

УДК 519.7

ПЕРЕЧИСЛЕНИЕ БЕНТ-ФУНКЦИЙ НА МИНИМАЛЬНОМ РАССТОЯНИИ ОТ КВАДРАТИЧНОЙ БЕНТ-ФУНКЦИИ *)

Н. А. Коломеец

Аннотация. Исследуется построение бент-функций на минимальном расстоянии от квадратичной бент-функции, описываются все такие бент-функции от $2k$ переменных и показывается, что их число равно $2^k(2^1 + 1) \dots (2^k + 1)$. Находится нижняя оценка числа бент-функций на минимальном расстоянии от бент-функции из класса Мэйорана — МакФарланда.

Ключевые слова: бент-функция, минимальное расстояние, квадратичная бент-функция.

Введение

Бент-функции — булевы функции от чётного числа переменных, максимально удалённые от класса аффинных функций. Впервые бент-функции рассмотрены Ротхаусом [9]. Бент-функции имеют большое число приложений в криптографии, теории кодирования и теории информации. Тем не менее, для них до сих пор существует много нерешённых проблем. Наиболее важная проблема — описание всех бент-функций. В частности, нахождение конструкций бент-функций.

В работе рассматривается построение бент-функций на минимальном расстоянии от квадратичной бент-функции. В [1] показано, что две бент-функции от $2k$ переменных находятся на расстоянии 2^k (минимально возможное расстояние между двумя различными бент-функциями) тогда и только тогда, когда они отличаются на аффинном подпространстве размерности k и аффинны на нём. В данной работе описываются все бент-функции на минимальном расстоянии от квадратичной бент-функции (теорема 1), а также показывается, что число таких бент-функций от $2k$ переменных равно $2^k(2^1 + 1) \dots (2^k + 1)$ (теорема 2). Извест-

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 11-01-00997) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт 02.740.11.0362).

но, что все квадратичные бент-функции аффинно эквивалентны функции $x_1x_{k+1} \oplus x_2x_{k+2} \oplus \dots \oplus x_kx_{2k}$, которая принадлежит классу Мэйорана — МакФарланда. Поэтому далее рассматриваем более общую задачу нахождения нижней оценки числа бент-функций на минимальном расстоянии от произвольной бент-функции из класса Мэйорана — МакФарланда (теорема 3). В заключении приводим некоторые факты и гипотезу об оценке числа бент-функций на расстоянии 2^k от произвольной бент-функции.

1. Определения

Через \mathbb{Z}_2^n обозначим n -мерное векторное пространство над \mathbb{Z}_2 , через \oplus — сложение по модулю 2. Под *расстоянием* между двумя булевыми функциями будем понимать расстояние Хэмминга (число векторов, на которых функции различаются). Степень алгебраической нормальной формы булевой функции называется *алгебраической степенью* функции. Булева функция называется *аффинной*, если её алгебраическая степень не превосходит 1, и *квадратичной*, если её алгебраическая степень равна 2. Множество $L \subseteq \mathbb{Z}_2^n$ называется *аффинным подпространством*, если $L = a \oplus U$, где a — вектор из \mathbb{Z}_2^n и U — линейное подпространство в \mathbb{Z}_2^n . Для векторов u и v через $\langle u, v \rangle$ обозначим их скалярное произведение по модулю 2. Булева функция f от n переменных называется *аффинной на множестве* $D \subseteq \mathbb{Z}_2^n$, если существуют $a \in \mathbb{Z}_2^n$, $c \in \mathbb{Z}_2$ такие, что для всех $x \in D$ выполняется $f(x) = \langle a, x \rangle \oplus c$. Напомним, что

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

называется *преобразованием Уолша — Адамара* для функции f , а числа $W_f(v)$ называются *коэффициентами Уолша — Адамара*. Булева функция f от $2k$ переменных называется *бент-функцией*, если все её коэффициенты Уолша — Адамара равны $\pm 2^k$. Множество всех бент-функций от $2k$ переменных обозначается через \mathfrak{B}_{2k} . Обзор работ и результатов по бент-функциям можно найти, например, в [4].

