ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь–март 2018. Том 25, № 1. С. 98–119

УДК 519.7 DOI: 10.17377/daio.2018.25.557

СПЕКТР РАССТОЯНИЙ ХЭММИНГА МЕЖДУ САМОДУАЛЬНЫМИ БЕНТ-ФУНКЦИЯМИ ИЗ КЛАССА МЭЙОРАНА — МАКФАРЛАНДА *)

А. В. Куценко

Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия

E-mail: AlexandrKutsenko@bk.ru

Аннотация. Бент-функция называется *самодуальной*, если она совпадает со своей дуальной функцией. Исследуются метрические свойства самодуальных бент-функций, построенных с помощью известных конструкций. Получен полный спектр расстояний Хэмминга между самодуальными бент-функциями, построенными с помощью конструкции Мэйорана — МакФарланда. С помощью этого результата найдено минимальное расстояние Хэмминга между рассмотренными функциями. Библиогр. 22.

Ключевые слова: расстояние Хэмминга, самодуальная бент-функция, конструкция Мэйорана — МакФарланда.

Введение

В данной работе рассматриваются бент-функции — булевы функции от чётного числа переменных, обладающие максимально возможной нелинейностью — одним из важнейших криптографических свойств — и в силу этого представляющие большой интерес. Стоит отметить, что наряду с максимальной нелинейностью бент-функции обладают и другими криптографическими свойствами, а также имеют большое число приложений в алгебре и теории кодирования. Термин «бент-функция» был введён Ротхаусом в 60-х годах XX века [19]. Известно, что в Советском Союзе в это же время также изучались максимально нелинейные булевы функции. Понятие *минимальная функция* — аналог бент-функции —

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 17–41–543364), Министерства образования и науки Российской Федерации (программа 5–100) и Регионального научно-образовательного математического центра Новосибирского государственного университета.

было предложено советскими учёными В. А. Елисеевым и О. П. Степченковым в 1962 г. (см. [21]). С бент-функциями связан ряд открытых проблем. В частности, вопросы, касающиеся классификации этих функций, построения новых конструкций. Неизвестно точное число бент-функций, известны лишь оценки на него. Заслуживают внимания проблемы, касающиеся метрических свойств бент-функций, также имеющие непосредственное отношение к вопросу мощности класса бент-функций. В частности, в [1] (см. также [15]) установлено, что расстояние Хэмминга между двумя различными бент-функциями от n переменных не меньше чем $2^{n/2}$. В [5] доказано, что между двумя бент-функциями от n переменных достижимы расстояния вида $2^{n/2+1} - 2^p$, где $1 \leqslant p \leqslant n/2$. В статье [14] приводятся другие известные результаты по данному направлению.

Для каждой бент-функции однозначно определяется дуальная к ней булева функция, также являющаяся бент-функцией. Изучению свойств дуальных функций посвящен ряд работ. Например, в [7] изучались дуальные функции к бент-функциям с показателем Нихо, дуальные функции к бент-функциям Касами рассмотрены в статье [16]. Дуальные функции к бент-функциям Диллона найдены в [8]. Установлено соответствие между алгебраическими степенями бент-функции и дуальной к ней, из которого следует, что функция, дуальная к бент-функции от n переменных, имеющей максимальную степень, также имеет максимальную степень, равную $n/2$ (см. [12]). Утверждение, связывающее коэффициенты алгебраических нормальных форм бент-функции и дуальной к ней функции, представлено в монографии [10]. Изучению дуальных функций на конечных группах посвящена статья [22]. Также установлено, что бент-функции и функции, дуальные к ним, разложимы или не разложимы в сумму двух бент-функций одновременно [6].

Следует заметить, что в некоторых работах термин «дуальность» применительно к множеству бент-функций имеет иной смысл: в [20] доказано, что аффинную функцию можно определить как функцию, находящуюся на максимально возможном удалении от множества бент-функций. В силу того, что бент-функция определяется как функция, максимально удалённая от множества аффинных функций, устанавливается дуальность между их определениями. Основанный на данном свойстве подход к изучению бент-функций получил дальнейшее развитие в работе [4].

Бент-функция, совпадающая со своей дуальной, называется *самодуальной*. Открытые вопросы, актуальные для класса бент-функций, ак-

туальны и для самодуальных бент-функций. Сложной задачей является полная характеризация и описание класса самодуальных бент-функций, нахождение оценок на его мощность. Этим и другим вопросам посвящен ряд работ. В частности, в [9] перечислены все классы аффинной эквивалентности самодуальных бент-функций от 2, 4, 6 переменных и всех квадратичных самодуальных бент-функций от 8 переменных относительно аффинного преобразования, сохраняющего самодуальность; установлено, что расстояние Хэмминга между произвольной самодуальной и анти-самодуальной бент-функциями от n переменных в точности равно 2^{n-1}. В [13] приведена классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных можно найти в [11]. В [18] были предложены новые конструкции самодуальных бент-функций.

В настоящей работе изучаются метрические свойства самодуальных бент-функций. Рассмотрена задача нахождения возможных расстояний Хэмминга между различными самодуальными бент-функциями из класса Мэйорана — МакФарланда. Получен полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда. Данный спектр имеет следующий вид (теорема 1):

$$\{2^{n-1}, 2^{n-1}(1 \pm 2^{-r}), r = 0, 1, \ldots, n/2 - 1\},$$

где $n \geqslant 4$ — число переменных. На основании этого результата сделан вывод: минимальное расстояние Хэмминга между рассмотренными функциями в точности равно 2^{n-2} (следствие 1).

1. Определения

Булевой функцией от n переменных называется произвольное отображение вида $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2$, *двоичным вектором* длины n — набор $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$. Через $\mathcal{F}_n$ обозначим множество всех булевых функций от n переменных. Символом $\oplus$ обозначается операция сложения по модулю 2. Пусть $M_k(\mathbb{Z}_2)$ — множество квадратных $(k \times k)$-матриц над полем $\mathbb{Z}_2$, $I_k \in M_k(\mathbb{Z}_2)$ — единичная матрица порядка k. Пусть $A \in M_k(\mathbb{Z}_2)$, тогда через $A^T \in M_k(\mathbb{Z}_2)$ обозначается транспонированная к A матрица. Обозначим $\mathbf{0}_k = (0, 0, \ldots, 0) \in \mathbb{Z}_2^k$. Через $\langle x, y\rangle$ обозначается аналог скалярного произведения по модулю 2:

$$\langle x, y\rangle = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n,$$

где $x, y \in \mathbb{Z}_2^n$.

Двоичная симметричная матрица с нулевой диагональю называется *симплектической*.

Преобразованием Уолша — Адамара булевой функции $f \in \mathcal{F}_n$ называется целочисленная функция $W_f\colon \mathbb{Z}_2^n \to \mathbb{Z}$, заданная равенством

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle},$$

где $y \in \mathbb{Z}_2^n$. Набор значений $W_f(y)$ однозначно определяет булеву функцию f, а числа из этого набора называются *коэффициентами Уолша — Адамара*.

Расстояние Хэмминга $\operatorname{dist}(f, g)$ между двумя булевыми функциями $f, g \in \mathcal{F}_n$ равно числу двоичных векторов x длины n, для которых $f(x) \neq g(x)$. *Весом Хэмминга* $\operatorname{wt}(f)$ булевой функции $f \in \mathcal{F}_n$ называется число двоичных векторов длины n, на которых функция f принимает значение 1; *весом Хэмминга* $\operatorname{wt}(x)$ вектора $x \in \mathbb{Z}_2^n$ — число $\sum\limits_{i=1}^{n} x_i$.

