление которых функцией след задается соотношениями

$$u(i) = \text{Tr}(c\alpha^i), \quad u'(i) = \text{Tr}(c'\alpha^i), \quad i \geq 0, \quad (18)$$

где $c, c' \in (S')^*$. Тогда

$$C_{u,u'}(t) = \sum_{i=0}^{T-1} \chi(\text{Tr}(c\alpha^i) - \text{Tr}(c'\alpha^{i+t})) = \sum_{i=0}^{2(2^m-1)-1} \chi(\text{Tr}((c - c'\alpha^t)\alpha^i)).$$

Обозначим

$$\gamma = c - c'\alpha^t \quad (19)$$

и разобьем сумму на две — по четным и по нечетным i :

$$C_{u,u'}(t) = \sum_{i=0}^{2^m-1} \chi(\text{Tr}(\gamma\alpha^{2i})) + \sum_{i=0}^{2^m-1} \chi(\text{Tr}(\alpha\gamma\alpha^{2i})).$$

Так как $F(x)$ — многочлен максимального периода, то α^{2i} пробегает множество $\Gamma(S')^*$. Поэтому, согласно (17),

$$C_{u,u'}(t) = \eta(\gamma), \quad \text{где} \quad \eta(\gamma) = \zeta(\gamma) + \zeta(\alpha\gamma). \quad (20)$$

Следовательно, для нахождения значений кросс-корреляционной функции последовательностей из B , как и в [9], достаточно найти значения суммы $\eta(\gamma)$.

При вычислении суммы $\eta(\gamma)$ будет использоваться следующее утверждение.

Лемма 2 ([9], с. 1109). Пусть $\alpha \in (R')^*$ — элемент порядка $2(2^m - 1)$ вида $\alpha = \alpha_0 + 2\alpha_1 = \alpha_0(1 + 2\delta)$, где $\delta = \alpha_0^{-1}\alpha_1$, причем $\bar{\delta} \neq 0, 1$. Тогда в совокупности смежных классов

$$(1 - \alpha^{2s+1})\Gamma(R')^*, \quad 0 \leq s \leq 2^m - 2, \quad s \neq 2^{m-1} - 1, \quad (21)$$

группы $(R')^*$ по подгруппе $\Gamma(R')^*$ классы

$$(1 + 2z)\Gamma(R')^*, \quad z \in R', \quad z \notin \{0, 1 + \delta\}, \quad \text{tr}(\bar{z}\bar{\delta}) = 0,$$

встречаются по два раза, классы

$$(1 + 2z)\Gamma(R')^*, \quad z \in R', \quad z \notin \{0, 1 + \delta\}, \quad \text{tr}(\bar{z}\bar{\delta}) = 1,$$

не встречаются, классы $\Gamma(R')^*$ и $-\alpha\Gamma(R')^*$ (получающиеся при $z = 0$, $z = 1 + \delta$, в обоих случаях $\text{tr}(\bar{z}\bar{\delta}) = 0$) встречаются по одному разу.

Если $\text{tr}(\bar{\delta}) = 1$, то класс вида $c\Gamma(R')^*$ появляется среди классов (21) тогда и только тогда, когда класс $-c\Gamma(R')^*$ не появляется.

Рассмотрим 2-адическое представление (12) корня $\alpha \in S'$ многочлена $F(x)$

$$\alpha = \alpha_0 + 2\alpha_1 + \theta\alpha_\theta, \quad \alpha_0, \alpha_1, \alpha_\theta \in \Gamma(S'), \quad (22)$$

и обозначим

$$\hat{\delta} = \bar{\alpha}_0^{-1}(\bar{\alpha}_1 + \bar{\alpha}_\theta) \in \bar{R}'.$$

Теорема 1. Если $\hat{\delta} \neq 0, 1$ и $\text{tr}(\hat{\delta}) = 1$, то для любого $\gamma \in (S')^*$

$$|2 + \eta(\gamma)|^2 = 2^{m+1}.$$

Доказательство. Как и в [9, с. 1110], рассмотрим величину

$$\zeta(\gamma)\bar{\zeta}(\alpha\gamma) = \sum_{x,y \in \Gamma(S')^*} \chi(\text{Tr}(\gamma x - \alpha\gamma y)) = \sum_{x,y \in \Gamma(S')^*} \chi\left(\text{Tr}\left(\gamma x \left(1 - \alpha \cdot \frac{y}{x}\right)\right)\right).$$

Если $x \in \Gamma(S')^*$ фиксирован и y пробегает $\Gamma(S')^*$, то дробь $z = \frac{y}{x}$ пробегает $\Gamma(S')^*$. Следовательно,

$$\zeta(\gamma)\bar{\zeta}(\alpha\gamma) = \sum_{x,z \in \Gamma(S')^*} \chi(\text{Tr}(\gamma x (1 - \alpha z))). \quad (23)$$

В сумме (23) выделим слагаемые, соответствующие $z = \alpha_0^{-1}$; сумма этих слагаемых равна

$$\sum_{x \in \Gamma(S')^*} \chi(\text{Tr}(\gamma x (1 - \alpha\alpha_0^{-1}))) = \sum_{x \in \Gamma(S')^*} \chi(\text{Tr}(-\gamma x \alpha_0^{-1}(2\alpha_1 + \theta\alpha_\theta))).$$

В силу (9) и (14) эту сумму можно переписать в виде

$$\sum_{x \in \Gamma(S')^*} (-1)^{\text{tr}(\overline{\gamma x} \overline{\alpha_0}^{-1} (\overline{\alpha_1} + \overline{\alpha_\theta}))}.$$

Так как по условию теоремы $\overline{\gamma}(\overline{\alpha_1} + \overline{\alpha_\theta}) \neq 0$, то согласно (16) эта сумма равна -1 . Следовательно, соотношение (23) можно записать в виде

$$\zeta(\gamma) \overline{\zeta}(\alpha\gamma) = -1 + \sum_{x \in \Gamma(S')^*} \sum_{z \in \Gamma(S')^* \setminus \{\alpha_0^{-1}\}} \chi(\text{Tr}(\gamma x(1 - \alpha z))).$$

Вместо элемента $\alpha = \alpha_0 + 2\alpha_1 + \theta\alpha_\theta \in (S')^*$ рассмотрим элемент

$$\hat{\alpha} = \alpha_0 + 2(\alpha_1 + \alpha_\theta) \in (R')^*.$$

Отметим, что $\alpha_0 = \hat{\alpha}_0$. В силу (9) и (14) $\text{Tr}(\theta z) = \text{Tr}(2z)$. Поэтому

$$\chi(\text{Tr}(\gamma x(1 - \alpha z))) = \chi(\text{Tr}(\gamma x(1 - \hat{\alpha} z))).$$

