Math-Net.Ru

Общероссийский математический портал

А. Д. Бугров, О. В. Камловский, Параметры одного класса функций, заданных на конечном поле, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 4, 31–52

DOI: <https://doi.org/10.4213/mvk268>

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: 54.80.97.219

26 апреля 2023 г., 13:13:36

**Параметры одного класса функций,
заданных на конечном поле**

А. Д. Бугров, О. В. Камловский

ООО «Центр сертификационных исследований», Москва

Получено 18.IV.2018

Аннотация. Изучается класс функций над полем $GF(q)$, построенных на основе линейных рекуррентных последовательностей над кольцом $GR(q^n, p^n)$ с отмеченным характеристическим многочленом. Для данного класса исследуются: близость функций, близость к классу всех аффинных функций, число построенных функций и мощности прообразов элементов при действии функций. Показано, что указанный класс состоит из функций, значительно удаленных от класса всех аффинных функций

Ключевые слова: линейные рекуррентные последовательности, дискретные функции, конечные поля, кольцо Галуа, кросс-корреляционная функция

Parameters of a class of functions over a finite field

A. D. Bugrov, O. V. Kamlovskii

Certification Research Center, LLC, Moscow

Abstract. We study the class of functions defined on a finite field $GF(q)$ and constructed by means of linear recurrent sequences over the Galois ring $GR(q^n, p^n)$. For this class we investigate: the distances between functions, the distance to the class of affine functions, the number of constructed functions and the number of preimages of elements under action of functions. It is shown that the functions are significantly distant from the class of all affine functions.

Key words: linear recurrent sequences, discrete functions, finite fields, Galois ring, cross-correlation function

Citation: *Mathematical Aspects of Cryptography*, 2018, v. 9, № 4, pp. 31–52 (Russian)

© Академия криптографии Российской Федерации, 2018 г.

Введение

Линейные рекуррентные последовательности (ЛРП) над кольцами Галуа получили широкое распространение при построении различных генераторов псевдослучайных чисел (см. [1–4]). Выходные последовательности таких генераторов зачастую представляют собой усложнения знаков ЛРП с использованием некоторой функции усложнения. Интересен вопрос о возможности использования ЛРП для построения самих функций усложнения. Одним из основных свойств таких функций должна быть достаточная удаленность от класса всех аффинных функций.

Нелинейность функций, построенных по ЛРП над простыми полями, изучалась в [5]. Полученные в этой работе теоретические оценки нелинейности рассматриваемых функций являются довольно грубыми ввиду сложности самой задачи. В [6, 7] предлагалось использовать ЛРП над кольцом $\mathbf{Z}_{2^n}$ вычетов по модулю 2^n для построения кодов, достаточно удаленных от кода Рида–Маллера первого порядка. Идеи этой работы использовались в [8–10] для построения различных классов булевых функций. Один из них состоит из булевых функций f от m переменных, для которых нелинейность $nl(f)$ (расстояние Хэмминга до класса всех аффинных булевых функций от m переменных) удовлетворяет соотношению

$$nl(f) \geq 2^{m-1} - \left(\frac{2}{\pi} \ln(2^{n-1}) + 1 \right) (2^{n-1} - 1) 2^{m/2-1},$$

а алгебраическая степень $\deg f$ при $m > 2^n$ вычисляется по формуле $\deg f = 2^{n-1}$ (см. [8, 9]).

В данной работе рассматривается более общий класс функций от m переменных, заданных на произвольном конечном поле $P = GF(q)$. Он строится с использованием ЛРП над кольцом Галуа $GR(q^n, p^n)$. В случае $q = 2$ данный класс совпадает с классом булевых функций, изучавшимся в [8, 9]. Для построенного класса получены оценки: близости к классу аффинных функций, взаимной близости функций из класса, числа функций в классе и мощности прообразов элементов при действии функций. В случае $q = 2$ приводятся вычисленные с использованием ЭВМ точные значения нелинейности, алгебраической степени, показателя корреляционной иммунности и наличия сбалансированности функций, дополняющие аналогичные результаты из [8].

1. Определение класса функций

Пусть p — простое число, $q = p^t$, где t — натуральное число, $P = GF(q)$ — конечное поле из q элементов, $R = GR(q^n, p^n)$ — кольцо Галуа из q^n элементов, имеющее характеристику p^n (см. [11, 12]). Для кольца R факторкольцо $\bar{R} = R/pR$ является полем из q элементов. Далее для удобства изложения будем считать, что $\bar{R} = P$. Операции сложения в R и $\bar{R}$ будем обозначать одним символом $+$. Контекст будет однозначно определять, в какой алгебре производится операция. Образ элемента $a \in R$ при действии естественного эпиморфизма колец $R \rightarrow \bar{R}$ обозначим через $\bar{a}$. Естественный эпиморфизм колец $R \rightarrow \bar{R}$ индуцирует эпиморфизм колец многочленов $R[x] \rightarrow \bar{R}[x]$. Образ многочлена

$$A(x) = \sum a_i x^i \in R[x]$$

при этом эпиморфизме будем обозначать через $\bar{A}(x)$, где

$$\bar{A}(x) = \sum \bar{a}_i x^i \in \bar{R}[x].$$

Многочлен $G(x) \in R[x]$ назовем *унитарным*, если его старший коэффициент равен единице, и *реверсивным*, если его свободный член обратим в R . Реверсивный унитарный многочлен $G(x) \in R[x]$ называется *отмеченным*, если периоды многочленов $G(x)$ и $\bar{G}(x)$ равны. Известно, что для каждого реверсивного унитарного многочлена $F(x) \in P[x]$, не имеющего кратных корней в своем поле разложения, найдется единственный соответствующий $F(x)$ отмеченный многочлен $G(x) \in R[x]$, для которого $\bar{G}(x) = F(x)$ (см. [13, § 4]). Способ построения отмеченного многочлена $G(x)$, соответствующего многочлену $F(x)$, основанный на применении алгоритма Гензеля, весьма сложен, но в случае $p = 2$ существует довольно простой рекурсивный способ его построения по $F(x)$ (см. [13]). Всюду далее $F(x) \in P[x]$, $G(x) \in R[x]$ — такие реверсивные многочлены, что $F(x)$ неприводим над полем P , $m = \deg F(x) = \deg G(x)$, $\bar{G}(x) = F(x)$ и периоды многочленов удовлетворяют условиям $T = T(G) = T(F) = q^m - 1$. В этом случае говорят, что $G(x)$ — отмеченный многочлен *максимального периода*.

Обозначим через $L_R(G)$ множество всех ЛРП над кольцом R с характеристическим многочленом $G(x)$ и через $L_R^*(G)$ множество всех ЛРП $v \in L_R(G)$, для которых верно неравенство $\bar{v} \neq (0)$, где (0) — нулевая последовательность, а $\bar{v}$ — последовательность, полученная из v заменой каждого элемента его образом при естественном эпиморфизме из R в $\bar{R}$. Последовательность $\bar{v}$ является ЛРП с характеристическим многочленом $F(x)$ (см. [13]).

