ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 58 **2022** **Вып. 4**

УДК 621.391 : 519.12 : 519.719

© 2022 г. **О.В. Камловский, К.Н. Панков**

КЛАССЫ СБАЛАНСИРОВАННЫХ ФУНКЦИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ, ОБЛАДАЮЩИХ МАЛЫМ ЗНАЧЕНИЕМ ЛИНЕЙНОЙ ХАРАКТЕРИСТИКИ

Приводятся сбалансированные функции над конечными полями, обладающие малым значением линейной характеристики. Ранее линейные характеристики похожих классов функций исследовались лишь для случая поля из двух элементов.

Ключевые слова: сбалансированные функции, линейная характеристика функций, конечные поля, устойчивые функции.

DOI: 10.31857/S055529232204009X, **EDN:** NBPDHY

§ 1. Введение

Одной из важных прикладных математических задач является построение сбалансированных функций над конечными полями, достаточно удаленных от класса всех аффинных функций от заданного числа переменных. Данная проблема значительно проработана для случая булевых функций (см., например, [1–5]). Один из путей ее решения заключается в построении различных классов булевых бент-функций, которые наиболее удалены от всех аффинных функций, и последующем их усложнении с целью получения сбалансированных функций.

Аналогичные вопросы для функций над произвольными конечными полями решаются сложнее. В работе [6] были определены бент-функции над конечными полями. Позже в [7] были рассмотрены бент-функции над произвольными конечными абелевыми группами. В ней для измерения похожести функций использовалась функция “близость”, основанная на том, что две функции f и g наиболее непохожи друг на друга, если последовательность, состоящая из всех значений функции $f - g$ сбалансирована, т.е. в ней каждый элемент поля появляется с одинаковой частотой. В работах [8, 9] похожесть функций над полями характеристики два описывалась функцией “согласие”, отличавшейся от функции “близость” только нормирующим множителем. В работе [10] в качестве меры приближения функции классом всех аффинных функций над конечным полем была определена линейная характеристика функции. Данная характеристика функции тесно связана с понятием корреляции между функциями и последовательностями.

Основными результатами работы являются широкие классы сбалансированных функций над конечными полями, для которых указаны оценки значений линейной характеристики. С целью понимания основных результатов статьи приводятся уже известные результаты в удобных для нас обозначениях.

§ 2. Линейная характеристика функций

Пусть $P = GF(q)$ – произвольное конечное поле из q элементов, $q = p^t$, где p – простое число, а t – натуральное. В данной работе обозначение P всегда будет подразумевать выбор такого поля.

Рассмотрим функцию $f\colon P^n \to P$ от n переменных, заданную на поле P. Будем использовать обозначение $f = f(x_1, \ldots, x_n) = f(\vec{x})$, где $\vec{x} = (x_1, \ldots, x_n)$. Назовем функцию f сбалансированной, если для всех $a \in P$ мощность полного прообраза элемента a при действии отображения f удовлетворяет условию $|f^{-1}(a)| = q^{n-1}$.

Группа всех аддитивных характеров поля P (гомоморфизмов группы $(P, +)$ в мультипликативную группу $\mathbb{C}^*$ поля комплексных чисел) состоит из гомоморфизмов (см., например, [11])

$$\chi_a(x) = e^{2\pi i \frac{\mathrm{Tr}_{P_0}^P(ax)}{p}} = \exp\left\{2\pi i \frac{\mathrm{Tr}_{P_0}^P(ax)}{p}\right\}, \quad x \in P, \tag{1}$$

где $a \in P$, $P_0 = GF(p)$, $\mathrm{Tr}_{P_0}^P$ – функция следа из поля P в простое подполе P_0. Характер χ_0 называют тривиальным характером.

Коэффициентом кросс-корреляции между функциями $f(\vec{x})$ и $g(\vec{x})$, соответствующим характеру χ_a, называют комплексное число

$$C_a(f, g) = \sum_{x_1, \ldots, x_n \in P} \chi_a(f(\vec{x}) - g(\vec{x})). \tag{2}$$

Модуль коэффициента $C_a(f, g)$ характеризует близость между функциями $f(\vec{x})$ и $g(\vec{x})$ (см. [12]).

Обозначим через $A_n(P)$ множество всех аффинных функций $g(\vec{x})$ от n переменных над полем P, т.е. функций вида

$$g(\vec{x}) = a_0 + a_1 x_1 + \ldots + a_n x_n,$$

где $a_0, a_1, \ldots, a_n \in P$. Для линейной функции $g_0(\vec{x})$ от n переменных над полем P будем использовать обозначение

$$g_0(\vec{x}) = a_1 x_1 + \ldots + a_n x_n = \langle \vec{a}, \vec{x} \rangle,$$

где $\vec{a} = (a_1, \ldots, a_n)$, $\vec{x} = (x_1, \ldots, x_n)$.

Мультипликативную группу поля P обозначим через P^*. Линейной характеристикой функции f назовем число

$$C(f) = \max_{a \in P^*} \max_{g \in A_n(P)} |C_a(f, g)|. \tag{3}$$

Предложение 1. *Справедливо равенство*

$$C(f) = \max_{a \in P^*} \max_{a_1, \ldots, a_n \in P} \left| \sum_{x_1, \ldots, x_n \in P} \exp\left\{2\pi i \frac{\mathrm{Tr}_{P_0}^P(af(\vec{x}) - a_1 x_1 - \ldots - a_n x_n)}{p}\right\} \right|.$$

Доказательство. Заметим, что $C_a(f, a_0 + \langle \vec{a}, \vec{x} \rangle) = \chi_a(-a_0) C_a(f, \langle \vec{a}, \vec{x} \rangle)$, и так как $|\chi_a(-a_0)| = 1$, то согласно равенствам (1), (2)

$$C(f) = \max_{a \in P^*} \max_{a_1, \ldots, a_n \in P} |C_a(f, \langle \vec{a}, \vec{x} \rangle)| =$$

$$= \max_{a \in P^*} \max_{a_1, \ldots, a_n \in P} \left| \sum_{x_1, \ldots, x_n \in P} \exp\left\{2\pi i \frac{\mathrm{Tr}_{P_0}^P(af(\vec{x}) - aa_1 x_1 - \ldots - aa_n x_n)}{p}\right\} \right|.$$

Отсюда получаем

$$C(f) = \max_{a\in P^*} \max_{a_1,\ldots,a_n\in P} \left| \sum_{x_1,\ldots,x_n\in P} \exp\left\{ 2\pi i \frac{\mathrm{Tr}_{P_0}^{P}(af(\vec{x}) - a_1x_1 - \ldots - a_nx_n)}{p} \right\} \right|. \quad \blacktriangle$$

