

Группа автоморфизмов множества бент-функций<sup>1</sup>

Н. Н. Токарева

Бент-функции — это булевы функции от четного числа переменных, удаленные от множества всех аффинных функций на максимально возможное расстояние. В работе показано, что каждое изометричное отображение множества булевых функций от  $n$  переменных в себя, оставляющее класс бент-функций на месте, является комбинацией аффинного преобразования координат и сдвига на аффинную функцию. Доказано, что аффинные функции — это в точности все те булевы функции, которые удалены от класса бент-функций на максимально возможное расстояние.

## 1 Введение

Бент-функции — это булевы функции от четного числа переменных, удаленные от множества всех аффинных функций на максимально возможное расстояние. Впервые они были введены О. Ротхаусом [6]. В настоящее время бент-функции активно изучаются и имеют много приложений в теории кодирования, криптографии, цифровой сотовой связи и других областях, см. подробнее обзоры [3, 4]. Тем не менее в области бент-функций много открытых вопросов. Среди них — вопрос о группе автоморфизмов множества бент-функций, ответ на который дается в данной работе.

Пусть  $A$  — невырожденная двоичная  $n \times n$ -матрица, пусть  $b$  и  $c$  — двоичные векторы длины  $n$ , и  $d$  — константа. Известно, что любое отображение вида  $g(x) \rightarrow g(Ax + b) + \langle c, x \rangle + d$ , заданное на множестве булевых функций от  $n$  переменных, оставляет класс бент-функций на месте. Существуют ли другие изометричные отображения множества булевых функций в себя, оставляющие неподвижным класс бент-функций? В данной работе показано, что других таких отображений нет.

Рассмотрим структуру статьи. Основная часть статьи посвящена доказательству того, что для любой неаффинной функции  $f$  найдется такая бент-функция  $g$ , что функция  $f + g$  не является бент-функцией (Теорема 1). Другими словами, множество бент-функций замкнуто относительно прибавления только аффинных булевых функций. Из этого факта будет следовать, что аффинные функции — это в точности все те булевы функции, которые удалены от класса бент-функций на максимально возможное расстояние. Т. е. существует в некотором смысле «дуальность» между определениями бент-функций и аффинных функций. Далее устанавливается, что множество бент-функций и множество

<sup>1</sup>Исследование выполнено при поддержке гранта Президента РФ для молодых российских ученых (грант МК-1250.2009.1), Российского фонда фундаментальных исследований (проекты 08-01-00671, 09-01-00528, 10-01-00424) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009-2013 гг. (гос. контракт 02.740.11.0429).

аффинных функций имеют одинаковые группы автоморфизмов. Этой общей группой является полупрямое произведение полной аффинной группы  $GA(n)$  на  $\mathbb{Z}_2^{n+1}$  (Теорема 2).

## 2 Определения и факты

Пусть  $\langle x, y \rangle$  обозначает обычное скалярное произведение двоичных векторов  $x, y \in \mathbb{Z}_2^n$  по модулю 2. Расстоянием Хэмминга  $d(x, y)$  между векторами  $x$  и  $y$  называется число координат, в которых они различаются.

Под расстоянием  $dist(f, g)$  между булевыми функциями  $f$  и  $g$  будем понимать расстояние между их векторами значений. Через  $supp(f)$  обозначим носитель функции  $f$ , т. е. множество тех векторов, на которых  $f$  равна единице. Известно, что каждая булева функция  $f$  может быть представлена в алгебраической нормальной форме, степень которой обозначим через  $deg(f)$ . Булевы функции степени 1 называются аффинными и имеют вид  $\langle c, x \rangle + d$  для подходящего вектора  $c$  и константы  $d$ . Множество всех аффинных функций от  $n$  переменных обозначим через  $\mathcal{A}_n$ .

Преобразованием Уолша—Адамара булевой функции  $f$  от  $n$  переменных называется целочисленная функция  $W_f(y) = \sum_x (-1)^{\langle x, y \rangle + f(x)}$ . Бент-функцией называется булева функция от  $n$  переменных ( $n$  четно) такая, что модуль каждого коэффициента Уолша—Адамара  $W_f(y)$  этой функции равен  $2^{n/2}$ . Производной булевой функции  $f$  по направлению  $y$  называется функция  $f(x) + f(x + y)$ . Заметим, что булева функция  $f$  аффинна тогда и только тогда, когда ее производная по любому направлению является константой.