Булевы функции f и g от n переменных называются *аффинно эквивалентными*, если существует невырожденная матрица A размера $n \times n$, вектор b длины n и аффинная функция l от n переменных такие, что $g(x) = f(Ax \oplus b) \oplus l(x)$.

Пусть $D \subseteq \mathbb{Z}_2^n$, через Ind_D обозначим индикатор множества D , т. е. булеву функцию от n переменных, которая принимает значение 1 только на элементах множества D . Через $a^{(i)}$ обозначим i -й столбец матрицы A , а через a_{ij} — элемент этой матрицы.

Минимальное возможное расстояние между двумя различными бент-функциями от $2k$ переменных равно 2^k . Обозначим это расстояние через d_k . В [1] доказано

Утверждение 1. Пусть $f \in \mathfrak{B}_{2k}$, $L \subseteq \mathbb{Z}_2^{2k}$. Тогда $g(x) = f(x) \oplus \text{Ind}_L(x)$ — бент-функция на расстоянии d_k от бент-функции f тогда и только тогда, когда множество L является аффинным подпространством размерности k и функция f аффинна на L .

Утверждение 1 в одну сторону (конструкция бент-функции с помощью подпространства размерности k) можно найти в [2, 6].

В нашей работе для построения бент-функций на расстоянии d_k используется это утверждение, т.е. задача сводится к поиску аффинных подпространств размерности k в \mathbb{Z}_2^{2k} , на которых заданная бент-функция аффинна.

2. Бент-функции на минимальном расстоянии от квадратичной бент-функции

В следующих разделах построим все бент-функции на расстоянии d_k от бент-функции $x_1x_{k+1} \oplus x_2x_{k+2} \oplus \dots \oplus x_kx_{2k}$ и подсчитаем их число.

Утверждение 2 [7]. Любая квадратичная бент-функция от $2k$ переменных аффинно эквивалентна бент-функции

$$f_0^{2k}(x) = x_1x_{k+1} \oplus x_2x_{k+2} \oplus \dots \oplus x_kx_{2k}.$$

Заметим, что аффинно эквивалентные бент-функции имеют одно и то же число бент-функций на любом заданном расстоянии. Поэтому, используя утверждение 2, достаточно подсчитать число бент-функций на расстоянии d_k от бент-функции f_0^{2k} , тогда от остальных квадратичных бент-функций число бент-функций на расстоянии d_k будет таким же.

Для рассмотрения бент-функций на расстоянии d_k от функции f_0^{2k} сделаем следующее: приведём некоторые утверждения об аффинности функций в общем и функции f_0^{2k} в частности на некотором подпространстве (разд. 3), рассмотрим удобные базисы для представления подпространств (разд. 4), опишем аффинные подпространства размерности k , на которых аффинна функция f_0^{2k} (разд. 5), подсчитаем число таких подпространств (разд. 6) и приведём некоторые примеры для малых размерностей (разд. 7).

3. Аффинность булевой функции на подпространстве

Каждому линейному подпространству L можно поставить в соответствие некоторую базисную матрицу. Будем считать, что базисом пространства являются столбцы этой матрицы. Следующее утверждение позволяет определить, аффинна ли булева функция на некотором подпространстве.

Утверждение 3. Пусть g — произвольная булева функция от n переменных и B — базисная матрица размера $n \times k$ для некоторого линейного подпространства L размерности k в \mathbb{Z}_2^n . Тогда g аффинна на подпространстве L тогда и только тогда, когда $g'(u) = g(Bu)$ от k переменных аффинна.

ДОКАЗАТЕЛЬСТВО УТВЕРЖДЕНИЯ 3 тривиально.

Следующая лемма содержит критерий аффинности функции f_0^{2k} на подпространстве с некоторой базисной матрицей B .

