Math-Net.Ru

Общероссийский математический портал

Д. Н. Былков, О. В. Камловский, Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент, *Матем. вопр. криптогр.*, 2012, том 3, выпуск 4, 25–53

DOI: <https://doi.org/10.4213/mvk66>

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: 3.93.64.190

26 апреля 2023 г., 06:21:30

УДК: 511.336+519.113.6

Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент

Д. Н. Былков, О. В. Камловский

ООО «Центр сертификационных исследований», Москва

Получено 20.V.2011

В работе рассматриваются семейства булевых функций, построенных на основе старших координатных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ с отмеченным характеристическим многочленом максимального периода. Для этих семейств изучаются веса функций, степень нелинейности функций, расстояния между функциями и мощности семейств. Показано, что существует изменение порядка следования аргументов функций (одинаковое для всех функций), при котором семейство содержит функции, близкие к бент-функциям.

Ключевые слова: линейные рекуррентные последовательности, старшие координатные последовательности, степень нелинейности булевой функции, расстояние до множества аффинных функций

**Parameters of Boolean functions generated by the most significant bits
of linear recurrent sequences**

D. N. Bylkov, O. V. Kamlovskii

LLC "Certification Research Center", Moscow

Abstract. The families of Boolean functions generated by the most significant bits of linear recurrent sequences over the ring $\mathbb{Z}_{2^n}$ with the marked characteristic polynomial are considered. For these families we investigate their cardinalities, the weights and the degree of nonlinearity of functions, distances between functions. We prove that there exists a rearrangement of arguments (one and the same for all functions in the family) such that the family contains functions which are close to some bent-functions.

Key words: linear recurrent sequences, most significant bit sequences, degree of nonlinearity of Boolean function, distance to the affine functions set

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 4, pp. 25–53 (Russian).

Введение

Пусть n — натуральное число, $R = \mathbb{Z}_{2^n}$, $F(x)$ — многочлен степени m над кольцом R . Назовем многочлен $F(x)$ *реверсивным*, если его свободный коэффициент обратим в кольце R . Обозначим через $\overline{F}(x)$ многочлен над полем $GF(2)$, полученный из многочлена $F(x)$ приведением всех его коэффициентов по модулю 2. Унитарный (со старшим коэффициентом, равным единице) реверсивный многочлен $F(x) \in R[x]$ называется *отмеченным*, если периоды (см., например, [1, 3]) многочленов $F(x)$ и $\overline{F}(x)$ равны: $T(F) = T(\overline{F})$. Известно, что для каждого унитарного реверсивного многочлена $f(x) \in GF(2)[x]$, не имеющего кратных корней в своем поле разложения, найдется единственный отмеченный многочлен $F(x) \in R[x]$ такой, что $\overline{F}(x) = f(x)$ (см. [1, утверждение 4.2]). Более того, существует довольно простой рекурсивный способ построения по многочлену $f(x)$ искомого многочлена $F(x)$ (см. [1, равенство (4.8)]).

Отмеченный многочлен $F(x)$ степени m , имеющий период $T(F) = 2^m - 1$, называется *отмеченным многочленом максимального периода* над кольцом R . Всюду в дальнейшем будем считать, что $F(x)$ — отмеченный многочлен максимального периода над кольцом R . Обозначим через $L_R(F)$ множество всех линейных рекуррентных последовательностей (ЛРП) над кольцом R с характеристическим многочленом $F(x)$ и через $L_R(F)^*$ — множество всех ЛРП $u \in L_R(F)$, у которых в начальном векторе $(u(0), u(1), \dots, u(m-1))$ есть хотя бы один обратимый элемент кольца R . Каждая последовательность $u \in L_R(F)^*$ будет иметь период $T(u) = T(F) = 2^m - 1$.

Подмножество $K = \{k_0, k_1\} \subset \mathbb{Z}_{2^n}$ назовем *координатным множеством* кольца $\mathbb{Z}_{2^n}$ (см., например, [2]), если числа k_0 и k_1 имеют различную четность. Всюду в дальнейшем будем считать, что k_0 — четное число, а k_1 — нечетное число. Важным примером координатного множества является *двоичное координатное множество* $K = \{0, 1\}$. Если K — координатное множество кольца $\mathbb{Z}_{2^n}$, то каждый элемент $a \in \mathbb{Z}_{2^n}$ однозначно представим в виде

$$a = a_0 + 2a_1 + 2^2a_2 + 2^3a_3 + \dots + 2^{n-1}a_{n-1}, \quad (1)$$

где $a_t \in K$ для всех $t \in \{0, 1, \dots, n-1\}$. Здесь операции сложения и умножения рассматриваются как операции в кольце $\mathbb{Z}_{2^n}$. Элемент $a_t = \varkappa_t^K(a)$, участвующий в равенстве (1), будем называть *t -й координатой* элемента a в координатном множестве K , где $t \in \{0, 1, \dots, n-1\}$.

Пусть u — последовательность элементов кольца $\mathbb{Z}_{2^n}$. Для координатного множества K кольца $\mathbb{Z}_{2^n}$ и каждого $t \in \{0, 1, \dots, n-1\}$ рассмотрим

последовательность u_t над множеством K , полученную по правилу

$$u_t(i) = \mathcal{K}_t^K(u(i)), i \geq 0.$$

Последовательность $u_t = \mathcal{K}_t^K(u)$ будем называть t -й *координатной последовательностью* последовательности u в координатном множестве K , а последовательность $u_{n-1} = \mathcal{K}_{n-1}^K(u)$ — *старшей координатной последовательностью* последовательности u в координатном множестве K .

Последовательность $u_{n-1} = \mathcal{K}_{n-1}^K(u)$ часто рассматривают как псевдослучайную последовательность, являющуюся усложнением исходной последовательности u . Последовательность u_{n-1} устроена довольно сложно, что позволяет говорить об эффекте самоусложнения в последовательности u . Так, если $K = \{0, 1\}$, то ранг последовательности u_{n-1} будет равен $O(m^{2^{n-1}})$ при $m \rightarrow \infty$ (см. [2], [3, §5], [4, теорема 7]). Как правило, для произвольного координатного множества K по последовательности u_{n-1} однозначно восстанавливается исходная последовательность u (см. [5–8]).

В связи с этим представляет интерес изучение булевых функций, построенных на основе последовательностей $u_{n-1} = \mathcal{K}_{n-1}^K(u)$, соответствующих всем ЛРП $u \in L_R(F)^*$. Обозначим через v последовательность в алфавите $\Omega = \{0, 1\}$, полученную из последовательности u_{n-1} заменой каждого ее элемента k_0 на 0 и каждого элемента k_1 на 1. Другими словами, если $r_2(a)$ — остаток от деления числа $a \in \mathbb{Z}$ на 2, то

$$v(i) = r_2(u_{n-1}(i)) = r_2(\mathcal{K}_{n-1}^K(u(i))), i \geq 0. \quad (2)$$

Зададим булеву функцию $f = f(x_1, x_2, \dots, x_m)$ от m переменных следующей таблицей:

x_1	x_2	$\dots$	x_{m-1}	x_m	$f(x_1, x_2, \dots, x_{m-1}, x_m)$
0	0	$\dots$	0	0	$r_2(\mathcal{K}_{n-1}^K(0))$
0	0	$\dots$	0	1	$v(0)$
0	0	$\dots$	1	0	$v(1)$
0	0	$\dots$	1	1	$v(2)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	1	$\dots$	1	1	$v(2^m - 2)$

В этой таблице аргументы $(x_1, x_2, \dots, x_m)$ функции f располагаются в лексикографическом порядке. Для указанной булевой функции f будем использовать обозначение $f = f_{u,K}$. Обозначим через $B_n(K, F)$ множество всех булевых функций $f = f_{u,K}$, соответствующих всем ЛРП u из множества $L_R(F)^*$.

Следует отметить, что при $n = 1$ рассматриваемый класс последовательностей $L_R(F)^*$ совпадает с множеством всех ЛРП максимального периода $2^m - 1$ над полем из двух элементов с характеристическим многочленом $F(x)$. В этом случае $K = \Omega = \mathbb{Z}_2$, $u = u_{n-1} = v$ и класс $B_n(K, F)$ состоит из $2^m - 1$ сбалансированных (имеющих вес 2^{m-1}) функций.

Определим величину σ_n следующим равенством:

$$\sigma_n = \frac{2}{\pi} \ln(2^{n-1}) + 1. \quad (3)$$

В данной работе, в частности, доказывается, что:

1) вес $\|f\|$ каждой функции $f \in B_n(K, F)$ удовлетворяет неравенствам

$$2^{m-1} - \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1} \leq \|f\| \leq 2^{m-1} + \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1}, \quad (4)$$

2) для любых функций $f_1 = f_{u_1, K}$, $f_2 = f_{u_2, K}$ из множества $B_n(K, F)$, таких, что $u_2 \neq cu_1$ для всех $c \in R^*$, расстояние Хемминга $\rho(f_1, f_2)$ между f_1 и f_2 удовлетворяет условиям

$$2^{m-1} - \sigma_n^2(2^{n-1} - 1)2^{\frac{m}{2}-1} \leq \rho(f_1, f_2) \leq 2^{m-1} + \sigma_n^2(2^{n-1} - 1)2^{\frac{m}{2}-1}, \quad (5)$$

3) при $m \geq 4n - 2$ выполнены равенства

$$|B_n(K, F)| = |L_R(F)^*| = 2^{(n-1)m} (2^m - 1), \quad (6)$$

4) если $m > 2^n$, то степень нелинейности $\deg f$ каждой булевой функции $f \in B_n(K, F)$ удовлетворяет условию $\deg f \leq m - 1$.

Кроме того, в работе рассматривается класс $B'_n(K, F)$ булевых функций от m переменных, полученный из функций класса $B_n(K, F)$ изменением порядка следования аргументов (одинакового для всех функций). В частности, для функций из класса $B'_n(K, F)$ справедливы соотношения (4), (5) и (6). Доказывается, что:

1) коэффициент нелинейности (расстояние Хэмминга до класса аффинных функций) N_f каждой булевой функции $f \in B'_n(K, F)$ удовлетворяет неравенству

$$N_f \geq 2^{m-1} - \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1},$$

2) все функции из класса $B'_2(K, F)$ являются квадратичными, причем они бент-функции, если m — четное число, и платовидные функции порядка $m - 1$, если m — нечетное число,

3) если $m > 2^n$, то степень нелинейности каждой булевой функции $f \in B'_n(K, F)$ удовлетворяет условию $\deg f = 2^{n-1}$.

Вопрос об оценке параметра N_f для функций $f \in B_n(K, F)$ пока остается нерешенным. В работе [9] показано, что при $n = 1$ и $m \rightarrow \infty$ справедливо равенство $N_f = 2^{m-1} - O(2^{7m/8} m^{1/4})$. Таким образом, даже при $n = 1$ не удастся получить оценок, похожих на оценки для функций из класса $B'_n(K, F)$.

В конце работы приводятся таблицы значений коэффициентов нелинейности N_f и степени нелинейности $\deg f$ булевых функций f из классов $B_n(K, F)$ и $B'_n(K, F)$. Показано, что при некоторых ЛРП u и координатных множествах K рассматриваемые функции являются бент-функциями.