Рассмотрим, как ведет себя параметр $C(f)$ в частном случае $P = GF(2) = \{0, e\}$. В этой ситуации

$$\exp\left\{ 2\pi i \frac{\mathrm{Tr}_{P_0}^{P}(af(\vec{x}) - a_1x_1 - \ldots - a_nx_n)}{p} \right\} = (-1)^{f(\vec{x})\oplus a_1x_1\oplus\ldots\oplus a_nx_n},$$

коэффициент кросс-корреляции $C_e(f, \langle\vec{a}, \vec{x}\rangle)$ равен коэффициенту Уолша – Адамара

$$W_f(\vec{a}) = \sum_{x_1,\ldots,x_n\in P} (-1)^{f(\vec{x})\oplus a_1x_1\oplus\ldots\oplus a_nx_n}$$

булевой функции f, и справедливо равенство

$$C(f) = \max_{\vec{a}\in P^n} |W_f(\vec{a})|.$$

Отметим, что в двоичном случае наиболее удобной для использования является нелинейность $\mathrm{nl}(f)$ булевой функции f, которая равна расстоянию Хэмминга между столбцом значений функции f и столбцами значений всех аффинных двоичных функций от n переменных. Известно (см., например, [4]), что

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\max_{\vec{a}\in P^n} |W_f(\vec{a})| = 2^{n-1} - \frac{1}{2}C(f).$$

В случае произвольного конечного поля P понятие нелинейности функции, основанное на расстоянии Хэмминга, используется в работе [13].

Пусть

$$f\colon P^n \to P, \quad g(\vec{x}) = a_0 + a_1x_1 + \ldots + a_nx_n, \quad b \in P.$$

Обозначим через $N(f, g, b)$ число всех векторов $\vec{x} \in P^n$, таких что $f(\vec{x}) - g(\vec{x}) = b$.

Предложение 2. *Справедлива оценка*

$$\left|N(f, g, b) - q^{n-1}\right| \leqslant \frac{q-1}{q}C(f),$$

где $C(f)$ – линейная характеристика функции f.

Доказательство. Согласно [11]

$$\frac{1}{q}\sum_{a\in P} \chi_a(x) = \begin{cases} 1, & \text{если } x = 0, \\ 0, & \text{если } x \neq 0, \end{cases} \tag{4}$$

где χ_a – характер, определенный равенством (1). Используя это соотношение, получаем

$$N(f, g, b) = \frac{1}{q}\sum_{\vec{x}\in P^n}\sum_{a\in P} \chi_a(f(\vec{x}) - g(\vec{x}) - b).$$

Учитывая, что $\chi_0(z) = 1$ для всех $z \in P$, и выделяя отдельно слагаемое, соответствующее случаю $a = 0$, имеем

$$N(f,g,b) - q^{n-1} = \frac{1}{q} \sum_{a \in P^*} \chi_a(-b) \sum_{\vec{x} \in P^n} \chi_a(f(\vec{x}) - g(\vec{x})).$$

Тогда

$$\left|N(f,g,b) - q^{n-1}\right| \leqslant \frac{1}{q} \sum_{a \in P^*} |C_a(f,g)| \leqslant \frac{q-1}{q} C(f). \quad \blacktriangle$$

Функцию $f\colon P^n \to P$ назовем бент-функцией (см. [6, 7]), если $|C_a(f,g)| = q^{n/2}$ для всех $a \in P^*$ и всех $g \in A_n(P)$. Приведем определение бент-функции в терминах линейной характеристики. Непосредственно из результатов работ [6, 7, 9] вытекает следующий результат.

Предложение 3. *Для каждой функции $f\colon P^n \to P$ верна оценка*

$$C(f) \geqslant q^{\frac{n}{2}},$$

которая обращается в равенство тогда и только тогда, когда f является бент-функцией.

§ 3. Некоторые известные результаты

Приведем известные факты, относящиеся к теории функций, заданных на конечных полях. Они понадобятся в дальнейшем для доказательства основных результатов. При этом будем использовать удобные для нас обозначения.

Пусть $n = 2k$, π – подстановка на множестве P^k с координатными функциями $\pi_1, \ldots, \pi_k$, а $h\colon P^k \to P$ – произвольная функция. Для всех $\vec{x}, \vec{y} \in P^k$ определим функцию $f\colon P^n \to P$ равенством

$$f(\vec{x}, \vec{y}) = \langle \pi(\vec{x}), \vec{y} \rangle + h(\vec{x}) = \pi_1(\vec{x}) y_1 + \ldots + \pi_k(\vec{x}) y_k + h(\vec{x}). \tag{5}$$

Такие функции для поля из двух элементов были впервые рассмотрены в статье [14]. Приведем теорему, вытекающую из результатов работы [15].

Теорема 1. *Функция f, определенная равенством* (5), *является бент-функцией, причем для всех $a \in P^*$ и линейных функций $g(\vec{x}, \vec{y}) = \langle (\vec{a}, \vec{b}), (\vec{x}, \vec{y}) \rangle$ верно равенство*

$$C_a(f,g) = q^k \chi_a\big(h(\pi^{-1}(\vec{b})) - \langle \vec{a}, \pi^{-1}(\vec{b}) \rangle\big).$$

Указанное множество бент-функций называется классом Майораны – Макфарланда. Ранее в случае, когда q – простое число, теорема 1 была доказана в работах [16, 17]. Бент-функция $f\colon P^n \to P$ называется регулярной [17], если для всех $a \in P^*$ и $g \in A_n(P)$ выполнено равенство $C_a(f,g) = q^{n/2} e^{2\pi i k(a,g)/p}$, где $0 \leqslant k(a,g) \leqslant p-1$. Функции из класса Майораны – Макфарланда являются регулярными.

Приведем критерий Г. Вейля [18] сбалансированности последовательности элементов поля в удобной для дальнейшего изложения форме. Назовем последовательность $c_0, \ldots, c_{t-1}$ элементов поля P сбалансированной, если в ней каждый элемент поля P появляется одинаковое число раз. В частности, отсюда будет следовать, что t делится на q.

Предложение 4 [18]. *Последовательность $c_0, \ldots, c_{t-1}$ сбалансирована тогда и только тогда, когда для всех $a \in P^*$*

$$\sum_{i=0}^{t-1} \chi_a(c_i) = 0.$$

Укажем критерий сбалансированности функции $f\colon P^n \to P$ в терминах коэффициентов кросс-корреляции. Функция f сбалансирована тогда и только тогда, когда сбалансирована последовательность $f(x_1, \ldots, x_n)$, $x_1, \ldots, x_n \in P$, всех ее значений. Согласно предложению 4 это равносильно условию

$$\sum_{x_1,\ldots,x_n \in P} \chi_a(f(x_1, \ldots, x_n)) = C_a(f, 0) = 0$$

для всех $a \in P^*$. Таким образом, справедлив следующий факт.

