

# Описание $k$ -бент-функций от четырех переменных <sup>1</sup>

Н. Н. Токарева

Дано простое описание класса 2-бент-функций от четырех переменных. Этот класс состоит из 384-х квадратичных функций с 12-ю различными типами квадратичной части. Тем самым, все  $k$ -бент-функции с числом переменных не больше четырех полностью описаны.

**Ключевые слова.**  $k$ -Бент-функции,  $k$ -преобразование Уолша—Адамара.

## Введение

Булева функция  $f$  от четного числа  $m$  переменных называется *бент-функцией*, если она удалена в метрике Хэмминга от множества всех аффинных булевых функций на максимально возможное расстояние. Эквивалентно, бент-функцию  $f$  можно определить как функцию, для которой все коэффициенты Уолша-Адамара

$$W_f(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{(\mathbf{u}, \mathbf{v}) \oplus f(\mathbf{v})}, \quad \text{где } \mathbf{u} \in \mathbb{Z}_2^m,$$

равны  $\pm 2^{m/2}$ . Бент-функции являются классическим объектом исследования в различных областях дискретной математики и имеют большое число приложений, см. например, обзор К. Карле [7].

Известно, что задача описания бент-функций для произвольного  $m$ , или хотя бы нахождения хороших нижних и верхних оценок числа таких функций является очень сложной. Об этом свидетельствует, например, тот факт, что число 6 является максимальным значением для  $m$ , при котором еще известно точное значение числа бент-функций (равное  $5\,425\,430\,528 \simeq 2^{32,3}$ , см. описание в [6], [9], и более раннюю работу [10]), несмотря на длительный срок их исследования (с 60–70-х годов XX века [11]) и большой интерес к этим объектам.

$k$ -Бент-функции были введены в [4] как обобщение бент-функций. Целый параметр  $k$  меняется от 1 до  $m/2$ , и с его ростом происходит усиление нелинейных свойств бент-функций. Бент-функции и 1-бент-функции совпадают. Известны конструкции  $k$ -бент-функций

---

<sup>1</sup>Исследование выполнено при финансовой поддержке интеграционного проекта СО РАН N 35 «Древовидный каталог математических Интернет-ресурсов mathtree.ru», Российского фонда фундаментальных исследований (проекты 07-01-00248, 08-01-00671) и Фонда содействия отечественной науке.

при любом  $k$ , см. [4], и тот факт, что использование их в качестве функций шифрования предельно повышает стойкость блочного шифра к квадратичным аппроксимациям специального вида, см. [5].

В данной работе приводится простое описание класса 2-бент-функций от четырех переменных. Этот класс состоит из 384-х квадратичных функций с 12-ю различными типами квадратичной части. Тем самым, параметр  $m = 6$  становится наименьшим, при котором  $k$ -бент-функции пока не описаны.

## §1. Основной результат

Пусть  $m$  — целое число,  $\mathfrak{F}_m$  — класс всех булевых функций от  $m$  переменных. Пусть  $\mathbf{v} = (v_1, \dots, v_m)$ ,  $\mathbf{u} = (u_1, \dots, u_m)$  — двоичные векторы длины  $m$ . При любом целом  $k$ ,  $1 \leq k \leq m/2$ , в [4] определяется бинарная операция  $\langle \cdot, \cdot \rangle_k : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2$  как:

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \left( \bigoplus_{i=1}^k \bigoplus_{j=i}^k (u_{2i-1} \oplus u_{2i})(u_{2j-1} \oplus u_{2j})(v_{2i-1} \oplus v_{2i})(v_{2j-1} \oplus v_{2j}) \right) \oplus \langle \mathbf{u}, \mathbf{v} \rangle,$$

где  $\langle \mathbf{u}, \mathbf{v} \rangle = u_1 v_1 \oplus \dots \oplus u_m v_m$  — обычное скалярное произведение двоичных векторов и символ  $\oplus$  обозначает сложение по модулю 2. Операции  $\langle \cdot, \cdot \rangle_k$  тесно связаны с нелинейными двоичными кодами типа Адамара специального вида, а те в свою очередь — с  $\mathbb{Z}_4$ -линейными кодами Адамара [1], [8]. Свойства операции  $\langle \cdot, \cdot \rangle_k$  позволяют считать ее нелинейным аналогом скалярного произведения. Целочисленная функция  $W_f^{(k)}$ , заданная на множестве  $\mathbb{Z}_2^m$  равенством

$$W_f^{(k)}(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus f(\mathbf{v})} \text{ для любого } \mathbf{u} \in \mathbb{Z}_2^m,$$