Пусть $\psi : R \rightarrow P$ — произвольное отображение, $u_1, \dots, u_m$ — линейно независимая система ЛРП из множества $L_P(F)$ (для всех $(c_1, \dots, c_m) \in P^m \setminus \vec{0}$ выполнено $c_1 u_1 + \dots + c_m u_m \neq (0)$), $v \in L_R^*(G)$. Рассмотрим функцию $f = f_{u_1, \dots, u_m, v, \psi} : P^m \rightarrow P$ от m переменных, определенную по правилу $f(0, 0, \dots, 0) = \psi(0)$ и для всех $i = 0, 1, \dots, q^m - 2$

$$f(u_1(i), u_2(i), \dots, u_m(i)) = \psi(v(i)). \quad (1)$$

Так как $u_1, \dots, u_m$ — линейно независимая система ЛРП максимального периода $q^m - 1$, то среди векторов $(u_1(i), \dots, u_m(i))$, где $i = 0, 1, \dots, q^m - 2$, появляются по одному разу все ненулевые векторы из P^m (см., например, [14]). Таким образом, правило (1) однозначно задает функцию f . Таблицу данной функции легко построить с использованием регистров сдвига над кольцом R и полем P . Пусть $u \in L_P(F)$, $u \neq (0)$, тогда в качестве последовательностей u_j , $j = 1, \dots, m$, годятся последовательности $x^{j-1}u$ со знаками $u_j(i) = u(i+j-1)$, $i \geq 0$. При выборе $u = \bar{v}$ функция f строится с использованием одного линейного регистра сдвига над кольцом R . Отметим, что такой способ построения функции f был впервые предложен А. А. Нечаевым и сообщен авторам.

Всюду далее будем считать, что последовательности $u_1, \dots, u_m$ фиксированы, и будем использовать обозначение $f = f_{u_1, \dots, u_m, v, \psi} = f_{v, \psi}$. Введем следующие обозначения для классов функций:

$$D(F, \psi) = \bigcup_{v \in L_R^*(G)} f_{v, \psi}, \quad D(m, \psi) = \bigcup_F D(F, \psi),$$

где объединение берется по всем возможным неприводимым многочленам $F(x)$ степени m над полем P , имеющим период $T(F) = q^m - 1$. Нас будут интересовать свойства функций из классов $D(F, \psi)$ и $D(m, \psi)$.

2. Близость функций

Пусть $f, g : P^m \rightarrow P$ — некоторые функции. Через $\text{Tr}_{P_0}^P$ будем обозначать функцию «след» из поля P в простое подполе P_0 , задаваемую равенством

$$\text{Tr}_{P_0}^P(x) = x + x^p + \dots + x^{p^{t-1}}, \quad x \in P.$$

Для любого $b \in P$ через χ_b будем обозначать аддитивный характер поля P (см., например, [15])

$$\chi_b(x) = e^{2\pi i \text{Tr}_{P_0}^P(bx)/p}, \quad x \in P.$$

Определим коэффициент кросс-корреляции между функциями f и g (см. [16]) равенством

$$C_b(f, g) = \sum_{\vec{x} \in P^m} \chi_b(f(\vec{x}) - g(\vec{x})), \quad b \in P \setminus \{0\}.$$

Введем обозначение

$$C(f, g) = \max_{b \in P \setminus \{0\}} |C_b(f, g)|.$$

Известно (см. [16, 17]), что $C(f, g) = 0$ тогда и только тогда, когда среди разностей $f(\vec{x}) - g(\vec{x})$, где $\vec{x} \in P^m$, каждый элемент из P появляется ровно $|P|^{m-1}$ раз, т. е. рассматриваемая последовательность сбалансированна (см. [18]).

Обозначим через $\langle \vec{a}, \vec{x} \rangle$ скалярное произведение векторов $\vec{a}, \vec{x} \in P^m$. Пусть g пробегает все множество аффинных функций от m переменных над полем P , т. е.

$$g(\vec{x}) = g(x_1, \dots, x_m) = \langle \vec{a}, \vec{x} \rangle + b = a_1 x_1 + a_2 x_2 + \dots + a_m x_m + b,$$

где $a_1, \dots, a_m, b$ — некоторые элементы из P . Рассмотрим величину

$$C(f) = \max_g C(f, g) = \max_g \max_{b \in P \setminus \{0\}} |C_b(f, g)|, \quad (2)$$

которая характеризует «близость» f к классу всех аффинных функций от m переменных над полем P . Чем меньше величина $C(f)$, тем более удалена функция f от класса всех аффинных функций.

Несложно заметить, что $C(f)$ достигает максимума на множестве $\{\langle \vec{a}, \vec{x} \rangle \mid \vec{a} \in P^m\}$ всех линейных функций от m переменных над полем P . Соотношение $C(f) = q^m$ равносильно тому, что f является аффинной функцией над полем P .

В [19] близость функций $f, g : P^m \rightarrow P$ определяется как

$$\delta(f, g) = \frac{q}{q-1} \sum_{y \in P} \left(\mathbf{P}(f-g=y) - \frac{1}{q} \right)^2,$$

где вероятность $\mathbf{P}$ вычисляется при условии, что аргументы функций f и g выбираются случайно и равновероятно. Согласно [20] верно равенство

$$\delta(f, g) = \frac{1}{(q-1)q^{2m}} \sum_{b \in P \setminus \{0\}} |C_b(f, g)|^2.$$

Таким образом, нахождение точных значений коэффициентов $C_b(f, g)$ или получение оценок сверху их модулей позволяет, соответственно, найти величину $\delta(f, g)$ или получить ее оценку сверху.

3. Близость функций из класса

Приведем некоторые обозначения и результаты из теории колец Галуа (см., например, [11, § 2, 3]). Рассмотрим p -адическое множество $\Gamma(R) = \{\alpha \in R \mid \alpha^q = \alpha\}$. Каждый элемент x кольца R может быть единственным образом представлен в виде p -адического разложения

$$x = \gamma_0(x) + p\gamma_1(x) + \dots + p^{n-1}\gamma_{n-1}(x),$$

где $\gamma_j: R \rightarrow \Gamma(R)$, $j \in \overline{0, n-1}$, — разрядные функции кольца R . Обозначим через R_0 множество, состоящее из элементов $0, e, 2e, \dots, (p^n - 1)e$, где e — единица кольца R . Множество R_0 является подкольцом кольца R , изоморфным кольцу $\mathbf{Z}_{p^n}$. Через $\text{Aut}(R/R_0)$ обозначим множество всех автоморфизмов кольца R , оставляющих на месте каждый элемент кольца R_0 . Группоид $(\text{Aut}(R/R_0), \circ)$ относительно операции композиции отображений является циклической группой порядка t , порожденной автоморфизмом $\varkappa_0$. Автоморфизм $\varkappa_0$ действует на каждый элемент $x \in R$, имеющий p -адическое разложение $x = \gamma_0(x) + p\gamma_1(x) + \dots + p^{n-1}\gamma_{n-1}(x)$, следующим образом:

$$\varkappa_0(x) = \gamma_0(x)^p + p\gamma_1(x)^p + \dots + p^{n-1}\gamma_{n-1}(x)^p.$$

Функция след $\text{Tr}_{R_0}^R$ из кольца R в кольцо R_0 определяется равенством

$$\text{Tr}_{R_0}^R(x) = \sum_{\varkappa \in \text{Aut}(R/R_0)} \varkappa(x).$$

Для любого элемента $c \in R$ отображение $\widehat{\chi}_c: R \rightarrow \mathbf{C}^*$, определяемое соотношением

$$\widehat{\chi}_c(x) = e^{2\pi i \text{Tr}_{R_0}^R(cx)/p^n}, \quad x \in R,$$

является характером аддитивной группы кольца R (аддитивным характером кольца R), причем если a и b — различные элементы кольца R , то $\widehat{\chi}_a \neq \widehat{\chi}_b$. Других характеров аддитивной группы кольца R нет (см. [21, § 3]). В дальнейшем будем использовать обозначение $\widehat{\chi}_e = \widehat{\chi}$.