Следовательно,

$$\begin{aligned} \zeta(\gamma) \overline{\zeta}(\alpha\gamma) &= -1 + \sum_{x \in \Gamma(R')^*} \sum_{z \in \Gamma(R')^* \setminus \{\hat{\alpha}_0^{-1}\}} \chi(\text{Tr}(\gamma x(1 - \hat{\alpha} z))) = \\ &= -1 + \sum_{z \in \Gamma(R')^* \setminus \{\hat{\alpha}_0^{-1}\}} \sum_{x \in (1 - \hat{\alpha} z) \Gamma(R')^*} \chi(\text{Tr}(\gamma x)). \end{aligned}$$

Так как по условию теоремы $\overline{\alpha_1} + \overline{\alpha_\theta} \neq 0$, то элемент $\hat{\alpha}$ имеет порядок $2(2^m - 1)$. При этом $\hat{\alpha}^2 = \alpha_0^2$, поэтому группа $\Gamma(R')^*$ порождается элементом $\hat{\alpha}^2$. Следовательно, каждый элемент $z \in \Gamma(R')^*$ однозначно представляется в виде $z = \hat{\alpha}^{2s}$, $0 \leq s \leq 2^m - 2$. Если $s = 2^{m-1} - 1$, то $\alpha_0 z = \alpha_0 \hat{\alpha}^{2s} = \alpha_0^{2^{s+1}} = \alpha_0^{2^{m-1}} = 1$, т. е. $z = \alpha_0^{2s} = \alpha_0^{-1}$. Отсюда

$$\zeta(\gamma) \overline{\zeta}(\alpha\gamma) = -1 + \sum_{\substack{s=0 \\ s \neq 2^{m-1}-1}}^{2^m-2} \sum_{x \in (1 - \hat{\alpha}^{2s+1}) \Gamma(R')^*} \chi(\text{Tr}(\gamma x)).$$

Заметим, что суммирование происходит по всем смежным классам, перечисленным в (21). Применяя лемму 2, условия которой выполнены в силу условий доказываемой теоремы, получим

$$\zeta(\gamma) \overline{\zeta}(\alpha\gamma) = -1 + 2 \sum_{\substack{z \in \Gamma(R')^* \\ \text{tr}(\overline{z}\hat{\alpha})=0}} \sum_{x \in (1+2z) \Gamma(R')^*} \chi(\text{Tr}(\gamma x)) - \sum_{x \in \Gamma(R')^* \cup (-\hat{\alpha} \Gamma(R')^*)} \chi(\text{Tr}(\gamma x)).$$

Как отмечалось выше, $\chi(\text{Tr}(\gamma\hat{\alpha}x)) = \chi(\text{Tr}(\gamma\alpha x))$, поэтому по определению (17) последняя сумма равна $\zeta(\gamma) + \zeta(-\alpha\gamma) = \zeta(\gamma) + \bar{\zeta}(\alpha\gamma)$. В итоге

$$\zeta(\gamma)\bar{\zeta}(\alpha\gamma) = -1 - \zeta(\gamma) - \bar{\zeta}(\alpha\gamma) + 2 \sum_{\substack{z \in \Gamma(R') \\ \text{tr}(\bar{z}\hat{\delta})=0}} \sum_{x \in (1+2z)\Gamma(R')^*} \chi(\text{Tr}(\gamma x)). \quad (24)$$

Теперь рассмотрим сопряженную величину $\bar{\zeta}(\gamma)\zeta(\alpha\gamma)$. Для нее верно равенство

$$\bar{\zeta}(\gamma)\zeta(\alpha\gamma) = -1 - \bar{\zeta}(\gamma) - \zeta(\alpha\gamma) + 2 \sum_{\substack{z \in \Gamma(R') \\ \text{tr}(\bar{z}\hat{\delta})=0}} \sum_{x \in -(1+2z)\Gamma(R')^*} \chi(\text{Tr}(\gamma x)).$$

Так как $-(1+2z) = 1+2(z+1)$, то области суммирования по z, x в последней сумме можно записать следующим образом:

$$x \in (1+2(z+1))\Gamma(R')^*, \quad \text{где } z \in \Gamma(R'), \quad \text{tr}(\bar{z}\hat{\delta}) = 0.$$

Заменим z на $\gamma_0(z+1)$. Тогда z снова пробегает $\Gamma(R')$. Получим

$$x \in (1+2z)\Gamma(R')^*, \quad \text{где } z \in \Gamma(R'), \quad \text{tr}((\bar{z}+1)\hat{\delta}) = 0.$$

Так как по условию $\text{tr}(\hat{\delta}) = 1$, то последнее условие равносильно следующему:

$$x \in (1+2z)\Gamma(R')^*, \quad \text{где } z \in \Gamma(R'), \quad \text{tr}(\bar{z}\hat{\delta}) = 1.$$

Таким образом,

$$\bar{\zeta}(\gamma)\zeta(\alpha\gamma) = -1 - \bar{\zeta}(\gamma) - \zeta(\alpha\gamma) + 2 \sum_{\substack{z \in \Gamma(R') \\ \text{tr}(\bar{z}\hat{\delta})=1}} \sum_{x \in (1+2z)\Gamma(R')^*} \chi(\text{Tr}(\gamma x)).$$

Складывая с (24), получим

$$\begin{aligned} \zeta(\gamma)\bar{\zeta}(\alpha\gamma) + \bar{\zeta}(\gamma)\zeta(\alpha\gamma) &= -2 - \zeta(\gamma) - \bar{\zeta}(\alpha\gamma) - \bar{\zeta}(\gamma) - \zeta(\alpha\gamma) + \\ &+ 2 \sum_{z \in \Gamma(R')} \sum_{x \in (1+2z)\Gamma(R')^*} \chi(\text{Tr}(\gamma x)). \end{aligned}$$

Так как множество $\{1+2z: z \in \Gamma(R')\}$ является полной системой представителей группы $(R')^*$ по подгруппе $\Gamma(R')^*$, то последняя сумма равна $\sum_{x \in (R')^*} \chi(\text{Tr}(\gamma x))$. Эта сумма равна нулю по лемме 1(г), значит,

$$\zeta(\gamma)\bar{\zeta}(\alpha\gamma) + \bar{\zeta}(\gamma)\zeta(\alpha\gamma) = -2 - \zeta(\gamma) - \bar{\zeta}(\alpha\gamma) - \bar{\zeta}(\gamma) - \zeta(\alpha\gamma).$$