Ранее при $n = 2$ связь последовательностей u_{n-1} с бент-функциями была замечена при изучении кода Кердока (см. [10, 11]). Множества всех столбцов значений (последних столбцов в табличном задании) булевых функций из классов $B_n(K, F)$ и $B'_n(K, F)$ образуют подкоды семейств кодов, изученных в работах [12] и [13]. В данной работе для рассматриваемых подкодов получены более точные оценки параметров. Если при $n = 2$ во всех столбцах значений булевых функций из класса $B_2(K, F)$ выколоть первую координату, то получится подкод кода, изучавшегося в работе [14], для которого было найдено кодовое расстояние.

§ 1. Веса функций

Рассмотрим вопрос о весах функций из класса $B_n(K, F)$.

Утверждение 1. Если $F(x)$ — отмеченный многочлен степени m над кольцом $R = \mathbb{Z}_{2^n}$, $T(F) = 2^m - 1$, $K = \{k_0, k_1\}$ — координатное множество кольца R , то для всех $f \in B_n(K, F)$

$$2^{m-1} - \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1} \leq \|f\| \leq 2^{m-1} + \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1},$$

где σ_n — величина, определенная равенством (3).

Доказательство. Пусть $f = f_{u,K}$, где $u \in L_R(F)^*$. Для последовательности $u_{n-1} = \chi_{n-1}^K(u)$ обозначим через $N(z, u_{n-1})$ число появлений элемента $z \in K$ среди элементов $u_{n-1}(0), u_{n-1}(1), \dots, u_{n-1}(T(F) - 1)$. Как показано в [15, теорема 2], имеют место неравенства

$$\omega(z) - \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1} \leq N(z, u_{n-1}) \leq \omega(z) + \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1},$$

где

$$\omega(z) = \begin{cases} 2^{m-1} - 1, & \text{если } z = \chi_{n-1}^K(0), \\ 2^{m-1}, & \text{если } z \neq \chi_{n-1}^K(0). \end{cases}$$

Учитывая определение булевой функции $\hat{f} = \hat{f}_{u,K}$, получим

$$\|\hat{f}\| = \begin{cases} N(k_1, u_{n-1}) + 1, & \text{если } k_1 = \mathcal{K}_{n-1}^K(0), \\ N(k_1, u_{n-1}), & \text{если } k_1 \neq \mathcal{K}_{n-1}^K(0). \end{cases}$$

Таким образом,

$$2^{m-1} - \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1} \leq \|\hat{f}\| \leq 2^{m-1} + \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1}. \quad \square$$

Полученные оценки (верхняя и нижняя) при $n = 1$ обращаются в равенства и устанавливают соотношение $\|\hat{f}\| = 2^{m-1}$. Вопрос о том, всегда ли при $n \geq 2$ в классе $B_n(K, F)$ будут существовать сбалансированные функции, в общем случае имеет отрицательный ответ. Воспользуемся полным описанием частот появлений элементов на циклах ЛРП при $n = 2$, полученным в работе [16] (см. также [17]), и вытекающим отсюда полным описанием частот элементов в их старших координатных последовательностях u_{n-1} (см. [15, следствие 1]).

Если $m = 2\lambda$, то при каждом $K = \{k_0, k_1\}$ и каждом отмеченном многочлене $F(x)$ максимального периода над кольцом $\mathbb{Z}_4$ в классе $B_n(K, F)$ возможны лишь два типа весов, представленных в следующей таблице:

Вес функции $\hat{f} = \hat{f}_{u,K}$	Число ЛРП $u \in L_R(F)^*$
$2^{m-1} - 2^{\lambda-1}$	$(2^{m-1} + (1 - k_0)2^{\lambda-1})(2^m - 1)$
$2^{m-1} + 2^{\lambda-1}$	$(2^{m-1} + (k_0 - 1)2^{\lambda-1})(2^m - 1)$

Если $m = 2\lambda + 1$, то при каждом $K = \{k_0, k_1\}$ и каждом отмеченном многочлене $F(x)$ максимального периода над кольцом $\mathbb{Z}_4$ в классе $B_n(K, F)$ возможны лишь три типа весов, представленных в следующей таблице:

Вес функции $\hat{f} = \hat{f}_{u,K}$	Число ЛРП $u \in L_R(F)^*$
2^{m-1}	$2^{m-1}(2^m - 1)$
$2^{m-1} - 2^\lambda$	$(2^{m-2} + (1 - k_0)2^{\lambda-1})(2^m - 1)$
$2^{m-1} + 2^\lambda$	$(2^{m-2} + (k_0 - 1)2^{\lambda-1})(2^m - 1)$

Таким образом, при $n = 2$ и любом четном значении m в классе $B_n(K, F)$ отсутствуют сбалансированные функции, а при $n = 2$ и любом нечетном значении m ровно половина функций из класса $B_n(K, F)$ являются сбалансированными.

§ 2. Кросс-корреляционная функция старших координатных последовательностей

Пусть $F(x)$ — отмеченный многочлен степени m над кольцом $R = \mathbb{Z}_{2^n}$, $T(F) = T = 2^m - 1$. Важные свойства класса $B_n(K, F)$ удается описать на основе свойств координатных последовательностей ЛРП $u \in L_R(F)^*$.

Рассмотрим произвольные координатные множества K_1, K_2 кольца R , последовательности $u_1, u_2 \in L_R(F)^*$ и двоичные последовательности v_1, v_2 , полученные по правилу

$$v_1(i) = r_2(\chi_{n-1}^{K_1}(u_1(i))), \quad v_2(i) = r_2(\chi_{n-1}^{K_2}(u_2(i))), \quad i \geq 0.$$

Нас будет интересовать оценка модуля кросс-корреляционной функции $C_{v_1, v_2}(\tau)$ последовательностей v_1 и v_2 , которая определяется для всех $\tau \in \{0, 1, \dots, T-1\}$ равенством

$$C_{v_1, v_2}(\tau) = \sum_{i=0}^{T-1} (-1)^{v_1(i) - v_2(i+\tau)}. \quad (7)$$

Введем на множестве $L_R(F)^*$ бинарное отношение $\sim$, положив $u_1 \sim u_2$ для последовательностей $u_1, u_2 \in L_R(F)^*$ тогда и только тогда, когда найдутся такие $c \in R^*$ и $t \in \mathbb{N}_0$, что

$$u_1 = cx^t u_2, \quad (8)$$

т. е. $u_1(i) = cu_2(i+t)$ для всех $i \geq 0$. Очевидно, что отношение $\sim$ является отношением эквивалентности на множестве $L_R(F)^*$.

Утверждение 2. Пусть $u_1 \sim u_2$, тогда найдутся единственные элементы $c \in R^*$ и $t \in \{0, 1, \dots, T-1\}$, для которых $u_1 = cx^t u_2$.

Доказательство. Допустим, что $u_1 = c_1 x^{t_1} u_2$ и $u_1 = c_2 x^{t_2} u_2$, где $c_1, c_2 \in R^*$, $t_1, t_2 \in \{0, 1, \dots, T-1\}$. Тогда $c_1 x^{t_1} u_2 - c_2 x^{t_2} u_2 = (0)$. Представим ЛРП u_2 с помощью функции след

$$u_2(i) = \text{Tr}_R^S(b\alpha^i), \quad i \geq 0,$$

где $S = GR(2^{mn}, 2^n)$ — расширение Галуа кольца R , α — корень многочлена $F(x)$ в кольце S , $b \in S^*$ (см. [11]). Тогда получим равенства

$$\text{Tr}_R^S(b(c_1 \alpha^{t_1} - c_2 \alpha^{t_2}) \alpha^i) = 0, \quad i \geq 0.$$

В силу однозначности представления ЛРП из множества $L_R(F)$ функцией след это возможно только при $b(c_1 \alpha^{t_1} - c_2 \alpha^{t_2}) = 0$. Так как элемент b обратим,

то приходим к равенству $c_1 \alpha^{t_1} = c_2 \alpha^{t_2}$, т. е. $c_1 c_2^{-1} = \alpha^{t_2 - t_1}$. Ввиду того, что $|R^*| = 2^{n-1}$ и мультипликативный порядок $\text{ord } \alpha$ элемента α удовлетворяет условию $\text{ord } \alpha = T = 2^m - 1$, последнее равенство возможно только при $c_1 = c_2$ и $t_1 = t_2$. $\square$

Из доказанного утверждения следует, что каждый из рассматриваемых классов эквивалентных последовательностей имеет мощность $2^{n-1}T$, а число классов эквивалентных последовательностей равно $2^{(n-1)(m-1)}$.

Рассмотрим аддитивный характер χ кольца $\mathbb{Z}_{2^n}$, определенный на элементах этого кольца равенством

$$\chi(x) = e^{2\pi i \frac{x}{2^n}}. \quad (9)$$

Нам понадобится следующее вспомогательное утверждение.

Лемма 1 ([15]). Пусть K — координатное множество кольца $\mathbb{Z}_{2^n}$. Тогда для всех $a \in \mathbb{Z}_{2^n}$ имеет место равенство

$$(-1)^{\mathfrak{K}_{n-1}^K(a)} = \sum_{j=0}^{2^n-1} \mu_{j,K} \chi(aj), \quad (10)$$

в котором комплексные числа $\mu_{j,K}$ задаются равенствами

$$\mu_{j,K} = \frac{1}{2^n} \sum_{s=0}^{2^n-1} (-1)^{\mathfrak{K}_{n-1}^K(s)} \chi(-sj), \quad (11)$$

причем

$$\sum_{j=0}^{2^n-1} |\mu_{j,K}| = \sum_{j \in R^*} |\mu_{j,K}| \leq \sigma_n, \quad (12)$$

где величина σ_n определена равенством (3).

Лемма 2 ([18, 19]). Если $F(x)$ — отмеченный многочлен степени m над кольцом $R = \mathbb{Z}_{2^n}$, $T(F) = T = 2^m - 1$, u — ненулевая последовательность из $L_R(F)$, χ — аддитивный характер кольца R , определенный равенством (9), то

$$\left| \sum_{i=0}^{T-1} \chi(u(i)) + 1 \right| \leq (2^{n-1} - 1) 2^{\frac{m}{2}}.$$

Теорема 1. Для кросс-корреляционной функции $C_{v_1, v_2}(\tau)$, определенной равенством (7), имеет место оценка

$$\left| C_{v_1, v_2}(\tau) + (-1)^{\mathfrak{K}_{n-1}^{K_1}(0) + \mathfrak{K}_{n-1}^{K_2}(0)} \right| \leq \sigma_n^2 (2^{n-1} - 1) 2^{\frac{m}{2}},$$

которая справедлива для всех $\tau \in \{0, 1, \dots, T-1\}$, если $u_1 \not\sim u_2$, и для всех $\tau \in \{0, 1, \dots, T-1\}$, $\tau \neq t$, где t удовлетворяет равенству (8), если $u_1 \sim u_2$.