называется  $k$ -преобразованием Уолша-Адамара булевой функции  $f \in \mathfrak{F}_m$ . Для  $W_f^{(k)}$  согласно [4] имеет место формула обращения и аналог равенства Парсеваля. Из последнего вытекает, что

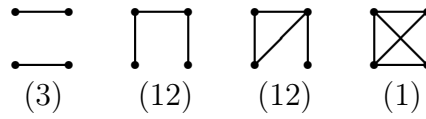
$$\max_{\mathbf{u} \in \mathbb{Z}_2^m} |W_f^{(k)}(\mathbf{u})| \geq 2^{m/2}.$$

При четном  $m$  булева функция  $f \in \mathfrak{F}_m$  называется  $k$ -бент-функцией, если все коэффициенты  $W_f^{(j)}(\mathbf{u})$ ,  $j = 1, \dots, k$ , равны  $\pm 2^{m/2}$ . Эквивалентно, такие функции можно определять как функции, одинаково плохо аппроксимируемые всеми функциями вида  $\langle \mathbf{u}, \mathbf{v} \rangle_k$ . Пусть  $\mathfrak{B}_m^k$  — класс всех  $k$ -бент-функций от  $m$  переменных. Тогда  $\mathfrak{B}_m^1$  совпадает с классом обычных бент-функций, поскольку  $W_f^{(1)}(\mathbf{u}) = W_f(\hat{\mathbf{u}})$  для любого  $\mathbf{u} \in \mathbb{Z}_2^m$ , где  $\hat{\mathbf{u}} = (u_2, u_1, u_3, \dots, u_m)$ . Справедливы строгие включения  $\mathfrak{B}_m^1 \supset \dots \supset \mathfrak{B}_m^{m/2}$ , причем каждое множество  $\mathfrak{B}_m^k$  непусто, см. подробнее [4].

Рассмотрим малые значения параметра  $m$ .

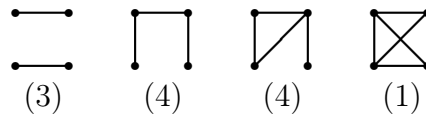
Случай  $m = 2$ . Класс  $\mathfrak{B}_2^1$  состоит из всех функций, векторы значений которых имеют нечетный вес Хэмминга;  $|\mathfrak{B}_2^1| = 8$ .

Случай  $m = 4$ . Известно [3], что множество  $\mathfrak{B}_4^1$  состоит из 896-ти булевых функций, причем каждая функция является квадратичной, т. е. степени нелинейности (или *ранга*) 2. Множество  $\mathfrak{B}_4^1$  можно разделить на 28 классов по 32 функции. Алгебраические нормальные формы (или *многочлены Жегалкина*, а кратко АНФ) функций из каждого класса обладают одинаковой квадратичной частью, произвольной линейной частью и любым свободным членом. Если рассмотреть граф на множестве переменных, а ребрами соединить те вершины, которые образуют слагаемое в квадратичной части АНФ функции, то эти 28 типов можно задать следующим образом:

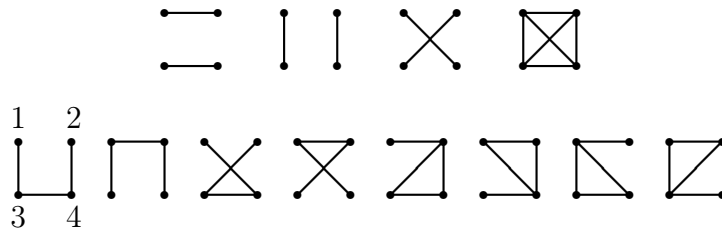


Под каждым графом указано число типов, которые он определяет. Например, имеется 12 типов квадратичной части, состоящей из трех слагаемых, и только один тип из шести слагаемых.