Следствие 1. *Функция f является сбалансированной тогда и только тогда, когда $C_a(f, 0) = 0$ для всех $a \in P^*$.*

Пусть $k \in \mathbb{N}$, $f\colon P^n \to P$. Для любых элементов $a_1, \ldots, a_k \in P$ и различных натуральных чисел $i_1, \ldots, i_k \in \{1, 2, \ldots, n\}$ обозначим через $f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}$ функцию, полученную из $f(x_1, \ldots, x_n)$ фиксацией переменных $x_{i_1}, \ldots, x_{i_k}$ значениями $a_1, \ldots, a_k$ соответственно. Назовем функцию f корреляционно-иммунной порядка k [19], если для всех $a_1, \ldots, a_k \in P$, $i_1, \ldots, i_k \in \{1, 2, \ldots, n\}$, таких что $1 \leqslant i_1 < \ldots < i_k \leqslant n$, и всех $z \in P$ для прообразов элемента z при действии отображений $f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}$ и f верны равенства

$$\left| \left(f_{i_1,\ldots,i_k}^{a_1,\ldots,a_k}\right)^{-1}(z) \right| = \frac{|f^{-1}(z)|}{q^k}. \tag{6}$$

Данное определение обобщает на случай произвольного поля P понятие корреляционно-иммунной булевой функции порядка k (см., например, [4]). Корреляционно-иммунную функцию f порядка k, являющуюся сбалансированной, называют еще k-устойчивой, или k-эластичной функцией. Отметим, что наряду с известными применениями в области защиты информации для симметричных криптосистем, k-устойчивые функции как частный случай k-устойчивых отображений (см. [20]) используются в задачах построения протоколов квантового распределения ключей (см., например, [21]).

Несложно заметить, что если функция является корреляционно-иммунной порядка k, то она является корреляционно-иммунной порядка $k-1$. Кроме того, если функция f является 1-устойчивой, то f сбалансирована. Поэтому сбалансированные функции считают 0-устойчивыми. Обозначим через $\|\vec{a}\|$ число ненулевых координат вектора $\vec{a}$. Для корреляционно-иммунных функций f порядка k справедлив аналог теоремы, доказанной ранее для случая $q = 2$ в работе [22].

Теорема 2 [19]. *Функция $f\colon P^n \to P$ является корреляционно-иммунной порядка k тогда и только тогда, когда для каждого $\vec{a} \in P^n$, такого что $1 \leqslant \|\vec{a}\| \leqslant k$, при всех $a \in P^*$ имеет место равенство $C_a(f, (\vec{a}, \vec{x})) = 0$.*

С использованием критерия сбалансированности функции непосредственно из теоремы 2 получим критерий k-устойчивости функции.

Следствие 2 [19]. *Функция $f\colon P^n \to P$ является k-устойчивой тогда и только тогда, когда для каждого $\vec{a} \in P^n$, такого что $0 \leqslant \|\vec{a}\| \leqslant k$, при всех $a \in P^*$ имеет место равенство $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$.*

Пусть $g_1, \ldots, g_{n+1}$ – произвольные подстановки поля P,

$f(x_1, \ldots, x_n) = g_{n+1}(g_1(x_1) + \ldots + g_n(x_n))$.

Для всех $\{i_1, \ldots, i_{n-1}\} \subset \{1, \ldots, n\}$, $a_1, \ldots, a_{n-1} \in P$, $z \in P$ справедливо равенство

$$\left| \left(f_{i_1,\ldots,i_{n-1}}^{a_1,\ldots,a_{n-1}} \right)^{-1} (z) \right| = 1,$$

так как если $\{j\} = \{1, \ldots, n\} \setminus \{i_1, \ldots, i_{n-1}\}$, то

$f_{i_1,\ldots,i_{n-1}}^{a_1,\ldots,a_{n-1}}(x_j) = g_{n+1}(g_j(x_j) + c)$,

где $c \in P$ – некоторая константа. Таким образом, f является $(n-1)$-устойчивой функцией, и класс k-устойчивых функций непуст при каждом $k < n$.

Остается актуальной задача нахождения числа k-устойчивых функций над конечным полем. В настоящее время получены только асимптотические (см., например, [23]) и рекуррентные (см. [24]) оценки для случаев булевых функций и отображений.

Пусть e – единица поля P. Функция $f\colon P^n \to P$ задается многочленом

$$f(x_1, \ldots, x_n) = \sum_{a_1,\ldots,a_n \in P} f(a_1, \ldots, a_n)\big(e - (x_1 - a_1)^{q-1}\big) \ldots \big(e - (x_n - a_n)^{q-1}\big)$$

(см. [11, 25]), который после раскрытия скобок принимает вид

$$f(x_1, \ldots, x_n) = \sum_{i_1=0}^{q-1} \ldots \sum_{i_n=0}^{q-1} c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n},$$

где $c_{i_1 \ldots i_n} \in P$. Среди всех многочленов от n переменных, имеющих степень по каждой переменной не выше $q-1$, многочлен, задающий функцию f, будет единственным. Степень монома $c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$ определяется по правилу

$$\deg c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} = \begin{cases} i_1 + \ldots + i_n, & \text{если } c_{i_1 \ldots i_n} \neq 0, \\ -\infty, & \text{если } c_{i_1 \ldots i_n} = 0. \end{cases}$$

Степень функции f (см., например, [26]) определяется равенством

$$\deg f = \max\big\{\deg c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} : 0 \leqslant i_1 \leqslant q-1, \ldots, 0 \leqslant i_n \leqslant q-1\big\}.$$

Каждое число $j \in \{0, 1, \ldots, q-1\}$ запишем в p-ичном представлении:

$j = j_0 + pj_1 + \ldots + p^{t-1} j_{t-1}$,

где $j_0, j_1, \ldots, j_{t-1} \in \{0, 1, \ldots, p-1\}$. В этом случае число

$\|j\|_p = j_0 + j_1 + \ldots + j_{t-1}$

назовем p-ичным весом числа j. Степенью нелинейности монома $c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$ назовем величину

$$\mathrm{dl}\, c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} = \begin{cases} \|i_1\|_p + \ldots + \|i_n\|_p, & \text{если } c_{i_1 \ldots i_n} \neq 0, \\ -\infty, & \text{если } c_{i_1 \ldots i_n} = 0. \end{cases}$$

Степень нелинейности функции f (см., например, [26]) определяется равенством

$$\mathrm{dl}\, f = \max\big\{\mathrm{dl}\, c_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} : 0 \leqslant i_1 \leqslant q-1, \ldots, 0 \leqslant i_n \leqslant q-1\big\}.$$

Согласно результатам работы [19], если f – сбалансированная функция, то

$\deg f \leqslant n(q-1)-1, \quad \mathrm{dl}\, f \leqslant nt(p-1)-1.$

§ 4. Конструкция разветвления функций

Пусть $P = \{r_1, \ldots, r_q\}$, и пусть $f_{r_i}\colon P^{n-1} \to P$, $i = 1, \ldots, q$, – функции от $n-1$ переменных. Зададим функцию $f\colon P^n \to P$ по правилу

$$f(x_1, x_2, \ldots, x_n) = \begin{cases} f_{r_1}(x_2, \ldots, x_n), & \text{если } x_1 = r_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ f_{r_q}(x_2, \ldots, x_n), & \text{если } x_1 = r_q. \end{cases} \tag{7}$$

Функцию f будем называть разветвлением функций $f_{r_1}, \ldots, f_{r_q}$.