Пользуясь полученным соотношением, находим

$$\begin{aligned}
 |2 + \eta(\gamma)|^2 &= |2 + \zeta(\gamma) + \zeta(\alpha\gamma)|^2 = \\
 &= (2 + \zeta(\gamma) + \zeta(\alpha\gamma))(2 + \bar{\zeta}(\gamma) + \bar{\zeta}(\alpha\gamma)) = \\
 &= 4 + 2\zeta(\gamma) + 2\zeta(\alpha\gamma) + 2\bar{\zeta}(\gamma) + 2\bar{\zeta}(\alpha\gamma) + \\
 &\quad + \zeta(\gamma)\bar{\zeta}(\gamma) + \zeta(\gamma)\bar{\zeta}(\alpha\gamma) + \zeta(\alpha\gamma)\bar{\zeta}(\gamma) + \zeta(\alpha\gamma)\bar{\zeta}(\alpha\gamma) = \\
 &= 2 + \zeta(\gamma) + \zeta(\alpha\gamma) + \bar{\zeta}(\gamma) + \bar{\zeta}(\alpha\gamma) + \zeta(\gamma)\bar{\zeta}(\gamma) + \zeta(\alpha\gamma)\bar{\zeta}(\alpha\gamma) = \\
 &= (\zeta(\gamma) + 1)(\bar{\zeta}(\gamma) + 1) + (\zeta(\alpha\gamma) + 1)(\bar{\zeta}(\alpha\gamma) + 1) = \\
 &= |\zeta(\gamma) + 1|^2 + |\zeta(\alpha\gamma) + 1|^2.
 \end{aligned}$$

Так как $|\zeta(\gamma) + 1|^2 = 2^m$ согласно утверждению 2 из [5], то

$$|2 + \eta(\gamma)|^2 = 2^{m+1},$$

что и требовалось доказать. $\square$

Как видно из последних выкладок, равенство теоремы 1 равносильно тому, что для чисел $z_1 = 1 + \zeta(\gamma)$ и $z_2 = 1 + \zeta(\alpha\gamma)$ выполняется соотношение $|z_1 + z_2|^2 = |z_1|^2 + |z_2|^2$, т.е. числа z_1 и z_2 , изображенные как векторы на комплексной плоскости, ортогональны. Это отмечалось в [9, с. 1110].

Теперь несложно описать значения, принимаемые тригонометрической суммой $\eta(\gamma)$. При этом будет использоваться следующее описание значений тригонометрической суммы $\zeta(\gamma)$, полученное в [5, теорема 3]:

$$\zeta(\gamma) = \begin{cases} 2^m - 1, & \text{если } \gamma_0 = 0, \gamma_1 = \gamma_\theta, \\ -1, & \text{если } \gamma_0 = 0, \gamma_1 \neq \gamma_\theta, \\ -1 \pm 2^s \pm \omega 2^s, & \text{если } \gamma_0 \neq 0, m = 2s + 1 \text{ нечетно,} \\ -1 \pm 2^s, -1 \pm \omega 2^s, & \text{если } \gamma_0 \neq 0, m = 2s \text{ четно.} \end{cases} \quad (25)$$

Теорема 2. Пусть элемент $\gamma \in S'$ имеет p -адическое разложение $\gamma = \gamma_0 + 2\gamma_1 + \theta\gamma_\theta$ и выполнены условия теоремы 1. Тогда функция $\eta(\gamma) = \zeta(\gamma) + \zeta(\alpha\gamma)$ принимает следующие значения:

$$\eta(\gamma) = \begin{cases} 2(2^m - 1), & \text{если } \gamma_0 = 0, \gamma_1 = \gamma_\theta, \\ -2, & \text{если } \gamma_0 = 0, \gamma_1 \neq \gamma_\theta, \\ -2 \pm 2^{s+1}, -2 \pm \omega 2^{s+1}, & \text{если } \gamma_0 \neq 0, m = 2s + 1 \text{ нечетно,} \\ -2 \pm 2^s \pm \omega 2^s, & \text{если } \gamma_0 \neq 0, m = 2s \text{ четно.} \end{cases}$$

Доказательство. Пусть $\gamma_0 = 0$. Тогда $\gamma = 2\gamma_1 + \theta\gamma_\theta$ и $\alpha\gamma = 2\alpha_0\gamma_1 + \theta\alpha_0\gamma_\theta$. Из (25) следует, что

$$\zeta(\gamma) = \zeta(\alpha\gamma) = \begin{cases} 2^m - 1, & \text{если } \gamma_0 = 0, \gamma_1 = \gamma_\theta, \\ -1, & \text{если } \gamma_0 = 0, \gamma_1 \neq \gamma_\theta. \end{cases}$$

Отсюда следует доказываемые соотношения в случае $\gamma_0 = 0$.

Пусть теперь $\gamma_0 \neq 0$. По теореме 1 имеем $|2 + \eta(\gamma)|^2 = 2^{m+1}$. Пусть $2 + \eta(\gamma) = a + b\omega$, где $a, b \in \mathbb{Z}$, $\omega = \sqrt{-1}$. Как отмечено без доказательства в [9, Proposition 1] или с доказательством в [5, теорема 3] (в доказательстве m нужно заменить на $m+1$), уравнение $|a + b\omega|^2 = 2^{m+1}$ имеет решения $(a, b) = (\pm 2^s, \pm 2^s)$, если $m+1 = 2s+1$ нечетно, и $(a, b) = (\pm 2^s, 0)$ или $(0, \pm 2^s)$, если $m+1 = 2s$ четно. Пользуясь этим, получим требуемые соотношения. $\square$

Таким образом, сумма $\eta(\gamma)$ принимает 6 различных значений. Теперь подсчитаем кратности, с которыми принимаются эти значения при всевозможных $\gamma \in S'$. Напомним, что кратность значения $z \in \mathbb{C}$ функции η определяется как

$$N_\eta(z) = |\eta^{-1}(z)| = |\{\gamma \in S' : \eta(\gamma) = z\}|.$$

Распределением значений функции $\eta(\gamma)$ называется набор всех пар $(z, N_\eta(z))$, $z \in \eta(S')$.