В данной работе мы приводим простое описание класса  $\mathfrak{B}_4^2$ , используя интерпретацию в терминах графов. Рассмотрим граф на четырех вершинах, которые пронумеруем цифрами от 1 до 4. Считаем, что вершина с номером  $i$  соответствует переменной  $v_i$ . Разделим вершины графа на две доли  $\{1, 2\}$  и  $\{3, 4\}$ . Из 28-ми графов, приведенных выше, выберем только те, в которых число ребер, соединяющих вершины из разных долей, четно. Получим серию из следующих 12-ти графов:



А именно, нумеруя вершины слева направо и сверху вниз, имеем



Основной результат состоит в том, что множество  $\mathfrak{B}_4^2$  является объединением 12-ти классов 1-бент-функций, каждый из которых отвечает одному из указанных графов. Все функции из одного

класса различаются только линейной частью и свободным членом, их число равно 32. Таким образом,  $|\mathfrak{B}_4^2| = 384$ . Докажем этот факт.

Переходя от графов к алгебраическим нормальным формам функций, основное утверждение формулируется следующим образом.

**Утверждение.** Пусть параметры  $i_1, i_2, i_3$  и  $i_4$  принимают различные значения от 1 до 4. Тогда множество функций  $\mathfrak{B}_4^2$  состоит из всех функций степени 2 с квадратичными частями вида:

$$\begin{aligned} v_{i_1}v_{i_2} \oplus v_{i_3}v_{i_4} & \quad (3 \text{ типа}); \\ v_{i_1}v_{i_2} \oplus v_{i_1}v_{i_3} \oplus v_{i_2}v_{i_4} & \text{ при } \{i_1, i_2\} = \{1, 2\} \text{ или } \{3, 4\} \quad (4 \text{ типа}); \\ v_{i_1}v_{i_2} \oplus v_{i_2}v_{i_3} \oplus v_{i_3}v_{i_4} \oplus v_{i_1}v_{i_3} & \text{ при } \{i_1, i_2\} = \{1, 2\} \text{ или } \{3, 4\} \quad (4 \text{ типа}); \\ v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4 & \quad (1 \text{ тип}). \end{aligned}$$

**Доказательство.** Очевидно, что  $\mathfrak{B}_4^2$  содержит только функции степени 2. Заметим, что если функция  $f$  принадлежит  $\mathfrak{B}_4^2$ , то функция  $f \oplus 1$  также содержится в этом классе. Рассмотрим произвольную функцию  $f_{\mathbf{w}} \in \mathfrak{B}_4^2$  степени 2 вида  $f_{\mathbf{w}}(\mathbf{v}) = f(\mathbf{v}) \oplus \langle \mathbf{w}, \mathbf{v} \rangle$ , где вектор  $\mathbf{w}$  фиксирован и через  $f(\cdot)$  обозначена квадратичная часть функции. Выясним при каких условиях функция  $f_{\mathbf{w}}$  является 2-бент-функцией, т. е. когда все 2-коэффициенты Уолша-Адамара этой функции равны  $\pm 4$ . Для произвольного вектора  $\mathbf{u} = (u_1, u_2, u_3, u_4)$  рассмотрим коэффициент  $W_{f_{\mathbf{w}}}^{(2)}(\mathbf{u})$ .

Пусть  $\mathbb{Z}_2^4 = V_0 \cup V_1$ , где множество  $V_1$  имеет вид

$$V_1 = \{ (1010), (1001), (0110), (0101) \},$$

и множество  $V_0$  содержит все остальные векторы длины 4. Заметим, что для любого вектора  $\mathbf{u} \in V_0$  выполняется  $(u_1 \oplus u_2)(u_3 \oplus u_4) = 0$ , тогда как  $(u_1 \oplus u_2)(u_3 \oplus u_4) = 1$  для любого  $\mathbf{u} \in V_1$ . По определению имеем

$$\begin{aligned} \langle \mathbf{u}, \mathbf{v} \rangle_2 = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \oplus \\ u_2v_1 \oplus u_1v_2 \oplus u_4v_3 \oplus u_3v_4. \end{aligned}$$

Тогда для любого вектора  $\mathbf{u} \in V_0$  выполняется

$$W_{f_{\mathbf{w}}}^{(2)}(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_2 \oplus f_{\mathbf{w}}(\mathbf{v})} = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \tilde{\mathbf{u}}, \mathbf{v} \rangle \oplus f_{\mathbf{w}}(\mathbf{v})} = W_{f_{\mathbf{w}}}(\tilde{\mathbf{u}}),$$

где  $\tilde{\mathbf{u}} = (u_2, u_1, u_4, u_3)$ , и следовательно  $W_{f_{\mathbf{w}}}^{(2)}(\mathbf{u}) = \pm 4$ , поскольку  $f_{\mathbf{w}}$  является 1-бент-функцией.