Эквивалентно, бент-функции могут быть определены так [1]:

**Утверждение 1.** Булева функция  $g$  является бент-функцией, тогда и только тогда, когда ее производная по любому ненулевому направлению  $y$  уравновешена, т. е. выполняется  $\sum_x (-1)^{g(x) + g(x+y)} = 0$ .

Множество всех бент-функций от  $n$  переменных обозначим через  $\mathcal{B}_n$ . Хорошо известно следующее свойство бент-функций.

**Утверждение 2.** Пусть  $A$  — невырожденная двоичная  $n \times n$ -матрица,  $b$  и  $c$  — двоичные векторы,  $d$  — константа. Любое отображение вида  $g(x) \rightarrow g(Ax + b) + \langle c, x \rangle + d$ , заданное на множестве булевых функций от  $n$  переменных, оставляет класс бент-функций на месте.

Далее нам потребуется известная конструкция бент-функций Мак-Фарланда [5].

**Утверждение 3.** Функция  $f(x', x'') = \langle x', \pi(x'') \rangle + h(x'')$  является бент-функцией от  $n$  переменных, где  $\pi$  — любая перестановка на  $\mathbb{Z}_2^{n/2}$  и булева функция  $h$  от  $n/2$  переменных произвольна.

Заметим, что разбиение переменных на две равные части  $x'$  и  $x''$  может быть любым.

Рассмотрим векторы, у которых фиксированы значения некоторых  $n - k$  координат, а значения остальных координат выбираются произвольно. Множество всех таких векторов называется *гранью размерности  $k$*  пространства  $\mathbb{Z}_2^n$ . Например, множество  $\Gamma = \{ (x', x'') : x'' = a \}$  является гранью размерности  $n/2$ , где  $x', x'' \in \mathbb{Z}_2^{n/2}$ .

### 3 О сдвигах класса бент-функций

Докажем следующий факт, из которого в качестве следствий и будут получены основные результаты работы.

**Теорема 1.** *Для любой неаффинной функции  $f$  найдется такая бент-функция  $g$ , что функция  $f + g$  не является бент-функцией.*

**Доказательство.** Предположим, что для некоторой фиксированной функции  $f$  такой, что  $\deg(f) \geq 2$ , справедливо  $f + \mathcal{B}_n = \mathcal{B}_n$ . Покажем, что это приведет к противоречию.

Идея доказательства состоит в следующем. Сначала покажем, что некоторая сумма должна быть равна нулю для любой бент-функции, см. далее сумму (1). Затем в классе МакФарланда найдем бент-функцию-контрпример  $g'$ , для которой это равенство не будет выполняться. Бент-функция  $g'$  будет получена из специально выбранной бент-функции  $g$  инвертированием ее значений на некоторой грани  $\Gamma$  размерности  $n/2$ . Ключевым условием для возможности выбора такой грани является то, что для некоторого ненулевого  $y$ , множество  $D = \text{supp}(f(x) + f(x + y))$  будет собственным подмножеством пространства  $\mathbb{Z}_2^n$ , что возможно тогда и только тогда, когда  $f$  неаффинна.

Доказательство удобно разделить на несколько этапов.

**Равенство для любой бент-функции.** Поскольку  $\deg(f) \geq 2$ , то найдется такой ненулевой вектор  $y$ , что производная функции  $f$  по направлению  $y$  не является константой. Можно считать, что  $y = 1$ . Действительно, так как если  $y$  — другой ненулевой вектор, то от функции  $f$  перейдем к функции  $f'(x) = f(Ax)$ , где  $A \cdot 1 = y$ . Очевидно, что производная функции  $f'$  по направлению 1 не константа, и так же как и для  $f$ , выполняется равенство  $f' + \mathcal{B}_n = \mathcal{B}_n$  (т. е. можно доказывать теорему для  $f'$ ). Поэтому всюду далее считаем, что  $y = 1$ .