Имеет место следующее разложение композиции $\chi_b \circ \psi: R \rightarrow \mathbf{C}^*$ отображений χ_b и ψ по базису характеров группы $(R, +)$ (см., например, [22, равенство (12)], [23]):

$$\chi_b(\psi(x)) = \sum_{r \in R} \nu_{r,b} \widehat{\chi}(rx), \quad x \in R, \quad (3)$$

где

$$\nu_{r,b} = \frac{1}{q^n} \sum_{s \in R} \chi_b(\psi(s)) \widehat{\chi}(-rs). \quad (4)$$

Введем обозначения

$$\sigma(\chi_b \circ \psi) = \sum_{r \in R} |\nu_{r,b}|, \quad \sigma(\psi) = \max_{b \in P \setminus \{0\}} \sigma(\chi_b \circ \psi). \quad (5)$$

Назовем отображение $\psi: R \rightarrow P$ *сбалансированным* (см. [18]), если при каждом $a \in P$ уравнение $\psi(x) = a$ имеет ровно $|R|/|P| = q^{n-1}$ решений относительно неизвестного $x \in R$.

Теорема 1. Пусть $\psi_1, \psi_2: R \rightarrow P$ — сбалансированные отображения, а система ЛРП v_1, v_2 линейно независима над кольцом R , тогда

$$C(f_{v_1, \psi_1}, f_{v_2, \psi_2}) \leq \sigma(\psi_1) \sigma(\psi_2) (p^{n-1} - 1) q^{m/2} \leq (p^{n-1} - 1) q^{m/2 + n}.$$

Доказательство. Зафиксируем произвольный элемент $b \in P \setminus \{0\}$. Пусть при $i = 1, 2$

$$\nu_{r,b}^{(i)} = \frac{1}{q^n} \sum_{s \in R} \chi_b(\psi_i(s)) \widehat{\chi}(-rs), \quad r \in R. \quad (6)$$

Тогда

$$\begin{aligned} C_b(f_{v_1, \psi_1}, f_{v_2, \psi_2}) &= \sum_{\vec{x} \in P^m} \chi_b(f_{v_1, \psi_1}(\vec{x}) - f_{v_2, \psi_2}(\vec{x})) = \\ &= \chi_b(\psi_1(\vec{0}) - \psi_2(\vec{0})) + \sum_{i=0}^{q^m-2} \chi_b(\psi_1(v_1(i)) - \psi_2(v_2(i))) = \\ &= \sum_{r \in R} \nu_{r,b}^{(1)} \sum_{s \in R} \nu_{s,-b}^{(2)} + \sum_{i=0}^{q^m-2} \sum_{r,s \in R} \nu_{r,b}^{(1)} \nu_{s,-b}^{(2)} (\widehat{\chi}(rv_1(i) + sv_2(i))) = \\ &= \sum_{r,s \in R} \nu_{r,b}^{(1)} \nu_{s,-b}^{(2)} \left(\sum_{i=0}^{q^m-2} \widehat{\chi}(rv_1(i) + sv_2(i)) + 1 \right). \end{aligned}$$

По условию отображения ψ_1, ψ_2 сбалансированны, поэтому, с учетом равенства (6),

$$\nu_{0,b}^{(1)} = \nu_{0,-b}^{(2)} = 0.$$

Следовательно, в последнем равенстве достаточно ограничиться суммированием по всем $r, s \neq 0$. Если $r, s \neq 0$, то по условию последовательность $rv_1 + sv_2$ будет ненулевой ЛРП с характеристическим многочленом $G(x)$.

В [24, теорема 2.1] показано, что для каждой ненулевой ЛРП δ с характеристическим многочленом $G(x)$ над кольцом R имеет место соотношение

$$\left| \sum_{i=0}^{T-1} \widehat{\chi}(\delta(i)) + 1 \right| \leq (p^{n-1} - 1) q^{m/2}. \quad (7)$$

Таким образом, используя неравенство (7), получим

$$\begin{aligned} |C_b(f_{v_1, \psi_1}, f_{v_2, \psi_2})| &\leq \left| \sum_{r, s \in R} \nu_{r, b}^{(1)} \nu_{s, -b}^{(2)} \left(\sum_{i=0}^{q^{m-2}} \widehat{\chi}(rv_1(i) + sv_2(i)) + 1 \right) \right| \leq \\ &\leq \sigma(\chi_b \circ \psi_1) \sigma(\chi_{-b} \circ \psi_2) (p^{n-1} - 1) q^{m/2}. \end{aligned}$$

Остается воспользоваться оценками из [23, теорема 1]:

$$\sigma(\psi_i) \leq q^{n/2}, \quad i = 1, 2. \quad \square$$

Определим бинарную операцию $\oplus$ на множестве $\Gamma(R)$ правилом

$$\alpha \oplus \beta = \gamma_0(\alpha + \beta).$$

Известно, что $(\Gamma(R), \oplus, \cdot)$ — поле из q элементов (см. [11, утверждение 2]). Определим отображение

$$\tau: (P, +, \cdot) \rightarrow (\Gamma(R), \oplus, \cdot)$$

по правилу $\tau(\bar{r}) = \gamma_0(r)$. Определение τ корректно, τ — изоморфизм полей, и справедливо равенство $\bar{r} = [\gamma_0(r)]$. Следовательно, композиция ограничения естественного эпиморфизма колец $R \rightarrow \bar{R} = P$ на $\Gamma(R)$ и изоморфизма $\tau: P \rightarrow \Gamma(R)$ является тождественным преобразованием поля P :

$$\overline{\tau(\bar{r})} = \overline{\gamma_0(r)} = [\gamma_0(\gamma_0(r))] = [\gamma_0(r)] = \bar{r}. \quad (8)$$

Несложно видеть, что для любого элемента $r \in R$ верно равенство

$$p^{n-1}r = p^{n-1}\tau(\bar{r}),$$

которое будет использоваться далее.

Лемма 1. Пусть $x \in P$, тогда верно соотношение $\chi(x) = \widehat{\chi}(p^{n-1}\tau(x))$.