Т е о р е м а 3. *Пусть функция f построена по правилу* (7). *Тогда*:

1) *Функция f сбалансирована тогда и только тогда, когда для всех $a \in P^*$*

$$C_a(f_{r_1}, 0) + \ldots + C_a(f_{r_q}, 0) = 0;$$

2) *Если функции $f_{r_1}, \ldots, f_{r_q}$ являются корреляционно-иммунными порядка k и для всех $a \in P^*$ выполнено*

$$C_a(f_{r_1}, 0) = \ldots = C_a(f_{r_q}, 0),$$

то функция f является корреляционно-иммунной порядка k;

3) *Если функции $f_{r_1}, \ldots, f_{r_q}$ являются k-устойчивыми, то функция f является k-устойчивой*;

4) *Линейные характеристики функций связаны соотношением*

$$C(f) \leqslant C(f_{r_1}) + \ldots + C(f_{r_q});$$

5) $\deg f \leqslant q - 1 + \max\{\deg f_{r_i} : i = 1, \ldots, q\}$;

6) $\mathrm{dl}\, f \leqslant (p-1)t + \max\{\mathrm{dl}\, f_{r_i} : i = 1, \ldots, q\}$.

Д о к а з а т е л ь с т в о. Рассмотрим символ Кронекера

$$\delta_{x,a} = \begin{cases} e, & \text{если } x = a, \\ 0, & \text{если } x \neq a, \end{cases}$$

определенный для всех $x, a \in P$, где e – единица поля P. Тогда

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{q} \delta_{x_1, r_i} f_{r_i}(x_2, \ldots, x_n).$$

Для всех $a \in P^*$ рассмотрим

$$C_a(f, \langle \vec{a}, \vec{x} \rangle) = \sum_{x_1, \ldots, x_n \in P} \chi_a\big(f(x_1, \ldots, x_n) - a_1x_1 - \ldots - a_nx_n\big) =$$

$$= \sum_{i=1}^{q} \sum_{x_2, \ldots, x_n \in P} \chi_a\big(f_{r_i}(x_2, \ldots, x_n) - a_1r_i - a_2x_2 - \ldots - a_nx_n\big) =$$

$$= \sum_{i=1}^{q} \chi_a(-a_1r_i) \sum_{x_2, \ldots, x_n \in P} \chi_a\big(f_{r_i}(x_2, \ldots, x_n) - a_2x_2 - \ldots - a_nx_n\big).$$

Получаем

$$C_a(f, \langle \vec{a}, \vec{x} \rangle) = \sum_{i=1}^{q} \chi_a(-a_1 r_i) C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n). \tag{8}$$

Утверждение 1) следует из равенства

$$C_a(f, 0) = C_a(f_{r_1}, 0) + \ldots + C_a(f_{r_q}, 0)$$

и следствия 1.

Докажем утверждение 2). Согласно теореме 2 достаточно доказать, что для всех $a \in P^*$ и $\vec{a} = (a_1, \ldots, a_n) \in P^n$, таких что $1 \leqslant \|\vec{a}\| \leqslant k$, выполнено $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$. Если $a_1 = 0$, то $1 \leqslant \|(a_2, \ldots, a_n)\| \leqslant k$, и по теореме 2

$$C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n) = 0, \quad i = 1, \ldots, q.$$

Значит, $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$. Если $a_1 \neq 0$ и $1 \leqslant \|(a_2, \ldots, a_n)\| \leqslant k - 1$, то по теореме 2

$$C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n) = 0, \quad i = 1, \ldots, q,$$

и $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$. Осталось рассмотреть случай, когда $a_1 \neq 0$ и $(a_2, \ldots, a_n) = \vec{0}$. В этом случае согласно (8)

$$C_a(f, \langle \vec{a}, \vec{x} \rangle) = \sum_{i=1}^{q} \chi_a(-a_1 r_i) C_a(f_{r_i}, 0).$$

Так как $C_a(f_{r_1}, 0) = \ldots = C_a(f_{r_q}, 0)$, то

$$C_a(f, \langle \vec{a}, \vec{x} \rangle) = C_a(f_{r_1}, 0) \sum_{i=1}^{q} \chi_a(-a_1 r_i).$$

Из соотношений (4) следует, что

$$\sum_{i=1}^{q} \chi_a(-a_1 r_i) = 0,$$

поэтому $C_a(f, \langle \vec{a}, \vec{x} \rangle) = 0$.

Утверждение 3) непосредственно следует из утверждений 1), 2) и следствий 1, 2.

Утверждение 4) вытекает из соотношений

$$|C_a(f, \langle \vec{a}, \vec{x} \rangle)| \leqslant \sum_{i=1}^{q} |\chi_a(-a_1 r_i) C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n)| =$$
$$= \sum_{i=1}^{q} |C_a(f_{r_i}, a_2 x_2 + \ldots + a_n x_n)| \leqslant \sum_{i=1}^{q} C(f_{r_i}),$$

справедливых для всех $a \in P^*$ и $\vec{a} \in P^n$.

Используя интерполяционную формулу Лагранжа, получим

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{q} \delta_{x_1, r_i} f_{r_i}(x_2, \ldots, x_n) =$$
$$= \sum_{i=1}^{q} \frac{(x_1 - r_1) \ldots (x_1 - r_{i-1})(x_1 - r_{i+1}) \ldots (x_1 - r_q)}{(r_i - r_1) \ldots (r_i - r_{i-1})(r_i - r_{i+1}) \ldots (r_i - r_q)} f_{r_i}(x_2, \ldots, x_n).$$

Непосредственно из этого равенства следуют утверждения 5) и 6). ▲

Впервые аналогичная конструкция для булевых функций была рассмотрена в работе [27], где были доказаны аналоги утверждений 2) и 3) теоремы 3.