Пусть  $g$  — произвольная бент-функция. Тогда  $f + g$  — также бент-функция, и согласно утверждению 1 выполняются равенства

$$\sum_x (-1)^{g(x)+g(x+y)} = 0,$$

$$\sum_x (-1)^{g(x)+f(x)+g(x+y)+f(x+y)} = 0.$$

Вычитая из первого равенства второе, получаем

$$\sum_x (-1)^{g(x)+g(x+y)} (1 - (-1)^{f(x)+f(x+y)}) = 0.$$

Обозначим через  $D$  множество  $\text{supp}(f(x) + f(x + y))$ . Тогда для любой бент-функции  $g$  должно выполняться

$$\sum_{x \in D} (-1)^{g(x) + g(x+y)} = 0. \quad (1)$$

**Выбор грани.** Так как функция  $f(x) + f(x + y)$  — не константа, то множество  $D$  не пусто и не совпадает со всем булевым кубом. Тогда существует  $(n/2)$ -мерная грань  $\Gamma$  такая, что она имеет непустое пересечение и с множеством  $D$  и с его дополнением  $\mathbb{Z}_2^n \setminus D$ , т. е. выполняется

$$0 < m < |\Gamma| = 2^{n/2}, \quad (2)$$

где  $m = |\Gamma \cap D|$ . Действительно, такую грань всегда можно построить, например, через любой вектор  $u \notin D$  и один из векторов  $v$  или  $v + y$ , где  $v \in D$ , так как либо расстояние  $d(u, v)$  либо  $d(u, v + y)$  окажется не превосходящим  $n/2$ .

Заметим, что грань  $\Gamma + y$  также имеет пересечение мощности  $m$  с множеством  $D$ , поскольку, как нетрудно заметить,  $D + y = D$ . Отметим также, что грани  $\Gamma$  и  $\Gamma + y$  не пересекаются (в силу выбора  $y = 1$ ). Имеет место следующее разбиение множества  $D$ :

$$D = (\Gamma \cap D) \cup ((\Gamma + y) \cap D) \cup (D \setminus (\Gamma \cup (\Gamma + y))), \quad (3)$$

которое потребуется нам в дальнейшем.

Без ограничения общности считаем, что грань  $\Gamma$  имеет вид

$$\Gamma = \{(x', x'') : x'' = a\} \text{ для некоторого вектора } a \in \mathbb{Z}_2^{n/2}$$

(в случае, если фиксированные координаты грани расположены иначе, доказательство проводится аналогично). Пусть множество  $\Gamma \cap D$  представляется в виде

$$\Gamma \cap D = \{(b^{(1)}, a), (b^{(2)}, a), \dots, (b^{(m)}, a)\},$$

для подходящих векторов  $b^{(1)}, b^{(2)}, \dots, b^{(m)}$  длины  $n/2$ .

**Специальное подмножество бент-функций.** Рассмотрим подмножество  $G$  бент-функций вида  $g(x', x'') = \langle x', \pi(x'') \rangle$  из класса Мак-Фарланда таких, что перестановки  $\pi$  являются линейными преобразованиями пространства, т. е. каждая  $\pi$  определяется как  $\pi(x'') = Ax''$ , для подходящей невырожденной матрицы  $A$ . Покажем, что в классе  $G$  найдется такая бент-функция  $g$ , что сумма

$$S = \sum_{x \in \Gamma \cap D} (-1)^{g(x) + g(x+y)}$$

будет не равна нулю. Действительно, распишем эту сумму, подставляя вид произвольной функции из  $G$ . Поскольку  $\pi(x'' + y'') = A(x'' + y'') = Ax'' + Ay''$ , где  $y = (y', y'')$ , имеем

$$g(x) + g(x + y) = \langle x', Ax'' \rangle + \langle x' + y', Ax'' + Ay'' \rangle =$$

$$\langle x', Ay'' \rangle + \langle y', Ax'' + Ay'' \rangle.$$

Тогда, подставляя в сумму  $S$ , получаем

$$S = (-1)^\gamma \sum_{i=1}^m (-1)^{\langle b^{(i)}, Ay'' \rangle},$$

где  $\gamma = \langle y', Aa + Ay'' \rangle$  — константа, зависящая от конкретного выбора матрицы  $A$ . Поскольку  $y''$  — ненулевой вектор (по нашему выбору  $y'' = 1$ ), и матрица  $A$  может быть любой невырожденной матрицей, то вектор  $z = Ay''$  также может быть произвольным ненулевым вектором длины  $n/2$ . Таким образом, наша задача — показать, что найдется такой ненулевой вектор  $z$ , что не равна нулю сумма