Доказательство. Пусть $x \in P$, тогда $\tau(x)$ представим в виде:

$$\tau(x) = \gamma_0(\tau(x)).$$

Используя результаты из [11, §2, §3], получим равенства

$$\begin{aligned} \text{Tr}_{R_0}^R(p^{n-1}\tau(x)) &= \sum_{\kappa \in \text{Aut}(R/R_0)} \kappa(p^{n-1}\gamma_0(\tau(x))) = \\ &= \sum_{i=0}^{t-1} \kappa_0^i(p^{n-1}\gamma_0(\tau(x))) = \sum_{i=0}^{t-1} p^{n-1}\gamma_0(\tau(x))^{p^i} = \\ &= \sum_{i=0}^{t-1} p^{n-1}\tau(x)^{p^i} = p^{n-1} \sum_{i=0}^{t-1} \tau(x)^{p^i} = \\ &= p^{n-1} \tau\left(\sum_{i=0}^{t-1} x^{p^i}\right) = p^{n-1} \tau(\text{Tr}_{P_0}^P(x)) = p^{n-1} \text{Tr}_{P_0}^P(x). \end{aligned}$$

Следовательно,

$$\chi(x) = e^{2\pi i \text{Tr}_{P_0}^P(x)/p} = e^{2\pi i \text{Tr}_{R_0}^R(p^{n-1}\tau(x))/p^n} = \widehat{\chi}(p^{n-1}\tau(x)). \quad (9)$$

Лемма доказана. $\square$

Изучим один важный класс отображений ψ . Будем говорить, что отображение $\psi: R \rightarrow P$ *биективно по старшему разряду*, если для каждого $a \in R$ с p -адическим представлением

$$a = a_0 + pa_1 + p^2a_2 + \dots + p^{n-1}a_{n-1}, \quad a_0, a_1, a_2, \dots, a_{n-1} \in \Gamma(R),$$

при любых фиксированных $a_0, \dots, a_{n-2} \in \Gamma(R)$ отображение

$$\psi_{a_0, \dots, a_{n-2}}: \Gamma(R) \rightarrow P,$$

действующее по правилу

$$\psi_{a_0, \dots, a_{n-2}}(a_{n-1}) = \psi(a), \quad a_{n-1} \in \Gamma(R),$$

является биективным. Отметим, что каждое такое отображение ψ сбалансированно. Примером рассматриваемых отображений ψ являются отображения вида

$$\psi(a) = \pi(\bar{a}_{n-1}) + \eta(a_0, a_1, \dots, a_{n-2}),$$

где π — произвольная подстановка поля P , а $\eta: \Gamma(R)^{n-1} \rightarrow P$ — произвольное отображение.

Лемма 2. Если отображение ψ биективно по старшему разряду, то $\nu_{r,b} = 0$ для всех $r \in pR$, $b \in P \setminus 0$.

Доказательство. Учитывая лемму 1 и равенство

$$p^{n-1}r = p^{n-1}\tau(\bar{r}), \quad r \in R,$$

получим

$$\begin{aligned} \nu_{r,b} &= \frac{1}{q^n} \sum_{s \in R} \chi_b(\psi(s)) \hat{\chi}(-rs) = \\ &= \frac{1}{q^n} \sum_{s \in R} \chi_b(\psi(s)) \hat{\chi}(-s_0r - \dots - s_{n-2}p^{n-2}r) \hat{\chi}(-s_{n-1}p^{n-1}r) = \\ &= \frac{1}{q^n} \sum_{s \in R} \chi_b(\psi(s)) \hat{\chi}(-s_0r - \dots - s_{n-2}p^{n-2}r) = \\ &= \frac{1}{q^n} \sum_{s_0, \dots, s_{n-2} \in \Gamma(R)} \hat{\chi}(-s_0r - \dots - s_{n-2}p^{n-2}r) \sum_{s_{n-1} \in \Gamma(R)} \chi_b(\psi_{s_0, \dots, s_{n-2}}(s_{n-1})). \end{aligned}$$

Так как χ_b — нетривиальный аддитивный характер, то согласно [15]

$$\sum_{s_{n-1} \in \Gamma(R)} \chi_b(\psi_{s_0, \dots, s_{n-2}}(s_{n-1})) = \sum_{x \in P} \chi_b(x) = 0. \quad \square$$

В дальнейшем будет показано, что верно и обратное утверждение.

Лемма 3. Если отображение ψ биективно по старшему разряду, то

$$\sigma(\psi) \leq (q-1)^{1/2} q^{(n-1)/2}.$$

Доказательство. В силу леммы 2 и неравенства Коши–Буняковского верны следующие переходы:

$$\sigma(\chi_b \circ \psi) = \sum_{r \in R \setminus pR} |\nu_{r,b}| \leq \sqrt{\sum_{r \in R \setminus pR} 1} \sqrt{\sum_{r \in R} |\nu_{r,b}|^2} = (q-1)^{1/2} q^{(n-1)/2};$$

здесь использовано также равенство Парсеваля

$$\sum_{r \in R} |\nu_{r,b}|^2 = 1. \quad \square$$

Следствие 1. Если отображения ψ_1, ψ_2 биективны по старшему разряду, то в условиях теоремы 1 верна оценка

$$C(f_{v_1, \psi_1}, f_{v_2, \psi_2}) \leq (p^{n-1} - 1)(q - 1)q^{n-1+m/2}.$$

4. Близость к аффинным функциям

Изучим для построенных функций f величину $C(f)$, определенную равенством (2).

Теорема 2. Пусть $f \in D(m, \psi)$. Тогда

- 1) если $n = 1$, то $C(f) = q^m$ и f — аффинная функция над полем P ,
- 2) если $n > 1$ и отображение ψ биективно по старшему разряду, то

$$C(f) \leq \sigma(\psi)(p^{n-1} - 1)q^{m/2} \leq (p^{n-1} - 1)(q - 1)^{1/2}q^{(m+n-1)/2}.$$

Доказательство. Пусть $f = f_{v, \psi}$. Рассмотрим коэффициент кросс-корреляции между функциями $\langle \vec{a}, \vec{x} \rangle$ и f для произвольного ненулевого b :

$$\begin{aligned} C_b(\langle \vec{a}, \vec{x} \rangle, f(\vec{x})) &= \sum_{\vec{c} \in P^m} \chi_b(a_1 c_1 + \dots + a_m c_m - f(\vec{c})) = \\ &= \chi_b(-\psi(0)) + \\ &\quad + \sum_{i=0}^{T-1} \chi_b(a_1 u_1(i) + \dots + a_m u_m(i) - f(u_1(i), \dots, u_m(i))). \end{aligned}$$

Пусть

$$\varphi(x_1, \dots, x_m) = a_1 x_1 + \dots + a_m x_m, \quad x_1, \dots, x_m \in P.$$

Разложим отображение $\chi_b \circ \varphi: P^m \rightarrow \mathbf{C}^*$ по базису характеров группы $\underbrace{P \oplus \dots \oplus P}_m$ (см. [22, равенство (12)]):

$$\begin{aligned} \chi_b(\varphi(u_1(i), \dots, u_m(i))) &= \\ &= \sum_{\vec{y}=(y_1, \dots, y_m) \in P^m} W_{\chi_b \circ \varphi}(\vec{y}) \chi(y_1 u_1(i) + \dots + y_m u_m(i)), \end{aligned} \quad (10)$$

где $W_{\chi_b \circ \varphi}(\vec{y})$ — спектральные коэффициенты, которые определяются равенствами

$$\begin{aligned} W_{\chi_b \circ \varphi}(\vec{y}) &= \frac{1}{q^m} \sum_{\vec{s}=(s_1, \dots, s_m) \in P^m} (\chi_b \circ \varphi)(\vec{s}) \chi(-s_1 y_1 - \dots - s_m y_m) = \\ &= \frac{1}{q^m} \sum_{\vec{s}=(s_1, \dots, s_m) \in P^m} \chi(b a_1 s_1 + \dots + b a_m s_m) \chi(-s_1 y_1 - \dots - s_m y_m) = \\ &= \delta_{\vec{y}, b \vec{a}} = \begin{cases} 1, & \text{если } \vec{y} = b \vec{a}, \\ 0, & \text{если } \vec{y} \neq b \vec{a}. \end{cases} \end{aligned}$$