Представление булевой функции $f \in \mathcal{F}_n$ в виде

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{k=1}^{n} \bigoplus_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} a_{i_1 i_2 \ldots i_k} x_{i_1} x_{i_2} \ldots x_{i_k} \oplus a_0,$$

где $a_0, a_{i_1 i_2 \ldots i_k} \in \mathbb{Z}_2$ — коэффициенты, называется *полиномом Жегалкина*, или *алгебраической нормальной формой* (*АНФ*). Выражения вида $x_{i_1} x_{i_2} \ldots x_{i_k}$ называются *мономами степени* k.

Степенью $\deg f$ булевой функции f называется наибольшая степень монома, входящего в АНФ этой функции с ненулевым коэффициентом. Если все коэффициенты (за исключением, быть может, a_0) равны нулю, степень функции также считается равной нулю.

В случае, когда n — чётное число, а все коэффициенты Уолша — Адамара булевой функции f от n переменных по модулю равны $2^{n/2}$, функция f называется *бент-функцией*.

Широко известна *конструкция Мэйорана — МакФарланда* бент-функций, предложенная в 1973 г. [17]. Пусть π — любая подстановка на множестве двоичных векторов длины $n/2$ и h — произвольная булева функция от $n/2$ переменных. Тогда функция $f(x, y) = \langle x, \pi(y) \rangle \oplus h(y)$ является бент-функцией от n переменных. Стоит отметить, что мощность данного класса, равная $2^{2^{n/2}}(2^{n/2})!$, до появления более точных оценок использовалась в качестве нижней оценки на мощность всего класса бент-функций.

Для каждой бент-функции $f \in \mathcal{F}_n$ равенством

$$W_f(y) = (-1)^{\tilde{f}(y)} 2^{n/2}, \quad y \in \mathbb{Z}_2^n,$$

однозначно определяется *дуальная* к ней функция $\tilde{f} \in \mathcal{F}_n$.

Дуальные функции обладают некоторыми свойствами, в частности, каждая дуальная функция $\tilde{f}$ сама является бент-функцией, а дуальная к ней функция $\tilde{\tilde{f}}$ совпадает с бент-функцией f (см. [8]).

Бент-функция, совпадающая со своей дуальной, называется *самодуальной* бент-функцией. Бент-функция, совпадающая с отрицанием своей дуальной, называется *анти-самодуальной* бент-функцией.

Согласно предложенным в работе [13] обозначениям пусть $\mathrm{SB}^+_{\mathcal{M}}(n)$ ($\mathrm{SB}^-_{\mathcal{M}}(n)$) — множество самодуальных (анти-самодуальных) бент-функций от n переменных из класса Мэйорана — МакФарланда.

Более подробно ознакомиться с классом бент-функций можно, например, в [21].

2. Вспомогательные утверждения

В этом разделе приведены утверждения, которые будут использоваться для получения основного результата.

В [9] были найдены необходимые и достаточные условия самодуальности бент-функции, построенной с помощью конструкции Мэйорана — МакФарланда.

Утверждение 1 [9]. *Пусть n — чётное натуральное число и бент-функция $f \in \mathcal{F}_n$ представима в виде*

$$f(x, y) = \langle x, \pi(y) \rangle \oplus h(y), \quad x, y \in \mathbb{Z}_2^{n/2},$$

где π — подстановка на множестве $\mathbb{Z}_2^{n/2}$, h — булева функция от $n/2$ переменных. Тогда бент-функция f будет самодуальной (анти-самодуальной) в том и только том случае, когда $h(y) = \langle b, y \rangle \oplus \varepsilon$, $\pi(y) = L(y) \oplus a$, где $a, b \in \mathbb{Z}_2^{n/2}$, $\varepsilon \in \mathbb{Z}_2$, $L \colon \mathbb{Z}_2^{n/2} \to \mathbb{Z}_2^{n/2}$ — линейный автоморфизм такой, что $\langle x, L(y) \rangle = \langle L^{-1}(x), y \rangle$ для всех $x, y \in \mathbb{Z}_2^{n/2}$, $a = L(b)$ и вес Хэмминга вектора $L(b)$ есть чётное (нечётное) число.

Лемма 1. *Пусть $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij}) \in M_k(\mathbb{Z}_2)$. Если $AA^T = BB^T = I_k$, а $c_{ij} = a_{ij} \oplus b_{ij}$, $i, j = 1, 2, \ldots, k$, то столбцы матрицы C образуют линейно зависимое подмножество векторов из $\mathbb{Z}_2^k$.*

Доказательство. Сначала докажем, что в каждой строке матриц A и B нечётное число единиц. Можно считать, что каждая строка матрицы A и каждый столбец матрицы A^T суть элементы множества $\mathbb{Z}_2^k$. Обозначим через $A_i \in \mathbb{Z}_2^k$ и $(A^T)^j \in \mathbb{Z}_2^k$ i-ю строку матрицы A и j-й столбец матрицы A^T соответственно, $i, j = 1, 2, \ldots, k$.

Имеем

$$\langle A_i, A_j \rangle = \langle A_i, (A^T)^j \rangle = \bigoplus_{r=1}^{k} a_{ir} a_{jr} = (I_k)_{ij}.$$

Тогда

$$1 = \langle A_i, A_i \rangle = \bigoplus_{l=1}^{k} a_{il} a_{il} = \bigoplus_{l=1}^{k} a_{il}.$$

Таким образом, $\bigoplus\limits_{l=1}^{k} a_{il} = 1$ при каждом $i \in \{1, 2, \ldots, k\}$, следовательно, в каждой строке матрицы A число единиц нечётно. Аналогично можно показать, что в каждой строке матрицы B число единиц также нечётно.

Так как каждая строка матрицы C получается сложением по модулю 2 соответствующих строк матриц A и B, она содержит чётное число единиц. Отсюда получаем, что $C^1 \oplus C^2 \oplus \ldots \oplus C^k = \mathbf{0}_k$, где $C^j \in \mathbb{Z}_2^k$ — j-й столбец матрицы C, $j = 1, 2, \ldots, k$. Стало быть, столбцы матрицы C образуют линейно зависимое множество в $\mathbb{Z}_2^k$. Лемма 1 доказана.

Лемма 2. *Если функция $f \in \mathcal{F}_n$ представима в виде*

$$f(x) = \langle a, x \rangle, \quad x \in \mathbb{Z}_2^n,$$

где $a \in \mathbb{Z}_2^n$ и $wt(a) > 0$, то $wt(f) = 2^{n-1}$.

Доказательство. Заметим лишь, что число решений линейного уравнения $\langle a, x \rangle = 1$ равно 2^{n-1}. Лемма 2 доказана.

Пусть m — натуральное число. Согласно [3, гл. 13] для произвольного $0 \leqslant r \leqslant m$ двоичный *код Рида — Маллера* $RM(r, m)$ порядка r длины 2^m определяется как множество всех векторов из $\mathbb{Z}_2^{2^m}$, соответствующих булевым функциям, каждая из которых представима многочленом степени не выше r.

Пусть $r = 2$, тогда типичное кодовое слово имеет вид

$$S(v) = \bigoplus_{1 \leqslant i \leqslant j \leqslant m} q_{ij} v_i v_j \oplus \bigoplus_{1 \leqslant i \leqslant m} l_i v_i \oplus \varepsilon = \langle Qv, v \rangle \oplus \langle L, v \rangle \oplus \varepsilon,$$

где $Q = (q_{ij})$ — верхняя треугольная двоичная $(m \times m)$-матрица, $L = (l_1, l_2, \ldots, l_m) \in \mathbb{Z}_2^m$, $\varepsilon \in \mathbb{Z}_2$. Если *квадратичная форма* $\langle Qv, v \rangle$ фиксирована, а аффинная функция $\langle L, v \rangle \oplus \varepsilon$ пробегает код Рида — Маллера

первого порядка $\mathrm{RM}(1,m)$, то $S(v)$ пробегает смежный класс кода Рида — Маллера второго порядка $\mathrm{RM}(2,m)$ по коду $\mathrm{RM}(1,m)$. Этот смежный класс полностью характеризуется формой $\langle Qv,v\rangle$ (см. [3, гл. 15]).