$$\sum_{i=1}^m (-1)^{\langle b^{(i)}, z \rangle}. \quad (4)$$

**Поиск вектора  $z$ .** Предположим обратное. Пусть для каждого ненулевого вектора  $z$  сумма (4) равна нулю. Рассмотрим двоичную матрицу  $M$  размера  $(n/2) \times m$ , столбцами которой являются все векторы  $b^{(1)}, \dots, b^{(m)}$ . Тогда сумма (4) есть ни что иное как разность между числом нулей и числом единиц в линейной комбинации строк матрицы  $M$ , определяемой вектором  $z$  (строка  $i$  входит в комбинацию, если  $z_i = 1$ ). По предположению, матрица  $M$  должна удовлетворять условию: *любая ненулевая линейная комбинация строк матрицы  $M$  содержит одинаковое число нулей и единиц*. Несложно понять, что с точностью до перестановки столбцов, эта матрица должна иметь вид

$$\begin{pmatrix} 0 \dots 0 & 0 \dots 0 & 0 \dots 0 & 0 \dots 0 & 1 \dots 1 & 1 \dots 1 & 1 \dots 1 & 1 \dots 1 \\ 0 \dots 0 & 0 \dots 0 & 1 \dots 1 & 1 \dots 1 & 0 \dots 0 & 0 \dots 0 & 1 \dots 1 & 1 \dots 1 \\ 0 \dots 0 & 1 \dots 1 & 0 \dots 0 & 1 \dots 1 & 0 \dots 0 & 1 \dots 1 & 0 \dots 0 & 1 \dots 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \underbrace{\phantom{0 \dots 0}}_{m/8} & \underbrace{\phantom{0 \dots 0}}_{m/8} & \underbrace{\phantom{0 \dots 0}}_{m/8} & \underbrace{\phantom{0 \dots 0}}_{m/8} & \underbrace{\phantom{1 \dots 1}}_{m/8} & \underbrace{\phantom{1 \dots 1}}_{m/8} & \underbrace{\phantom{1 \dots 1}}_{m/8} & \underbrace{\phantom{1 \dots 1}}_{m/8} \end{pmatrix}$$

Отсюда сразу замечаем, что число столбцов матрицы должно быть не меньше чем  $2^{n/2}$ , где  $n/2$  — число строк. Таким образом, для существования такой матрицы  $M$  необходимо, чтобы выполнялось  $m \geq 2^{n/2}$ . Но это противоречит условию на выбор грани  $\Gamma$ , а именно неравенству (2). Следовательно, всегда найдется вектор  $z$  такой, что сумма (4) не равна нулю. Зафиксируем этот вектор  $z$ .

**Построение функции-контрпримера.** Пусть  $A$  — невырожденная матрица такая, что  $Ay'' = z$ , пусть перестановка  $\pi$  определяется равенством  $\pi(x'') = Ax''$ . Из условия выбора вектора  $z$  следует, что для функции  $g(x', x'') = \langle x', \pi(x'') \rangle$  справедливо

$$S = \sum_{x \in \Gamma \cap D} (-1)^{g(x) + g(x+y)} \neq 0. \quad (5)$$

Определим новую бент-функцию  $g'$ , отличающуюся от  $g$  лишь на грани  $\Gamma$ . Далее мы увидим, что функции  $f + g$  и  $f + g'$  не могут одновременно быть бент-функциями, что и приведет к противоречию с основным предположением. Итак, пусть  $g'(x', x'') = g(x', x'') + h(x'')$ , где

$$h(x'') = \begin{cases} 1, & \text{если } x'' = a; \\ 0, & \text{иначе.} \end{cases}$$

Другими словами,  $g'$  получена из функции  $g$  инвертированием ее значений на грани  $\Gamma$ . Так как  $g$  из класса МакФарланда, то функция  $g'$  тоже бент-функция. Заметим, что тогда в силу разбиения (3) имеем

$$\begin{aligned} \sum_{x \in D} (-1)^{g'(x) + g'(x+y)} &= \left( \sum_{x \in \Gamma \cap D} (-1)^{g(x) + 1 + g(x+y) + 0} \right) + \\ &\left( \sum_{x \in (\Gamma+y) \cap D} (-1)^{g(x) + 0 + g(x+y) + 1} \right) + \left( \sum_{x \in (D \setminus (\Gamma \cup (\Gamma+y)))} (-1)^{g(x) + g(x+y)} \right) = \\ &\left( \sum_{x \in (D \setminus (\Gamma \cup (\Gamma+y)))} (-1)^{g(x) + g(x+y)} \right) - 2S. \end{aligned}$$