Отсюда получим, что

$$\begin{aligned} C_b(\langle \vec{a}, \vec{x} \rangle, f(\vec{x})) &= \\ &= \chi_b(-\psi(0)) + \\ &\quad + \sum_{i=0}^{T-1} \chi_b(\varphi(u_1(i), \dots, u_m(i)) - \psi(v(i))) = \\ &= \chi_b(-\psi(0)) + \\ &\quad + \sum_{i=0}^{T-1} \sum_{\vec{y} \in P^m} W_{\chi_b \circ \varphi}(\vec{y}) \chi(y_1 u_1(i) + \dots + y_m u_m(i)) \sum_{r \in R} \nu_{r, -b} \widehat{\chi}(r v(i)) = \\ &= \chi_b(-\psi(0)) + \\ &\quad + \sum_{r \in R} \nu_{r, -b} \sum_{i=0}^{T-1} \widehat{\chi}(p^{n-1} \tau(b a_1 u_1(i)) + \dots + p^{n-1} \tau(b a_m u_m(i)) + r v(i)) = \\ &= \sum_{r \in R} \nu_{r, -b} \left(\sum_{i=0}^{T-1} \widehat{\chi}(\delta_{a_1, \dots, a_m, r}(i)) + 1 \right), \end{aligned}$$

где $\delta_{a_1, \dots, a_m, r}$ — последовательность над кольцом R с элементами

$$\delta_{a_1, \dots, a_m, r}(i) = r v(i) + p^{n-1} \tau(b a_1 u_1(i)) + \dots + p^{n-1} \tau(b a_m u_m(i)), \quad i \geq 0.$$

При $n = 1$ знаки последовательности $\delta_{a_1, \dots, a_m, r}$ имеют вид

$$\delta_{a_1, \dots, a_m, r}(i) = rv(i) + ba_1u_1(i) + \dots + ba_mu_m(i).$$

Существуют такие $a_1, \dots, a_m \in P$, что $\delta_{a_1, \dots, a_m, r} = (0)$, а значит, при таких элементах

$$C_b(\langle \vec{a}, \vec{x} \rangle, f(\vec{x})) = \sum_{r \in R} \nu_{r, -b} \left(\sum_{i=0}^{T-1} \hat{\chi}(0) + 1 \right) = q^m \chi_b(-\psi(0)).$$

Таким образом, $C(f) = q^m$ и f — аффинная функция от m переменных над полем P .

Пусть $n > 1$ и отображение ψ биективно по старшему разряду. Тогда $\nu_{r, -b} = 0$ для всех $r \in pR$ по лемме 2. Поэтому достаточно ограничиться суммированием по всем обратимым элементам кольца R . При $n > 1$ последовательность $\delta_{a_1, \dots, a_m, r}$ будет ненулевой, так как $\gamma_0(\delta_{a_1, \dots, a_m, r}(i)) = \gamma_0(rv(i))$ и последовательность rv содержит хотя бы один обратимый элемент кольца R . Кроме того, последовательность $\delta_{a_1, \dots, a_m, r}$ является ЛРП с характеристическим многочленом $G(x)$. Таким образом, используя неравенство (7), получим

$$|C_b(g(\vec{x}), \langle \vec{a}, \vec{x} \rangle)| \leq \left(\sum_{r \in R} |\nu_{r, -b}| \right) (p^{n-1} - 1) q^{m/2} = \sigma(\chi_{-b} \circ \psi) (p^{n-1} - 1) q^{m/2}, \quad (11)$$

и, учитывая лемму 3,

$$|C_b(g(\vec{x}), \langle \vec{a}, \vec{x} \rangle)| \leq \sigma(\psi)(p^{n-1} - 1) q^{m/2} \leq (p^{n-1} - 1) (q - 1)^{1/2} q^{(m+n-1)/2}. \quad \square$$

Следствие 2. Пусть $n > 1$ и отображение ψ биективно по старшему разряду. Тогда при $m \geq n + (2n - 2) / \log_p q$ в классе $D(m, \psi)$ нет аффинных функций.

Доказательство. Пусть $t = \log_p q$. Так как $p^{n-1} - 1 < q^{(n-1)/t}$, то

$$(p^{n-1} - 1) (q - 1)^{1/2} q^{(m+n-1)/2} < q^{(n-1)/t} q^{(m+n)/2} < q^m.$$

Следовательно, $C(f) < q^m$ для всех $f \in D(m, \psi)$ по теореме 2. $\square$

5. Мощности класса и прообразов элементов

Приведем оценки величины $|D(F, \psi)|$.

Утверждение 1. Если ψ — сбалансированное отображение и $\deg F(x) = m$, то

$$q^{mn} - q^{(n-1)m} \geq |D(F, \psi)| \geq q^m - 1.$$

Доказательство. Мощность класса $D(F, \psi)$ не больше мощности класса $L_R^*(G)$, которая равна $q^{mn} - q^{(n-1)m}$. Кроме того, мощность класса $D(F, \psi)$ не меньше мощности множества

$$\psi(R^m \setminus (pR)^m) = \{(\psi(r_1), \dots, \psi(r_m)) \mid (r_1, \dots, r_m) \in R^m \setminus (pR)^m\}.$$

Отображение ψ естественным образом разбивает множество R^m на классы эквивалентности мощности $q^{(n-1)m}$, внутри которых принимает одинаковые значения. Поэтому

$$|\psi(R^m \setminus (pR)^m)| \geq \frac{|R^m \setminus (pR)^m|}{q^{(n-1)m}} = q^m - 1. \quad \square$$

Заметим, что при $n = 1$ оба неравенства в утверждении 1 обращаются в равенства.

Следствие 3. Если $n = 1$ и функция ψ сбалансированная, то

$$D(F, \psi) = \{(\vec{a}, \vec{x}) + \psi(0) \mid \vec{a} \in P^m \setminus (0, \dots, 0)\}.$$

Доказательство. Из п.1 теоремы 2 и утверждения 1 следует, что класс $D(F, \psi)$ состоит из $q^m - 1$ различных аффинных функций, т.е.

$$D(F, \psi) \subset \{(\vec{a}, \vec{x}) + \psi(0) \mid \vec{a} \in P^m\}.$$

В силу того что в последовательности v появляются все элементы поля P , выполнено соотношение $\psi(0) \notin D(F, \psi)$. $\square$

Теорема 3. Если $\deg F(x) = m$ и отображение ψ биективно по старшему разряду, то при $m \geq 2n + 2(n-1)/\log_p q$ все функции в классе $D(F, \psi)$ различны и имеют место равенства

$$|D(F, \psi)| = |L_R^*(G)| = q^{nm} - q^{(n-1)m}.$$

Доказательство. Воспользуемся результатом работы [25], из которого следует, что если в каждой ЛРП $v \in L_R^*(F)$ появляются все элементы кольца R , то последовательности с элементами $\psi(v_1(i))$ и $\psi(v_2(i))$, $i \geq 0$, различны для любых различных ЛРП $v_1, v_2 \in L_R(F)$. Остается заметить, что согласно [21, следствие 5] все элементы кольца R появляются в каждой ЛРП $v \in L_R^*(F)$ при выполнении неравенства

$$T(F) = q^m - 1 \geq p^{n-1} (q^n - 1) q^{m/2},$$

которое следует из соотношений

$$m \geq \frac{2n-2}{\log_p q} + 2n,$$

$$q^m \geq p^{n-1} q^{n+m/2},$$

$$q^m \geq p^{n-1} q^{n+m/2} - p^{n-1} q^{m/2} + 1,$$

$$T(F) = q^m - 1 \geq p^{n-1} (q^n - 1) q^{m/2}.$$

Теорема доказана. $\square$

Прообраз элемента z при отображении f будем обозначать через $f^{-1}(z)$.