Относительно спектра весов кодов Рида — Маллера второго порядка известно следующее

Утверждение 2 [3, гл. 15]. *Если ранг симметрической матрицы $B=(b_{ij})\in M_m(\mathbb{Z}_2)$, где $b_{ij}=q_{ij}\oplus q_{ji}$, $i,j=1,2,\dots,m$, равен $2r$, то спектр весов смежного класса $\mathcal{B}$ кода $RM(2,m)$ по коду $RM(1,m)$ равен*

$$\{2^{m-1}(1-2^{-r}),2^{m-1},2^{m-1}(1+2^{-r})\}.$$

Утверждение 3 (теорема Диксона [3, гл. 15]). 1. *Для каждой симплектической матрицы B ранга $2h$ существует такая обратимая двоичная матрица R, что у матрицы RBR^T все элементы равны нулю, за исключением двух диагоналей, лежащих непосредственно над и под главной диагональю, и эти диагонали имеют вид $1010\dots100\dots0$, где число единиц равно h.*

2. *Любую булеву функцию, степень которой не превосходит 2, имеющую вид $\langle Qv,v\rangle\oplus L(v)\oplus\varepsilon$, где Q — верхняя треугольная двоичная матрица, а L и ε произвольны, можно привести к виду*

$$T(y)=\bigoplus_{i=1}^{h}y_{2i-1}y_{2i}\oplus L'(y)\oplus\varepsilon$$

преобразованием переменных $y=vR^{-1}$, где R — матрица, определяемая в п. 1 при $B=Q\oplus Q^T$.

3. *Если $L'(y)$ линейно зависит только от $y_1,y_2,\dots,y_{2h}$, то существует аффинное преобразование, приводящее $T(y)$ к виду*

$$\bigoplus_{i=1}^{h}x_{2i-1}x_{2i}\oplus\varepsilon_1,\quad \varepsilon_1\in\mathbb{Z}_2.$$

Лемма 3. *Вес Хэмминга функции $f\in\mathcal{F}_{2k}$, имеющей вид*

$$f(x)=\bigoplus_{i=1}^{r}x_{2i-1}x_{2i}\oplus\varepsilon,\quad x\in\mathbb{Z}_2^{2k},$$

где $\varepsilon\in\mathbb{Z}_2$ и $1\leqslant r\leqslant k$, равен $2^{2k-1}(1-(-1)^{\varepsilon}2^{-r})$.

Доказательство. Положим $\varepsilon = 0$. Обозначим через $S \subset \mathbb{Z}_2^{2r}$ подмножество векторов $(x_1, x_2, \ldots, x_{2r}) \in \mathbb{Z}_2^{2r}$, на которых квадратичная часть функции f равна единице. Ясно, что $\mathrm{wt}(f) = 2^{2k-2r} \cdot |S|$. Пусть через $\lceil n \rceil$ обозначается верхняя целая часть числа $n \in \mathbb{R}$. Запишем выражение для $|S|$:

$$|S| = \sum_{m=1}^{\lceil \frac{r}{2} \rceil} \binom{r}{2m-1} \sum_{j=0}^{r-m} \binom{r-m}{j} 2^j = \sum_{m=1}^{\lceil \frac{r}{2} \rceil} \binom{r}{2m-1} 3^{r-m}$$

$$= 3^r \sum_{i=0}^{r} \binom{r}{i} \frac{1-(-1)^i}{2} \left(\frac{1}{3}\right)^i = \frac{3^r}{2} \left\{ \sum_{t=0}^{r} \binom{r}{t} \left(\frac{1}{3}\right)^t - \sum_{l=0}^{r} \binom{r}{l} \left(-\frac{1}{3}\right)^l \right\}$$

$$= \frac{3^r}{2} \left\{ \left(\frac{4}{3}\right)^r - \left(\frac{2}{3}\right)^r \right\} = 2^{2r-1} - 2^{r-1}.$$

Тогда

$$\mathrm{wt}(f) = 2^{2k-2r}|S| = 2^{2k-2r}(2^{2r-1} - 2^{r-1}) = 2^{2k-1}(1 - 2^{-r}).$$

При $\varepsilon = 1$ выражение для веса Хэмминга примет вид

$$\mathrm{wt}(f) = 2^{2k} - 2^{2k-2r}|S| = 2^{2k} - 2^{2k-1}(1 - 2^{-r}) = 2^{2k-1}(1 + 2^{-r}).$$

Лемма 3 доказана.

Пусть $k \geqslant 2$. Через e_i обозначим элемент множества $\mathbb{Z}_2^{2k}$, у которого i-я координата равна единице, а все остальные — нулю, $i = 1, 2, \ldots, 2k$. Рассмотрим симплектическую матрицу $Q^{(2k)} \in M_{2k}(\mathbb{Z}_2)$, строки которой определены следующим образом:

$$(Q^{(2k)})_i = \begin{cases} e_{i+k} \oplus e_{i+1+k} & \text{при } i \in \{1, 2, \ldots, k-1\}, \\ e_{k+1} \oplus e_{2k} & \text{при } i = k, \\ \mathbf{0}_{2k} & \text{при } i = \{k+1, k+2, \ldots, 2k\}. \end{cases}$$

Справедлива

Лемма 4. *Булева функция*

$$f(x) = \langle Qx, x \rangle \oplus \langle a, x \rangle, \quad x \in \mathbb{Z}_2^{2k},$$

где $a = (1, 1, 0, 0, \ldots, 0) \in \mathbb{Z}_2^{2k}$, *линейным преобразованием переменных может быть приведена к виду*

$$\bigoplus_{i=1}^{k-1} y_{2i-1} y_{2i} \oplus \langle a', y \rangle, \quad y \in \mathbb{Z}_2^{2k},$$

где $a' \in \mathbb{Z}_2^{2k}$, *причём* $a'_{2k-1} = a'_{2k} = 0$.

Доказательство проведём индукцией по k. Для удобства матрицу $Q \in M_{2k}(\mathbb{Z}_2)$, построенную с помощью указанной выше конструкции, будем обозначать через $Q_0^{(2k)}$. Через $H^{(2k)}$ обозначим симплектическую матрицу порядка $2k \times 2k$, у которой все элементы равны нулю, за исключением двух диагоналей, лежащих непосредственно над и под главной диагональю, и эти диагонали имеют вид $1010\ldots100\ldots0$, где число единиц равно $k-1$. Матрицу, соответствующую искомому линейному преобразованию, будем обозначать через $R^{(2k)} = \left(r_{ij}^{(2k)}\right) \in M_{2k}(\mathbb{Z}_2)$.

База индукции: при $k=2$ симплектическая матрица $B^{(4)} = Q_0^{(4)} \oplus (Q_0^{(4)})^T$, ранг которой равен 2, имеет вид

$$B^{(4)} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Рассмотрим обратимую матрицу

$$R^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}.$$

Непосредственная проверка показывает, что

$$R^{(4)} B^{(4)} (R^{(4)})^T = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = H^{(4)}.$$

Тогда согласно теореме Диксона замена переменных $y = x(R^{(4)})^{-1}$ преобразует функцию f к виду

$$y_1 y_2 \oplus \langle a', y \rangle, \quad y \in \mathbb{Z}_2^4,$$

где $a' \in \mathbb{Z}_2^4$. Кроме того,

$$\langle a', y \rangle = \left\langle (1,1,0,0), (y_1,y_2,y_3,y_4) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \right\rangle = y_1,$$

т. е. $a'_2 = a'_3 = a'_4 = 0$.