Доказательство. Справедливо равенство

$$C_{v_1, v_2}(\tau) = \sum_{i=0}^{T-1} (-1)^{\varkappa_{n-1}^{K_1}(u_1(i))} (-1)^{\varkappa_{n-1}^{K_2}(u_2(i+\tau))},$$

из которого с помощью соотношения (10) получим

$$C_{v_1, v_2}(\tau) = \sum_{i=0}^{T-1} \sum_{j_1=0}^{2^n-1} \mu_{j_1, K_1} \chi(u_1(i)j_1) \sum_{j_2=0}^{2^n-1} \mu_{j_2, K_2} \chi(u_2(i+\tau)j_2).$$

Изменив порядок суммирования, находим что

$$C_{v_1, v_2}(\tau) = \sum_{j_1, j_2=0}^{2^n-1} \mu_{j_1, K_1} \mu_{j_2, K_2} \sum_{i=0}^{T-1} \chi(u_{j_1, j_2, \tau}(i)), \quad (13)$$

где $u_{j_1, j_2, \tau}$ — последовательность элементов кольца $\mathbb{Z}_{2^n}$, определенная при всех $j_1, j_2 \in \mathbb{Z}_{2^n}$, $\tau \in \mathbb{N}_0$ равенством

$$u_{j_1, j_2, \tau}(i) = u_1(i)j_1 + u_2(i+\tau)j_2, \quad i \geq 0.$$

Подставляя в равенство (10) значение $a = 0$, получим

$$\sum_{j_1, j_2=0}^{2^n-1} \mu_{j_1, K_1} \mu_{j_2, K_2} = \left(\sum_{j_1=0}^{2^n-1} \mu_{j_1, K_1} \right) \left(\sum_{j_2=0}^{2^n-1} \mu_{j_2, K_2} \right) = (-1)^{\varkappa_{n-1}^{K_1}(0) + \varkappa_{n-1}^{K_2}(0)}.$$

Поэтому можно переписать равенство (13) в виде

$$C_{v_1, v_2}(\tau) + (-1)^{\varkappa_{n-1}^{K_1}(0) + \varkappa_{n-1}^{K_2}(0)} = \sum_{j_1, j_2=0}^{2^n-1} \mu_{j_1, K} \mu_{j_2, K} \left(\sum_{i=0}^{T-1} \chi(u_{j_1, j_2, \tau}(i)) + 1 \right).$$

Тогда

$$\left| C_{v_1, v_2}(\tau) + (-1)^{\varkappa_{n-1}^{K_1}(0) + \varkappa_{n-1}^{K_2}(0)} \right| \leq \sum_{j_1, j_2=0}^{2^n-1} |\mu_{j_1, K} \mu_{j_2, K}| \left| \sum_{i=0}^{T-1} \chi(u_{j_1, j_2, \tau}(i)) + 1 \right|. \quad (14)$$

Согласно равенству (12) коэффициенты $\mu_{j, K} = 0$ при всех $j \in 2\mathbb{Z}_{2^n}$, поэтому в соотношении (14) достаточно рассматривать суммирование по всем

$j_1, j_2 \in R^*$. При всех таких элементах по выбору τ последовательность $v_{j_1, j_2, \tau}$ является ненулевой ЛРП из множества $L_R(F)$, поэтому согласно лемме 2

$$\left| \sum_{i=0}^{T-1} \chi(u_{j_1, j_2, \tau}(i)) + 1 \right| \leq (2^{n-1} - 1)2^{\frac{m}{2}}.$$

С использованием соотношения (12) получим

$$\sum_{j_1, j_2=0}^{2^n-1} |\mu_{j_1, K_1} \mu_{j_2, K_2}| = \left(\sum_{j_1=0}^{2^n-1} |\mu_{j_1, K_1}| \right) \left(\sum_{j_2=0}^{2^n-1} |\mu_{j_2, K_2}| \right) \leq \sigma_n^2.$$

Таким образом,

$$\left| C_{v_1, v_2}(\tau) + (-1)^{\varkappa_{n-1}^{K_1}(0) + \varkappa_{n-1}^{K_2}(0)} \right| \leq \sigma_n^2 (2^{n-1} - 1)2^{\frac{m}{2}}. \quad \square$$

Теорема 1 обобщает оценку из [13, теорема 7.1] на случай произвольного координатного множества K . Кроме того, для случая $K = \{0, 1\}$ она усиливает соответствующую оценку.

Следствие 1. Пусть $F(x)$ — отмеченный многочлен степени m максимального периода над кольцом $R = \mathbb{Z}_{2^n}$, K — координатное множество кольца R , $u \in L_R(F)^*$, $u_{n-1} = \varkappa_{n-1}^K(u)$, v — двоичная последовательность, полученная из u_{n-1} по правилу (2), тогда при условии

$$m \geq 4 \log_2(n+1) + 2n - 6, \quad (15)$$

выполнены равенства

$$T(v) = T(u_{n-1}) = T(u) = T(F) = 2^m - 1.$$

Доказательство. Очевидно, что $T(v) \mid T(u_{n-1})$, $T(u_{n-1}) \mid T(u)$, $T(u) = T(F)$, поэтому достаточно доказать, что $T(v) = T(u)$. Допустим, что $T(v) = \tau$ и $\tau < T = T(F)$, тогда, положив $K_1 = K_2 = K$, $u_1 = u_2 = u$ в условии теоремы 1, получим $v_1 = v_2 = v$ и неравенство

$$|C_{v_1, v_2}(\tau) + 1| \leq \sigma_n^2 (2^{n-1} - 1)2^{\frac{m}{2}}.$$

С другой стороны, из равенства $v = x^\tau v$ имеем $C_{v_1, v_2}(\tau) = 2^m - 1$, а значит,

$$2^m \leq \sigma_n^2 (2^{n-1} - 1)2^{\frac{m}{2}}. \quad (16)$$

Полученное неравенство противоречит условию, поскольку справедливо соотношение $\sigma_n \leq (n+1)/2$. $\square$

Таким образом, если при условии $m \geq 4 \log_2(n+1) + 2n - 6$ в столбце, определяющем значения булевой функции $f = f_{u,K}$, исключить первый элемент, то в полученном столбце будет отсутствовать эффект сокращения периода.

§ 3. Расстояния между функциями

Пусть $F(x)$ — отмеченный многочлен степени m над кольцом $R = \mathbb{Z}_{2^n}$, $T(F) = 2^m - 1$. С помощью теоремы 1 получим теперь оценки расстояния $\rho(f_1, f_2)$ (числа векторов $\vec{a} = (a_1, a_2, \dots, a_m) \in \Omega^m$, для которых $f_1(\vec{a}) \neq f_2(\vec{a})$) между функциями f_1 и f_2 из класса $B_n(K, F)$.

Рассмотрим более общую задачу. Пусть K_1, K_2 — координатные множества кольца $R = \mathbb{Z}_{2^n}$, u_1, u_2 — произвольные ЛРП над кольцом R с характеристическим многочленом $F(x)$, $f_1 = f_{u_1, K_1}$, $f_2 = f_{u_2, K_2}$. Будем говорить, что последовательности u_1 и u_2 пропорциональны относительно R^* , если найдется такой элемент $c \in R^*$, что $u_1 = cu_2$.

Утверждение 3. Если ЛРП $u_1, u_2 \in L_R(F)^*$ не пропорциональны относительно R^* , то расстояние между булевыми функциями $f_1 = f_{u_1, K_1}$ и $f_2 = f_{u_2, K_2}$ удовлетворяет неравенствам

$$2^{m-1} - \sigma_n^2(2^{n-1} - 1)2^{\frac{m}{2}-1} \leq \rho(f_1, f_2) \leq 2^{m-1} + \sigma_n^2(2^{n-1} - 1)2^{\frac{m}{2}-1},$$

где величина σ_n определена равенством (3). В частности, при условии (15) $f_1 \neq f_2$.

Доказательство. Рассмотрим двоичные последовательности v_1 и v_2 , задаваемые равенствами

$$v_1(i) = r_2(\chi_{n-1}^{K_1}(u_1(i))), \quad v_2(i) = r_2(\chi_{n-1}^{K_2}(u_2(i))), \quad i \geq 0.$$

Заметим, что для всех $x, y \in \Omega = \{0, 1\}$ справедливы равенства

$$\frac{1}{2}(1 + (-1)^{x \pm y}) = \begin{cases} 1, & \text{если } x = y, \\ 0, & \text{если } x \neq y, \end{cases}$$

тогда

$$2^m - \rho(f_1, f_2) = \frac{1}{2}(1 + (-1)^{\chi_{n-1}^{K_1}(0) + \chi_{n-1}^{K_2}(0)}) + \frac{1}{2} \sum_{i=0}^{2^m-2} (1 + (-1)^{v_1(i) - v_2(i)}).$$

Отсюда с использованием равенства (7) получим

$$2^{m-1} - \rho(f_1, f_2) = \frac{1}{2} \left(C_{v_1, v_2}(0) + (-1)^{\varkappa_{n-1}^{K_1}(0) + \varkappa_{n-1}^{K_2}(0)} \right)$$

и, согласно теореме 1,

$$\left| 2^{m-1} - \rho(f_1, f_2) \right| \leq \sigma_n^2(2^{n-1} - 1)2^{\frac{m}{2}-1}.$$

Таким образом,

$$2^{m-1} - \sigma_n^2(2^{n-1} - 1)2^{\frac{m}{2}-1} \leq \rho(f_1, f_2) \leq 2^{m-1} + \sigma_n^2(2^{n-1} - 1)2^{\frac{m}{2}-1}.$$

Полученная нижняя оценка величины $\rho(f_1, f_2)$ больше нуля тогда и только тогда, когда не выполнено соотношение (16), поэтому $f_1 \neq f_2$ при условии (15). $\square$

§ 4. Мощность класса булевых функций

Рассмотрим вопрос о числе функций в классе $B_n(K, F)$. Утверждение 3 не позволяет сделать вывод о том, что все функции в классе $B_n(K, F)$ различны, так как в нем есть функции, соответствующие пропорциональным ЛРП относительно R^* .

Утверждение 4. Пусть $F(x)$ — отмеченный многочлен степени m максимального периода над кольцом $R = \mathbb{Z}_{2^n}$, K — координатное множество кольца R , тогда при $m \geq 4n - 2$ все функции в классе $B_n(K, F)$ различны и имеют место равенства

$$|B_n(K, F)| = |L_R(F)^*| = 2^{(n-1)m}(2^m - 1).$$

Доказательство. Воспользуемся результатом работы [8], из которого следует, что если в каждой ЛРП $u \in L_R(F)^*$ появляются все элементы кольца R , то $\varkappa_{n-1}^K(u_1) \neq \varkappa_{n-1}^K(u_2)$ для любых различных ЛРП $u_1, u_2 \in L_R(F)$. Остается заметить, что если $m \geq 4n - 2$, то в каждой ЛРП $u \in L_R(F)^*$ появляются все элементы кольца R (см. [19, следствие 5]). $\square$

Отметим, что для случая $n = 2$ условия утверждения 4 можно ослабить. Из описания частот появлений элементов на циклах ЛРП с отмеченным характеристическим многочленом $F(x)$ максимального периода над кольцом $\mathbb{Z}_4$ (см. [16]) следует, что при $m \geq 3$ в рассматриваемых ЛРП появляются все элементы кольца $\mathbb{Z}_4$. Таким образом, $|B_n(K, F)| = 4^m - 2^m$ при $n = 2$ и всех $m \geq 3$.