Утверждение 2. Пусть ψ — сбалансированное отображение, $f \in D(m, \psi)$. Тогда для любого $z \in P$ верны неравенства

$$\left| |f^{-1}(z)| - q^{m-1} \right| \leq \sigma(\psi)(p^{n-1}-1)(q-1)q^{m/2-1} \leq (p^{n-1}-1)(q-1)q^{(n+m)/2-1}.$$

Доказательство. Пусть N_z — количество появлений $z \in P$ среди элементов $\psi(v(0)), \dots, \psi(v(T-1))$. Если $z \neq \psi(0)$, то согласно [23, теорема 5]

$$q^{m-1} - S \leq N_z \leq q^{m-1} + S,$$

а при $z = \psi(0)$

$$q^{m-1} - 1 - S \leq N_z \leq q^{m-1} - 1 + S,$$

где $S = \sigma(\psi)(p^{n-1}-1)(q-1)q^{m/2-1}$. Остается воспользоваться соотношениями

$$|f^{-1}(z)| = \begin{cases} N_z, & \text{если } \psi(0) \neq z, \\ N_z + 1, & \text{если } \psi(0) = z, \end{cases}$$

и неравенством $\sigma(\psi) \leq q^{n/2}$. $\square$

6. Разрядные множества и отображения

Разрядным множеством кольца R называется любое его подмножество

$$K = \{k_0, k_1, \dots, k_{q-1}\},$$

все элементы которого попарно не сравнимы по идеалу pR (см. [2, 3]). Например, множество $\Gamma(R)$ является разрядным множеством кольца R (см. [11, лемма 3]). Если K — разрядное множество кольца R , то каждый элемент $a \in R$ однозначно представим в виде

$$a = a_0 + pa_1 + \dots + p^{n-1}a_{n-1}, \quad (12)$$

где $a_i \in K$, $i \in \overline{0, n-1}$. Равенство (12) называется разрядным представлением элемента a в множестве K , а элемент a_i , где $i \in \overline{0, n-1}$, называется i -м разрядом элемента a в множестве K . Элемент a_{n-1} называется старшим разрядом. Для каждого $i \in \overline{0, n-1}$ зададим разрядное отображение

$$\chi_i^K(a) = a_i.$$

По аналогии с отображениями ψ , биективными по старшему разряду, определим отображения, биективные по старшему разряду в разрядном множестве K . Оказывается, это определение не зависит от выбора разрядного множества K .

Утверждение 3. Если $\psi: R \rightarrow P$, то равносильны следующие утверждения:

- 1) ψ биективно по старшему разряду,
- 2) ψ биективно по старшему разряду в каждом разрядном множестве $K \subset R$,
- 3) для коэффициентов $\nu_{r,b}$, определенных равенством (4), при всех $r \in pR$ и $b \in P \setminus 0$ выполнено $\nu_{r,b} = 0$.

Доказательство. Очевидно, что из п. 2 следует п. 1. Из п. 1 следует п. 3, как это доказано в лемме 2. Остается показать, что из п. 3 следует п. 2. Согласно [15, теорема 7.7] (см. также [17]) если $c_1, \dots, c_q$ — последовательность элементов поля P , то в этой последовательности каждый элемент из P появляется ровно по одному разу тогда и только тогда, когда

$$\sum_{i=1}^q \chi_b(c_i) = 0 \quad \text{для всех} \quad b \in P \setminus 0.$$

Поэтому достаточно доказать, что при любых фиксированных $a_0, \dots, a_{n-2} \in K$ и $b \neq 0$ имеет место соотношение

$$\sum_{a_{n-1} \in K} \chi_b(\psi_{a_0, \dots, a_{n-2}}(a_{n-1})) = 0. \quad (13)$$

Из равенства (3) следует, что

$$\chi_b(\psi(a)) = \sum_{r \in R^*} \nu_{r,b} \hat{\chi}(ra),$$

где суммирование осуществляется по всем обратимым элементам r кольца R . Значит,

$$\begin{aligned} \sum_{a_{n-1} \in K} \chi_b(\psi_{a_0, \dots, a_{n-2}}(a_{n-1})) &= \\ &= \sum_{r \in R^*} \nu_{r,b} e^{2\pi i \operatorname{Tr}_{R_0}^R (ra_0 + \dots + p^{n-2} r a_{n-2})/p^n} \sum_{a_{n-1} \in K} e^{2\pi i \operatorname{Tr}_{R_0}^R (p^{n-1} r a_{n-1})/p^n}. \end{aligned}$$

Для доказательства равенства (13) остается показать, что

$$\sum_{a_{n-1} \in K} e^{2\pi i \operatorname{Tr}_{R_0}^R (p^{n-1} r a_{n-1})/p^n} = 0.$$

Пусть

$$r = r_0 + pr_1 + \dots + p^{n-1}r_{n-1}, \quad \text{где } r_0, \dots, r_{n-1} \in K,$$

тогда

$$\bar{r}_0 \neq \bar{0}, \quad p^{n-1}ra_{n-1} = p^{n-1}r_0a_{n-1} = p^{n-1}\tau(\bar{r}_0\bar{a}_{n-1})$$

и согласно лемме 1

$$\sum_{a_{n-1} \in K} e^{2\pi i \operatorname{Tr}_{R_0}^R (p^{n-1}ra_{n-1})/p^n} = \sum_{\bar{a}_{n-1} \in P} \chi_{\bar{r}_0}(\bar{a}_{n-1}) = 0. \quad \square$$

Заметим, что в случае $q = 2$, т. е. когда $R = \mathbf{Z}_{2^n}$, отображение ψ биективно по старшему разряду тогда и только тогда, когда

$$\psi(a) = \bar{a}_{n-1} + \eta(a_0, a_1, \dots, a_{n-2}),$$

где $\eta: \Gamma(R)^{n-1} \rightarrow P$ — произвольное отображение.

Приведем еще более частный класс отображений ψ , представляющих практический интерес. Рассмотрим разрядное множество $K = \{k_0, k_1, \dots, k_{p-1}\}$ кольца $R = \mathbf{Z}_{p^n}$. Будем говорить, что K образует арифметическую прогрессию, если

$$K = \{a, a + d, a + 2d, \dots, a + (p-1)d\},$$

для некоторых элементов $a, d \in R, a \equiv 0 \pmod{p}, (d, p) = 1$. В этом случае будем использовать обозначение $K = K_{a,d}$. Важным примером разрядного множества, образующего арифметическую прогрессию, является p -ичное разрядное множество $K_{0,1} = \{0, 1, \dots, p-1\}$.