Индукционный шаг: предположим, что для всех $k < k_0$ утверждение верно, где $k_0 \geqslant 3$. Пусть $k = k_0$. В этом случае симплектическая матрица $B^{(2k)} = Q_0^{(2k)} \oplus \left(Q_0^{(2k)}\right)^T$, ранг которой равен $2(k-1)$, имеет вид

$$B^{(2k)} = \left(\begin{array}{cc|cc} & & 1 & 1 \\ & & & 1 \quad 1 \\ & \mathbf{0}_{k\times k} & & \ddots \quad \ddots \\ & & & 1 \quad 1 \\ & & 1 & \quad\quad 1 \\ \hline 1 & \quad\quad 1 & & \\ 1 \quad 1 & & & \\ 1 \quad 1 & & & \\ \ddots \quad \ddots & & & \mathbf{0}_{k\times k} \\ & 1 \quad 1 & & \end{array}\right)$$

Рассмотрим три обратимых матрицы $R_1^{(2k)}, R_2^{2k}, R_3^{(2k)} \in M_{2k}(\mathbb{Z}_2)$:

$$\left(R_1^{(2k)}\right)_i = \begin{cases} e_i & \text{при } i \in \{1, 2, \ldots, k-2\}, \\ e_{k-1} \oplus e_k & \text{при } i = k-1, \\ e_{k+1} \oplus e_{2k} & \text{при } i = k, \\ e_{i+1} & \text{при } i \in \{k+1, k+2, \ldots, 2k-2\}, \\ e_k & \text{при } i = 2k-1, \\ e_{2k} & \text{при } i = 2k, \end{cases}$$

$$R_2^{(2k)} = \left(\begin{array}{c|cc} R^{(2k-2)} & \mathbf{0}_{2k-2}^T & \mathbf{0}_{2k-2}^T \\ \hline \mathbf{0}_{2k-2} & 1 & 0 \\ \mathbf{0}_{2k-2} & 0 & 1 \end{array}\right),$$

$$\left(R_3^{(2k)}\right)_i = \begin{cases} e_i & \text{при } i \in \{1, 2, \ldots, 2k-4\}, \\ e_{2k-1} & \text{при } i = 2k-3, \\ e_{2k} & \text{при } i = 2k-2, \\ e_{2k-3} & \text{при } i = 2k-1, \\ e_{2k-2} & \text{при } i = 2k, \end{cases}$$

где $i = 1, 2, \ldots, 2k$.

$$R_1^{(2k)} = \begin{array}{c} \\ k \\ \\ \\ \\ \\ 2k \end{array} \begin{array}{c} \begin{array}{cccc|c} & & & & k \end{array} \\ \left(\begin{array}{cccc|c|cccc} 1 & 0 & \dots & 0 & 0 & & & & \\ 0 & \ddots & & \vdots & \vdots & & & & \\ \vdots & & \ddots & 0 & 0 & & \mathbf{0}_{(k-1)\times k} & & \\ 0 & \dots & 0 & 1 & 1 & & & & \\ \hline 0 & \dots & \dots & 0 & 0 & 1 & 0 & \dots & 0 & 1 \\ \hline & & & & \vdots & 0 & \ddots & & \vdots & 0 \\ & & & & \vdots & \vdots & & \ddots & 0 & \vdots \\ & & \mathbf{0}_{k\times(k-1)} & & 0 & 0 & \dots & 0 & 1 & \vdots \\ & & & & 1 & 0 & \dots & \dots & 0 & 0 \\ & & & & 0 & 0 & \dots & \dots & 0 & 1 \end{array}\right) \end{array} 2k.$$

Обозначим $Q_j^{(2k)} = R_j^{(2k)} Q_{j-1}^{(2k)} \big(R_j^{(2k)}\big)^T \in M_{2k}(\mathbb{Z}_2)$, $j = 1, 2, 3$. Для данных матриц верно следующее:

$$Q_1^{(2k)} = R_1^{(2k)} Q_0^{(2k)} \big(R_1^{(2k)}\big)^T = \left(\begin{array}{c|cc} Q_0^{(2k-2)} & \mathbf{0}_{2k-2}^T & \mathbf{0}_{2k-2}^T \\ \hline \mathbf{0}_{2k-2} & 0 & 1 \\ \mathbf{0}_{2k-2} & 1 & 0 \end{array}\right),$$

$$Q_2^{(2k)} = R_2^{(2k)} Q_1^{(2k)} \big(R_2^{(2k)}\big)^T = \left(\begin{array}{c|cc} H^{(2k-2)} & \mathbf{0}_{2k-2}^T & \mathbf{0}_{2k-2}^T \\ \hline \mathbf{0}_{2k-2} & 0 & 1 \\ \mathbf{0}_{2k-2} & 1 & 0 \end{array}\right),$$

$$Q_3^{(2k)} = R_3^{(2k)} Q_2^{(2k)} \big(R_3^{(2k)}\big)^T = H^{(2k)}.$$

Таким образом,

$$\begin{aligned} R_3^{(2k)} R_2^{(2k)} R_1^{(2k)} Q_0^{(2k)} \big(R_1^{(2k)}\big)^T \big(R_2^{(2k)}\big)^T (R_3^{(2k)})^T \\ = R_3^{(2k)} R_2^{(2k)} R_1^{(2k)} Q_0^{(2k)} \big(R_3^{(2k)} R_2^{(2k)} R_1^{(2k)}\big)^T = H^{(2k)}. \end{aligned}$$

По индукционному предположению выражение

$$\langle (1, 1, 0, 0, \dots, 0), y R^{(2k-2)} \rangle,$$

где $y \in \mathbb{Z}_2^{2k-2}$, не зависит от y_{2k-3} и y_{2k-2}. Это эквивалентно тому, что

$$r_{2k-3,1}^{(2k-2)} = r_{2k-3,2}^{(2k-2)} \quad \text{и} \quad r_{2k-2,1}^{(2k-2)} = r_{2k-2,2}^{(2k-2)}.$$

В то же время

$$\big(R_3^{(2k)}R_2^{(2k)}\big)R_1^{(2k)} = \left(\begin{array}{cc|c} * & * & * \\ \hline r_{2k-3,1}^{(2k-2)} & r_{2k-3,2}^{(2k-2)} & * \\ r_{2k-2,1}^{(2k-2)} & r_{2k-2,2}^{(2k-2)} & * \end{array}\right) \left(\begin{array}{cc|c} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & * \\ \vdots & \vdots & * \\ 0 & 0 & * \end{array}\right)$$

$$= \left(\begin{array}{cc|c} ** & ** & ** \\ \hline r_{2k-3,1}^{(2k-2)} & r_{2k-3,2}^{(2k-2)} & ** \\ r_{2k-2,1}^{(2k-2)} & r_{2k-2,2}^{(2k-2)} & ** \end{array}\right),$$

следовательно, выражение $\langle a', y\rangle = \big\langle a, y\big(R_3^{(2k)}R_2^{(2k)}R_1^{(2k)}\big)\big\rangle$, где $y \in \mathbb{Z}_2^{2k}$, в свою очередь, не зависит от y_{2k-1} и y_{2k}, а значит, $a'_{2k-1} = a'_{2k} = 0$.

Таким образом, по теореме Диксона можно заключить, что искомое преобразование переменных $x = y(R^{(2k)})^{-1}$, $x, y \in \mathbb{Z}_2^{2k}$, определяется матрицей $R^{(2k)} = R_3^{(2k)}R_2^{(2k)}R_1^{(2k)}$. Лемма 4 доказана.

Связь между самодуальными и анти-самодуальными бент-функциями характеризует

Утверждение 4 [9]. *Расстояние Хэмминга между произвольной самодуальной и анти-самодуальной бент-функциями от чётного натурального числа переменных n в точности равно 2^{n-1}.*

3. Спектр расстояний Хэмминга

В этом разделе будет найден полный спектр расстояний Хэмминга между самодуальными и анти-самодуальными, а также анти-самодуальными бент-функциями из класса Мэйорана—МакФарланда. Всюду далее n — чётное натуральное число.