§ 5. Соотношения между семействами при различных координатных множествах

Рассмотрим вопрос о том, как соотносятся между собой семейства функций $B_n(K_1, F)$ и $B_n(K_2, F)$ при различных координатных множествах K_1, K_2 . Для каждого натурального числа d обозначим через $\stackrel{d}{\equiv}$ отношение сравнимости по идеалу dR в кольце $R = \mathbb{Z}_{2^n}$.

Нам потребуется следующий вспомогательный результат.

Лемма 3. Пусть K — координатное множество кольца R и элемент $x \in R$ имеет двоичное представление

$$x = x_0 + 2x_1 + \dots + 2^{n-1}x_{n-1}.$$

Тогда справедливо сравнение

$$\varkappa_{n-1}^K(x) \stackrel{2}{\equiv} x_{n-1} + g^K(x_0, \dots, x_{n-2}), \quad (17)$$

причем $g_0^K = g^K(0, \dots, 0) \stackrel{2}{\equiv} \varkappa_{n-1}^K(0)$.

Доказательство. Справедливо соотношение

$$2^{n-1}\varkappa_{n-1}^K(x) + \sum_{i=0}^{n-2} 2^i \varkappa_i^K(x) \stackrel{2^n}{\equiv} 2^{n-1}x_{n-1} + \sum_{i=0}^{n-2} 2^i x_i.$$

Отсюда имеем

$$\varkappa_{n-1}^K(x) \stackrel{2}{\equiv} x_{n-1} + \varkappa_{n-1}^{\{0,1\}} \left(\sum_{i=0}^{n-2} 2^i (x_i - \varkappa_i^K(x)) \right).$$

В силу того, что элемент $\sum_{i=0}^{n-2} 2^i (x_i - \varkappa_i^K(x))$ зависит лишь от $x \pmod{2^{n-1}}$ и координатного множества K , корректно обозначение

$$g^K(x_0, \dots, x_{n-2}) = \varkappa_{n-1}^{\{0,1\}} \left(\sum_{i=0}^{n-2} 2^i (x_i - \varkappa_i^K(x)) \right).$$

Подставляя в соотношение (17) элемент $x = 0$, получаем $g_0^K = g^K(0, \dots, 0) \stackrel{2}{\equiv} \varkappa_{n-1}^K(0)$. $\square$

Непосредственно из леммы 3 получим следующий результат.

Следствие 2.

$$\varkappa_{n-1}^{K_2}(x) \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(x) + g^{K_1}(x_0, \dots, x_{n-2}) + g^{K_2}(x_0, \dots, x_{n-2}).$$

Для каждой булевой функции f обозначим через $\bar{f}$ булеву функцию, противоположную к f (инвертированную), т. е. такую, что $\bar{f}(a_1, \dots, a_m) \neq f(a_1, \dots, a_m)$ для всех двоичных векторов $(a_1, \dots, a_m) \in \Omega^m$.

Утверждение 5. Пусть K_1, K_2 – координатные множества кольца R , тогда:

1) если $g^{K_1}(x_0, \dots, x_{n-2}) + g^{K_2}(x_0, \dots, x_{n-2}) \stackrel{2}{\equiv} 1$, то множество функций $B_n(K_2, F)$ получается инвертированием каждой функции из $B_n(K_1, F)$;

2) если $g^{K_1}(x_0, \dots, x_{n-2}) + g^{K_2}(x_0, \dots, x_{n-2}) \stackrel{2}{\equiv} x_0$, то $B_n(K_1, F) = B_n(K_2, F)$.

Доказательство. Пусть выполнено условие п. (1), тогда $\varkappa_{n-1}^{K_2}(x) \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(x) + 1$. Таким образом, для каждой ЛРП $u \in L_R(F)$ верно соотношение $\varkappa_{n-1}^{K_2}(u(i)) \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(u(i)) + 1, i \geq 0$, и поэтому $\bar{f}_{u, K_1} = \bar{f}_{u, K_2}$.

Пусть выполнено условие п. (2), тогда $\varkappa_{n-1}^{K_2}(x) \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(x) + x_0$. Отсюда и из сравнений $x_0 \stackrel{2}{\equiv} \varkappa_0^{K_1}(x) \stackrel{2}{\equiv} \varkappa_0^{K_2}(x)$ вытекает соотношение $\varkappa_{n-1}^{K_2}(x + 2^{n-1}x_0) \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(x)$. Для каждой ЛРП $u \in L_R(F)$ положим $u' = (1 + 2^{n-1})u = u + 2^{n-1}u_0$. Тогда u' – ЛРП над R с характеристическим многочленом $F(x)$ и справедливо сравнение $\varkappa_{n-1}^{K_2}(u') \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(u)$. Отсюда следует, что $\bar{f}_{u, K_1} = \bar{f}_{u', K_2}$. $\square$

Покажем, что существуют координатные множества, удовлетворяющие условиям утверждения 5.

Утверждение 6. Если $K_1 = \{k_0, k_1\}, K_2 = \{k_0 + 2^{n-1}, k_1 + 2^{n-1}\}$, то для произвольного $x \in R$ справедливо сравнение

$$\varkappa_{n-1}^{K_2}(x) \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(x) + 1. \quad (18)$$

Доказательство. Согласно [15, утверждение 1], для всех $x \in R$ имеют место соотношения

$$\varkappa_{n-1}^{K_1}(x) = k_0 \Leftrightarrow x \in M_1, \quad \varkappa_{n-1}^{K_2}(x) = k_0 + 2^{n-1} \Leftrightarrow x \in M_2,$$

где

$$M_1 = \{-k_0 + (k_1 - k_0)i : i = 0, 1, \dots, 2^{n-1} - 1\},$$

$$M_2 = \{-k_0 - 2^{n-1} + (k_1 - k_0)j : j = 0, 1, \dots, 2^{n-1} - 1\}.$$

Множества M_1 и M_2 не пересекаются. Действительно, из равенства $-k_0 + (k_1 - k_0)i = -k_0 - 2^{n-1} + (k_1 - k_0)j$ следует $(k_1 - k_0)(j - i) = 2^{n-1}$, что в силу обратимости элемента $k_1 - k_0$ влечет соотношение $j - i \in 2^{n-1}R$. Значит, для всех $x \in R$

$$r_2(\varkappa_{n-1}^{K_1}(x)) = 0 \Leftrightarrow r_2(\varkappa_{n-1}^{K_2}(x)) = 1. \quad \square$$

Из доказанного утверждения следует, что верхняя оценка величины $\rho(f_1, f_2)$, полученная в утверждении 3, станет неверной, если рассмотреть равные ЛРП u_1 и u_2 и подобрать K_1 и K_2 как в утверждении 6.

Утверждение 7. Если $K_1 = \{k_0, k_1\}$, $K_2 = \{k_0, k_1 + 2^{n-1}\}$, то для произвольного $x \in R$ справедливо сравнение

$$\varkappa_{n-1}^{K_2}(x) \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(x) + \varkappa_0^{K_1}(x). \quad (19)$$

Доказательство. Введем обозначение $x_i = \varkappa_i^{K_1}(x)$, $\widehat{x}_i = \varkappa_i^{K_2}(x)$, $i = 0, \dots, n-1$. Рассмотрим случай, когда $x_0 = \widehat{x}_0 = k_0$. Покажем, что справедливо сравнение $x_{n-1} \stackrel{2}{\equiv} \widehat{x}_{n-1}$. Зададим элементы $x'_i \in K_2$, $i = 0, \dots, n-1$, равенствами

$$x'_i = \varkappa_0^{K_2}(x_i) = \begin{cases} k_0, & \text{если } x_i = k_0, \\ k_1 + 2^{n-1}, & \text{если } x_i = k_1. \end{cases}$$

Тогда справедливы соотношения: $x_0 = x'_0$, $2^i x_i = 2^i x'_i$, $i = 1, \dots, n-1$. Отсюда следует равенство $x = \sum_{i=0}^{n-1} 2^i x'_i$, т. е. $x'_i = \varkappa_i^{K_2}(x)$, $i = 0, \dots, n-1$, и $x'_{n-1} = \varkappa_{n-1}^{K_2}(x) \stackrel{2}{\equiv} x_{n-1}$.

Теперь рассмотрим случай, когда $x_0 = k_1$, $\widehat{x}_0 = k_1 + 2^{n-1}$. Покажем, что справедливо сравнение $\widehat{x}_{n-1} \stackrel{2}{\equiv} x_{n-1} + 1$. Положим $x'_i = \varkappa_0^{K_2}(x_i)$, $i = 0, \dots, n-2$,

$$x'_{n-1} = \begin{cases} k_0, & \text{если } x_{n-1} = k_1, \\ k_1 + 2^{n-1}, & \text{если } x_{n-1} = k_0; \end{cases}$$

т. е. $x'_{n-1} \stackrel{2}{\equiv} x_{n-1} + 1$. В этом случае равенство $x = \sum_{i=0}^{n-1} 2^i x'_i$ доказывается непосредственной проверкой. Таким образом, $\varkappa_{n-1}^{K_2}(x) \stackrel{2}{\equiv} \varkappa_{n-1}^{K_1}(x) + \varkappa_0^{K_1}(x)$. $\square$

ЗАМЕЧАНИЕ 1. Из утверждения 5 следует, что для исследования семейств булевых функций $B_n(K, F)$ достаточно рассмотреть лишь четверть из всех координатных множеств K кольца R . В частности, для кольца $R = \mathbb{Z}_4$ — лишь двоичное координатное множество.

§ 6. Выбор упорядочивания и оценка коэффициента нелинейности

Рассмотрим другое упорядочивание аргументов булевых функций из класса $B_n(K, F)$, при котором можно достаточно хорошо оценить снизу расстояние от полученных функций f до класса всех аффинных функций. Для этого потребуется изучить коэффициенты Уолша–Адамара $W_f(\vec{a})$ (см., например, [20, стр. 77]), которые для каждого вектора $\vec{a} \in \Omega^m$, где $\Omega = \{0, 1\}$, определяются равенством

$$W_f(\vec{a}) = \sum_{\vec{x} \in \Omega^m} (-1)^{f(\vec{x}) \oplus \vec{a}\vec{x}} = \sum_{(x_1, \dots, x_m) \in \Omega^m} (-1)^{f(x_1, \dots, x_m) \oplus a_1 x_1 \oplus \dots \oplus a_m x_m}.$$

Тогда расстояние N_f от функции f до класса всех аффинных функций (коэффициент нелинейности функции f) находится по формуле

$$N_f = 2^{m-1} - \frac{1}{2} \max_{\vec{a} \in \Omega^m} |W_f(\vec{a})|.$$

Обозначим через $S = GR(2^{mn}, 2^n)$ кольцо Галуа характеристики 2^n , состоящее из 2^{mn} элементов и являющееся расширением кольца $R = \mathbb{Z}_{2^n}$ корнем α многочлена $F(x)$ (см. [11]). Пусть $\Gamma(S) = \{x \in S : x^{2^m} = x\}$ — 2-адическое координатное множество кольца S . Каждый элемент s кольца S однозначно представим в виде

$$s = s_0 + 2s_1 + 2^2s_2 + \dots + 2^{n-1}s_{n-1},$$

где $s_i \in \Gamma(S)$, $i = 0, 1, \dots, n-1$. Определим при каждом $i = 0, 1, \dots, n-1$ отображение $\gamma_i: S \rightarrow \Gamma(S)$ равенством $\gamma_i(s) = s_i$ для всех $s \in S$.