Утверждение 4 ([26]). Пусть $R = \mathbf{Z}_{p^n}, P = \mathbf{Z}_p, n \geq 2, K = K_{a,d}, \psi = \varkappa_{n-1}^K$. Тогда

$$\sigma(\psi) \leq \frac{2}{\pi} \ln(p^{n-1}) + \frac{13}{40}p + \frac{7}{20}.$$

Для отображений ψ , указанных в утверждении 4, оценка параметра $\sigma(\psi)$ оказывается более точной по сравнению с оценкой из леммы 3. Поэтому в оценках из теорем 1, 2 и утверждения 2 следует использовать результат утверждения 4.

7. Результаты вычислений на ЭВМ

Для изучения свойств функций класса $D(F, \psi)$ в случае кольца $R = \mathbf{Z}_{2^n}$ были проведены вычисления с использованием ЭВМ. В качестве отображения ψ было выбрано старшее разрядное отображение $\varkappa_{n-1}^{\{0,1\}} = \gamma_{n-1}$. Последовательности $u_1, \dots, u_m$ выбирались по правилу

$$u_1 = u, \quad u_2 = xu, \quad \dots, \quad u_m = x^{m-1}u.$$

Начальное заполнение $(u(0), \dots, u(m-1))$ ЛРП u выбиралось равным вектору $(0, \dots, 0, 1)$. Если зафиксировать многочлены $F(x), G(x)$ и ЛРП u , то по начальному заполнению ЛРП v однозначно строится функция $f_{u_1, \dots, u_m, v, \psi}$.

В таблице приведены результаты вычислений при значениях $m \in \overline{3, 8}$ и $n \in \overline{2, 4}$. Запись вида « $(w, d, c, b) - N$ » означает, что при переборе функций из класса $D(F, \psi)$ было найдено N функций с максимальным по модулю коэффициентом Уолша–Адамара w , алгебраической степени d , показателем корреляционной иммунности c (значение $c = 0$ обозначает ее отсутствие) и наличием сбалансированности b ($b = 0$ — нет, $b = 1$ — есть). Запись «Случайная выборка» под многочленом $G(x)$ означает, что перебирались не все возможные начальные заполнения ЛРП v , а производилась их случайная выборка с возвращением.

Таблица

n	$G(x)$	$(w, d, c, b) - N$
2	$x^3 - x^2 - 2x - 1$	$(4, 2, 1, 0) - 4, (4, 2, 0, 1) - 28$ $(4, 2, 0, 0) - 24$
	$x^4 - x^3 - 2x^2 - 3$	$(4, 2, 0, 0) - 240$
	$x^5 - 2x^4 - 3x^3 - 1$	$(8, 2, 1, 0) - 16, (8, 2, 0, 1) - 496$ $(8, 2, 0, 0) - 480$
	$x^6 - x^5 - 2x^3 - 3$	$(8, 2, 0, 0) - 4032$
	$x^7 - x^6 - 2x^3 - 1$	$(16, 2, 1, 0) - 64, (16, 2, 0, 1) - 8128$ $(16, 2, 0, 0) - 8064$
	$x^8 - x^7 - 2x^6 - 3x^5 - x^3 - 3$	$(16, 2, 0, 0) - 65280$
3	$x^3 - 2x^2 - 3x - 1$	$(4, 2, 1, 0) - 16, (4, 2, 0, 1) - 112$ $(4, 2, 0, 0) - 96, (6, 3, 0, 0) - 224$
	$x^4 - 5x^3 - 2x^2 - 4x - 7$	$(6, 4, 0, 0) - 1920, (10, 4, 0, 0) - 1680$ $(14, 4, 0, 0) - 240$
	$x^5 - 2x^4 - 7x^3 - 4x^2 - 1$	$(12, 4, 1, 0) - 20, (12, 4, 0, 1) - 7130$ $(12, 4, 0, 0) - 17650, (16, 4, 1, 0) - 4$ $(16, 4, 0, 1) - 1395, (16, 4, 0, 0) - 3561$ $(20, 4, 1, 0) - 2, (20, 4, 0, 1) - 620$ $(20, 4, 0, 0) - 1362$
	$x^6 - x^5 - 4x^4 - 2x^3 - 7$	$(12, 4, 0, 0) - 28224, (16, 4, 1, 1) - 95$ $(16, 4, 1, 0) - 160, (16, 4, 0, 1) - 40540$ $(16, 4, 0, 0) - 68069, (20, 4, 0, 0) - 60480$ $(24, 4, 1, 1) - 60, (24, 4, 1, 0) - 73$ $(24, 4, 0, 1) - 14871, (24, 4, 0, 0) - 21284$ $(28, 4, 0, 0) - 24192$
	$x^7 - x^6 - 4x^5 - 6x^3 - 1$ Случайная выборка	$(16, 4, 1, 1) - 13, (16, 4, 1, 0) - 31$ $(16, 4, 0, 1) - 1326, (16, 4, 0, 0) - 1823$ $(24, 4, 0, 1) - 6456, (24, 4, 0, 0) - 23733$ $(28, 4, 0, 0) - 157562, (32, 4, 0, 1) - 37008$ $(32, 4, 0, 0) - 113372, (36, 4, 0, 0) - 71311$ $(40, 4, 0, 1) - 12834, (40, 4, 0, 0) - 37681$
	$x^8 - 6x^7 - 5x^6 - 3x^5 - 5x^4 -$ $- 2x^3 - 6x^2 - 4x - 7$ Случайная выборка	$(36, 4, 0, 0) - 32, (44, 4, 0, 0) - 6493$ $(52, 4, 0, 0) - 4968, (60, 4, 0, 0) - 1424$ $(68, 4, 0, 0) - 112$
4	$x^3 - 10x^2 - 11x - 1$	$(4, 2, 1, 0) - 120, (4, 2, 0, 1) - 840$ $(4, 2, 0, 0) - 720, (6, 3, 0, 0) - 1792$ $(8, 1, 2, 1) - 14, (8, 1, 1, 1) - 42$ $(8, 1, 0, 1) - 42, (8, 0, 3, 0) - 14$
	$x^4 - 13x^3 - 2x^2 - 4x - 15$	$(4, 2, 0, 0) - 960, (6, 4, 0, 0) - 15600$ $(8, 3, 1, 0) - 194, (8, 3, 0, 1) - 10350$ $(8, 3, 0, 0) - 17056, (8, 2, 1, 1) - 384$ $(8, 2, 1, 0) - 96, (8, 2, 0, 1) - 1056$ $(8, 2, 0, 0) - 384, (10, 4, 0, 0) - 13200$ $(12, 3, 1, 0) - 72, (12, 3, 0, 1) - 1080$ $(12, 3, 0, 0) - 1008$