Лемма 1. Пусть B — любая базисная матрица размера $2k \times k$ линейного подпространства L размерности k в \mathbb{Z}_2^{2k} , а матрицы $A = (a_{ij})$ и $Y = (y_{ij})$ образованы первыми k и последними k строками матрицы B соответственно. Тогда функция f_0^{2k} аффинна на подпространстве L тогда и только тогда, когда выполняются соотношения

$$\langle a^{(i)}, y^{(j)} \rangle \oplus \langle a^{(j)}, y^{(i)} \rangle = 0, \quad i, j \in \{1, \dots, k\}, i \neq j,$$

где $a^{(i)}$ и $y^{(i)}$ — i -е столбцы матриц A и Y .

ДОКАЗАТЕЛЬСТВО. По утверждению 3 функция f_0^{2k} аффинна на подпространстве L тогда и только тогда, когда функция $f'(u) = f_0^{2k}(Bu)$ от k переменных аффинна.

Функция f' имеет следующую алгебраическую нормальную форму:

$$f'(u) = \left(\bigoplus_{j=1}^k a_{1j} u_j \right) \left(\bigoplus_{j=1}^k y_{1j} u_j \right) \oplus \dots \oplus \left(\bigoplus_{j=1}^k a_{kj} u_j \right) \left(\bigoplus_{j=1}^k y_{kj} u_j \right).$$

Степень функции f' , очевидно, будет не больше 2, поэтому для её аффинности достаточно и необходимо, чтобы все коэффициенты при $u_i u_j$ для $i \neq j$ были равны 0, т. е.

$$\bigoplus_{t=1}^k a_{ti} \cdot y_{tj} \oplus \bigoplus_{t=1}^k a_{tj} \cdot y_{ti} = 0.$$

Лемма 1 доказана.

Утверждение 4. Пусть g — произвольная квадратичная функция, аффинная на некотором аффинном подпространстве $u \oplus L$. Тогда g также аффинна на любом смежном классе подпространства L .

ДОКАЗАТЕЛЬСТВО. Заметим, что g аффинна на $a \oplus L$ тогда и только тогда, когда $g(x \oplus a)$ аффинна на L для любого вектора a . Так как g квадратичная, алгебраическая нормальная форма $g(x \oplus a)$ отличается от алгебраической нормальной формы g только аффинной частью. Поэтому g аффинна на L тогда и только тогда, когда $g(x \oplus a)$ аффинна на L . При этом g аффинна на $u \oplus L$ по условию. Следовательно, g аффинна на $a \oplus L$ для любого вектора a . Утверждение 4 доказано.

4. Представление подпространств

Будем описывать линейные подпространства с помощью базисных матриц Гаусса — Жордана (или сокращенно GJB-матриц). Отметим, что в наших обозначениях базисные векторы являются столбцами базисной матрицы.

Определение 1. Пусть G — матрица с k столбцами, образованная ненулевыми векторами $u^{(1)}, \dots, u^{(k)}$. Пусть $\ell(u^{(i)}) = \min \{j \mid u_j^{(i)} \neq 0\}$. Матрица G является GJB-матрицей, если выполняются следующие условия:

- (i) если $i_1 < i_2$, то $\ell(u^{(i_1)}) < \ell(u^{(i_2)})$;
- (ii) если $i_1 \neq i_2$, то $u_{\ell(u^{(i_2)})}^{(i_1)} = 0$.

В этом случае через $\ell(G)$ обозначим множество $\{\ell(u^{(1)}), \dots, \ell(u^{(k)})\}$. Все строки матрицы G с номерами из множества $\ell(G)$ будем называть *ведущими строками*, остальные — *неведущими*. Через L_G обозначим подпространство с базисом $u^{(1)}, \dots, u^{(k)}$. Заметим, что столбцы матрицы G действительно являются базисными векторами пространства L_G , а матрицу G^T называют также *редуцированной ступенчатой матрицей*.

ПРИМЕР 1. Матрица

$$G = \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \right)$$

является GJB-матрицей для подпространства размерности 3 в \mathbb{Z}_2^6 с $\ell(G) = \{1, 3, 5\}$.

Утверждение 5. Любое линейное подпространство имеет единственную GJB-матрицу.