Множество $\Gamma(S)^* = \Gamma(S) \setminus \{0\}$ замкнуто относительно умножения элементов кольца S и является циклической группой порядка $2^m - 1$. Зададим на множестве $\Gamma(S)$ операцию $\oplus$ равенством

$$c \oplus d = \gamma_0(c + d),$$

тогда $(\Gamma(S), \oplus, \cdot)$ — поле из 2^m элементов (см. [11]).

Пусть $\alpha_1, \dots, \alpha_m$ — самодвойственный базис поля $\Gamma(S)$, т. е.

$$\mathrm{tr}_2^{2^m}(\alpha_i \alpha_j) = \begin{cases} 1, & \text{если } i = j, \\ 0, & \text{если } i \neq j, \end{cases}$$

где $\mathrm{tr}_2^{2^m}$ — функция след из поля $\Gamma(S)$ в поле $GF(2)$. Такой базис существует для всех значений m (см. [21]).

Пусть $F(x)$ — отмеченный многочлен максимального периода над кольцом $R = \mathbb{Z}_{2^n}$, имеющий степень m . Каждую ЛРП $u \in L_R(F)^*$ представим с использованием функции след

$$u(i) = \mathrm{Tr}_R^S(b\alpha^i), \quad i \geq 0,$$

где $\alpha \in \Gamma(S)$ — корень многочлена $F(x)$, а b — некоторый обратимый элемент кольца S . Определим для каждого $i \in \{0, 1, \dots, 2^m - 2\}$ двоичный вектор $(x_1(i), \dots, x_m(i))$, исходя из равенства

$$\alpha^i = x_1(i)\alpha_1 \oplus \dots \oplus x_m(i)\alpha_m.$$

Зададим булеву функцию f от m переменных, положив

$$\begin{aligned} f(0, \dots, 0) &= r_2(\mathcal{K}_{n-1}^K(0)), \\ f(x_1(i), \dots, x_m(i)) &= r_2(\mathcal{K}_{n-1}^K(u(i))), \quad i = 0, 1, \dots, 2^m - 2. \end{aligned}$$

Булева функция f получается из булевой функции $f_{u,K}$ изменением порядка следования аргументов. Для построенной булевой функции f будем использовать обозначение $f = f'_{u,K}$. Множество всех булевых функций $f'_{u,K}$, соответствующих всем ЛРП $u \in L_R(F)^*$, обозначим через $B'_n(K, F)$. Класс $B'_n(K, F)$ получается из класса $B_n(K, F)$ изменением порядка следования аргументов функций, которое зависит только от многочлена $F(x)$. Отсюда следует, что для булевых функций f из класса $B'_n(K, F)$ справедливы аналогии утверждений 1, 3, 4, 5.

Теорема 2. Для коэффициентов $W_f(\vec{a})$ Уолша–Адамара булевой функции $f = f'_{u,K}$ при всех $n \geq 2$ имеет место оценка

$$|W_f(\vec{a})| \leq \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}},$$

где величина σ_n определена равенством (3), а m — степень многочлена $F(x)$.

Доказательство. Пусть $\vec{x} = (x_1(i), \dots, x_m(i))$, $x = x_1(i)\alpha_1 \oplus \dots \oplus x_m(i)\alpha_m = \alpha^i$, $i = 0, 1, \dots, 2^m - 2$, $\vec{a} = (a_1, \dots, a_m)$, $a = a_1\alpha_1 \oplus \dots \oplus a_m\alpha_m$, тогда, учитывая равенство

$$\mathrm{tr}_2^{2^m}(ax) = a_1x_1(i) \oplus \dots \oplus a_mx_m(i) = \vec{a}\vec{x},$$

справедливое для всех $x \in \Gamma(S)^*$, получим

$$W_f(\vec{a}) = \sum_{\vec{x} \in \Omega^m} (-1)^{\vec{a}\vec{x} \oplus f(\vec{x})} = (-1)^{z_{n-1}^K(0)} + \sum_{x \in \Gamma(S)^*} (-1)^{\text{tr}_2^{2^m}(ax)} (-1)^{z_{n-1}^K(\text{Tr}_R^S(bx))}. \quad (20)$$

Используя соотношение

$$(-1)^{\text{tr}_2^{2^m}(ax)} = \chi(\text{Tr}_R^S(2^{n-1}ax)),$$

где χ — характер, определенный равенством (9), и равенство (10), будем иметь

$$W_f(\vec{a}) = (-1)^{z_{n-1}^K(0)} + \sum_{x \in \Gamma(S)^*} \chi(\text{Tr}_R^S(2^{n-1}ax)) \sum_{j \in R} \mu_{j,K} \chi(\text{Tr}_R^S(bx)j). \quad (21)$$

Отсюда следует, что

$$W_f(\vec{a}) = \sum_{j \in R} \mu_{j,K} \left(\sum_{x \in \Gamma(S)^*} \chi(\text{Tr}_R^S((2^{n-1}a + bj)x)) + 1 \right).$$

Согласно соотношению (12), в полученном равенстве достаточно ограничиться суммированием по всем $j \in R^*$. Для всех таких j при $n \geq 2$ элемент $2^{n-1}a + bj$ отличен от нуля, поэтому, используя лемму 2, получим

$$|W_f(\vec{a})| \leq \sum_{j \in R} |\mu_{j,K}| \max_{j \in R^*} \left| \sum_{x \in \Gamma(S)^*} \chi(\text{Tr}_R^S((2^{n-1}a + bj)x)) + 1 \right| \leq \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}}.$$

□

Теорема 2 обобщает оценку из работы [13, теорема 6.1] на случай произвольного координатного множества K . Более того, при $K = \{0, 1\}$ теорема 2 уточняет эту оценку.

Следствие 3. Для коэффициента нелинейности N_f каждой булевой функции $f \in B'_n(K, F)$, где $n \geq 2$, справедливо неравенство

$$N_f \geq 2^{m-1} - \sigma_n(2^{n-1} - 1)2^{\frac{m}{2}-1}.$$

Следствие 4. При $n = 1$ класс $B'_n(K, F)$ состоит из всех линейных функций.

Доказательство. Из равенства (20) получим

$$W_f(\vec{a}) = 1 + \sum_{x \in GF(2^m)^*} (-1)^{\text{tr}_2^{2^m}((a+b)x)} = \begin{cases} 2^m, & \text{если } a = b, \\ 0, & \text{если } a \neq b. \end{cases} \quad \square$$

Следствие 5. При $n = 2$ и каждом четном m класс $B'_n(K, F)$ состоит из бент-функций, а при $n = 2$ и каждом нечетном m класс $B'_n(K, F)$ состоит из платовидных функций порядка $m - 1$.

Доказательство. Заметим, что $\chi(\text{Tr}_R^S(2^{n-1}ax)) = \chi(\text{Tr}_R^S(2^{n-1}ax)j)$ при $n = 2$ для $j = 1, 3$, тогда в силу равенства (21) и леммы 1

$$\begin{aligned} W_f(\vec{a}) &= (-1)^{\mathcal{Z}_{n-1}^K(0)} + \sum_{x \in \Gamma(S)^*} \sum_{j \in R} \mu_{j,K} \chi(\text{Tr}_R^S(2^{n-1}a + bx)j) = \\ &= (-1)^{\mathcal{Z}_{n-1}^K(0)} + \sum_{i=0}^{2^m-2} (-1)^{\mathcal{Z}_{n-1}^K(\omega(i))}, \end{aligned}$$

где ω — ЛРП над кольцом R , определенная равенством

$$\omega(i) = \text{Tr}_R^S((2^{n-1}a + b)\alpha^i), \quad i \geq 0.$$

Согласно [15, утверждение 3] для числа $N(z, \omega_{n-1})$ появлений элемента $z \in K$ на цикле ЛРП $\omega_{n-1} = \mathcal{Z}_{n-1}^K(\omega)$ справедливо равенство

$$N(z, \omega_{n-1}) = \frac{2^m - 1}{2} + \frac{(-1)^z}{2} \sum_{i=0}^{2^m-2} (-1)^{\omega_{n-1}(i)},$$

тогда

$$W_f(\vec{a}) = (-1)^{\mathcal{Z}_{n-1}^K(0)} + N(k_0, \omega_{n-1}) - N(k_1, \omega_{n-1}).$$

Используя полное описание частот $N(z, \omega_{n-1})$, полученное для случая $n = 2$ (см. [15, следствие 1]), будем иметь

$$W_f(\vec{a}) = \begin{cases} \pm 2^{m/2}, & \text{если } m \text{ четно,} \\ 0, \pm 2^{(m+1)/2}, & \text{если } m \text{ нечетно.} \end{cases} \quad \square$$

§ 7. Степень нелинейности функций

Рассмотрим теперь вопрос о степени нелинейности (алгебраической степени) $\deg f$ функций f из класса $B'_n(K, F)$. Напомним, что двоичным весом числа $k = \sum k_s 2^s$ называется число $\nu(k) = \sum k_s$. Нам потребуется следующий вспомогательный результат.

Лемма 4. Пусть $F(x)$ — отмеченный многочлен степени m максимального периода над кольцом $R = \mathbb{Z}_{2^n}$, $m > |R|$ и пусть также $u(i) = \text{Tr}_R^S(b\alpha^i)$, $i \geq 0$, тогда справедливо представление

$$\mathcal{Z}_{n-1}^K(u(i)) \stackrel{2}{=} \sum_{k: \nu(k)=2^{n-1}} b_0^k \alpha^{ik} + \sum_{k: \nu(k)<2^{n-1}} c_k \alpha^{ik} + \mathcal{Z}_{n-1}^K(0), \quad (22)$$

где $b_0 = \gamma_0(b)$, $c_k \in S$.