Теорема 3. Пусть $\alpha = \alpha_0 + 2\alpha_1 + \theta\alpha_\theta \in (S')^*$. Обозначим $\widehat{\delta} = \overline{\alpha}_0^{-1}(\overline{\alpha}_1 + \overline{\alpha}_\theta)$ и предположим, что $\widehat{\delta} \neq 0, 1$ и $\text{tr}(\widehat{\delta}) = 1$. Тогда функция $\eta = \eta(\gamma) : S' \rightarrow \mathbb{C}$, определяемая равенством $\eta(\gamma) = \zeta(\gamma) + \zeta(\alpha\gamma)$, имеет следующее распределение значений при $\gamma \in S'$. Если $\gamma \notin (S')^*$, то

$$\eta(\gamma) = \begin{cases} 2(2^m - 1) & (2^m \text{ раз}), \\ -2 & ((2^m - 1)2^m \text{ раз}). \end{cases} \quad (26)$$

Если $\gamma \in (S')^*$, то при нечетном $m = 2s + 1$

$$\eta(\gamma) = \begin{cases} -2 + 2^{s+1} & ((2^m - 1)(2^{4s} + 2^{3s+1}) \text{ раз}), \\ -2 - 2^{s+1} & ((2^m - 1)(2^{4s} - 2^{3s+1}) \text{ раз}), \\ -2 \pm \omega 2^{s+1} & ((2^m - 1) \cdot 2^{4s} \text{ раз}), \end{cases} \quad (27)$$

а при четном $m = 2s$

$$\eta(\gamma) = \begin{cases} -2 + 2^s \pm \omega 2^s & ((2^m - 1)(2^{4s-2} + 2^{3s-1}) \text{ раз}), \\ -2 - 2^s \pm \omega 2^s & ((2^m - 1)(2^{4s-2} - 2^{3s-1}) \text{ раз}). \end{cases} \quad (28)$$

Доказательство. Пусть $\gamma = \gamma_0 + 2\gamma_1 + \theta\gamma_\theta \in S'$. Если $\gamma \notin (S')^*$, то согласно (25)

$$\zeta(\gamma) = \begin{cases} 2^m - 1 & (2^m \text{ раз}), \\ -1 & (2^{2m} - 2^m \text{ раз}). \end{cases}$$

Так как

$$\alpha\gamma = (\alpha_0 + 2\alpha_1 + \theta\alpha_\theta)(2\gamma_1 + \theta\gamma_\theta) = 2\alpha_0\gamma_1 + \theta\alpha_0\gamma_\theta,$$

то $\zeta(\gamma) = \zeta(\alpha\gamma)$ и $\eta(\gamma) = 2\zeta(\gamma)$. Отсюда вытекает соотношение (26).

Пусть теперь $\gamma \in (S')^*$. Тогда $\eta(\gamma)$ принимает значения, перечисленные в теореме 2, и эти же значения указаны в (27), (28). Подсчитаем их кратности.

Пусть H — произвольная полная система представителей смежных классов группы $(S')^*$ по подгруппе $\Gamma(S')^*$. Множество H состоит из 2^{2m} элементов. Как и в доказательстве теоремы 4 из [5], будем считать выполненным условие

$$\gamma \in H \Rightarrow -\gamma \in H. \quad (29)$$

Ввиду определения (17) для всех γ , принадлежащих одному смежному классу группы $(S')^*$ по подгруппе $\Gamma(S')^*$, значения $\zeta(\gamma)$ одинаковы. Это же верно и для значений $\zeta(\alpha\gamma)$, а следовательно, и для значений $\eta(\gamma)$. Поэтому кратности значений функции $\eta(\gamma)$, $\gamma \in (S')^*$, равны кратностям значений функции $\eta(\gamma)$, $\gamma \in H$, умноженным на $|\Gamma(S')^*| = 2^m - 1$.

Обозначим последние кратности через M , N , P . А именно, если $m = 2s + 1$ нечетно, то положим

$$\begin{aligned} M &= |\{\gamma \in H : \eta(\gamma) = -2 + 2^{s+1}\}|, \\ N &= |\{\gamma \in H : \eta(\gamma) = -2 - 2^{s+1}\}|, \\ P &= |\{\gamma \in H : \eta(\gamma) = -2 + \omega 2^{s+1}\}|. \end{aligned}$$

Ввиду (17) $\zeta(-\gamma) = \bar{\zeta}(\gamma)$, а так как H удовлетворяет условию (29), то

$$P = |\{\gamma \in H : \eta(\gamma) = -2 - \omega 2^{s+1}\}|.$$

Если же $m = 2s$ четно, то положим

$$\begin{aligned} M &= |\{\gamma \in H : \eta(\gamma) = -2 + 2^s + \omega 2^s\}| = |\{\gamma \in H : \eta(\gamma) = -2 + 2^s - \omega 2^s\}|, \\ N &= |\{\gamma \in H : \eta(\gamma) = -2 - 2^s + \omega 2^s\}| = |\{\gamma \in H : \eta(\gamma) = -2 - 2^s - \omega 2^s\}|. \end{aligned}$$

Пусть $m = 2s$. Тогда $2(M+N) = |H| = 2^{2m} = 2^{4s}$. Применяя лемму 1(в), получим:

$$\sum_{\gamma \in H} \zeta(\gamma) = \sum_{\gamma \in H} \sum_{x \in \Gamma(S')^*} \chi(\text{Tr}(\gamma x)) = \sum_{y \in (S')^*} \chi(\text{Tr}(y)) = 0.$$

Отсюда

$$\sum_{\gamma \in H} \eta(\gamma) = \sum_{\gamma \in H} \zeta(\gamma) + \sum_{\gamma \in H} \zeta(\alpha\gamma) = 0 + 0 = 0. \quad (30)$$

Эту же сумму можно разбить на четыре суммы. Тогда из определений M и N следует, что

$$M(-2+2^s+\omega 2^s) + M(-2+2^s-\omega 2^s) + N(-2-2^s+\omega 2^s) + N(-2-2^s-\omega 2^s) = 0,$$

или, после сокращений, $2(M+N) = 2^s(M-N)$. Решением системы из двух уравнений

$$\begin{cases} 2(M+N) = 2^{4s}, \\ 2(M+N) = 2^s(M-N) \end{cases}$$

является $M = 2^{4s-2} + 2^{3s-1}$, $N = 2^{4s-2} - 2^{3s-1}$. Это кратности значений функции $\eta(\gamma)$ при $\gamma \in H$. Умножая их на $2^m - 1$, получим соотношение (28).