Утверждение 5. *Пусть $f, g \in SB^+_{\mathcal{M}}(n)$, где $n \geqslant 4$. Тогда*

$$\operatorname{dist}(f, g) \in \{2^{n-1}, 2^{n-1}(1 \pm 2^{-r}), r = 0, 1, \ldots, n/2 - 1\}$$

и все приведённые расстояния достижимы.

Доказательство. Положим $n = 2k$, где $k \geqslant 2$ — натуральное число. Рассмотрим произвольную пару самодуальных бент-функций f, g, удовлетворяющую условиям теоремы. Согласно утверждению 1

$$f(x, y) = \langle x, L_f(y) \oplus L_f(b_f)\rangle \oplus \langle b_f, y\rangle \oplus \varepsilon_f,$$
$$g(x, y) = \langle x, L_g(y) \oplus L_g(b_g)\rangle \oplus \langle b_g, y\rangle \oplus \varepsilon_g,$$

где $b_f, b_g \in \mathbb{Z}_2^k$, $\varepsilon_f, \varepsilon_g \in \mathbb{Z}_2$, $L_f, L_g \colon \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ — линейные автоморфизмы такие, что

$$\langle x, L_f(y)\rangle = \left\langle L_f^{-1}(x), y\right\rangle, \quad \langle x, L_g(y)\rangle = \left\langle L_g^{-1}(x), y\right\rangle$$

для всех $x, y \in \mathbb{Z}_2^k$, а векторы $L_f(b_f)$ и $L_g(b_g)$ имеют чётные веса Хэмминга.

Далее рассмотрим булеву функцию G, равную сумме функций f и g по модулю 2. Очевидно, что $\mathrm{wt}(f) = \mathrm{dist}(f, g)$. На первом этапе доказательства будет показано, что данная функция представима в виде $G(x, y) = G(v) = \langle Qv, v\rangle \oplus \langle L, v\rangle \oplus \varepsilon$ для последующего применения утверждения 2. На втором этапе для доказательства достижимости соответствующих весов Хэмминга будут приведены конкретные конструкции Q, L и ε.

Этап I. Рассмотрим следующую булеву функцию от $2k$ переменных:

$$G(x, y) = f(x, y) \oplus g(x, y) = (\langle x, L_f(y) \oplus L_f(b_f)\rangle \oplus \langle b_f, y\rangle \oplus \varepsilon_f) \\ \oplus (\langle x, L_g(y) \oplus L_g(b_g)\rangle \oplus \langle b_g, y\rangle \oplus \varepsilon_g).$$

Имеем

$$\mathrm{dist}(f, g) = \mathrm{wt}(f \oplus g) = \mathrm{wt}(G). \tag{1}$$

Для удобства будем использовать следующие обозначения:

$$L_f(b_f) \oplus L_g(b_g) = c = (c_1, c_2, \ldots, c_k) \in \mathbb{Z}_2^k,$$
$$b_f \oplus b_g = b = (b_1, b_2, \ldots, b_k) \in \mathbb{Z}_2^k, \quad \varepsilon_f \oplus \varepsilon_g = \varepsilon \in \mathbb{Z}_2.$$

Тогда

$$G(x, y) = \langle x, L_{fg}(y)\rangle \oplus \langle c, x\rangle \oplus \langle b, y\rangle \oplus \varepsilon, \tag{2}$$

где $L_{fg} \colon \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ — линейное отображение, определяемое равенством $L_{fg}(z) = L_f(z) \oplus L_g(z)$ для каждого $z \in \mathbb{Z}_2^k$. Через e_i обозначим вектор из $\mathbb{Z}_2^k$, у которого i-я координата равна единице, а все остальные — нулю, $i = 1, 2, \ldots, k$. Заметим, что любому линейному отображению $\varphi \colon \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ в данном базисе соответствует матрица $D = (d_{ij}) \in M_k(\mathbb{Z}_2)$ такая, что $(d_{1j}, d_{2j}, \ldots, d_{kj})^T = \varphi(e_j) \in \mathbb{Z}_2^k$, $j = 1, 2, \ldots, k$, и $\varphi(z) = Dz$ для каждого $z \in \mathbb{Z}_2^k$. Пусть линейному автоморфизму L_f в базисе, указанном выше, соответствует ортогональная матрица $L^f = \left(l_{ij}^f\right) \in M_k(\mathbb{Z}_2)$, линейному автоморфизму L_g — ортогональная матрица $L^g = \left(l_{ij}^g\right) \in M_k(\mathbb{Z}_2)$, линейному отображению L_{fg} — матрица $A = (a_{ij}) \in M_k(\mathbb{Z}_2)$. Тогда действие

автоморфизма L_f на вектор $y \in \mathbb{Z}_2^k$ будет равно $L_f(y) = L^f y$. Аналогично, действие автоморфизма L_g на вектор $y \in \mathbb{Z}_2^k$ есть $L_g(y) = L^g y$. Действие линейного отображения L_{fg} на вектор $y \in \mathbb{Z}_2^k$ будет $L_{fg}(y) = Ay$, но $L_{fg}(z) = L_f(y) \oplus L_g(y) = L^f y \oplus L^g y$, т. е. матрица A имеет вид

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1k} \\ a_{21} & a_{22} & \dots & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \dots & a_{kk} \end{pmatrix} = \begin{pmatrix} l^f_{11} \oplus l^g_{11} & l^f_{12} \oplus l^g_{12} & \dots & l^f_{1k} \oplus l^g_{1k} \\ l^f_{21} \oplus l^g_{21} & l^f_{22} \oplus l^g_{22} & \dots & l^f_{2k} \oplus l^g_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ l^f_{k1} \oplus l^g_{k1} & l^f_{k2} \oplus l^g_{k2} & \dots & l^f_{kk} \oplus l^g_{kk} \end{pmatrix}.$$

Перепишем выражение (2):

$$G(x, y) = \langle x, Ay \rangle \oplus \langle c, x \rangle \oplus \langle b, y \rangle \oplus \varepsilon.$$

Обозначим

$$v = (v_1, v_2, \dots, v_{2k}) = (x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_k) = (x, y) \in \mathbb{Z}_2^{2k},$$
$$L = (l_1, l_2, \dots, l_{2k}) = (c_1, c_2, \dots, c_k, b_1, b_2, \dots, b_k) = (c, b) \in \mathbb{Z}_2^{2k},$$
$$Q = (q_{ij}) \in M_{2k}(\mathbb{Z}_2),$$

где $q_{ij} = \begin{cases} a_{i,j-k} & \text{при } i \leqslant k < j \\ 0 & \text{иначе} \end{cases}$, $i, j = 1, 2, \dots, 2k$. Иначе говоря, верхняя треугольная матрица Q имеет вид

$$Q = \left(\begin{array}{c|cccc} \multirow{3}{*}{$\mathbf{0}_{k\times k}$} & a_{11} & a_{12} & \dots & a_{1k} \\ & a_{21} & a_{22} & \dots & a_{2k} \\ & \vdots & \vdots & \ddots & \vdots \\ & a_{k1} & a_{k2} & \dots & a_{kk} \\ \hline \mathbf{0}_{k\times k} & \multicolumn{4}{c}{\mathbf{0}_{k\times k}} \end{array}\right).$$

Пусть также $B = (b_{ij}) \in M_{2k}(\mathbb{Z}_2)$, где $b_{ij} = q_{ij} \oplus q_{ji}$, $i, j = 1, 2, \dots, 2k$, т. е.