Рассмотрим случай  $\mathbf{u} \in V_1$ . Имеем

$$W_{f_{\mathbf{w}}}^{(2)}(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \tilde{\mathbf{u}}, \mathbf{v} \rangle \oplus g_{\mathbf{w}}(\mathbf{v})} = W_{g_{\mathbf{w}}}(\tilde{\mathbf{u}}), \quad (1)$$

























где функция  $g_{\mathbf{w}}$  задана равенством  $g_{\mathbf{w}}(\mathbf{v}) = g(\mathbf{v}) \oplus \langle \mathbf{w}, \mathbf{v} \rangle$  и

$$g(\mathbf{v}) = (v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \oplus f(\mathbf{v}).$$

Выясним при каких условиях данные четыре коэффициента

$$W_{f_{\mathbf{w}}}^{(2)}(1010), W_{f_{\mathbf{w}}}^{(2)}(1001), W_{f_{\mathbf{w}}}^{(2)}(0110), W_{f_{\mathbf{w}}}^{(2)}(0101), \quad (2)$$

равны  $\pm 4$ . Для 12-ти из 28 возможных вариантов функции  $f$  функция  $g$  является 1-бент-функцией. А именно это 12 квадратичных функций  $f$ , указанные в формулировке утверждения:

$f(\mathbf{v})$	$g(\mathbf{v})$
 $v_1v_2 \oplus v_3v_4$	 $v_1v_2 \oplus \dots \oplus v_3v_4$
 $v_1v_3 \oplus v_2v_4$	 $v_1v_4 \oplus v_2v_3$
 $v_1v_4 \oplus v_2v_3$	 $v_1v_3 \oplus v_2v_4$
 $v_1v_2 \oplus \dots \oplus v_3v_4$	 $v_1v_2 \oplus v_3v_4$
 $v_1v_3 \oplus v_2v_4 \oplus v_3v_4$	 $v_1v_4 \oplus v_2v_3 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_3 \oplus v_2v_4$	 $v_1v_2 \oplus v_1v_4 \oplus v_2v_3$
 $v_1v_4 \oplus v_2v_3 \oplus v_3v_4$	 $v_1v_3 \oplus v_2v_4 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_4 \oplus v_2v_3$	 $v_1v_2 \oplus v_1v_3 \oplus v_2v_4$
 $v_1v_2 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$	 $v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_4 \oplus v_2v_4 \oplus v_3v_4$	 $v_1v_2 \oplus v_1v_3 \oplus v_2v_3 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_3v_4$	 $v_1v_2 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$
 $v_1v_2 \oplus v_1v_3 \oplus v_2v_3 \oplus v_3v_4$	 $v_1v_2 \oplus v_1v_4 \oplus v_2v_4 \oplus v_3v_4$

В каждом из этих 12-ти случаев, так как  $g$  есть 1-бент-функция, имеем  $W_{f_{\mathbf{w}}}^{(2)}(\mathbf{u}) = W_{g_{\mathbf{w}}}(\tilde{\mathbf{u}}) = \pm 4$ , и следовательно  $f_{\mathbf{w}}$  принадлежит классу 2-бент-функций при любом векторе  $\mathbf{w}$ . Таким образом, мы показали, что класс  $\mathfrak{B}_4^2$  содержит по крайней мере  $12 \times 32 = 384$  функции. Проверим, что если функция  $g$  не является 1-бент-функцией, то модуль хотя бы одного (например, первого) коэффициента среди коэффициентов (2) всегда не равен 4, и следовательно,  $f_{\mathbf{w}}$  не может быть 2-бент-функцией в этом случае.