Доказательство. Пусть $u = u_0 + 2u_1 + \dots + 2^{n-1}u_{n-1}$ — двоичное разложение ЛРП u . В [2] описано строение t -й координатной последовательности ЛРП максимального периода. Этот результат позволяет описать строение t -й координатной последовательности отмеченной ЛРП, так как отмеченная ЛРП получается из ЛРП максимального периода выборкой с шагом 2^{n-1} . Из результатов работы [2, теоремы 1.3, 1.5] следует, что

$$u_t(i) \stackrel{2}{\equiv} \sum_{k: \nu(k)=2^t} b_0^k \alpha^{ik} + \sum_{k: \nu(k)<2^t} c_k^{(t)} \alpha^{ik}, \quad c_k^{(t)} \in S. \quad (23)$$

Последнее соотношение можно переписать в виде

$$u_t(i) \stackrel{2}{\equiv} \sum_{k: \nu(k) \leq 2^t} d_k^{(t)} \alpha^{ik}, \quad d_k^{(t)} \in S. \quad (24)$$

По лемме 3 имеем:

$$\begin{aligned} \varkappa_{n-1}^K(u(i)) &\stackrel{2}{\equiv} u_{n-1}(i) + g^K(u_0(i), \dots, u_{n-2}(i)) \stackrel{2}{\equiv} \sum_{k: \nu(k)=2^{n-1}} b_0^k \alpha^{ik} + \\ &+ \sum_{k: \nu(k)<2^{n-1}} c_k^{(n-1)} \alpha^{ik} + \varkappa_{n-1}^K(0) + \sum_{r=1}^{n-1} \sum_{0 \leq i_1 < \dots < i_r \leq n-2} g_{i_1 \dots i_r} u_{i_1}(i) \cdots u_{i_r}(i). \end{aligned}$$

Покажем, что последовательность $u_{i_1} \cdots u_{i_r}$ представляется в виде суммы биномиальных последовательностей с корнями α^k , $\nu(k) < 2^{n-1}$. Действительно,

$$u_{i_1}(i) \cdots u_{i_r}(i) \stackrel{2}{\equiv} \sum_{\nu(k_1) \leq 2^{i_1}, \dots, \nu(k_r) \leq 2^{i_r}} d_{k_1}^{(i_1)} \cdots d_{k_r}^{(i_r)} \alpha^{i(k_1 + \dots + k_r)},$$

и остается заметить, что $\nu(k_1 + \dots + k_r) \leq 2^{i_1} + \dots + 2^{i_r} \leq 2^{n-1} - 1$. $\square$

Утверждение 8. Пусть $R = \mathbb{Z}_{2^n}$, $F(x) \in R[x]$ — отмеченный многочлен степени t максимального периода над кольцом R , тогда при $t > |R|$ для любой функции $f \in B'_n(K, F)$ справедливо соотношение $\deg f = 2^{n-1}$.

Доказательство. По построению класса $B'_n(K, F)$ имеем

$$f(x_1, \dots, x_m) \stackrel{2}{\equiv} \varkappa_{n-1}^K(\text{Tr}_R^S(b(x_1 \alpha_1 \oplus \dots \oplus x_m \alpha_m))), \quad (25)$$

причем для $(x_1, \dots, x_m) \neq \vec{0}$ справедливо соотношение $f(x_1, \dots, x_m) \stackrel{2}{\equiv} \varkappa_{n-1}^K(\text{Tr}_R^S(b \alpha^i))$, где $\alpha^i \stackrel{2}{\equiv} x_1 \alpha_1 \oplus \dots \oplus x_m \alpha_m$. Подставив сравнение (22)

в соотношение (25), получаем

$$\begin{aligned} f(x_1, \dots, x_m) &\stackrel{2}{=} \sum_{k: \nu(k)=2^{n-1}} b_0^k (x_1 \alpha_1 \oplus \dots \oplus x_m \alpha_m)^k + \\ &+ \sum_{k: \nu(k) < 2^{n-1}} c_k (x_1 \alpha_1 \oplus \dots \oplus x_m \alpha_m)^k + \mathcal{K}_{n-1}^K(0). \end{aligned} \quad (26)$$

Заметим, что после приведения подобных слагаемых в правой части этого сравнения получается многочлен над $\Gamma(R)$, поэтому его степень равна степени нелинейности функции f . Пусть $k = 2^{i_1} + \dots + 2^{i_t}$, $t = \nu(k)$, тогда справедливо равенство

$$(x_1 \alpha_1 \oplus \dots \oplus x_m \alpha_m)^k = (x_1 \alpha_1^{2^{i_1}} \oplus \dots \oplus x_m \alpha_m^{2^{i_1}}) \cdots (x_1 \alpha_1^{2^{i_t}} \oplus \dots \oplus x_m \alpha_m^{2^{i_t}}).$$

Отсюда следует, что степень многочлена $(x_1 \alpha_1 \oplus \dots \oplus x_m \alpha_m)^k$ равна $t = \nu(k)$. Воспользовавшись этим фактом и условием $b \in S^*$, получаем, что степень многочлена, стоящего в правой части сравнения (26), равна 2^{n-1} . Это значит, что $\deg f = 2^{n-1}$. $\square$

Покажем, что при условии $m > |R|$ вес любой функции f из классов $B_n(K, F)$ и $B'_n(K, F)$ является четным.

Утверждение 9. Пусть $F(x)$ — отмеченный многочлен степени m максимального периода над кольцом $R = \mathbb{Z}_{2^n}$, тогда при $m > |R|$ справедливо сравнение $\|f\| \stackrel{2}{=} 0$. В частности, $\deg f \leq m - 1$.

Доказательство. Вычислим $v \stackrel{2}{=} \sum_{i=0}^{2^m-2} \mathcal{K}_{n-1}^K(u(i))$. Из леммы 4 следует, что

$$\mathcal{K}_{n-1}^K(u(i)) \stackrel{2}{=} \sum_{k: \nu(k) \leq 2^{n-1}} d_k \alpha^{ik} + \mathcal{K}_{n-1}^K(0).$$

Отсюда имеем:

$$v \stackrel{2}{=} \sum_k d_k \left(\sum_{i=0}^{2^m-2} \alpha^{ik} \right) + \mathcal{K}_{n-1}^K(0).$$

Так как $m > |R|$, то при $\nu(k) \leq 2^{n-1}$ верно неравенство $\alpha^k \neq e$. Отсюда следует соотношение $\sum_{i=0}^{2^m-2} \alpha^{ki} \stackrel{2}{=} 0$, следовательно $v \stackrel{2}{=} \mathcal{K}_{n-1}^K(0)$. Нетрудно видеть, что $\|f\| \stackrel{2}{=} f(\vec{0}) + v \stackrel{2}{=} 0$. $\square$

§ 8. Результаты вычислений на ЭВМ

Для изучения свойств классов функций $B_n(K, F)$, $B'_n(K, F)$ были проведены вычисления с использованием ЭВМ. Для каждого из рассматриваемых классов функций B изучались следующие параметры:

1. $\deg_{\min}(\deg_{\max})$ — минимум (максимум) степеней нелинейности функций из B ;
2. $\min(N_f)(\max(N_f))$ — минимум (максимум) коэффициентов нелинейности функций из B .

В следующей таблице приведены результаты вычислений для всех отмеченных многочленов максимального периода степени не выше 10 над кольцом $\mathbb{Z}_4$. Здесь f_{coef} — строка коэффициентов многочлена (в ней коэффициенты расположены в порядке возрастания номеров, начиная от свободного коэффициента до старшего коэффициента, который равен 1), $N(m) = 2^{m-1} - 2^{m/2-1}$ — универсальная оценка сверху коэффициента нелинейности (см. [20, неравенство (6.3)]). Из замечания 1 следует, что для случая $R = \mathbb{Z}_4$ достаточно провести вычисления лишь в двоичном координатном множестве.

Таблица 1

$B_2(K, F)$					
f_{coef}	$\deg_{\min}$	$\deg_{\max}$	$\min(N_f)$	$\max(N_f)$	$N(m)$
(-1,-2,-1,1)	1	2	0	2	3
(-1,-3,-2,1)	1	2	0	2	3
(-3,0,-2,-1,1)	2	3	2	6	6
(-3,-1,-2,0,1)	2	3	2	6	6
(-1,0,0,-3,-2,1)	3	4	6	12	14
(-1,-1,-3,0,-1,1)	2	4	6	12	14
(-1,-1,-3,-1,-2,1)	1	4	0	12	14
(-1,-2,-1,0,0,1)	2	4	6	12	14
(-1,-2,-3,-1,-3,1)	3	4	2	12	14
(-1,-3,0,-1,-3,1)	3	4	4	12	14
(-3,0,0,-2,0,-1,1)	4	5	16	24	28
(-3,-1,0,-2,0,0,1)	4	5	16	24	28
(-3,-1,0,-3,-3,-2,1)	4	5	18	26	28
(-3,-1,-2,0,-3,-3,1)	4	5	16	24	28
(-3,-2,-3,-3,0,-1,1)	3	5	18	28	28
(-3,-3,-3,0,-2,-1,1)	4	5	16	24	28
(-1,0,0,-2,0,0,-1,1)	5	6	36	52	60
(-1,0,0,-3,0,-2,0,1)	5	6	36	52	60
(-1,0,-2,0,-1,0,0,1)	5	6	38	52	60
(-1,0,-2,-2,-1,-1,-3,1)	5	6	38	52	60
(-1,0,-2,-3,-3,-1,-2,1)	5	6	36	52	60

(-1,-1,-1,-2,-2,-3,-2,1)	5	6	38	52	60
(-1,-1,-1,-3,-1,-1,-2,1)	5	6	38	52	60
(-1,-1,-3,-2,-1,-1,-3,1)	4	6	40	52	60
(-1,-1,-3,-3,-2,-1,-3,1)	4	6	38	52	60
(-1,-1,-3,-3,-2,-2,0,1)	5	6	38	52	60
(-1,-2,-1,-2,-2,-3,-3,1)	5	6	38	52	60
(-1,-2,-3,0,-3,-2,-1,1)	5	6	38	56	60
(-1,-2,-3,-1,-1,-2,0,1)	5	6	36	52	60
(-1,-2,-3,-3,-1,-3,-3,1)	5	6	38	52	60
(-1,-3,0,0,-2,0,0,1)	5	6	36	52	60
(-1,-3,-2,-1,0,-1,-2,1)	5	6	36	56	60
(-1,-3,-2,-1,-2,-2,-1,1)	5	6	38	52	60
(-1,-3,-2,-2,-3,-2,-1,1)	5	6	38	52	60
(-3,0,0,-1,0,-3,-2,-1,1)	6	7	84	112	120
(-3,0,0,-3,0,-1,-3,-2,1)	6	7	86	110	120
(-3,0,-2,-2,-1,-3,-1,-2,1)	6	7	84	110	120
(-3,-1,0,0,-2,-1,-3,-2,1)	6	7	90	112	120
(-3,-1,0,-2,0,0,-3,-3,1)	6	7	84	110	120
(-3,-1,-2,-3,0,-1,0,0,1)	6	7	86	112	120
(-3,-2,-1,0,-3,-1,-3,-3,1)	6	7	86	110	120
(-3,-2,-1,-3,-1,-2,-2,0,1)	6	7	84	110	120
(-3,-2,-3,-1,0,-3,0,0,1)	6	7	88	110	120
(-3,-2,-3,-1,-2,0,0,-1,1)	6	7	90	112	120
(-3,-2,-3,-2,0,-3,-3,-2,1)	6	7	88	112	120
(-3,-2,-3,-3,0,-2,-3,-2,1)	6	7	88	112	120
(-3,-3,-1,-3,-2,0,-3,-3,1)	6	7	86	112	120
(-3,-3,-3,0,0,-2,0,-1,1)	6	7	84	110	120
(-3,-3,-3,0,-2,-3,-1,-3,1)	6	7	86	112	120
(-3,-3,-3,-1,-3,0,-1,-2,1)	6	7	88	110	120
(-1,0,0,0,0,-3,0,-2,0,1)	7	8	198	230	248
(-1,0,0,-1,0,-1,-1,-3,-3,1)	7	8	192	228	248
(-1,0,0,-1,-2,-3,-3,-2,0,1)	7	8	188	228	248
(-1,0,0,-2,-2,-3,-1,0,-1,1)	7	8	196	230	248
(-1,0,-2,0,-1,0,0,0,0,1)	7	8	198	230	248
(-1,0,-2,0,-3,-3,-2,-2,-1,1)	6	8	200	228	248
(-1,0,-2,-1,-1,-2,-3,0,0,1)	7	8	188	228	248
(-1,0,-2,-1,-3,0,-1,-1,-3,1)	7	8	198	230	248
(-1,0,-2,-1,-3,-3,-1,-1,-2,1)	7	8	194	236	248
(-1,0,-2,-2,-1,-2,-1,-3,-2,1)	7	8	198	228	248
(-1,0,-2,-3,-1,-1,-2,-1,-3,1)	7	8	198	230	248
(-1,-1,-1,0,-2,-2,0,-3,-2,1)	7	8	178	228	248
(-1,-1,-1,-1,-3,0,0,0,-1,1)	7	8	198	228	248
(-1,-1,-1,-1,-3,-1,-1,0,-1,1)	7	8	196	230	248
(-1,-1,-1,-2,-2,0,-1,-1,-3,1)	7	8	196	232	248