Рассмотрим теперь случай $m = 2s + 1$. Тогда $M + N + 2P = |H| = 2^{2m} = 2^{4s+2}$. Сумма (30) по-прежнему равна нулю, откуда

$$M(-2+2^{s+1}) + N(-2-2^{s+1}) + P(-2+\omega 2^{s+1}) + P(-2-\omega 2^{s+1}) = 0$$

или $M + N + 2P = 2^s(M - N)$. Чтобы найти третье уравнение, связывающее M , N и P , аналогично [9] вычислим «второй момент»

$$\begin{aligned} \hat{m}_2 &= \sum_{\gamma \in H} \eta(\gamma)^2 = \sum_{\gamma \in H} (\zeta(\gamma) + \zeta(\alpha\gamma))^2 = \\ &= \sum_{\gamma \in H} (\zeta^2(\gamma) + 2\zeta(\gamma)\zeta(\alpha\gamma) + \zeta^2(\alpha\gamma)) = 2(-2^{2m}) + 2 \sum_{\gamma \in H} \zeta(\gamma)\zeta(\alpha\gamma), \end{aligned} \quad (31)$$

где в последнем равенстве использовано значение второго момента $m_2 = -2^{2m}$ функции ζ , найденное в доказательстве теоремы 4 из [5]. Аналогично (23)

$$\zeta(\gamma)\zeta(\alpha\gamma) = \sum_{x, z \in \Gamma(S')^*} \chi(\text{Tr}(\gamma x(1 + \alpha z))). \quad (32)$$

Так же, как в доказательстве теоремы 1, выделим здесь слагаемые, соответствующие $z = \alpha_0^{-1}$:

$$\sum_{x \in \Gamma(S')^*} \chi(\text{Tr}(\gamma x(1 + \alpha \alpha_0^{-1}))) = \sum_{x \in \Gamma(S')^*} \chi(\text{Tr}(\gamma x(2 + \alpha_0^{-1}(2\alpha_1 + \theta \alpha_\theta)))).$$

В силу (9) и (14) эта сумма равна

$$\sum_{x \in \Gamma(S')^*} (-1)^{\text{tr}(\overline{\gamma x}(1 + \overline{\alpha_0}^{-1}(\overline{\alpha_1} + \overline{\alpha_\theta})))} = \sum_{x \in \Gamma(S')^*} (-1)^{\text{tr}(\overline{\gamma x}(1 + \widehat{\delta}))},$$

так как по условию теоремы $1 + \widehat{\delta} \neq 0$, то она равна -1 ввиду (16). Следовательно, соотношение (32) можно записать в виде

$$\zeta(\gamma)\zeta(\alpha\gamma) = -1 + \sum_{x \in \Gamma(S')^*} \sum_{z \in \Gamma(S')^* \setminus \{\alpha_0^{-1}\}} \chi(\text{Tr}(\gamma x(1 + \alpha z))).$$

Подставим это равенство в выражение (31) для второго момента:

$$\begin{aligned} \widehat{m}_2 &= 2(-2^{2m}) - 2|H| + 2 \sum_{\gamma \in H} \sum_{x \in \Gamma(S')^*} \sum_{z \in \Gamma(S')^* \setminus \{\alpha_0^{-1}\}} \chi(\text{Tr}(\gamma x(1 + \alpha z))) = \\ &= -2^{2m+1} - 2^{2m+1} + 2 \sum_{x \in (S')^*} \sum_{z \in \Gamma(S')^* \setminus \{\alpha_0^{-1}\}} \chi(\text{Tr}(x(1 + \alpha z))). \end{aligned}$$

При $z \neq \alpha_0^{-1}$ элемент $c = 1 + \alpha z$ обратим, поэтому по лемме 1(г) последняя сумма равна нулю, значит,

$$\widehat{m}_2 = -2^{2m+2} = -2^{4s+4}.$$

С другой стороны, сумму $\widehat{m}_2$ можно разбить на 4 суммы согласно определению M и N :

$$\begin{aligned} \widehat{m}_2 &= M(-2 + 2^{s+1})^2 + N(-2 - 2^{s+1})^2 + \\ &\quad + P(-2 + \omega 2^{s+1})^2 + P(-2 - \omega 2^{s+1})^2 = -2^{4s+4}. \end{aligned}$$

После сокращений, с учетом двух уже имеющихся уравнений относительно M и N , получим равенство $M + N - 2P = 0$. Решая систему из трех уравнений

$$\begin{cases} M + N + 2P = 2^{4s+2}, \\ M + N + 2P = 2^s(M - N), \\ M + N - 2P = 0, \end{cases}$$

находим, что $M = 2^{4s} + 2^{3s+1}$, $N = 2^{4s} - 2^{3s+1}$, $P = 2^{4s}$. Это кратности значений функции $\eta(\gamma)$ при $\gamma \in H$. Умножая их на $2^m - 1$, получим кратности значений функции $\eta(\gamma)$ при $\gamma \in (S')^*$, т. е. требуемые соотношения (27). $\square$

В ходе доказательства теоремы был получен следующий результат.

Следствие. Пусть H — произвольная полная система представителей смежных классов группы $(S')^*$ по подгруппе $\Gamma(S')^*$, удовлетворяющая условию (29):

$$\gamma \in H \Rightarrow -\gamma \in H.$$

Тогда функция $\eta(\gamma)$ при $\gamma \in H$ имеет следующее распределение значений: при нечетном $m = 2s + 1$

$$\eta(\gamma) = \begin{cases} -2 + 2^{s+1} & (2^{4s} + 2^{3s+1} \text{ раз}), \\ -2 - 2^{s+1} & (2^{4s} - 2^{3s+1} \text{ раз}), \\ -2 \pm \omega 2^{s+1} & (2^{4s} \text{ раз}), \end{cases}$$

при четном $m = 2s$

$$\eta(\gamma) = \begin{cases} -2 + 2^s \pm \omega 2^s & (2^{4s-2} + 2^{3s-1} \text{ раз}), \\ -2 - 2^s \pm \omega 2^s & (2^{4s-2} - 2^{3s-1} \text{ раз}). \end{cases}$$

6. Кросс-корреляционная функция семейства B

Для $z \in \mathbb{C}$ обозначим через $N_B(z)$ кратность, с которым функция $C_{u,v}(t)$ принимает значение z на семействе B :

$$N_B(z) = |\{(u, v, t) : C_{u,v}(t) = z, u, v \in B, 0 \leq t < T\}|, \quad T = 2(2^m - 1).$$

Набор пар $(z, N_B(z))$, где числа $z \in \mathbb{C}$ берутся такими, что $N_B(z) > 0$, называется распределением значений кросс-корреляционной функции семейства B , а число $N_B(z)$ — кратностью значения z .

Пользуясь найденными в теореме 3 кратностями значений $N_\eta(z)$ функции $\eta(\gamma)$ и соотношениями (20), найдем кратности значений $N_B(z)$ кросс-корреляционной функции $C_{u,v}(t)$ для последовательностей $u, v \in B$.