В случае $f_{r_1} = \ldots = f_{r_q}$ функция f, построенная по правилу (7), удовлетворяет равенству $f(x_1, \ldots, x_n) = f_{r_1}(x_2, \ldots, x_n)$. Если $r_1 = 0$, $f_{r_2} = \ldots = f_{r_q} = f_1$, $f_0 \neq f_1$, то

$$f(x_1, x_2, \ldots, x_n) = \begin{cases} f_0(x_2, \ldots, x_n), & \text{если } x_1 = 0, \\ f_1(x_2, \ldots, x_n), & \text{если } x_1 \neq 0, \end{cases}$$

и функция f будет задаваться формулой

$$f(x_1, x_2, \ldots, x_n) = x_1^{q-1} f_1(x_2, \ldots, x_n) + (e - x_1^{q-1}) f_0(x_2, \ldots, x_n).$$

Рассмотрим теперь важную с практической точки зрения конструкцию разветвления бент-функций. Пусть $n = 2k$, $\vec{x}, \vec{y} \in P^k$, $f_{r_i}(\vec{x}, \vec{y}) = \langle \pi_i(\vec{x}), \vec{y} \rangle + h_i(\vec{y})$ – бент-функция из класса Майораны – Макфарланда, где $i = 1, \ldots, q$. Рассмотрим функцию

$$f(x, \vec{x}, \vec{y}) = \sum_{i=1}^{q} \delta_{x, r_i} f_{r_i}(\vec{x}, \vec{y}), \quad x \in P, \tag{9}$$

построенную по правилу (7) из функций $f_{r_1}, \ldots, f_{r_q}$.

Теорема 4. *Пусть функция f построена по правилу* (9). *Тогда*:

1) *Функция f сбалансирована тогда и только тогда, когда все элементы*

$$h_1(\pi_1^{-1}(\vec{0})), \ldots, h_q(\pi_q^{-1}(\vec{0}))$$

попарно различны;

2) *Линейная характеристика функции f удовлетворяет неравенству*

$$C(f) \leqslant q^{\frac{n}{2}+1}.$$

Доказательство. Докажем утверждение 1). Согласно теореме 1 для всех $a \in P^*$ выполнено

$$C_a(f_{r_i}, 0) = q^k \chi_a(h_i(\pi_i^{-1}(\vec{0}))), \quad i = 1, \ldots, q.$$

По теореме 3 и следствию 1 функция f сбалансирована тогда и только тогда, когда

$$C_a(f, 0) = \sum_{i=1}^{q} C_a(f_{r_i}, 0) = q^k \sum_{i=1}^{q} \chi_a(h_i(\pi_i^{-1}(\vec{0}))) = 0$$

для всех $a \in P^*$. Из предложения 4 следует, что это равносильно сбалансированности последовательности $h_1(\pi_1^{-1}(\vec{0})), \ldots, h_q(\pi_q^{-1}(\vec{0}))$.

Утверждение 2) непосредственно следует из теоремы 3 и равенств

$$C(f_{r_i}) = q^{n/2}, \quad i = 1, \ldots, q. \quad ▲$$

§ 5. Конструкция Майораны – Макфарланда

Применим конструкцию Майораны – Макфарланда для построения сбалансированных функций. Пусть $n = 2k$, и пусть φ – линейное преобразование на множестве P^k с координатными функциями $\varphi_1, \ldots, \varphi_k$, определенное по правилу

$$\varphi(\vec{x}) = \vec{x} M,$$

где $M = (m_{ij})_{k\times k}$ – матрица размера $k \times k$ над полем P, имеющая ранг $k-1$. Для произвольной функции $h\colon P^k \to P$ и всех $\vec{x}, \vec{y} \in P^k$ определим функцию $f\colon P^n \to P$ равенством

$$f(\vec{x},\vec{y}) = \langle\varphi(\vec{x}),\vec{y}\rangle + h(\vec{x}) = \varphi_1(\vec{x})y_1 + \ldots + \varphi_k(\vec{x})y_k + h(\vec{x}). \tag{10}$$

Множество $\varphi^{-1}(\vec{0})$ является линейным пространством размерности 1, порожденным некоторым ненулевым вектором $\vec{c} \in P^n$, т.е.

$$\varphi^{-1}(\vec{0}) = \{r\vec{c}\colon\ r \in P\}.$$

Отметим, что в классической конструкции Майораны – Макфарланда в качестве отображения φ берется произвольная подстановка на множестве P^k. В этом случае функция f, задаваемая равенством (10), является бент-функцией.

Т е о р е м а 5. *Пусть функция f определена равенством* (10). *Тогда*:

1) *f – сбалансированная функция тогда и только тогда, когда $h(a\vec{c}) \neq h(b\vec{c})$ для всех различных $a, b \in P$;*
2) *Если* $\deg h \geqslant 3$, *то* $\deg f = \deg h$;
3) *Если* $\mathrm{dl}\, h \geqslant 3$, *то* $\mathrm{dl}\, f = \mathrm{dl}\, h$;
4) $C(f) \leqslant q^{\frac{n}{2}+1}$.

Д о к а з а т е л ь с т в о. Обозначим через L линейное пространство, порожденное системой всех строк матрицы M. Тогда, если $\vec{b} \notin L$, то $\varphi^{-1}(\vec{b}) = \varnothing$, а если $\vec{b} \in L$, то

$$\varphi^{-1}(\vec{b}) = \vec{d} + \varphi^{-1}(\vec{0}), \tag{11}$$

где $\vec{d}$ – фиксированный вектор, такой что $\vec{d}M = \vec{b}$. Рассмотрим для всех $\vec{a}, \vec{b} \in P^k$ и $a \in P^*$ коэффициент кросс-корреляции

$$C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) = \sum_{\vec{x}\in P^k} \chi_a(h(\vec{x}) - \langle\vec{a},\vec{x}\rangle) \sum_{\vec{y}\in P^k} \chi_a(\langle\varphi(\vec{x}),\vec{y}\rangle - \langle\vec{b},\vec{y}\rangle) =$$

$$= \sum_{\vec{x}\in P^k} \chi_a(h(\vec{x}) - \langle\vec{a},\vec{x}\rangle) \sum_{\vec{y}\in P^k} \chi_a(\langle\varphi(\vec{x}) - \vec{b},\vec{y}\rangle).$$

Заметим, что

$$\sum_{\vec{y}\in P^k} \chi_a(\langle\varphi(\vec{x}) - \vec{b},\vec{y}\rangle) = \begin{cases} q^k, & \text{если } \varphi(\vec{x}) = \vec{b}, \\ 0, & \text{если } \varphi(\vec{x}) \neq \vec{b}, \end{cases}$$