$(-1,-1,-1,-3,-3,0,-3,0,0,1)$	7	8	192	230	248
$(-1,-1,-3,0,-3,-1,-2,-1,-2,1)$	7	8	186	230	248
$(-1,-1,-3,-1,0,0,-3,-2,-1,1)$	7	8	200	230	248
$(-1,-1,-3,-1,0,0,-3,-3,-2,1)$	7	8	196	228	248
$(-1,-1,-3,-1,0,-3,0,-1,-2,1)$	6	8	198	230	248
$(-1,-1,-3,-2,-3,-3,-1,-2,0,1)$	7	8	198	230	248
$(-1,-1,-3,-3,0,-1,-3,-2,0,1)$	7	8	198	230	248
$(-1,-1,-3,-3,0,-2,-2,-3,-3,1)$	7	8	196	232	248
$(-1,-2,-1,0,0,-3,-2,-1,-2,1)$	7	8	196	228	248
$(-1,-2,-1,0,-2,-2,0,-3,-3,1)$	7	8	178	228	248
$(-1,-2,-1,-1,0,0,-3,-1,-3,1)$	7	8	196	228	248
$(-1,-2,-1,-1,-2,-1,-3,0,-1,1)$	7	8	194	228	248
$(-1,-2,-1,-3,-2,-3,-2,-2,0,1)$	7	8	200	228	248
$(-1,-2,-3,0,-1,0,-3,-1,-3,1)$	6	8	198	230	248
$(-1,-2,-3,0,-3,-1,-3,-1,-2,1)$	7	8	198	230	248
$(-1,-2,-3,-1,-3,-1,0,-1,-2,1)$	7	8	198	230	248
$(-1,-2,-3,-2,-1,0,0,-3,-2,1)$	7	8	198	228	248
$(-1,-2,-3,-2,-3,-1,0,-1,-3,1)$	7	8	186	230	248
$(-1,-2,-3,-2,-3,-2,-2,0,-1,1)$	7	8	192	230	248
$(-1,-2,-3,-3,-1,-1,-3,-2,0,1)$	7	8	194	236	248
$(-1,-3,0,0,0,-1,-3,-3,-3,1)$	7	8	198	228	248
$(-1,-3,0,-1,-1,-1,0,-2,-1,1)$	7	8	180	228	248
$(-1,-3,0,-1,-3,0,-1,-2,-1,1)$	7	8	196	228	248
$(-1,-3,0,-1,-3,-2,-3,-3,-2,1)$	7	8	192	228	248
$(-1,-3,0,-2,-2,-1,0,-2,-1,1)$	6	8	196	230	248
$(-1,-3,0,-2,-2,-1,-2,-1,-2,1)$	6	8	192	228	248
$(-1,-3,0,-3,-1,-2,-2,0,0,1)$	7	8	196	230	248
$(-1,-3,0,-3,-3,-1,-3,-3,-3,1)$	7	8	196	230	248
$(-1,-3,-2,0,-3,-2,-2,0,-1,1)$	6	8	198	230	248
$(-1,-3,-2,0,-3,-3,-3,0,-1,1)$	7	8	182	228	248
$(-1,-3,-2,-1,0,0,-3,-1,-3,1)$	7	8	200	232	248
$(-1,-3,-2,-2,-1,-1,0,-2,0,1)$	7	8	200	228	248
$(-1,-3,-2,-3,0,-1,-3,0,-1,1)$	7	8	196	228	248
$(-3,0,0,0,0,-2,0,-1,0,0,1)$	8	9	418	472	496
$(-3,0,0,0,-2,-3,0,-2,-3,-3,1)$	8	9	426	476	496
$(-3,0,0,0,-2,-3,-2,-1,-3,-2,1)$	8	9	420	470	496
$(-3,0,0,-1,0,0,-2,-1,-2,-1,1)$	8	9	418	472	496
$(-3,0,0,-1,0,-2,0,0,0,0,1)$	8	9	418	472	496
$(-3,0,0,-2,0,-2,-3,-1,0,-1,1)$	8	9	420	470	496
$(-3,0,-2,0,-1,-3,0,-1,-1,-3,1)$	8	9	408	472	496
$(-3,0,-2,0,-1,-3,-2,-2,-3,-2,1)$	8	9	408	472	496
$(-3,0,-2,-1,-1,-2,-2,-2,-3,-2,1)$	8	9	424	470	496
$(-3,0,-2,-1,-3,-3,0,0,-3,-3,1)$	8	9	356	472	496
$(-3,0,-2,-3,-1,0,-3,0,-1,-3,1)$	8	9	416	474	496

(-3,0,-2,-3,-1,-1,-1,0,-2,-1,1)	7	9	414	472	496
(-3,0,-2,-3,-3,-3,-1,-3,-3,-3,1)	7	9	422	476	496
(-3,-1,0,0,-2,-1,-3,0,-1,-3,1)	8	9	420	472	496
(-3,-1,0,-1,-1,-3,-3,-1,-1,-2,1)	8	9	420	470	496
(-3,-1,0,-1,-3,-2,0,-2,0,0,1)	8	9	420	470	496
(-3,-1,0,-2,0,0,-3,0,-2,-1,1)	8	9	424	472	496
(-3,-1,0,-2,-2,-2,-3,-2,-1,-2,1)	8	9	420	474	496
(-3,-1,0,-2,-2,-3,0,0,-3,-2,1)	8	9	416	472	496
(-3,-1,0,-3,-3,0,-3,-1,-3,-3,1)	8	9	422	472	496
(-3,-1,0,-3,-3,-2,-1,-2,-2,-1,1)	8	9	424	476	496
(-3,-1,-2,0,-1,-1,-1,-3,-2,0,1)	8	9	416	472	496
(-3,-1,-2,0,-3,0,0,-2,0,-1,1)	8	9	424	472	496
(-3,-1,-2,0,-3,0,-2,-3,-1,-3,1)	8	9	426	470	496
(-3,-1,-2,0,-3,-3,-3,-3,-3,-3,1)	8	9	420	472	496
(-3,-1,-2,-1,0,-3,-3,-2,-1,-2,1)	8	9	420	478	496
(-3,-1,-2,-1,-2,0,0,-1,0,0,1)	8	9	418	472	496
(-3,-1,-2,-2,-1,-2,-3,-3,0,-1,1)	8	9	422	474	496
(-3,-2,-1,0,-3,-2,-3,0,-1,-3,1)	8	9	424	472	496
(-3,-2,-1,-1,-1,-3,-1,-2,-1,-3,1)	8	9	416	474	496
(-3,-2,-1,-1,-3,-3,-1,-1,0,-1,1)	8	9	420	470	496
(-3,-2,-1,-2,-3,-2,-2,-2,0,-1,1)	8	9	420	472	496
(-3,-2,-1,-2,-3,-3,0,-1,-2,-1,1)	8	9	420	476	496
(-3,-2,-1,-3,-1,0,-2,-2,-3,-3,1)	8	9	426	472	496
(-3,-2,-1,-3,-3,-1,0,-2,-3,-2,1)	7	9	368	472	496
(-3,-2,-3,0,0,-3,-2,-2,0,-1,1)	8	9	416	472	496
(-3,-2,-3,0,-2,0,-2,-1,-3,-2,1)	8	9	416	472	496
(-3,-2,-3,-1,-2,0,-2,0,-3,-2,1)	8	9	416	472	496
(-3,-2,-3,-1,-2,-2,0,-1,-1,-3,1)	8	9	422	472	496
(-3,-2,-3,-1,-2,-3,-2,0,0,0,1)	8	9	420	470	496
(-3,-2,-3,-2,0,-1,-3,-3,-1,-2,1)	8	9	368	472	496
(-3,-2,-3,-2,-2,-2,-1,-1,-2,0,1)	8	9	424	472	496
(-3,-2,-3,-2,-2,-3,-1,0,-2,0,1)	8	9	408	472	496
(-3,-2,-3,-3,0,0,-3,-2,-1,-3,1)	8	9	418	472	496
(-3,-3,-1,0,-3,0,-1,-3,-2,0,1)	8	9	416	472	496
(-3,-3,-1,0,-3,-1,-2,0,0,-1,1)	8	9	420	472	496
(-3,-3,-1,0,-3,-2,-3,0,-1,-2,1)	7	9	422	472	496
(-3,-3,-1,-1,0,-2,-2,-1,-3,-2,1)	8	9	422	472	496
(-3,-3,-1,-1,0,-3,-1,0,-2,0,1)	8	9	408	472	496
(-3,-3,-1,-2,-1,-2,0,-2,-3,-3,1)	8	9	422	476	496
(-3,-3,-1,-2,-1,-3,-1,-1,-1,-2,1)	8	9	416	474	496
(-3,-3,-1,-2,-3,0,0,-3,-3,-2,1)	8	9	418	474	496
(-3,-3,-1,-3,-2,0,-3,0,-2,-1,1)	8	9	428	472	496
(-3,-3,-3,0,0,-3,-3,-1,-2,0,1)	8	9	356	472	496
(-3,-3,-3,-1,-3,0,-3,-3,0,-1,1)	8	9	422	474	496

$(-3,-3,-3,-2,0,-2,-1,-2,-1,-3,1)$	8	9	422	474	496
$(-3,-3,-3,-2,0,-3,-2,0,0,1)$	8	9	426	474	496
$(-3,-3,-3,-2,-2,0,-1,-3,-1,-2,1)$	8	9	424	472	496
$(-3,-3,-3,-3,-1,-3,-3,-3,-2,0,1)$	8	9	422	474	496
$(-3,-3,-3,-3,-3,-3,-3,0,-2,-1,1)$	8	9	420	472	496

Из таблицы 1 видно, что рассматриваемые классы $B_2(K, F)$ содержат аффинные функции (для них $N_f = 0$) при $m = 3$ для каждого из двух отмеченных многочленов $F(x)$ степени 3, а при $m = 5$ — только для одного из шести многочленов $F(x)$ степени 5. При всех остальных значениях m , где $m \leq 10$, в классах $B_2(K, F)$ нет аффинных функций. Для случая $m = 4$ при каждом отмеченном многочлене $F(x)$ класс $B_2(K, F)$ содержит квадратичные бент-функции, а для $m = 6$ существует единственный многочлен $F(x)$, для которого класс $B_2(K, F)$ содержит бент-функции, причем их степень нелинейности равна 3.