Таблица (продолжение)

n	$G(x)$	$(w, d, c, b) - N$
4	$x^5 - 2x^4 - 15x^3 - 4x^2 - 8x - 1$	(10, 5, 0, 0) – 106144, (12, 4, 1, 0) – 281 (12, 4, 0, 1) – 96410, (12, 4, 0, 0) – 245549 (12, 3, 0, 0) – 4960, (14, 5, 0, 0) – 367040 (16, 4, 1, 0) – 149, (16, 4, 0, 1) – 45570 (16, 4, 0, 0) – 108041, (18, 5, 0, 0) – 34720 (20, 4, 1, 0) – 8, (20, 4, 0, 1) – 1860 (20, 4, 0, 0) – 3092, (20, 3, 0, 0) – 1984
	$x^6 - 9x^5 - 4x^4 - 2x^3 - 8x^2 - 15$ Случайная выборка	(14, 6, 0, 0) – 266, (16, 5, 0, 1) – 724 (16, 5, 0, 0) – 2864, (16, 4, 1, 0) – 2 (16, 4, 0, 1) – 26, (16, 4, 0, 0) – 33 (18, 6, 0, 0) – 22020, (20, 5, 0, 1) – 2320 (20, 5, 0, 0) – 10131, (20, 4, 0, 0) – 175 (22, 6, 0, 0) – 21633, (24, 5, 0, 1) – 826 (24, 5, 0, 0) – 3901, (24, 4, 0, 1) – 54 (24, 4, 0, 0) – 110, (26, 6, 0, 0) – 4109 (28, 5, 0, 1) – 229, (28, 5, 0, 0) – 724 (30, 6, 0, 0) – 105, (32, 5, 0, 1) – 9 (32, 5, 0, 0) – 25, (32, 4, 0, 1) – 6 (32, 4, 0, 0) – 29, (34, 6, 0, 0) – 35
	$x^7 - 9x^6 - 12x^5 - 14x^3 - 1$ Случайная выборка	(22, 7, 0, 0) – 3, (24, 6, 0, 1) – 18 (24, 6, 0, 0) – 88, (26, 7, 0, 0) – 722 (28, 6, 0, 1) – 205, (28, 6, 0, 0) – 1220 (30, 7, 0, 0) – 1976, (32, 6, 0, 1) – 212 (32, 6, 0, 0) – 1661, (34, 7, 0, 0) – 1418 (36, 6, 0, 1) – 121, (36, 6, 0, 0) – 792 (38, 7, 0, 0) – 376, (40, 6, 0, 1) – 33 (40, 6, 0, 0) – 232, (42, 7, 0, 0) – 150 (44, 6, 0, 1) – 10, (44, 6, 0, 0) – 62 (46, 7, 0, 0) – 45, (48, 6, 0, 1) – 1 (48, 6, 0, 0) – 8, (50, 7, 0, 0) – 14
	$x^8 - 14x^7 - 5x^6 - 11x^5 - 5x^4 - 10x^3 - 6x^2 - 12x - 15$ Случайная выборка	(34, 8, 0, 0) – 58, (38, 8, 0, 0) – 2593 (42, 8, 0, 0) – 20290, (46, 8, 0, 0) – 32043 (50, 8, 0, 0) – 26128, (54, 8, 0, 0) – 14802 (58, 8, 0, 0) – 7355, (62, 8, 0, 0) – 2470 (66, 8, 0, 0) – 666, (70, 8, 0, 0) – 378 (74, 8, 0, 0) – 85

Список литературы

- [1] Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В., *Основы криптографии: Учебное пособие*, М.: Гелиос АРВ, 2001, 480 с.
- [2] Кузьмин А. С., Куракин В. Л., Нечаев А. А., “Псевдослучайные и полилинейные последовательности”, *Труды по дискретной математике*, **1** (1997), 139–202.
- [3] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., “Linear recurring sequences over rings and modules”, *J. Math. Sciences*, **76**:6 (1995), 2793–2915.
- [4] Rueppel R. A., *Analysis and design of stream ciphers*, Berlin: Springer-Verlag, 1986, 244 p.
- [5] Shparlinski I. E., Winterhof A., “On the nonlinearity of linear recurrence sequences”, *Appl. Math. Letters*, **19**:4 (2006), 340–344.
- [6] Lathtonen L., Ling S., Sole P., Zinoviev D., “ $\mathbf{Z}_8$ -Kerdock codes and pseudorandom binary sequences”, *J. Complexity*, **20**:8 (2004), 318–330.
- [7] Sole P., Zinoviev D., “Galois rings and pseudorandom sequences”, *Lect. Notes Comput. Sci.*, **4887** (2007), 16–33.
- [8] Былков Д. Н., Камловский О. В., “Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент”, *Математические вопросы криптографии*, **3**:4 (2012), 25–53.
- [9] Былков Д. Н., “Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент”, *Прикладная дискретная математика. Приложение*, № 7 (2014), 59–60.
- [10] Камловский О. В., “Расстояние между двоичными представлениями линейных рекуррент над полем $GF(2^k)$ и кольцом $\mathbf{Z}_{2^n}$ ”, *Математические вопросы криптографии*, **7**:1 (2016), 73–84.
- [11] Нечаев А. А., “Код Кердока в циклической форме”, *Дискретная математика*, **1**:4 (1989), 123–139.
- [12] McDonald B. R., *Finite rings with identity*, New York: Dekker, 1974, 429 p.
- [13] Нечаев А. А., “Цикловые типы линейных подстановок над конечными коммутативными кольцами”, *Матем. сб.*, **184**:3 (1993), 21–56.
- [14] Лаксов Д., “Линейные рекуррентные последовательности над конечными полями”, *Математика. Сб. перев.*, **11**:6 (1967), 145–158.
- [15] Лидл Р., Нидеррайтер Г., *Конечные поля*, **1, 2**: М.: Мир, 1988, 822 с.
- [16] Golomb S. W., Gong G., *Signal design for good correlation. For wireless communication, Cryptography, and radar*, Cambridge, U.K.: Cambridge Univ. Press, 2005, 438 с.
- [17] Кейперс Л., Нидеррайтер Г., *Равномерное распределение последовательностей*, М.: Наука, 1985, 408 с.
- [18] *Словарь криптографических терминов*, Под ред. Б. А. Погорелова, В. Н. Сачкова, М.: МЦНМО, 2006, 92 с.
- [19] Солодовников В. И., “О совпадении класса бент-функций с классом функций, минимально близких к линейным”, *Прикладная дискретная математика*, № 3 (17) (2012), 25–33.
- [20] Бугров А. Д., “Кусочно-аффинные подстановки конечных полей”, *Прикладная дискретная математика*, № 4 (30) (2015), 5–23.

- [21] Камловский О. В., “Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа”, *Матем. сб.*, **200**:4 (2009), 31–52.
- [22] Солодовников В. И., “Бент-функции из конечной абелевой группы в конечную абелеву группу”, *Дискретная математика*, **14**:1 (2000), 99–113.
- [23] Камловский О. В., “Спектральный метод оценки числа решений систем нелинейных уравнений с линейными рекуррентными аргументами”, *Дискретная математика*, **28**:2 (2016), 27–43.
- [24] Камловский О. В., Кузьмин А. С., “Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа”, *Фундам. и прикл. математика*, **6**:4 (2000), 1083–1094.
- [25] Былков Д. Н., “Класс усложнений линейных рекуррент над кольцом Галуа, не приводящий к потере информации”, *Проблемы передачи информации*, **46**:3 (2010), 51–59.
- [26] Камловский О. В., “Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа”, *Изв. РАН. Сер. матем.*, **77**:6 (2013), 71–96.