Теорема 4. Пусть $F(x) \in S[x]$ — многочлен степени $m \geq 1$ максимального периода $T = 2(2^m - 1)$ с корнем $\alpha = \alpha_0 + 2\alpha_1 + \theta\alpha_\theta \in S'$. Обозначим $\hat{\delta} = \bar{\alpha}_0^{-1}(\bar{\alpha}_1 + \bar{\alpha}_\theta)$ и предположим, что $\hat{\delta} \neq 0, 1$ и $\text{tr}(\hat{\delta}) = 1$. Тогда функция кросс-корреляции $C_{u,v}(t)$, $u, v \in B$, $0 \leq t < T$, принимает следующие значения со следующими кратностями:

$$C_{u,v}(t) = \begin{cases} 2(2^m - 1) & ((2^m - 1)^2 \cdot 2^{3m+1} \text{ раз}), \\ -2 & ((2^m - 1)^3 \cdot 2^{3m+1} \text{ раз}). \end{cases} \quad (33)$$

при нечетном $m = 2s + 1$

$$C_{u,v}(t) = \begin{cases} -2 + 2^{s+1} & ((2^m - 1)^2(2^{3m+1} - 2^{2m+2})(2^{4s} + 2^{3s+1}) \text{ раз}), \\ -2 - 2^{s+1} & ((2^m - 1)^2(2^{3m+1} - 2^{2m+2})(2^{4s} - 2^{3s+1}) \text{ раз}), \\ -2 \pm \omega 2^{s+1} & ((2^m - 1)^2(2^{3m+1} - 2^{2m+2}) \cdot 2^{4s} \text{ раз}), \end{cases} \quad (34)$$

при четном $m = 2s$

$$C_{u,v}(t) = \begin{cases} -2 + 2^s \pm \omega 2^s & ((2^m - 1)^2(2^{3m+1} - 2^{2m+2})(2^{4s-2} + 2^{3s-1}) \text{ раз}), \\ -2 - 2^s \pm \omega 2^s & ((2^m - 1)^2(2^{3m+1} - 2^{2m+2})(2^{4s-2} - 2^{3s-1}) \text{ раз}). \end{cases} \quad (35)$$

Доказательство. Пусть последовательности $u, u' \in B$ имеют представления (18) функцией след. Согласно (19), (20) $C_{u,u'}(t) = \eta(\gamma)$, где $\gamma = c - c'\alpha^t$. Обозначим через

$$N_1(\gamma) = |\{(c, c', t) : \gamma = c - c'\alpha^t, c, c' \in (S')^*, 0 \leq t < T\}|$$

число решений уравнения $\gamma = c - c'\alpha^t$. Тогда, очевидно,

$$N_B(z) = \sum_{\gamma \in S', \eta(\gamma)=z} N_1(\gamma).$$

Ниже мы увидим, что $N_1(\gamma)$ не зависит от γ , тогда

$$N_B(z) = N_1(\gamma) \sum_{\gamma \in S', \eta(\gamma)=z} 1 = N_1(\gamma) N_\eta(z), \quad (36)$$

где $N_\eta(z)$ найдено в теореме 3. Найдем величину $N_1(\gamma)$ для фиксированного $\gamma \in S'$.

Пусть $\bar{\gamma} = 0$. Тогда уравнение $c = c'\alpha^t + \gamma$ для любых фиксированных c', t имеет единственное решение $c \in (S')^*$. Поэтому число решений этого уравнения равно числу пар (c', t) :

$$N_1(\gamma) = |(S')^*| \cdot T = 2^{2m}(2^m - 1) \cdot 2(2^m - 1) = (2^m - 1)^2 \cdot 2^{2m+1}.$$

Теперь можно найти $N_B(z)$ для $z \in \{2(2^m - 1), -2\}$. По теореме 3 в этих случаях равенство $\eta(\gamma) = z$ выполняется при $\gamma \notin (S')^*$, т. е. $\bar{\gamma} = 0$. Поэтому

$$N_B(z) = N_1(\gamma) N_\eta(z) = (2^m - 1)^2 \cdot 2^{2m+1} \cdot N_\eta(z).$$

Используя формулу (26) для $N_\eta(z)$, получим соотношения (33).

Пусть $\bar{\gamma} \neq 0$. В этом случае для фиксированных c', t уравнение $c = c'\alpha^t + \gamma$ имеет решение $c \in (S')^*$ тогда и только тогда, когда элемент $c'\alpha^t + \gamma$ обратим, т. е. $\bar{c}' \neq -\bar{\gamma}\bar{\alpha}^t$. Таким образом, для каждого фиксированного t , $0 \leq t < T$, уравнение имеет единственное решение, если $\bar{c}' \neq -\bar{\gamma}\bar{\alpha}^t$, и не имеет решений, если $\bar{c}' = -\bar{\gamma}\bar{\alpha}^t$. Общее число решений уравнения равно числу таких пар (c', t) , что $\bar{c}' \neq -\bar{\gamma}\bar{\alpha}^t$, т. е.

$$\begin{aligned} N_1(\gamma) &= (|(S')^*| - |J(S')|) \cdot T = (2^{2m}(2^m - 1) - 2^{2m}) \cdot 2(2^m - 1) = \\ &= (2^m - 1)(2^{3m+1} - 2^{2m+2}). \end{aligned}$$

Заметим, что, как и в случае $\bar{\gamma} = 0$, значение $N_1(\gamma)$ не зависит от γ . Пользуясь формулой (36) и теоремой 3, получаем соотношения (34) и (35). $\square$

Следствие. Для кросс-корреляционной функции последовательностей из семейства B справедлива оценка

$$C_{\max} \leq 2 + \sqrt{T + 2}.$$

Доказательство. Значение $2(2^m - 1)$ является фазовым и при нахождении $C_{\max}$ не учитывается. Максимальное по модулю среди остальных значений функции $C_{u,v}(t)$ равно $-2 - 2^{s+1}$ при нечетном $m = 2s + 1$ и $-2 - 2^s \pm \omega 2^s$ при четном $m = 2s$. С учетом того, что $T + 2 = 2^{m+1}$, получаем: при $m = 2s + 1$

$$C_{\max} \leq 2 + 2^{s+1} = 2 + \sqrt{2^{2s+2}} = 2 + \sqrt{2^{m+1}} = 2 + \sqrt{T + 2}$$

и при $m = 2s$

$$C_{\max} \leq \sqrt{(-2 - 2^s)^2 + (2^s)^2} = \sqrt{2^{2s+1} + 4 \cdot 2^s + 4} < 2 + \sqrt{2^{2s+1}} = 2 + \sqrt{T + 2}.$$

$\square$

Рассмотрим теперь произвольное семейство $\tilde{B}$, являющееся полным множеством представителей сдвигов последовательностей семейства B . Так как B содержит $2^{3m} - 2^{2m}$ последовательностей периода $T = 2(2^m - 1)$, то множество $\tilde{B}$ содержит $(2^{3m} - 2^{2m})/T = 2^{2m-1}$ последовательностей. Кросс-корреляционная функция последовательностей семейства $\tilde{B}$ принимает те же значения, что и кросс-корреляционная функция последовательностей семейства B . Подсчитаем распределение кратностей этих значений для семейства $\tilde{B}$ и покажем, что это распределение не зависит от выбора представителей в семейство $\tilde{B}$.