Доказательство. GJB-матрицу G для любого линейного подпространства можно определить следующим образом: любой i -й столбец матрицы $u^{(i)}$ — вектор из пространства L_G , который имеет больше всего младших нулей, а также $u_{\ell(u_j)}^{(i)} = 0$ для любого $j > i$. Отсюда следует, что у любого подпространства L существует GJB-матрица. Докажем единственность такой матрицы. Предположим, что существует два вектора $u^{(i)}$ и $u'^{(i)}$ для некоторого i , удовлетворяющие приведённому выше свойству. Тогда вектор $u^{(i)} \oplus u'^{(i)}$ имеет как минимум на один младший нуль больше, а совпадающие координаты векторов $u^{(i)}$ и $u'^{(i)}$ у их суммы будут нулевыми. Утверждение 5 доказано.

Таким образом, всевозможные GJB-матрицы размера $n \times k$ взаимно однозначно соответствуют всевозможным линейным подпространствам размерности k в \mathbb{Z}_2^n .

5. Построение бент-функций на минимальном расстоянии от квадратичной бент-функции

Введём определение допустимой GJB-матрицы. Пусть GJB-матрица G для подпространства размерности k в \mathbb{Z}_2^{2k} имеет вид $\left(\begin{array}{c|c} A & 0 \\ \hline Z & Y \end{array} \right)$, где матрица A размера $k \times t$, а Y — размера $k \times (k - t)$. Поскольку G — GJB-матрица, должны выполняться следующие два условия: (i) A, Y — GJB-матрицы; (ii) все строки матрицы Z с номерами из $\ell(Y)$ нулевые.

Удалим из матриц Z и A все строки с номерами из $\ell(Y)$ и обозначим получившиеся матрицы через Z' и A' соответственно. Наложим дополнительные условия на элементы Z' : (iii) $L_Y = L_A^\perp$; (iv) элементы матрицы Z' являются решениями системы уравнений

$$\begin{pmatrix} a'^{(2)T} & a'^{(1)T} & 0 & 0 & \dots & 0 \\ \dots & & & & & \\ a'^{(t)T} & 0 & 0 & \dots & 0 & a'^{(1)T} \\ \dots & & & & & \\ 0 & a'^{(3)T} & a'^{(2)T} & 0 & \dots & 0 \\ \dots & & & & & \\ 0 & a'^{(t)T} & 0 & \dots & 0 & a'^{(2)T} \\ \dots & & & & & \\ 0 & 0 & 0 & \dots & a'^{(t)T} & a'^{(t-1)T} \end{pmatrix} \cdot \begin{pmatrix} z'^{(1)} \\ z'^{(2)} \\ \vdots \\ z'^{(t)} \end{pmatrix} = 0, \quad (1)$$

где матрица M системы размера $(t(t-1)/2) \times t^2$ (если $t \leq 1$, то на элементы Z' нет ограничений).

Если верны вышеперечисленные условия, то матрицу G назовём *допустимой* порядка t .

Следующая теорема описывает все аффинные подпространства, на которых аффинна квадратичная бент-функция.

Теорема 1. Пусть L — аффинное подпространство размерности k в \mathbb{Z}_2^{2k} . Бент-функция f_0^{2k} аффинна на L тогда и только тогда, когда L является линейным подпространством с допустимой GJB-матрицей или смежным классом такого подпространства.

ДОКАЗАТЕЛЬСТВО. Используя утверждение 4, можно без ограничения общности считать, что L — линейное подпространство.