Поскольку выполняется

$$g_{\mathbf{w}}(\mathbf{v}) = \begin{cases} f_{\mathbf{w}}(\mathbf{v}), & \text{при } \mathbf{v} \in V_0 \\ f_{\mathbf{w}}(\mathbf{v}) \oplus 1, & \text{при } \mathbf{v} \in V_1, \end{cases}$$

коэффициент  $W_{f_{\mathbf{w}}}^{(2)}(1010)$  согласно (1) можно представить в виде

$$W_{f_{\mathbf{w}}}^{(2)}(1010) = W_{g_{\mathbf{w}}}(0101) = S_0 - S_1,$$

где

$$S_{\delta} = \sum_{\mathbf{v} \in V_{\delta}} (-1)^{((0101), \mathbf{v}) \oplus f_{\mathbf{w}}(\mathbf{v})}, \text{ при } \delta = 0, 1.$$

Так как  $f_{\mathbf{w}}$  является 1-бент-функцией, имеем

$$W_{f_{\mathbf{w}}}(0101) = S_0 + S_1 = \pm 4.$$

Тогда, как нетрудно заметить, в качестве необходимого условия для равенства  $S_0 - S_1 = \pm 4$  величина  $S_1$  должна быть равна  $\pm 4$  или 0. Расписывая  $S_1$ , получаем

$$S_1 = (-1)^{w_1} ((-1)^{w_3 \oplus f(1010)} + (-1)^{w_4 \oplus f(1001)}) + (-1)^{w_2} ((-1)^{w_3 \oplus f(0110)} + (-1)^{w_4 \oplus f(0101)}).$$

Тогда, как несложно заметить, для выполнения  $S_1 \in \{\pm 4, 0\}$  необходимо, чтобы на множестве  $V_1$  функция  $f$  принимала значение 1 четное число раз. Но АНФ каждой функции  $f$  из оставшихся 16-ти содержит нечетное число одночленов из множества

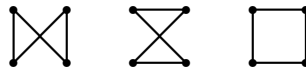
$$\{v_1v_3, v_1v_4, v_2v_3, v_2v_4\},$$

т. е. при интерпретации на графе — нечетное число ребер между долями  $\{1, 2\}$  и  $\{3, 4\}$ , а следовательно на множестве  $V_1$  каждая такая функция принимает значение 1 нечетное число раз. Таким образом, необходимое условие для  $W_{f_{\mathbf{w}}}^{(2)}(1010) = \pm 4$  не выполнено, и следовательно в этом случае функция  $f_{\mathbf{w}}$  не является 2-бент-функцией ни при каком векторе  $\mathbf{w}$ . Утверждение доказано.

## §2. Замечания

Интересным следствием из Утверждения является тот факт, что если к 2-бент-функции от четырех переменных прибавить произвольную аффинную функцию, то в результате снова получится 2-бент-функция. Автор предполагает, что причиной этого является «эффект малых значений» и при  $m > 4$  подобное свойство для  $k$ -бент-функций наблюдаться не будет.

Заметим, что при определении  $k$ -бент-функций существенными являются способ разбиения переменных на пары и порядок этих пар. Можно рассматривать более общий подход, при котором аппроксимации булевых функций ведутся всеми функциями вида  $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$ , где  $\pi$  — произвольная подстановка на  $m$  элементах, и тогда указанные выше ограничения снимаются. Из Утверждения следует, что функция  $f \in \mathfrak{B}_4^1$  является 2-бент-функцией при любом разбиении переменных на пары тогда и только тогда, когда пересечение графа ее квадратичной части с каждым из графов



содержит четное число ребер. Легко видеть, что такому условию удовлетворяют только функции с квадратичной частью вида



Их число равно 128. Несложно теперь заметить, что множество из 28-ми графов квадратичных частей 1-бент-функций разбивается на четыре множества. Одно состоит из четырех указанных выше графов, отвечающих 2-бент-функциям при любом разбиении переменных на пары, и остальные три множества содержат по восемь графов, отвечающих 2-бент-функциям при каждом из трех таких возможных разбиений в отдельности.

В заключение приведем ту весьма скромную информацию о числе  $k$ -бент-функций при малых значениях  $m$ , известную в настоящий момент. Результаты по 1-бент-функциям и оценки их числа при любом  $m$  можно найти в [2] и [7].