$$B = \left(\begin{array}{cccc|cccc} \multicolumn{4}{c|}{\multirow{3}{*}{$\mathbf{0}_{k\times k}$}} & a_{11} & a_{12} & \dots & a_{1k} \\ \multicolumn{4}{c|}{} & a_{21} & a_{22} & \dots & a_{2k} \\ \multicolumn{4}{c|}{} & \vdots & \vdots & \ddots & \vdots \\ \multicolumn{4}{c|}{} & a_{k1} & a_{k2} & \dots & a_{kk} \\ \hline a_{11} & a_{21} & \dots & a_{k1} & \multicolumn{4}{c}{\multirow{3}{*}{$\mathbf{0}_{k\times k}$}} \\ a_{12} & a_{22} & \dots & a_{k2} & & & & \\ \vdots & \vdots & \ddots & \vdots & & & & \\ a_{1k} & a_{2k} & \dots & a_{kk} & & & & \end{array}\right).$$

В принятых обозначениях имеем

$$G(x,y) = G(v) = \langle Qv, v\rangle \oplus \langle L, v\rangle \oplus \varepsilon.$$

Пусть ранг матрицы A, совпадающий с рангом матрицы Q, равен r. Тогда, очевидно, ранг матрицы B будет равен $2r$. В этом случае согласно утверждению 2 справедливо

$$\mathrm{wt}(G) \in \{2^{2k-1}, 2^{2k-1}(1-2^{-r}), 2^{2k-1}(1+2^{-r})\}.$$

Этап II. Покажем, что все веса, фигурирующие в утверждении 2, достижимы. Для получения данного спектра весов следует рассмотреть все возможные значения, которые может принимать ранг матрицы A. Данный ранг ограничен сверху числом $k-1$ в силу леммы 1.

Случай $r = 0$.

Вес 2^{2k}. Например, $L^f = L^g = I_k$, $b_f = b_g = (1,1,0,0,\ldots,0) \in \mathbb{Z}_2^k$, $\varepsilon_f = 0$, $\varepsilon_g = 1$. Тогда $L = \mathbf{0}_{2k}$ и $G \equiv 1$, т. е. $\mathrm{wt}(G) = 2^{2k}$.

Вес 2^{2k-1}. Пусть $b_f \neq b_g$, например, $b_f = (1,1,0,0,\ldots,0) \in \mathbb{Z}_2^k$, $b_g = \mathbf{0}_k$, $L^f = L^g = I_k$, $\varepsilon = 0$, тогда $G(v) = \langle L, v\rangle$ — линейная функция, причём $L \neq \mathbf{0}_{2k}$. По лемме 2 вес Хэмминга такой линейной функции равен 2^{2k-1}.

Вес 0. Данный вес достигается при $L^f = L^g$, $b_f = b_g$, $\varepsilon_f = \varepsilon_g$.

Случай $r = 1, 2, \ldots, k-2$.

Пусть $b_f = b_g = \mathbf{0}_k$, тогда $L = \mathbf{0}_{2k}$, т. е. у булевой функции G нулевая линейная часть, а матрица A имеет ненулевой ранг. Согласно теореме Диксона квадратичная часть булевой функции G может быть приведена к виду $q(z) = \bigoplus\limits_{i=1}^{r} z_{2i-1}z_{2i} \oplus \varepsilon$, где r — ранг матрицы Q, совпадающий с рангом матрицы A. Используя лемму 3, заключаем, что вес Хэмминга функции G равен $2^{2k-1}(1-(-1)^{\varepsilon}2^{-r})$. Осталось надлежащим образом подобрать ε, а в качестве примера пары соответствующих автоморфизмов L_f и L_g можно взять линейные отображения с матрицами I_k и L^g соответственно, где строки матрицы L^g имеют вид

$$(L^g)_i = \begin{cases} e_{i+1} & \text{при } i \in \{1,2,\ldots,r\}, \\ e_1 & \text{при } i = r+1, \\ e_i & \text{при } i \in \{r+2, r+3, \ldots, k\}, \end{cases}$$

где $i = 1, 2, \ldots, k$.

Вес $2^{2k-1}(1-2^{-r})$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 0$.

Вес $2^{2k-1}(1+2^{-r})$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 1$.

Случай $r = k - 1$.

Повторяя рассуждения из предыдущего случая, взяв те же самые L_f, b_f, b_g и выбрав в качестве автоморфизма L_g линейное отображение с матрицей

$$(L^g)_i = \begin{cases} e_{i+1} & \text{при } i \in \{1, 2, \ldots, k-1\}, \\ e_1 & \text{при } i = k, \end{cases}$$

где $i = 1, 2, \ldots, k$, получим функцию G, для которой справедливо

$$\mathrm{wt}(G) = 2^{2k-1}(1 - (-1)^{\varepsilon} 2^{-(k-1)}).$$

Вес $2^{2k-1}(1 - 2^{-(k-1)})$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 0$.
Вес $2^{2k-1}(1 + 2^{-(k-1)})$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 1$.

Получаем, что все возможные значения $\mathrm{wt}(G)$ достижимы. С учётом (1) имеем

$$\mathrm{dist}(f, g) \in \{2^{2k-1}, 2^{2k-1}(1 \pm 2^{-r}), r = 0, 1, \ldots, k-1\},$$

и все приведённые расстояния достижимы.

В силу того, что $k = n/2$, получаем требуемое. Утверждение 5 доказано.

Утверждение 6. *Пусть $f, g \in SB^-_{\mathcal{M}}(n)$, где $n \geqslant 4$. Тогда*

$$\mathrm{dist}(f, g) \in \{2^{n-1}, 2^{n-1}(1 \pm 2^{-r}), r = 0, 1, \ldots, n/2 - 1\}$$

и все приведённые расстояния достижимы.

Доказательство. Положим $n = 2k$, где $k \geqslant 2$ — натуральное число. Рассмотрим произвольную пару анти-самодуальных бент-функций f, g, удовлетворяющую условиям утверждения. Согласно утверждению 1

$$f(x, y) = \langle x, L_f(y) \oplus L_f(b_f) \rangle \oplus \langle b_f, y \rangle \oplus \varepsilon_f,$$
$$g(x, y) = \langle x, L_g(y) \oplus L_g(b_g) \rangle \oplus \langle b_g, y \rangle \oplus \varepsilon_g,$$

где $b_f, b_g \in \mathbb{Z}_2^k$, $\varepsilon_f, \varepsilon_g \in \mathbb{Z}_2$, $L_f, L_g \colon \mathbb{Z}_2^k \to \mathbb{Z}_2^k$ — линейные автоморфизмы такие, что

$$\langle x, L_f(y) \rangle = \langle L_f^{-1}(x), y \rangle, \quad \langle x, L_g(y) \rangle = \langle L_g^{-1}(x), y \rangle$$

для всех $x, y \in \mathbb{Z}_2^k$, а векторы $L_f(b_f)$ и $L_g(b_g)$ имеют нечётные веса Хэмминга.

Дальнейшее доказательство будет проводится по той же схеме, что и доказательство утверждения 5.

Этап I. Повторяя рассуждения, приведённые на первом этапе доказательства утверждения 5, можно показать, что

$$f(x,y) \oplus g(x,y) = G(x,y) = G(v) = \langle Qv, v\rangle \oplus \langle L, v\rangle \oplus \varepsilon,$$

где обозначения v, Q, L, ε, а также A, B, L^f, L^g имеют тот же смысл, что и ранее.

Пусть, как и прежде, ранг матрицы A, совпадающий с рангом матрицы Q, равен r. Тогда ранг матрицы B будет равен $2r$. В этом случае согласно утверждению 2 справедливо

$$\mathrm{wt}(G) \in \{2^{2k-1}, 2^{2k-1}(1-2^{-r}), 2^{2k-1}(1+2^{-r})\}.$$

Этап II. Покажем, что все веса, фигурирующие в утверждении 2, достижимы. Для получения данного спектра весов следует рассмотреть все возможные значения, которые может принимать ранг матрицы A. Данный ранг ограничен сверху числом $k-1$ в силу леммы 1.