Пусть G — GJB-матрица для подпространства L . Обозначим верхнюю половину матрицы G через D , а нижнюю — через V . Пусть $d^{(i)}$ и $v^{(i)}$ — i -е столбцы матриц D и V соответственно. По лемме 1 функция f_0^{2k} аффинна на подпространстве L тогда и только тогда, когда

$$\langle d^{(i)}, v^{(j)} \rangle \oplus \langle d^{(j)}, v^{(i)} \rangle = 0, \quad i, j \in \{1, \dots, k\}, i \neq j. \quad (2)$$

Рассмотрим эти соотношения как систему уравнений относительно переменных $v^{(i)} \in \mathbb{Z}_2^k$ и коэффициентов $d^{(i)} \in \mathbb{Z}_2^k$. Очевидно, что любую GJB-матрицу G можно представить в виде $\left(\begin{array}{c|c} A & 0 \\ \hline Z & Y \end{array} \right)$, где матрицы A и Y — GJB-матрицы размера $k \times t$ и $k \times (k-t)$ соответственно для некоторого $t \in \{0, \dots, k\}$. Тогда для столбцов матрицы Y система уравнений (2) имеет вид

$$\langle a^{(i)}, y^{(j)} \rangle \oplus \langle 0, z^{(i)} \rangle = 0, \quad i \in \{1, \dots, t\}, j \in \{1, \dots, k-t\},$$

или просто

$$\langle a^{(i)}, y^{(j)} \rangle = 0, \quad i \in \{1, \dots, t\}, j \in \{1, \dots, k-t\}. \quad (3)$$

Уравнения (2) для столбцов матрицы Z можно разделить на две части:

$$\langle a^{(i)}, z^{(j)} \rangle \oplus \langle a^{(j)}, z^{(i)} \rangle = 0, \quad i, j \in \{1, \dots, t\}, i \neq j, \quad (4)$$

$$\langle 0, z^{(j)} \rangle \oplus \langle a^{(j)}, y^{(i-t)} \rangle = 0, \quad i \in \{t+1, \dots, k\}, j \in \{1, \dots, t\}. \quad (5)$$

Однако из уравнений (3) следует, что $\langle a^{(j)}, y^{(i-t)} \rangle = 0$. Поэтому уравнения (2) превращаются в уравнения (3) относительно $y^{(i)}$ и (4) относительно $z^{(i)}$.

Поскольку G — GJB-матрица, строки матрицы Z с номерами из $\ell(Y)$ нулевые. Следовательно, уравнения (4) записываются в виде

$$\langle a'^{(i)}, z'^{(j)} \rangle \oplus \langle a'^{(j)}, z'^{(i)} \rangle = 0, \quad i, j \in \{1, \dots, t\}, \quad i > j, \quad (6)$$

где $a'^{(i)}$ и $z'^{(j)}$ — столбцы матриц A' и Z' соответственно, полученных из A и Z удалением строк с номерами из $\ell(Y)$.

Таким образом, f_0^{2k} аффинна на L тогда и только тогда, когда выполняются соотношения (3) и (6). Решениями $y^{(j)}$ системы (3) являются любые элементы подпространства L_A^\perp . Но Y является GJB-матрицей, поэтому она определяется однозначно по A как GJB-матрица для L_A^\perp .

Уравнения (6) можно представить в виде системы линейных уравнений (1), если считать $(z'^{(1)T}, \dots, z'^{(t)T})^T$ столбцом переменных. Следовательно, соотношения (2) выполняются тогда и только тогда, когда матрица G допустима. Теорема 1 доказана.

Приведём некоторые крайние случаи: при $t = 0$ имеется единственная допустимая GJB-матрица $B = \begin{pmatrix} 0 \\ E \end{pmatrix}$. При $t = k$ допустимые GJB-матрицы имеют вид $B = \begin{pmatrix} E \\ T \end{pmatrix}$, где T — произвольная симметричная матрица. Число таких матриц равно $2^{k(k+1)/2}$.