Пусть

$\tilde{B} = \{u_1, u_2, \dots, u_{2^{2m-1}}\}$, где $u_n(i) = \text{Tr}(c_n \alpha^i)$, $i \geq 0$, $1 \leq n \leq 2^{2m-1}$,
 $c_n \in (S')^*$. Обозначим

$$\hat{H} = \{c_1, c_2, \dots, c_{2^{2m-1}}\} \subset (S')^*.$$

Рассмотрим произвольную последовательность $u(i) = \text{Tr}(c\alpha^i)$ из семейства B . Все последовательности из B получаются при переборе всех элементов $c \in (S')^*$, так что между последовательностями $u \in B$ и элементами $c \in (S')^*$ имеется взаимно однозначное соответствие. Для фиксированной последовательности $u \in B$ рассмотрим все ее сдвиги $x^t u$ и выясним, какие элементы из $(S')^*$ соответствуют этим сдвигам.

Сдвигу $x^t u$ соответствует элемент $c\alpha^t$, поэтому всем сдвигам последовательности u соответствует множество элементов $\{c\alpha^t : 0 \leq t < T = 2(2^m - 1)\}$. Учитывая, что $\alpha^2 = \alpha_0^2 \in \Gamma(S')^*$, запишем это множество в виде

$$\{c\alpha_0^{2s} : 0 \leq s < 2^m - 1\} \cup \{c\alpha \cdot \alpha_0^{2s} : 0 \leq s < 2^m - 1\}.$$

Так как $\text{ord } \alpha = T$, то $\text{ord } \alpha_0^2 = 2^m - 1$, т. е. α_0^2 — образующий элемент группы $\Gamma(S')^*$. Следовательно, указанное множество есть объединение двух смежных классов $[c] \cup [c\alpha]$ группы $(S')^*$ по подгруппе $\Gamma(S')^*$.

Отсюда следует, что все элементы из $\hat{H} \cup \hat{H}\alpha$ лежат в различных смежных классах группы $(S')^*$ по подгруппе $\Gamma(S')^*$ и составляют полную систему представителей $(S')^*$ по $\Gamma(S')^*$.

Для $z \in \mathbb{C}$ обозначим через $N_{\tilde{B}}(z)$ кратности значений функции $C_{u,v}(t)$ на семействе $\tilde{B}$:

$$N_{\tilde{B}}(z) = |\{(i, j, t) : 1 \leq i, j \leq 2^{2m-1}, 0 \leq t < T, C_{u_i, u_j}(t) = z\}|.$$

Эти кратности найдены в следующей теореме.

Теорема 5. Пусть $F(x) \in S[x]$ — многочлен степени $m \geq 1$ максимального периода $T = 2(2^m - 1)$, удовлетворяющий условиям теоремы 4: $\hat{\delta} \neq 0, 1$ и $\text{tr}(\hat{\delta}) = 1$. Пусть $B = L_S^*(F)$, и пусть $\tilde{B}$ — некоторое полное множество представителей сдвигов последовательностей семейства B . Тогда $\tilde{B}$ состоит из 2^{2m-1} последовательностей периода T , и функция кросс-корреляции $C_{u,v}(t)$, $u, v \in \tilde{B}$, $0 \leq t < T$, принимает следующие значения со следующими кратностями:

$$C_{u,v}(t) = \begin{cases} 2(2^m - 1) & (2^{3m-1} \text{ раз}), \\ -2 & ((2^m - 1) \cdot 2^{3m-1} \text{ раз}); \end{cases} \quad (37)$$

при нечетном $m = 2s + 1$

$$C_{u,v}(t) = \begin{cases} -2 + 2^{s+1} & ((2^{3m-1} - 2^{2m})(2^{4s} + 2^{3s+1}) \text{ раз}), \\ -2 - 2^{s+1} & ((2^{3m-1} - 2^{2m})(2^{4s} - 2^{3s+1}) \text{ раз}), \\ -2 \pm \omega 2^{s+1} & ((2^{3m-1} - 2^{2m}) \cdot 2^{4s} \text{ раз}); \end{cases} \quad (38)$$

при четном $m = 2s$

$$C_{u,v}(t) = \begin{cases} -2 + 2^s \pm \omega 2^s & ((2^{3m-1} - 2^{2m})(2^{4s-2} + 2^{3s-1}) \text{ раз}), \\ -2 - 2^s \pm \omega 2^s & ((2^{3m-1} - 2^{2m})(2^{4s-2} - 2^{3s-1}) \text{ раз}). \end{cases} \quad (39)$$

Доказательство. Согласно (19), (20)

$$C_{u_i, u_j}(t) = \eta(\gamma), \quad \text{где } \gamma = c_i - c_j \alpha^t.$$

Обозначим через

$$N_2(\gamma) = |\{(i, j, t): 1 \leq i, j \leq 2^{2m-1}, 0 \leq t < T, \gamma = c_i - c_j \alpha^t\}|$$

число решений уравнения $\gamma = c_i - c_j \alpha^t$. Тогда, очевидно,

$$N_{\bar{B}}(z) = \sum_{\gamma \in S', \eta(\gamma)=z} N_2(\gamma). \quad (40)$$

Найдем величину $N_2(\gamma)$ для $\gamma \in S'$.

Из определения $\hat{H}$ следует, что элемент $c_j \alpha^t$ при $1 \leq j \leq 2^{2m-1}$, $0 \leq t < T$ пробегает множество $(S')^*$. Поэтому для фиксированного i уравнение $c_j \alpha^t = c_i - \gamma$ имеет одно решение (j, t) , если $c_i - \gamma \in (S')^*$, и 0 решений, если $c_i - \gamma \notin (S')^*$. Следовательно,

$$N_2(\gamma) = |\{i: 1 \leq i \leq 2^{2m-1}, c_i - \gamma \in (S')^*\}|.$$

Отсюда

$$N_2(\gamma) = 2^{2m-1} - |\{c_i \in \hat{H}: \bar{c}_i = \bar{\gamma}\}| = 2^{2m-1} - |\hat{H}(\bar{\gamma})|,$$

где $\hat{H}(\bar{\gamma}) = \{h \in \hat{H}: \bar{h} = \bar{\gamma}\}$.