Случай $r = 0$.

Вес 2^{2k}. Например, $L^f = L^g = I_k$, $b_f = b_g = (1,0,0,\ldots,0) \in \mathbb{Z}_2^k$, $\varepsilon_f = 0$, $\varepsilon_g = 1$. Тогда $L = \mathbf{0}_{2k}$ и $G \equiv 1$, т. е. $\mathrm{wt}(G) = 2^{2k}$.

Вес 2^{2k-1}. Пусть $b_f \neq b_g$, например, $b_f = (1,0,0,\ldots,0) \in \mathbb{Z}_2^k$, $b_g = \mathbf{0}_k$, $L^f = L^g = I_k$, $\varepsilon = 0$. Тогда $G(v) = \langle L, v\rangle$ — линейная функция, причём $L \neq \mathbf{0}_{2k}$. По лемме 2 вес Хэмминга такой линейной функции равен 2^{2k-1}.

Вес 0 достигается при $L^f = L^g$, $b_f = b_g$, $\varepsilon_f = \varepsilon_g$.

Случай $r = 1, 2, \ldots, k-2$.

Пусть $b_f = b_g = e_k$. Тогда $L = \mathbf{0}_{2k}$, т. е. у булевой функции G нулевая линейная часть, а матрица A имеет ненулевой ранг. Ранее было показано, что в этом случае $\mathrm{wt}(G) = 2^{2k-1}(1-(-1)^{\varepsilon}2^{-r})$. В качестве примера пары соответствующих автоморфизмов L_f и L_g можно взять линейные отображения с матрицами I_k и L^g соответственно, где строки матрицы L^g имеют вид

$$(L^g)_i = \begin{cases} e_{i+1} & \text{при } i \in \{1,2,\ldots,r\}, \\ e_1 & \text{при } i = r+1, \\ e_i & \text{при } i \in \{r+2, r+3, \ldots, k\}, \end{cases}$$

где $i = 1, 2, \ldots, k$.

Вес $2^{2k-1}(1-2^{-r})$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 0$.

Вес $2^{2k-1}(1+2^{-r})$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 1$.

Случай $r = k - 1$.

Пусть $L^f = I_k$, $b_f = b_g = e_2$. Тогда $L = (1, 1, 0, 0, \ldots, 0) \in \mathbb{Z}_2^{2k}$. Выберем в качестве автоморфизма L_g линейное отображение с матрицей

$$(L^g)_i = \begin{cases} e_{i+1} & \text{при } i \in \{1, 2, \ldots, k-1\}, \\ e_1 & \text{при } i = k, \end{cases}$$

где $i = 1, 2, \ldots, k$. Используя лемму 4 и теорему Диксона, заключаем, что вес Хэмминга функции G равен $\mathrm{wt}(G) = 2^{2k-1}(1 - (-1)^{\varepsilon_1} 2^{-(k-1)})$, где $\varepsilon_1 = \varepsilon \oplus \bigoplus\limits_{i=1}^{k-1} l_{2i-1} l_{2i} = \varepsilon \oplus 1$ (см. [3, гл. 15]).

Вес $2^{2k-1}(1 - 2^{-(k-1)})$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 1$.

Вес $2^{2k-1}(1 + 2^{-(k-1)})$. Возьмём L_f, L_g, b_f, b_g, указанные выше, $\varepsilon = 0$.

Отметим, что в случае нечётного k можно обойтись без использования леммы 4, взяв $b_f = b_g = (1, 1, \ldots, 1) \in \mathbb{Z}_2^k$, для которых $L = \mathbf{0}_{2k}$.

Получаем, что все возможные значения $\mathrm{wt}(G)$ достижимы. С учётом (1) имеем

$$\mathrm{dist}(f, g) \in \{2^{2k-1}, 2^{2k-1}(1 \pm 2^{-r}), r = 0, 1, \ldots, k-1\},$$

и все приведённые расстояния достижимы.

В силу того, что $k = n/2$, получаем требуемое. Утверждение 6 доказано.

Теорема 1. *Пусть $f, g \in SB^+_{\mathcal{M}}(n) \cup SB^-_{\mathcal{M}}(n)$, где $n \geqslant 4$. Тогда*

$$\mathrm{dist}(f, g) \in \{2^{n-1}, 2^{n-1}(1 \pm 2^{-r}), r = 0, 1, \ldots, n/2 - 1\}.$$

При этом если $f, g \in SB^+_{\mathcal{M}}(n)$ или $f, g \in SB^-_{\mathcal{M}}(n)$, то все приведённые расстояния достижимы. Если же $f \in SB^+_{\mathcal{M}}(n)$, а $g \in SB^-_{\mathcal{M}}(n)$, то $\mathrm{dist}(f, g) = 2^{n-1}$.

Доказательство. Крайний случай напрямую следует из утверждения 4. Случай, когда функции f и g самодуальны (анти-самодуальны), следует из утверждения 5 (6). Теорема 1 доказана.

Следствие 1. *Пусть f, g — различные бент-функции от $n \geqslant 4$ переменных. Если $f, g \in SB^+_{\mathcal{M}}(n) \cup SB^-_{\mathcal{M}}(n)$, то*

$$\mathrm{dist}(f, g) \geqslant 2^{n-2}$$

и приведённая оценка точна.

Доказательство. Из теоремы 1 следует, что минимальное из расстояний есть $2^{n-1}\bigl(1-\frac{1}{2^1}\bigr)=2^{n-2}$. Следствие 1 доказано.

Стоит отметить, что из теории булевых функций известно, что для каждой булевой функции $F\in\mathcal{F}_m$ такой, что $\mathrm{wt}(F)>0$, справедливо $\mathrm{wt}(F)\geqslant 2^{m-\deg F}$ (см. [2]). В силу этого факта следствие 1 можно доказать, заметив лишь, что $\deg(f\oplus g)\leqslant 2$ и $f\neq g$ для рассматриваемых функций f и g, а также непосредственно указав соответствующую пару функций, находящихся на данном расстоянии друг от друга.

Осталось нерассмотренным значение $n=2$. В этом случае согласно утверждению 1 только две бент-функции из класса Мэйорана — МакФарланда самодуальны:

$$f_1(x_1,x_2)=x_1x_2 \quad \text{и} \quad g_1(x_1,x_2)=x_1x_2\oplus 1,$$

а функции

$$f_2(x_1,x_2)=x_1x_2\oplus x_1\oplus x_2 \quad \text{и} \quad g_2(x_1,x_2)=x_1x_2\oplus x_1\oplus x_2\oplus 1$$

анти-самодуальны. Очевидно, что

$$\mathrm{dist}(f_1,g_1)=\mathrm{dist}(f_2,g_2)=4=2^n, \quad \mathrm{dist}(f_1,g_2)=\mathrm{dist}(f_2,g_1)=2=2^{n-1}.$$

ЛИТЕРАТУРА

1. **Коломеец Н. А., Павлов А. В.** Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикл. дискрет. математика. 2009. № 4. С. 5–20.
2. **Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В.** Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
3. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
4. **Облаухов А. К.** О метрическом дополнении подпространств булева куба // Дискрет. анализ и исслед. операций. 2016. Т. 23, № 3. С. 93–106.
5. **Потапов В. Н.** Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Пробл. передачи информации. 2012. Т. 48, № 1. С. 54–63.
6. **Токарева Н. Н.** О разложении дуальной бент-функции в сумму двух бент-функций // Прикл. дискрет. математика. 2014. № 4. С. 59–61.
7. **Budaghyan L., Carlet C., Helleseth T., Kholosha A., Mesnager S.** Further results on Niho bent functions // IEEE Trans. Inf. Theory. 2012. Vol. 58, No. 11. P. 6979–6985.