Рассмотрим пример построения линейного подпространства, на котором аффинна функция $f_0^8(x)$, т. е. $k = 4$. Общий вид базисной матрицы B будет $\left(\begin{array}{c|c} A & 0 \\ \hline Z & Y \end{array} \right)$. Возьмём в качестве A следующую матрицу ранга 2:

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Получим одну из базисных матриц подпространства L_Y :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Выберем у подпространства L_Y GJB-матрицу Y (здесь $\ell(Y) = \{1, 2\}$):

$$Y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Отсюда $A' = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, и тогда $M = \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix}$. Таким образом, матрица Z' имеет вид

$$Z' = \begin{pmatrix} c_1 \oplus c_2 & c_3 \\ c_1 & c_2 \end{pmatrix}.$$

Например, для $c_1, c_2, c_3 = 1$ получим матрицу $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

В итоге приходим к GJB-матрице B для подпространства L_B , на котором функция $x_1x_5 \oplus x_2x_6 \oplus x_3x_7 \oplus x_4x_8$ аффинна:

$$B = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{array} \right).$$

6. Подсчёт числа бент-функций на минимальном расстоянии от квадратичной бент-функции

Перейдем к подсчёту числа бент-функций на расстоянии d_k от произвольной квадратичной бент-функции.

Лемма 2. *Строки матрицы M вида (1) линейно независимы.*

Доказательство. Пусть матрица Y' образована всеми неведущими строками матрицы Y . Заметим, что матрица Y' имеет размер $t \times t$. Покажем, что векторы $a'^{(1)}, \dots, a'^{(t)}$ линейно независимы. Заметим также, что из этого утверждения следует линейная независимость строк матрицы M .

Предположим, что существуют различные i_1, \dots, i_p такие, что

$$a'^{(i_1)} \oplus \dots \oplus a'^{(i_p)} = 0.$$

Тогда для любого $j = 1, \dots, k - t$ верно

$$0 = \langle y'^{(j)}, a'^{(i_1)} \oplus \dots \oplus a'^{(i_p)} \rangle = \langle y'^{(j)}, a'^{(i_1)} \rangle \oplus \dots \oplus \langle y'^{(j)}, a'^{(i_p)} \rangle.$$

Также для любого $q = 1, \dots, p$ выполняется

$$\langle y'^{(j)}, a'^{(i_q)} \rangle = \langle y^{(j)}, a^{(i_q)} \rangle \oplus a_{\ell(y^{(j)})i_q}.$$

Поскольку $L_Y = L_A^\perp$, то $\langle y^{(j)}, a^{(i_q)} \rangle = 0$. Поэтому верно

$$a_{\ell(y^{(j)})i_1} \oplus \dots \oplus a_{\ell(y^{(j)})i_p} = 0.$$

Элементы $a_{\ell(y^{(j)})i_q}$ суть все удалённые элементы из столбцов с номерами i_1, \dots, i_p . Следовательно, получаем

$$a^{(i_1)} \oplus \dots \oplus a^{(i_p)} = 0,$$

но векторы $a^{(1)}, \dots, a^{(t)}$ линейно независимы; противоречие. Стало быть, $a'^{(1)}, \dots, a'^{(t)}$ линейно независимы. Лемма 2 доказана.

Обозначим через S_k^t число линейных подпространств размерности t в \mathbb{Z}_2^k . Заметим, что число S_k^t можно посчитать по следующей формуле:

$$S_k^t = \frac{(2^k - 1) \dots (2^{k-t+1} - 1)}{(2^t - 1) \dots (2^1 - 1)}.$$

Эту формулу можно найти, например, в монографии [3].

Лемма 3. Для произвольных $k > 0$ и $0 < t < k$ верно равенство

$$S_k^t = S_{k-1}^t + 2^{k-t} S_{k-1}^{t-1}.$$

Для ДОКАЗАТЕЛЬСТВА ЛЕММЫ 3 достаточно воспользоваться приведённой формулой.

Теорема 2. Любая квадратичная бент-функция от $2k$ переменных имеет ровно $2^k \cdot (2^1 + 1) \dots (2^k + 1)$ бент-функций на расстоянии d_k .

ДОКАЗАТЕЛЬСТВО. Согласно утверждению 2 любая квадратичная бент-функция от $2k$ переменных аффинно эквивалентна f_0^{2k} . Покажем, что эта бент-функция аффинна ровно на $\sum_{t=0}^k 2^{t(t+1)/2} S_k^t$ линейных подпространствах размерности k . Тогда аффинных подпространств будет в 2^k раз больше, и по утверждению 1 получим число бент-функций на расстоянии d_k .