поэтому если $\vec{b} \notin L$, то $C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) = 0$, а если $\vec{b} \in L$, то

$$C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) = q^k \sum_{\vec{x}\in\varphi^{-1}(\vec{b})} \chi_a(h(\vec{x}) - \langle\vec{a},\vec{x}\rangle) =$$

$$= q^k \sum_{r\in P} \chi_a(h(\vec{d} + r\vec{c}) - \langle\vec{a},\vec{d} + r\vec{c}\rangle) =$$

$$= q^k \chi_a(-\langle\vec{a},\vec{d}\rangle) \sum_{r\in P} \chi_a(h(\vec{d} + r\vec{c}) - \langle\vec{a}, r\vec{c}\rangle).$$

В частности,

$$|C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle)| = q^k \left| \sum_{r\in P} \chi_a(h(\vec{d} + r\vec{c}) - \langle\vec{a}, r\vec{c}\rangle) \right|. \tag{12}$$

Докажем утверждение 1). Согласно следствию 1 функция f сбалансирована тогда и только тогда, когда $C_a(f,0)=0$ для всех $a\in P^*$. Из равенства (11) следует, что при $\vec{a}=\vec{b}=\vec{0}$ выполнено $\vec{d}=\vec{0}$, поэтому с использованием равенства (12) получим, что $C_a(f,0)=0$ для всех $a\in P^*$ тогда и только тогда, когда

$$\sum_{r\in P}\chi_a(h(\vec{0}+r\vec{c}))=0,$$

для всех $a\in P^*$. Согласно предложению 4 полученные соотношения равносильны сбалансированности последовательности, составленной из элементов $h(r\vec{c})$, $r\in P$, т.е. условию $h(a\vec{c})\neq h(b\vec{c})$ для всех различных $a,b\in P$.

Докажем утверждения 2) и 3). Имеем равенство

$$f(\vec{x},\vec{y})=y_1\vec{x}M_1^{\downarrow}+\ldots+y_k\vec{x}M_k^{\downarrow}+h(\vec{x})=\sum_{i,j=1}^{k}m_{ij}x_iy_j+h(\vec{x}),$$

из которого получаем

$$\deg f=\begin{cases}2, & \text{если } \deg h\leqslant 2,\\ \deg h, & \text{если } \deg h\geqslant 3,\end{cases}$$

$$\mathrm{dl}\, f=\begin{cases}2, & \text{если } \mathrm{dl}\, h\leqslant 2,\\ \mathrm{dl}\, h, & \text{если } \mathrm{dl}\, h\geqslant 3.\end{cases}$$

Утверждение 4) непосредственно следует из равенства (12). ▲

§ 6. Аналог конструкции Доббертина

Пусть $n=2k$, $\vec{x},\vec{y}\in P^k$, $h(\vec{x},\vec{y})$ – бент-функция над полем P от n переменных. По аналогии с работой [1] назовем бент-функцию h нормальной, если существует линейное многообразие $M=\vec{\alpha}+L$, где $\vec{\alpha}\in P^n$, а L – линейное пространство размерности k над полем P, такое что ограничение h на множество M является константой. Пусть эта константа равна c. Отметим, что бент-функции из класса Майораны – Макфарланда являются нормальными. Пример булевой бент-функции, не являющейся нормальной, был построен нетривиальным методом в работе [28].

Для построения сбалансированных функций используем нормальную бент-функцию. Рассмотрим $L_0=\{(\vec{0},\vec{y}):\ \vec{y}\in P^k\}$. Выберем обратимое линейное преобразование $\tau\colon P^n\to P^n$, такое что $\tau(L)=L_0$. Рассмотрим бент-функцию

$$\varphi(\vec{x},\vec{y})=h(\tau^{-1}(\vec{x},\vec{y})).$$

Ясно, что

$$\varphi(\tau(\vec{\alpha})+L_0)=h(\tau^{-1}(\tau(\vec{\alpha})+L_0))=h(\alpha+L)=c.$$

Пусть $\tau(\vec{\alpha})=(\vec{x}_0,\vec{y}_0)$, тогда $\tau(\vec{\alpha})+L_0=(\vec{x}_0,\vec{0})+L_0$ и $\varphi((\vec{x}_0,\vec{0})+L_0)=c$. Выберем произвольную функцию $g\colon P^k\to P$ и построим функцию $f(\vec{x},\vec{y})$ по правилу

$$f(\vec{x},\vec{y})=\begin{cases}g(\vec{y}), & \text{если } \vec{x}=\vec{x}_0,\\ \varphi(\vec{x},\vec{y}), & \text{если } \vec{x}\neq\vec{x}_0.\end{cases}\tag{13}$$

Впервые эта конструкция для булевых функций (при $q=2$) и в более частном виде, когда $c=0$, $\vec{x}_0=\vec{0}$, была предложена Г. Доббертином в работе [1]. Следующая теорема обобщает результаты этой работы на случай произвольного поля из q элементов.

Теорема 6. *Пусть функция f определена равенством* (13). *Тогда*:

1) *f – сбалансированная функция тогда и только тогда, когда g – сбалансированная функция*;
2) $C(f) \leqslant q^{\frac{n}{2}} + C(g)$;
3) *Если* $\deg\varphi \leqslant (q-1)n/2$ *и* $g(\vec{y}) \neq \text{const}$, *то* $\deg f = (q-1)n/2 + \deg g$;
4) *Если* $\operatorname{dl}\varphi \leqslant t(p-1)n/2$ *и* $g(\vec{y}) \neq \text{const}$, *то* $\operatorname{dl} f = t(p-1)n/2 + \operatorname{dl} g$.

Доказательство. Найдем для всех $a \in P^*$ и $\vec{a}, \vec{b} \in P^k$ коэффициент кросс-корреляции:

$$C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) = \sum_{\vec{x},\vec{y}\in P^k} \chi_a(f(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle) =$$

$$= \sum_{\vec{y}\in P^k} \chi_a(g(\vec{y}) - \langle\vec{a},\vec{x}_0\rangle - \langle\vec{b},\vec{y}\rangle) + \sum_{\substack{\vec{x},\vec{y}\in P^k \\ \vec{x}\neq\vec{x}_0}} \chi_a(\varphi(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle) =$$

$$= \chi_a(-\langle\vec{a},\vec{x}_0\rangle) C_a(g, \langle\vec{b},\vec{y}\rangle) + S(\vec{a},\vec{b}).$$

Вычислим величину

$$S(\vec{a},\vec{b}) = \sum_{\substack{\vec{x}\neq\vec{x}_0 \\ \vec{y}\in P^k}} \chi_a(\varphi(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle).$$

Для этого изучим

$$\sum_{\substack{\vec{x}=\vec{x}_0 \\ \vec{y}\in P^k}} \chi_a(\varphi(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle) = \sum_{\vec{y}\in P^k} \chi_a(c - \langle\vec{a},\vec{x}_0\rangle - \langle\vec{b},\vec{y}\rangle) =$$

$$= \chi_a(c - \langle\vec{a},\vec{x}_0\rangle) \sum_{\vec{y}\in P^k} \chi_a(-\langle\vec{b},\vec{y}\rangle).$$