$m$	$k$	Информация о классах $\mathfrak{B}_m^k$
2	1	$ \mathfrak{B}_2^1  = 8$
4	1, 2	$ \mathfrak{B}_4^1  = 896$ , см. описание в [3]; $ \mathfrak{B}_4^2  = 384$ , описание в данной работе; число в [4];
6	1, 2, 3	$ \mathfrak{B}_6^1  = 5\,425\,430\,528 \simeq 2^{32,3}$ , см. [6], [9], [10]; $ \mathfrak{B}_6^2  \geq 4 \cdot 896 = 3\,584$ , следует из [4]; $ \mathfrak{B}_6^3  \geq 4 \cdot 384 = 1\,536$ , следует из [4];
8	1, 2, 3, 4	$ \mathfrak{B}_8^1  \geq 1\,559\,994\,535\,674\,013\,286\,400 \simeq 2^{70,4}$ , см. [6]; $ \mathfrak{B}_8^2  > 2^{34,3}$ , следует из [6], [9], [10] и [4]; $ \mathfrak{B}_8^3  \geq 16 \cdot 896 = 14\,336$ , следует из [4]; $ \mathfrak{B}_8^4  \geq 16 \cdot 384 = 6\,144$ , следует из [4];

## Литература

- [1] Кротов Д. С.  $\mathbb{Z}_4$ -линейные совершенные коды // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7. N 4. С. 78–90 (translated at <http://arxiv.org/abs/0710.0198>).
- [2] Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004, 470 с.
- [3] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М: Связь, 1979, 744 с.
- [4] Токарева Н. Н. Бент-функции с более сильными свойствами нелинейности:  $k$ -бент-функции // Дискрет. анализ и исслед. операций. Сер. 1. 2007. Т. 14. N 4. С. 76–102.
- [5] Токарева Н. Н. О квадратичных аппроксимациях в блочных шифрах // Пробл. передачи информ. 2008. принято в печать.

- [6] *Agievich S. V.* On the representation of bent-functions by bent-rectangles // Fifth Int. Petrozavodsk conf. on probabilistic methods in discrete mathematics (Petrozavodsk, Russia. June 1–6, 2000). Proc. Boston: VSP, 2000. P. 121–135. Доступно по адресу <http://arxiv.org/abs/math/0502087v1>.
- [7] *Carlet C.* Boolean Functions for Cryptography and Error Correcting Codes // chapter of the monograph «Boolean methods and models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. Prelim. version is available at [www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf](http://www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf).
- [8] *Krotov D. S.*  $\mathbb{Z}_4$ -linear Hadamard and extended perfect codes // Proc. of the Int. Workshop on Coding and Cryptography (Paris, France. January 8–12, 2001). P. 329–334.
- [9] *Meng Q., Yang M. C., Zhang H.* A novel algorithm enumerating bent functions // доступно по адресу [http://eprint.iacr.org, 2004/274](http://eprint.iacr.org,2004/274).
- [10] *Preneel B.* Analysis and design of cryptographic hash functions // Ph. D. thesis, Katholieke Universiteit Leuven, 3001 Leuven, Belgium. 1993, 338 p.
- [11] *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. N 3. P. 300–305.

Информация об авторе:

Статья поступила  
14 марта 2008 г.

Токарева Наталья Николаевна  
Институт математики  
им. С. Л. Соболева СО РАН,  
пр. Академика Коптюга, 4,  
Новосибирский гос. университет,  
ул. Пирогова, 2,  
630090 Новосибирск,  
Россия.  
E-mail: [tokareva@math.nsc.ru](mailto:tokareva@math.nsc.ru)  
Web: [www.math.nsc.ru/~tokareva](http://www.math.nsc.ru/~tokareva)

## Description of $k$ -bent functions in four variables

Natalia N. Tokareva

We give a simple description for the class of 2-bent functions in four variables. This class consists of 384 quadratic functions with 12 distinct types of quadratic part. Thus, all  $k$ -bent functions with not more than four variables are classified.

**Keywords.**  $k$ -Bent-functions,  $k$ -Walsh—Hadamard transform.

Tokareva Natalia Nikolaevna

Sobolev Institute of Mathematics

Siberian Branch of the Russian Academy of Sciences

4 Acad. Koptug avenue,

Novosibirsk State University

2 Pirogova street

630090 Novosibirsk,

Russia.

E-mail: tokareva@math.nsc.ru

Web: [www.math.nsc.ru/~tokareva](http://www.math.nsc.ru/~tokareva)