По теореме 1 достаточно подсчитать число допустимых GJB-матриц размера $2k \times k$, так как различные GJB-матрицы соответствуют различным линейным подпространствам. Для любой допустимой GJB-матрицы

порядка t рассмотрим соответствующие ей матрицы A, Y, Z . Матрица A ранга t может быть выбрана S_k^t способами. Тогда матрица Y определяется однозначно. Для фиксированной матрицы A по теореме 1 и лемме 2 можно выбрать $2^{t(t+1)/2}$ матриц Z . Таким образом, получаем, что любая квадратичная функция аффинна ровно на $\sum_{t=0}^k 2^{t(t+1)/2} S_k^t$ линейных подпространствах. Обозначим это число через C_k и упростим данную формулу.

Докажем, что при $k > 0$ выполняется $C_k = (2^k + 1)C_{k-1}$. По лемме 3 $S_k^t = S_{k-1}^t + 2^{k-t} S_{k-1}^{t-1}$ для каждого t такого, что $0 < t < k$. Заметим, что для крайних значений параметра t справедливо $S_k^0 = S_{k-1}^0$ и $S_k^k = 2^{k-k} S_{k-1}^{k-1}$. Отсюда

$$C_k = \sum_{t=0}^k 2^{t(t+1)/2} S_k^t = \sum_{t=0}^{k-1} 2^{t(t+1)/2} S_{k-1}^t + \sum_{t=1}^k 2^{k-t} 2^{t(t+1)/2} S_{k-1}^{t-1}.$$

Заметим, что первая сумма равна C_{k-1} . Во второй сумме заменим t на $i+1$ и получим

$$C_k = C_{k-1} + \sum_{i=0}^{k-1} 2^{k-(i+1)} 2^{(i+1)(i+1+1)/2} S_{k-1}^i.$$

Так как $k - (i+1) + (i+1)(i+2)/2 = k + i(i+1)/2$, имеем

$$C_k = C_{k-1} + 2^k \sum_{i=0}^{k-1} 2^{i(i+1)/2} S_{k-1}^i = (2^k + 1)C_{k-1},$$

а также $C_1 = 3$. Следовательно, $C_k = (2^1 + 1) \dots (2^k + 1)$. Теорема 2 доказана.

Нетрудно показать, что

$$2^k \cdot (2^1 + 1) \dots (2^k + 1) < 3 \cdot 2^k \cdot 2^{k(k+1)/2}.$$

Поэтому более чем треть бент-функций на расстоянии d_k от квадратичной бент-функции можно получить очень просто, а именно, с помощью допустимых GJB-матриц вида $G = \begin{pmatrix} E \\ T \end{pmatrix}$, где T — произвольная симметричная матрица размера $k \times k$.

Также отметим, что все бент-функции на расстоянии d_k от любой из квадратичных бент-функций аффинно эквивалентны бент-функциям из класса Мэйорана — МакФарланда.

7. Примеры для малых размерностей

Обозначим через $*$ произвольный элемент \mathbb{Z}_2 . Тогда все допустимые GJB-матрицы при $k = 2$ выглядят следующим образом (выделены ведущие элементы): при $t = 0$ одна матрица

$$\left(\begin{array}{cc|cc} 0 & 0 & & \\ 0 & 0 & & \\ \hline 1 & 0 & & \\ 0 & 1 & & \end{array} \right),$$

при $t = 1$ получаем $3 \cdot 2 = 6$ матриц вида

$$\left(\begin{array}{cc|cc} 1 & 0 & & \\ 0 & 0 & & \\ \hline * & 0 & & \\ 0 & 1 & & \end{array} \right), \left(\begin{array}{cc|cc} 1 & 0 & & \\ 1 & 0 & & \\ \hline 0 & 1 & & \\ * & 1 & & \end{array} \right), \left(\begin{array}{cc|cc} 0 & 0 & & \\ 1 & 0 & & \\ \hline 0 & 1 & & \\ * & 0 & & \end{array} \right)$$

и при $t = 2$ имеется $1 \cdot 2^3 = 8$ матриц вида

$$\left(\begin{array}{cc|cc} 1 & 0 & & \\ 0 & 1 & & \\ \hline * & a & & \\ a & * & & \end{array} \right),$$

где a — некоторый элемент \mathbb{Z}_2 . Итого получаем пятнадцать линейных подпространств. Взяв также все смежные классы подпространств с приведёнными выше базисными матрицами, получим шестьдесят аффинных подпространств, на которых f_0^4 аффинна.