Заметим, что в случае нечетного m максимально возможное расстояние $\tilde{N}(m)$ от булевой функции f до класса всех аффинных функций от m переменных удовлетворяет условиям

$$2^{m-1} - 2^{\frac{m-1}{2}} \leq \tilde{N}(m) \leq N(m),$$

при этом $\tilde{N}(m) = 2^{m-1} - 2^{(m-1)/2}$, если $m \in \{1, 3, 5, 7\}$ (см. [20, §5.3]). Из таблицы 1 видно, что при каждом $m \in \{3, 5, 7\}$ существует не менее двух многочленов $F(x)$, для которых класс $B_2(K, F)$ содержит булевы функции, максимально удаленные от аффинных функций.

Рассмотрим следующие таблицы 2–4.

Таблица 2

$R = \mathbb{Z}_8, K = \{0, 1\}, \{0, 3\}, \{0, 5\}, \{0, 7\} B_3(K, F)$				
f_{coef}	$\deg_{\min}$	$\deg_{\max}$	$\min(N_f)$	$\max(N_f)$
$(-7, 0, 0, -2, -4, -1, 1)$	3	5	12	28
$(-7, -1, -4, -2, 0, 0, 1)$	3	5	12	26
$(-7, -1, -4, -3, -3, -2, 1)$	4	5	12	26
$(-7, -2, -3, -3, -4, -1, 1)$	4	5	12	26
$(-7, -5, -2, 0, -3, -7, 1)$	4	5	12	26
$(-7, -7, -3, 0, -2, -5, 1)$	4	5	12	26

Эти таблицы показывают, что при $n > 2$ выбор координатного множества существен при изучении свойств функций из классов $B_n(K, F)$. Отметим, что для первого из рассмотренных многочленов $F(x)$ в таблице 2 класс $B_3(K, F)$ содержит бент-функции от шести переменных, имеющие степень нелинейности 3. Из таблицы 3 видно, что классы $B_3(K, F)$ уже не содержат

Таблица 3

$R = \mathbb{Z}_8, K = \{2, 1\}, \{2, 3\}, \{2, 5\}, \{2, 7\} B_3(K, F)$				
f_{coef}	$\deg_{\min}$	$\deg_{\max}$	$\min(N_f)$	$\max(N_f)$
$(-7, 0, 0, -2, -4, -1, 1)$	4	5	12	26
$(-7, -1, -4, -2, 0, 0, 1)$	4	5	12	26
$(-7, -1, -4, -3, -3, -2, 1)$	4	5	14	26
$(-7, -2, -3, -3, -4, -1, 1)$	4	5	14	26
$(-7, -5, -2, 0, -3, -7, 1)$	4	5	12	26
$(-7, -7, -3, 0, -2, -5, 1)$	4	5	12	26

Таблица 4

$R = \mathbb{Z}_{16}, B_4(K, F)$					
K	f_{coef}	$\deg_{\min}$	$\deg_{\max}$	$\min(N_f)$	$\max(N_f)$
$\{0, 1\}$	$(-15, -9, -12, -3, -11, -10, 1)$	3	6	9	26
$\{0, 3\}$	$(-15, -9, -12, -3, -11, -10, 1)$	3	6	9	26
$\{0, 5\}$	$(-15, -9, -12, -3, -11, -10, 1)$	3	6	9	26
$\{0, 7\}$	$(-15, -9, -12, -3, -11, -10, 1)$	3	6	9	26
$\{2, 1\}$	$(-15, -9, -12, -3, -11, -10, 1)$	4	6	9	26
$\{2, 3\}$	$(-15, -9, -12, -3, -11, -10, 1)$	3	6	10	26
$\{2, 5\}$	$(-15, -9, -12, -3, -11, -10, 1)$	4	6	9	26
$\{2, 7\}$	$(-15, -9, -12, -3, -11, -10, 1)$	3	6	10	26

бент-функций для каждого из шести рассмотренных многочленов $F(x)$. Кроме того, по сравнению с выбором K в таблице 2, уже нет булевых функций степени нелинейности 3. Таблица 4 подтверждает зависимость степени нелинейности и коэффициента нелинейности функций из класса $B_n(K, F)$ от выбора координатного множества K . Кроме того, она показывает, что в условии утверждения 9 от ограничения $m > |R|$ нельзя отказаться.

Для многочлена $x^6 - 2x^5 - 3x^4 - 3x^3 - 4x^2 - x - 7 \in \mathbb{Z}_8[x]$ построены классы $B'_3(K, F)$ и вычислены параметры $\deg_{\min}$, $\deg_{\max}$, $\min(N_f)$, $\max(N_f)$. Оказалось, что они не зависят от выбора K и $\deg_{\min} = \deg_{\max} = 4$, $\min(N_f) = 18$, $\max(N_f) = 26$. Таблица 5 показывает, что в общем случае для функций $f \in B'_n(K, F)$ зависимость рассматриваемых параметров от множества K присутствует.

Рассмотренные в таблице 5 классы $B'_5(K, F)$ содержат бент-функции степени нелинейности 3 при $K = \{2, 5\}$ и $K = \{2, 7\}$, однако при других координатных множествах классы $B'_5(K, F)$ не содержат бент-функций. Соответствующие классы $B_5(K, F)$ не содержат бент-функций и содержат функции, более близкие к аффинным функциям ($\min N_f = 6$) по сравнению с функциями из классов $B'_5(K, F)$, где $\min N_f \in \{10, 11\}$. Кроме того,

Таблица 5

K	$\deg_{\min}$	$\deg_{\max}$	$\min(N_f)$	$\max(N_f)$
$R = \mathbb{Z}_{16}, B'_4(K, x^6 - 10x^5 - 11x^4 - 3x^3 - 12x^2 - 9x - 15)$				
$\{0,1\}, \{0,3\}, \{0,5\}, \{0,7\}$	4	6	15	25
$\{2,1\}, \{2,5\}$	4	6	9	25
$\{2,3\}, \{2,7\}$	3	6	14	25
$R = \mathbb{Z}_{32}, B'_5(K, x^6 - 26x^5 - 27x^4 - 19x^3 - 28x^2 - 9x - 31)$				
$\{0,1\}, \{0,3\}, \{0,5\}, \{0,7\}$	4	6	11	26
$\{2,1\}, \{2,3\}$	4	6	10	26
$\{2,5\}, \{2,7\}$	3	6	11	28
$R = \mathbb{Z}_{32}, B_5(K, x^6 - 26x^5 - 27x^4 - 19x^3 - 28x^2 - 9x - 31)$				
$\{0,1\}, \{0,3\}, \{0,5\}, \{0,7\}, \{2,1\}, \{2,3\}, \{2,5\}, \{2,7\}$	3	6	6	27

таблица 5 показывает, что ограничение $m > |R|$ является существенным не только в условии утверждения 9, но и в условии утверждения 8.

Список литературы

1. Нечаев А. А. Цикловые типы линейных подстановок над конечными коммутативными кольцами // Матем. сборник. — 1993. — Т. 184. № 3. — С. 21–56.
2. Кузьмин А. С., Нечаев А. А. Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и логика. — 1995. — Т. 34. № 2. — С. 169–189.
3. Кузьмин А. С., Куракин В. Л., Нечаев А. А. Псевдослучайные и полилинейные последовательности // В сб.: Труды по дискретной математике. — М.: ТВП, 1997. — Т. 1. — С. 139–202.
4. Kumar P. V., Helleseeth T. An expansion for the coordinates of the trace function over Galois rings // Appl. Algebra in Eng., Comm. and Comput. — 1997. — № 8. — Р. 353–361.
5. Кузьмин А. С., Нечаев А. А. Восстановление линейной рекурренты максимального периода над кольцом Галуа по ее старшей координатной последовательности // Дискретн. матем. — 2011. — Т. 23. № 2. — С. 3–31.
6. Кузьмин А. С., Маршалко Г. Б., Нечаев А. А. Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению // Матем. вопросы криптографии. — 2010. — Т. 1. № 2. — С. 31–56.
7. Былков Д. Н., Нечаев А. А. Алгоритм восстановления последовательностей, полученных линейным усложнением координатных последовательностей ЛРП над кольцом $R = \mathbb{Z}_{p^n}$ // Дискретн. матем. — 2010. — Т. 22. № 4. — С. 104–120.

8. Былков Д. Н. Класс усложнений линейных рекуррент над кольцом Галуа, не приводящий к потере информации // Проблемы передачи информации. — 2010. — Т. 46. № 3. — С. 51–59.
9. Shparlinski I. E., Winterhof A. On the nonlinearity of linear recurrence sequences // Appl. Math. Lett. — 2005. — Bd. 19. — P. 340–344.
10. Мак-Вильямс Ф. Д., Слоэн Н. Д. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.
11. Нечаев А. А. Код Кердока в циклической форме // Дискретн. матем. — 1989. — Т. 1. № 4. — С. 123–139.
12. Lahtonen L., Ling S., Sole P., Zinoviev D. $\mathbb{Z}_8$ -Kerdock codes and pseudorandom binary sequences // J. Complexity. — 2004. — V. 20. № 8. — P. 318–330.
13. Sole P., Zinoviev D. Low-correlation, high-nonlinearity sequences for multiple-code CDMA // IEEE Trans. Inform. Theory. — 2006. — V. 52. № 11. — P. 5158–5163.
14. Кузьмин А. С., Нечаев А. А. Построение помехоустойчивых кодов с использованием линейных рекуррент над кольцами Галуа // Успехи матем. наук. — 1992. — Т. 47. № 5. — С. 183–184.
15. Камловский О. В. Метод тригонометрических сумм для исследования частот r -грамм в старших координатных последовательностях линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ // Матем. вопросы криптографии. — 2010. — Т. 1. № 4. — С. 33–62.
16. Kuzmin A. S., Nechaev A. A. Complete weight enumerators of generalized Kerdock code and related linear codes over Galois ring // Discr. Appl. Math. — 2001. — V. 111. — P. 117–137.
17. Boztas S., Hammous R., Kumar P. V. 4-phase sequences with near-optimum correlation properties // IEEE Trans. Inform. Theory. — 1992. — V. 38. № 3. — P. 1101–1113.
18. Камловский О. В., Кузьмин А. С. Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа // Фундам. и прикл. математика. — 2000. — Т. 6. № 4. — С. 1083–1094.
19. Камловский О. В. Частотные характеристики линейных рекуррентных последовательностей над кольцами Галуа // Матем. сборник. — 2009. — Т. 200. № 4. — С. 31–52.
20. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.
21. Lempel A. Matrix factorization over $\mathbb{F}_2$ and trace-orthogonal basis of $\mathbb{F}_{2^n}$ // SIAM J. Comput. — 1975. — V. 4. — P. 175–186.