8. **Carlet C.** Boolean functions for cryptography and error-correcting codes // Boolean models and methods in mathematics, computer science, and engineering. New York: Cambridge Univ. Press, 2010. P. 257–397. (Encycl. Math. Appl.; Vol. 134).
9. **Carlet C., Danielson L. E., Parker M. G., Solé P.** Self-dual bent functions // Int. J. Inform. Coding Theory. 2010. Vol. 1, No. 4. P. 384–399.
10. **Cusick T. W., Stănică P.** Cryptographic Boolean functions and applications. London: Acad. Press, 2017. 288 p.
11. **Feulner T., Sok L., Solé P., Wassermann A.** Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. Vol. 68, No. 1. P. 395–406.
12. **Hou X.-D.** On the coefficients of binary bent functions // Proc. Amer. Math. Soc. 2000. Vol. 128, No. 4. P. 987–996.
13. **Hou X.-D.** Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. Vol. 63, No. 2. P. 183–198.
14. **Kolomeec N. A.** The graph of minimal distances of bent functions and its properties // Des. Codes Cryptogr. 2017. P. 1–16. DOI 10.1007/s10623-016-0306-4.
15. **Kolomeec N. A., Pavlov A. V.** Bent functions on the minimal distance // Proc. IEEE Region 8th Int. Conf. Computational Technologies in Electrical and Electronics Engineering (SIBIRCON 2010) (Irkutsk, Russia, July 11–15, 2010) Piscataway: IEEE, 2010. P. 145–149.
16. **Langevin P., Leander G.** Monomial bent functions and Stickelberger's theorem // Finite Fields Appl. 2008. Vol. 14, No. 3. P. 727–742.
17. **McFarland R. L.** A family of difference sets in non-cyclic groups // J. Comb. Theory, Ser. A. 1973. Vol. 15, No. 1. P. 1–10.
18. **Mesnager S.** Several new infinite families of bent functions and their duals // IEEE Trans. Inf. Theory. 2014. Vol. 60, No. 7. P. 4397–4407.
19. **Rothaus O.** On "bent" functions // J. Comb. Theory. Ser. A. 1976. Vol. 20, No. 3. P. 300–305.
20. **Tokareva N. N.** Duality between bent functions and affine functions // Discrete Math. 2012. Vol. 312, No. 3. P. 666–670.
21. **Tokareva N. N.** Bent functions: Results and applications to cryptography. London: Acad. Press, 2015. 220 p.
22. **Xu B.** Dual bent functions on finite groups and C-algebras // J. Pure Appl. Algebra. 2016. Vol. 220, No. 3. P. 1055–1073.

Куценко Александр Владимирович

Статья поступила
17 октября 2016 г.

Исправленный вариант —
27 июля 2017 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
January–March 2018. Volume 25, No. 1. P. 98–119

UDC 519.7 DOI: 10.17377/daio.2018.25.557

THE HAMMING DISTANCE SPECTRUM BETWEEN SELF-DUAL MAIORANA–MCFARLAND BENT FUNCTIONS

A. V. Kutsenko

Novosibirsk State University,
2 Pirogov St., 630090 Novosibirsk, Russia
E-mail: AlexandrKutsenko@bk.ru

Abstract. A bent function is *self-dual* if it is equal to its dual function. We study the metric properties of the self-dual bent functions constructed on using available constructions. We find the full Hamming distance spectrum between self-dual Maiorana–McFarland bent functions. Basing on this, we find the minimal Hamming distance between the functions under study. Bibliogr. 22.

Keywords: Hamming distance, self-dual bent function, Maiorana–McFarland bent function.

REFERENCES

1. **N. A. Kolomeec** and **A. V. Pavlov,** Properties of bent functions with minimal distance, *Prikl. Diskretn. Mat.,* No. 4, 5–20, 2009.
2. **O. A. Logachev, A. A. Sal'nikov, S. V. Smyshlyaev,** and **V. V. Yashchenko,** *Bulevy funktsii v teorii kodirovaniya i kriptologii* (Boolean functions in coding theory and cryptology), MTsNMO, Moscow, 2012.
3. **F. J. MacWilliams** and **N. J. A. Sloane,** *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977 (North-Holland Math. Libr., Vol. 16). Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki,* Svyaz', Moscow, 1979.
4. **A. K. Oblaukhov,** Metric complements to subspaces in the Boolean cube, *Diskretn. Anal. Issled. Oper.,* **23**, No. 3, 93–106, 2016. Translated in *J. Appl. Ind. Math.,* **10**, No. 3, 397–403, 2016.
5. **V. N. Potapov,** Cardinality spectra of components of correlation immune functions, bent functions, perfect colorings, and codes, *Probl. Peredachi Inf.,* **48**, No. 1, 54–63, 2012. Translated in *Probl. Inf. Transm.,* **48**, No. 1, 47–55, 2012.
6. **N. N. Tokareva,** On decomposition of a dual bent function into sum of two bent functions, *Prikl. Discretn. Mat.,* No. 4, 59–61, 2014.

7. **L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha,** and **S. Mesnager,** Further results on Niho bent functions, *IEEE Trans. Inf. Theory,* **58**, No. 11, 6979–6985, 2012.
8. **C. Carlet,** Boolean functions for cryptography and error-correcting codes, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering,* pp. 257–397, Cambridge Univ. Press, New York, 2010 (Encycl. Math. Its Appl., Vol. 134).
9. **C. Carlet, L. E. Danielson, M. G. Parker,** and **P. Solé,** Self-dual bent functions, *Int. J. Inf. Coding Theory.* **1**, No. 4, 384–399, 2010.
10. **T. W. Cusick** and **P. Stănică,** *Cryptographic Boolean Functions and Applications,* Acad. Press, London, 2017.
11. **T. Feulner, L. Sok, P. Solé,** and **A. Wassermann,** Towards the classification of self-dual bent functions in eight variables, *Des. Codes Cryptogr.,* **68**, No. 1, 395–406, 2013.
12. **X.-D. Hou,** On the coefficients of binary bent functions, *Proc. Amer. Math. Soc.,* **128**, No. 4, 987–996, 2000.
13. **X.-D. Hou,** Classification of self dual quadratic bent functions, *Des. Codes Cryptogr.,* **63**, No. 2, 183–198, 2012.
14. **N. A. Kolomeec,** The graph of minimal distances of bent functions and its properties, *Des. Codes Cryptogr.,* 1–16, 2017. DOI 10.1007/s10623-016-0306-4
15. **N. A. Kolomeec** and **A. V. Pavlov,** Bent functions on the minimal distance, *Proc. IEEE Region 8 Int. Conf. Comput. Technol. Electr. Electron. Eng., Irkutsk, Russia, July 11–15, 2010,* pp. 145–149, IEEE, Piscataway, 2010.
16. **P. Langevin** and **G. Leander,** Monomial bent functions and Stickelberger's theorem, *Finite Fields Appl.,* **14**, No. 3, 727–742, 2008.
17. **R. L. McFarland,** A family of difference sets in non-cyclic groups, *J. Comb. Theory, Ser. A,* **15**, No. 1, 1–10, 1973.
18. **S. Mesnager,** Several new infinite families of bent functions and their duals, *IEEE Trans. Inf. Theory,* **60**, No. 7, 4397–4407, 2014.
19. **O. Rothaus,** On "bent" functions, *J. Comb. Theory. Ser. A,* **20**, No. 3, 300–305, 1976.
20. **N. N. Tokareva,** Duality between bent functions and affine functions, *Discrete Math.,* **312**, No. 3, 666–670, 2012.
21. **N. N. Tokareva,** *Bent Functions: Results and Applications to Cryptography,* Acad. Press, London, 2015.
22. **B. Xu,** Dual bent functions on finite groups and C-algebras, *J. Pure Appl. Algebra,* **220**, No. 3, 1055–1073, 2016.

Alexander V. Kutsenko

Received
17 October 2016
Revised
27 July 2017