Так как

$$\sum_{\vec{y}\in P^k} \chi_a(-\langle\vec{b},\vec{y}\rangle) = \begin{cases} 0, & \text{если } \vec{b} \neq \vec{0}, \\ q^k, & \text{если } \vec{b} = \vec{0}, \end{cases}$$

что равно $q^k\delta_{\vec{b},\vec{0}}$, то

$$\sum_{\substack{\vec{x}=\vec{x}_0 \\ \vec{y}\in P^k}} \chi_a(\varphi(\vec{x},\vec{y}) - \langle\vec{a},\vec{x}\rangle - \langle\vec{b},\vec{y}\rangle) = \chi_a(c - \langle\vec{a},\vec{x}_0\rangle) q^k \delta_{\vec{b},\vec{0}}.$$

Следовательно,

$$S(\vec{a},\vec{b}) + \chi_a(c - \langle\vec{a},\vec{x}_0\rangle) q^k \delta_{\vec{b},\vec{0}} = C_a(\varphi, \langle\vec{a},\vec{x}\rangle + \langle\vec{b},\vec{y}\rangle),$$

и справедливо равенство

$$C_a(f, \langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle) =$$
$$= \chi_a(-\langle\vec{a},\vec{x}_0\rangle) \left(C_a(g, \langle\vec{b},\vec{y}\rangle) + \chi_a(\langle\vec{a},\vec{x}_0\rangle) C_a(\varphi, \langle\vec{a},\vec{x}\rangle + \langle\vec{b},\vec{y}\rangle) - \chi_a(c) q^k \delta_{\vec{b},\vec{0}} \right).$$

Рассмотрим величину

$$\sum_{\vec{a}\in P^k}\chi_a(\langle\vec{a},\vec{x}_0\rangle)C_a(\varphi,\langle\vec{a},\vec{x}\rangle+\langle\vec{b},\vec{y}\rangle)=$$
$$=\sum_{\vec{a}\in P^k}\chi_a(\langle\vec{a},\vec{x}_0\rangle)\sum_{\vec{x},\vec{y}\in P^k}\chi_a(\varphi(\vec{x},\vec{y})-\langle\vec{a},\vec{x}\rangle-\langle\vec{b},\vec{y}\rangle)=$$
$$=\sum_{\vec{x},\vec{y}\in P^k}\chi_a(\varphi(\vec{x},\vec{y})-\langle\vec{b},\vec{y}\rangle)\sum_{\vec{a}\in P^k}\chi_a(\langle\vec{a},\vec{x}_0-\vec{x}\rangle)=$$
$$=\sum_{\vec{y}\in P^k}\chi_a(\varphi(\vec{x},\vec{y})-\langle\vec{b},\vec{y}\rangle)q^k\delta_{\vec{x},\vec{x}_0}=q^k\sum_{\vec{y}\in P^k}\chi_a(\varphi(\vec{x}_0,\vec{y})-\langle\vec{b},\vec{y}\rangle)=$$
$$=q^k\sum_{\vec{y}\in P^k}\chi_a(c-\langle\vec{b},\vec{y}\rangle)=q^k\chi_a(c)\sum_{\vec{y}\in P^k}\chi_a(-\langle\vec{b},\vec{y}\rangle)=q^{2k}\chi_a(c)\delta_{\vec{b},\vec{0}}.$$

Подставим в полученную формулу значение $\vec{b}=\vec{0}$. Получим что сумма q^k слагаемых каждое из которых по модулю не превосходит q^k дает число, имеющее модуль равный q^{2k}. Это возможно только если каждое слагаемое рассматриваемой суммы равно $\chi_a(c)q^k$, т.е.

$$\chi_a(\langle\vec{a},\vec{x}_0\rangle)C_a(\varphi,\langle\vec{a},\vec{x}\rangle)=\chi_a(c)q^k.$$

Таким образом,

$$C_a(f,\langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle)=$$
$$=\begin{cases}\chi_a(-\langle\vec{a},\vec{x}_0\rangle)\left(C_a(g,\langle\vec{b},\vec{y}\rangle)+\chi_a(\langle\vec{a},\vec{x}_0\rangle)C_a(\varphi,\langle\vec{a},\vec{x}\rangle+\langle\vec{b},\vec{y}\rangle)\right), & \text{если } \vec{b}\neq\vec{0},\\ \chi_a(-\langle\vec{a},\vec{x}_0\rangle)C_a(g,0), & \text{если } \vec{b}=\vec{0},\end{cases}$$

и для модуля коэффициента кросс-корреляции справедливы равенства

$$|C_a(f,\langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle)|=$$
$$=\begin{cases}\left|C_a(g,\langle\vec{b},\vec{y}\rangle)+\chi_a(\langle\vec{a},\vec{x}_0\rangle)C_a(\varphi,\langle\vec{a},\vec{x}\rangle+\langle\vec{b},\vec{y}\rangle)\right|, & \text{если } \vec{b}\neq\vec{0},\\ |C_a(g,0)|, & \text{если } \vec{b}=\vec{0}.\end{cases}\qquad(14)$$

Докажем утверждение 1). Согласно следствию 1 функция f является сбалансированной тогда и только тогда, когда $C_a(f,0)=0$ для всех $a\in P^*$. Из равенств (14) следует, что это равносильно условию $C_a(g,0)=0$, $a\in P^*$, т.е. сбалансированности функции g.

Утверждение 2) следует из равенств (14), предложения 3 и соотношений

$$|C_a(f,\langle(\vec{a},\vec{b}),(\vec{x},\vec{y})\rangle)|\leqslant|C_a(g,\langle\vec{b},\vec{y}\rangle)|+|C_a(\varphi,\langle\vec{a},\vec{x}\rangle+\langle\vec{b},\vec{y}\rangle)|\leqslant C(g)+q^k.$$

Докажем утверждения 3) и 4). Пусть $\vec{x}_0=(c_1,\ldots,c_k)$, тогда

$$f(\vec{x},\vec{y})=\delta_{\vec{x},\vec{x}_0}(g(\vec{y})-c)+\varphi(\vec{x},\vec{y})=\prod_{i=1}^{k}\delta_{x_i,c_i}(g(\vec{y})-c)+\varphi(\vec{x},\vec{y})=$$
$$=\prod_{i=1}^{k}\frac{\prod\limits_{a\in P\setminus\{c_i\}}(x_i-a)}{\prod\limits_{a\in P\setminus\{c_i\}}(c_i-a)}(g(\vec{y})-c)+\varphi(\vec{x},\vec{y}).$$