Таким образом,

$$\sum_{x \in D} (-1)^{g'(x) + g'(x+y)} = \sum_{x \in D} (-1)^{g(x) + g(x+y)} - 4S.$$

Отсюда из равенства (1) и неравенства (5) следует, что

$$\sum_{x \in D} (-1)^{g'(x) + g'(x+y)} \neq 0.$$

Но равенство (1) должно выполняться для любой бент-функции, в том числе и для  $g'$ . Полученное противоречие доказывает теорему.  $\square$

## 4 Дуальность определений бент-функций и аффинных функций

При четном  $n$  класс бент-функций  $\mathcal{B}_n$  можно определить как множество функций, отстоящих от класса всех аффинных булевых функций  $\mathcal{A}_n$  на максимально возможное расстояние  $N_{\max}$ , т. е.

$$\mathcal{B}_n = \{g : \text{dist}(g, \mathcal{A}_n) = N_{\max}\}.$$

При этом известно, что  $N_{\max} = 2^{n-1} - 2^{(n/2)-1}$ . Но можно ли *обратить* это определение? Другими словами, верно ли, что  $\mathcal{A}_n$  — это множество всех булевых функций, отстоящих от класса  $\mathcal{B}_n$  на максимально возможное расстояние  $N'_{\max}$ ? Пусть

$$\mathcal{A}'_n = \{f : \text{dist}(f, \mathcal{B}_n) = N'_{\max}\}.$$

Покажем, что подобное *обращение* определений действительно возможно, т. е. справедливо  $N_{\max} = N'_{\max}$  и  $\mathcal{A}_n = \mathcal{A}'_n$ .

**Утверждение 4.** *Справедливо  $N'_{\max} = 2^{n-1} - 2^{(n/2)-1}$ .*

**Доказательство.** По определению  $N'_{\max} = \max_f \min_{g \in \mathcal{B}_n} \text{dist}(f, g)$ . Заметим, что  $\text{dist}(f, g) = 2^{n-1} - \frac{1}{2} W_{f+g}(0)$ . Поэтому

$$N'_{\max} = 2^{n-1} - \frac{1}{2} \min_f \max_{g \in \mathcal{B}_n} |W_{f+g}(0)|.$$

Зафиксируем любую бент-функцию  $g'$  от  $n$  переменных. Поскольку класс  $\mathcal{B}_n$  замкнут относительно добавления аффинных функций, то каждая функция вида  $g' + \ell_a$ , где  $\ell_a(x) = \langle a, x \rangle$ , является бент-функцией. Заметим, что  $W_{f+g'+\ell_a}(0) = W_{f+g'}(a)$ . Тогда, очевидно

$$\max_{g \in \mathcal{B}_n} |W_{f+g}(0)| \geq \max_{\substack{g \in \mathcal{B}_n, g = g' + \ell_a \\ \text{для некоторого } a}} |W_{f+g}(0)| = \max_a |W_{f+g'}(a)|.$$

Но из равенства Парсеваля для булевой функции  $f + g'$  следует, что  $\max_a |W_{f+g'}(a)| \geq 2^{n/2}$ . Отсюда получаем  $N'_{\max} \leq 2^{n-1} - 2^{(n/2)-1}$ . С другой стороны, расстояние  $2^{n-1} - 2^{(n/2)-1}$  до класса бент-функций достигается, например, для любой аффинной функции  $f$ . Утверждение доказано.  $\square$

**Утверждение 5.** *Выполняется  $\mathcal{A}_n = \mathcal{A}'_n$ .*

**Доказательство.** Очевидно, что  $\mathcal{A}_n \subseteq \mathcal{A}'_n$ . Предположим, что существует функция  $f \in \mathcal{A}'_n \setminus \mathcal{A}_n$ . Тогда по Теореме 1 найдется бент-функция  $g$  такая, что  $f + g$  не является бент-функцией. Т. е. существует вектор  $a$  такой, что  $|W_{f+g}(a)| > 2^{n/2}$ . Рассмотрим бент-функцию  $g'(x) = g(x) + \langle a, x \rangle$ . Для нее справедливо  $W_{f+g'}(0) = W_{f+g}(a)$  и в силу равенства  $\text{dist}(f, \mathcal{B}_n) = 2^{n-1} - \frac{1}{2} \max_{g \in \mathcal{B}_n} |W_{f+g}(0)|$  заключаем, что  $\text{dist}(f, \mathcal{B}_n) < N'_{\max}$ , что противоречит выбору  $f$ . Таким образом,  $\mathcal{A}_n = \mathcal{A}'_n$ .  $\square$

Заметим, что ключевым фактом, позволившим установить «дуальность» между определениями аффинных функций и бент-функций является Теорема 1.