Найдем $N_{\bar{B}}(z)$ при $z \in \{2(2^m - 1), -2\}$. По теореме 3 в этих случаях из равенства $\eta(\gamma) = z$ получаем, что $\gamma \notin (S')^*$, т.е. $\bar{\gamma} = 0$. Так как $\hat{H} \subset (S')^*$, то множество $\hat{H}(\bar{\gamma})$ пусто и $N_2(\gamma) = 2^{2m-1}$. Поэтому из (40) следует, что

$$N_{\bar{B}}(z) = \sum_{\gamma \in S', \eta(\gamma)=z} 2^{2m-1} = 2^{2m-1} N_{\eta}(z).$$

Значения $N_\eta(z)$ найдены в (26), откуда получаем соотношения (37).

Найдем $N_{\bar{B}}(z)$ при остальных z . В этих случаях $\gamma \in (S')^*$, т. е. $\bar{\gamma} \neq 0$. Тогда

$$N_{\bar{B}}(z) = \sum_{\gamma \in S', \eta(\gamma)=z} (2^{2m-1} - |\hat{H}(\bar{\gamma})|) = 2^{2m-1}N_\eta(z) - \sum_{\gamma \in S', \eta(\gamma)=z} |\hat{H}(\bar{\gamma})|.$$

Значение $N_\eta(z)$ найдено в теореме 3. Преобразуем последнюю сумму:

$$\begin{aligned} \sum_{\gamma \in S', \eta(\gamma)=z} |\hat{H}(\bar{\gamma})| &= \sum_{\gamma \in S', \eta(\gamma)=z} |\{h \in \hat{H} : \bar{h} = \bar{\gamma}\}| = \\ &= |\{(\gamma, h) \in S' \times \hat{H} : \eta(\gamma) = z, \bar{h} = \bar{\gamma}\}| = \sum_{h \in \hat{H}} |\{\gamma \in S' : \eta(\gamma) = z, \bar{\gamma} = \bar{h}\}| = \\ &= \sum_{h \in \hat{H}} |\{\gamma \in h + J(S') : \eta(\gamma) = z\}| = \sum_{h \in \hat{H}} N_{\eta, h+J(S')}(z), \end{aligned}$$

где $N_{\eta, h+J(S')}(z) = |\{\gamma \in h + J(S') : \eta(\gamma) = z\}|$. В итоге

$$N_{\bar{B}}(z) = 2^{2m-1}N_\eta(z) - \sum_{h \in \hat{H}} N_{\eta, h+J(S')}(z).$$

Заметим, что множество $h + J(S')$ (так же, как и $1 + J(S')$) образует полную систему представителей смежных классов группы $(S')^*$ по подгруппе $\Gamma(S')^*$. Действительно, каждый элемент $x \in (S')^*$ однозначно представляется в виде $x = x_0(1 + \Delta)$, где $x_0 = \gamma_0(x) \in \Gamma(S')^*$, $\Delta \in J(S')$, а значит, и в виде $x = x_0 h_0^{-1}(h_0 + h_0 \Delta)$, где $x_0 h_0^{-1} \in \Gamma(S')^*$, $h_0 + h_0 \Delta \in h + J(S')$. При этом множество $h + J(S')$ удовлетворяет условию (29):

$$\gamma \in h + J(S') \Rightarrow -\gamma \in h + J(S').$$

Поэтому величины $N_{\eta, h+J(S')}(z)$ — это кратности, найденные в следствии теоремы 3. В частности, они не зависят от h . Таким образом,

$$N_{\bar{B}}(z) = 2^{2m-1}N_\eta(z) - |\hat{H}| \cdot N_{\eta, h+J(S')}(z) = 2^{2m-1}(N_\eta(z) - N_{\eta, h+J(S')}(z)).$$

Сравнивая формулировки теоремы 3 и ее следствия, находим, что $N_\eta(z)$ в $2^m - 1$ раз больше, чем $N_{\eta, h+J(S')}(z)$. Отсюда

$$N_{\bar{B}}(z) = 2^{2m-1}(2^m - 2)N_{\eta, h+J(S')}(z) = (2^{3m-1} - 2^{2m})N_{\eta, h+J(S')}(z).$$

Пользуясь следствием теоремы 3, получаем соотношения (38), (39). $\square$

Список литературы

1. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Псевдослучайные и полилинейные последовательности. — В сб.: Труды по дискретной математике. Т. 1. — М.: ТВП, 1997, с. 139–202.
2. Нечаев А. А., Кузьмин А. С., Куракин В. Л. Структурные, аналитические и статистические свойства линейных и полилинейных рекуррент. — В сб.: Труды по дискретной математике. Т. 3. — М.: Физматлит, 2000, с. 155–194.
3. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Статистические свойства линейных рекуррент над кольцами Галуа и квазифробениусовыми модулями характеристики 4. — В сб.: Труды по дискретной математике. Т. 4. — М.: Физматлит, 2001, с. 91–128.
4. Нечаев А. А., Кузьмин А. С., Куракин В. Л. Вполне равномерные линейные рекурренты над кольцами Галуа и QF-модулями характеристики 4. — В сб.: Труды по дискретной математике. Т. 5. — М.: Физматлит, 2002, с. 103–158.
5. Куракин В. Л. Семейство последовательностей над кольцом из 8 элементов с низкой корреляцией. — Матем. вопросы криптографии, 2010, т. 1, № 4, с. 85–109.
6. Нечаев А. А. Код Кердока в циклической форме. — Дискретн. матем., т. 1, 1989, № 4, с. 123–139.
7. Нечаев А. А. Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам. — Фунд. и прикл. мат., ЦНИИТ МГУ, т. 1, 1995, № 1, с. 229–254.
8. Сидельников В. М. О взаимной корреляции последовательностей. — Докл. АН СССР, т. 12, 1971, с. 197–201.
9. Boztas S., Hammons R., Kumar P. V. 4-phase sequences with near-optimum correlation properties. — IEEE T-IT 38, 1992, № 3, p. 1101–1113.
10. McDonald B. R. Finite rings with identity. — New York, Marcel Dekker, 1974.
11. Nechaev A. A. Finite rings with applications. Handbook of Algebra, vol. 5. — Elsevier, 2008, p. 213–320.
12. Welch L. R. Lower bounds on the maximum cross correlation of signals. — IEEE T-IT 20, 1974, № 3, p. 397–399.