Справедливость утверждений 3) и 4) теперь очевидна. ▲

СПИСОК ЛИТЕРАТУРЫ

1. *Dobbertin H.* Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity // Fast Software Encryption (Proc. 2nd Int. Workshop FSE 1994. Leuven, Belgium. Dec. 14–16, 1994). Lect. Notes Comput. Sci. V. 1008. Berlin: Springer, 1995. P. 61–74. https://doi.org/10.1007/3-540-60590-8_5
2. *Chee S., Lee S., Kim K.* Semi-bent Functions // Advances in Cryptology—ASIACRYPT'94 (Proc. 4th Int. Conf. on the Theory and Applications of Cryptology. Wollongong, Australia. Nov. 28 – Dec. 1, 1994). Lect. Notes Comput. Sci. V. 917. Berlin: Springer, 1995. P. 107–118. https://doi.org/10.1007/BFb0000428
3. *Carlet C.* Boolean Functions for Cryptography and Error Correcting Codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge: Cambridge Univ. Press, 2010. P. 257–397.
4. *Логачев О.А., Сальников А.А., Смышляев С.В., Ященко В.В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО. 2012.
5. *Токарева Н.Н.* Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. опер. 2010. Т. 17. № 1. С. 34–64. http://mi.mathnet.ru/da599
6. Амбросимов А.С. Свойства бент-функций q-значной логики над конечными полями. Дискр. математика. 1994. Т. 6. № 3. С. 50–60. http://mi.mathnet.ru/dm639
7. *Солодовников В.И.* Бент-функции из конечной абелевой группы в конечную абелеву группу // Дискрет. матем. 2002. Т. 14. № 1. С. 99–113. https://doi.org/10.4213/dm234
8. *Кузьмин А.С., Марков В.Т., Нечаев А.А., Шишкин В.А., Шишков А.Б.* Бент-функции и гипербент-функции над полем из 2^l элементов // Пробл. передачи информ. 2008. Т. 44. № 1. С. 15–37. http://mi.mathnet.ru/ppi1263
9. *Кузьмин А.С., Нечаев А.А., Шишкин В.А.* Бент- и гипербент-функции над конечным полем // Тр. по дискр. матем. Т. 10. М.: Физматлит, 2007. С. 97–122.
10. *Бугров А.Д.* Кусочно-аффинные подстановки конечных полей // Прикл. дискр. матем. 2015. № 4 (30). С. 5–23. https://doi.org/10.17223/20710410/30/1
11. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1, 2. М.: Мир, 1988.
12. *Golomb S.W., Gong G.* Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar. New York: Cambridge Univ. Press, 2005.
13. *Рябов В.Г.* Нелинейность функций над конечными полями // Дискр. матем. 2021. Т. 33. № 4. С. 110–131. https://doi.org/10.4213/dm1674
14. *McFarland R.L.* A Family of Difference Sets in Non-cyclic Groups // J. Combin. Theory Ser. A. 1973. V. 15. № 1. P. 1–10. https://doi.org/10.1016/0097-3165(73)90031-9
15. *Carlet C., Ding C.* Highly Nonlinear Mappings // J. Complexity. 2004. V. 20. № 2–3. P. 205–244. https://doi.org/10.1016/j.jco.2003.08.008
16. *Nyberg K.* Construction of Bent Functions and Difference Sets // Advances in Cryptology—EUROCRYPT'90 (Proc. Workshop on the Theory and Application of Cryptographic Techniques. Aarhus, Denmark. May 21–24, 1990). Lect. Notes Comput. Sci. V. 473. Berlin: Springer, 1991. P. 151–160. https://doi.org/10.1007/3-540-46877-3_13
17. *Kumar P.V., Scholtz R., Welch L.R.* Generalized Bent Functions and Their Properties // J. Combin. Theory Ser. A. 1985. V. 40. № 1. P. 90–107. https://doi.org/10.1016/0097-3165(85)90049-4
18. *Кейперс Л., Нидеррайтер Г.* Равномерное распределение последовательностей. М.: Наука, 1985.
19. *Camion P., Canteaut A.* Correlation-Immune and Resilient Function over a Finite Alphabet and Their Applications in Cryptography // Designs Codes Cryptogr. 1999. V. 16. № 2. P. 121–149. https://doi.org/10.1023/A:1008337029047
20. *Панков К.Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Матем. вопр. криптогр. 2014. Т. 5. № 4. С. 73–97. https://doi.org/10.4213/mvk136

21. *Bennett C.H., Brassard G., Robert J.-M.* Privacy Amplification by Public Discussion // SIAM J. Comput. 1988. V. 17. № 2. P. 210–229. https://doi.org/10.1137/0217014
22. *Xiao G.-Z., Massey J.L.* A Spectral Characterization of Correlation-Immune Combining Functions // IEEE Trans. Inform. Theory. 1988. V. 34. № 3. P. 569–571. https://doi.org/10.1109/18.6037
23. *Pankov K.N.* Improved Asymptotic Estimates for the Numbers of Correlation-Immune and k-Resilient Vectorial Boolean Functions // Discrete Math. Appl. 2019. V. 29. № 3. P. 195–213. https://doi.org/10.1109/18.6037
24. *Панков К.Н.* Рекуррентные формулы для числа k-эластичных и корреляционно-имунных двоичных отображений // Прикл. дискрет. матем. Приложение. 2019. № 12. С. 62–66. https://doi.org/10.17223/2226308X/12/19
25. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра. Т. 2. М.: Гелиос АРВ, 2003.
26. *Черемушкин А.В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикл. дискр. матем. 2010. № 2 (8). С. 22–33. http://mi.mathnet.ru/pdm174
27. *Camion P., Carlet C., Charpin P., Sendrier N.* On Correlation-Immune Functions // Advances in Cryptology—CRYPTO'91 (Proc. 11th Annu. Int. Cryptology Conf. Santa Barbara, CA, USA. Aug. 11–15, 1991). Lect. Notes Comput. Sci. V. 576. Berlin: Springer, 1992. P. 86–100. https://doi.org/10.1007/3-540-46766-1_6
28. *Canteaut A., Daum M., Dobbertin H., Leander G.* Finding Nonnormal Bent Functions // Discrete Appl. Math. 2006. V. 154. № 2. P. 202–218. https://doi.org/10.1016/j.dam.2005.03.027

Камловский Олег Витальевич
МТУСИ, кафедра теории вероятностей
и прикладной математики
ov-kam@yandex.ru
Панков Константин Николаевич
МТУСИ, кафедра информационной безопасности
pankov_kn@mtuci.ru

Поступила в редакцию
25.08.2022
После доработки
08.11.2022
Принята к публикации
10.11.2022