## 5 Автоморфизмы бент-функций

Отображение  $\varphi$  множества всех булевых функций от  $n$  переменных в себя называется *изометричным*, если оно сохраняет расстояния между булевыми функциями, т. е.  $\text{dist}(\varphi(f), \varphi(g)) = \text{dist}(f, g)$ . Известно, что любое такое отображение однозначно представляется в виде

$$g(x) \rightarrow g(s(x)) + f(x), \quad (6)$$

где  $s : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  — любая подстановка,  $f$  — произвольная функция от  $n$  переменных.

*Группой автоморфизмов* подмножества булевых функций  $\mathcal{M}$  называется группа изометричных отображений множества всех булевых

функций в себя, оставляющих неподвижным множество  $\mathcal{M}$ . Обозначим эту группу через  $Aut(\mathcal{M})$ .

Напомним, что *полная аффинная группа*  $GA(n)$  состоит из всех отображений вида  $g(x) \rightarrow g(Ax + b)$ , где  $A$  — невырожденная матрица,  $b$  — произвольный вектор. Справедливо

**Утверждение 6.** *Группа  $Aut(\mathcal{A}_n)$  равна полупрямому произведению полной аффинной группы  $GA(n)$  на  $\mathbb{Z}_2^{n+1}$ .*

Действительно, для любого автоморфизма (6) сдвиг на функцию  $f$  может определяться только аффинной функцией (т. к. образ нулевой функции — также аффинная функция). Множество всех аффинных функций от  $n$  переменных образует группу, изоморфную  $\mathbb{Z}_2^{n+1}$ . Остается отметить, что каждая перестановка  $s$ , как известно, должна принадлежать группе  $GA(n)$ , см. например, [2].

**Теорема 2.** *Справедливо  $Aut(\mathcal{B}_n) = Aut(\mathcal{A}_n) = GA(n) \ltimes \mathbb{Z}_2^{n+1}$ .*

**Доказательство.** Очевидно, что  $Aut(\mathcal{A}_n) \subseteq Aut(\mathcal{B}_n)$ . Действительно, для любого отображения  $\varphi \in Aut(\mathcal{A}_n)$  и любой бент-функции  $g$  имеем  $dist(g, \mathcal{A}_n) = dist(\varphi(g), \varphi(\mathcal{A}_n)) = dist(\varphi(g), \mathcal{A}_n)$ . А следовательно, любая бент-функция под действием  $\varphi$  переходит в некоторую другую бент-функцию.

Аналогично,  $Aut(\mathcal{B}_n) \subseteq Aut(\mathcal{A}_n)$ . А именно для любого автоморфизма  $\psi \in Aut(\mathcal{B}_n)$  и любой аффинной функции  $f$  выполняется  $dist(f, \mathcal{B}_n) = dist(\psi(f), \psi(\mathcal{B}_n)) = dist(\psi(f), \mathcal{B}_n)$ . Отсюда согласно утверждениям 4 и 5 следует, что  $\psi(\mathcal{A}_n) = \mathcal{A}_n$ .

Получаем, что  $Aut(\mathcal{B}_n) = Aut(\mathcal{A}_n)$ . Из утверждения 6 следует конкретный вид этой группы.  $\square$

Таким образом, если отображение (6) переводит класс бент-функций в себя, то оно имеет вид  $g(x) \rightarrow g(Ax + b) + \langle c, x \rangle + d$ . Напомним, что бент-функции, получающиеся одна из другой с помощью такого отображения называются *аффинно эквивалентными*. Из полученных результатов следует, что более общего подхода к эквивалентности бент-функций на основе изометричных отображений не существует.

## Литература

- [1] *Логачев О. А., Сальников А. А., Яценко В. В.* Булевы функции в теории кодирования и криптологии. М.: Московский центр непрерывного математического образования, 2004.
- [2] *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки, М: 1979.
- [3] *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ // Прикладная Дискретная Математика. 2009. Т. 2, N 1. С. 15–37.



- [4] *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискретный анализ и исследование операций. 2010. Т. 17, N 1. С. 34–64.
- [5] *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. N 1. P. 1–10.
- [6] *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. N 3. P. 300–305.