Для $k = 3$ функция f_0^6 аффинна на линейных подпространствах со следующими допустимыми GJB-матрицами: при $t = 0$ одна матрица

$$\left(\begin{array}{ccc|ccc} 0 & 0 & 0 & & & \\ 0 & 0 & 0 & & & \\ 0 & 0 & 0 & & & \\ \hline 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array} \right),$$

при $t = 1$ получаем $7 \cdot 2 = 14$ матриц вида

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ 0 & 0 & 0 & & & \\ 0 & 0 & 0 & & & \\ \hline * & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array} \right), \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ 1 & 0 & 0 & & & \\ 0 & 0 & 0 & & & \\ \hline 0 & 1 & 0 & & & \\ * & 1 & 0 & & & \\ 0 & 0 & 1 & & & \end{array} \right), \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ 0 & 0 & 0 & & & \\ 1 & 0 & 0 & & & \\ \hline 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ * & 1 & 0 & & & \end{array} \right), \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & & & \\ 1 & 0 & 0 & & & \\ 1 & 0 & 0 & & & \\ \hline 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ * & 1 & 1 & & & \end{array} \right),$$

$$\left(\begin{array}{c|cc} 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 \\ \hline 0 & \mathbf{1} & 0 \\ * & 0 & 0 \\ 0 & 0 & \mathbf{1} \end{array} \right), \left(\begin{array}{c|cc} 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 \\ 1 & 0 & 0 \\ \hline 0 & \mathbf{1} & 0 \\ 0 & 0 & \mathbf{1} \\ * & 0 & 1 \end{array} \right), \left(\begin{array}{c|cc} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 \\ \hline 0 & \mathbf{1} & 0 \\ 0 & 0 & \mathbf{1} \\ * & 0 & 0 \end{array} \right),$$

при $t = 2$ имеется $7 \cdot 2^3 = 56$ матриц вида

$$\left(\begin{array}{cc|c} \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 \\ \hline * & a & 0 \\ a & * & 0 \\ 0 & 0 & \mathbf{1} \end{array} \right), \left(\begin{array}{cc|c} \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 \\ 1 & 0 & 0 \\ \hline 0 & 0 & \mathbf{1} \\ a & * & 0 \\ * & a & 1 \end{array} \right), \left(\begin{array}{cc|c} \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 \\ 0 & 1 & 0 \\ \hline * & a & 0 \\ 0 & 0 & \mathbf{1} \\ a & * & 1 \end{array} \right), \left(\begin{array}{cc|c} \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 \\ 1 & 1 & 0 \\ \hline 0 & 0 & \mathbf{1} \\ a & * & 1 \\ b & a \oplus b & 1 \end{array} \right),$$

$$\left(\begin{array}{cc|c} \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 \\ \hline * & a & 0 \\ 0 & 0 & \mathbf{1} \\ a & * & 0 \end{array} \right), \left(\begin{array}{cc|c} \mathbf{1} & 0 & 0 \\ 1 & 0 & 0 \\ 0 & \mathbf{1} & 0 \\ \hline 0 & 0 & \mathbf{1} \\ * & a & 1 \\ a & * & 0 \end{array} \right), \left(\begin{array}{cc|c} 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 \\ \hline 0 & 0 & \mathbf{1} \\ * & a & 0 \\ a & * & 0 \end{array} \right)$$

и при $t = 3$ получаем $1 \cdot 2^6 = 64$ матриц вида

$$\left(\begin{array}{ccc} \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 \\ 0 & 0 & \mathbf{1} \\ \hline * & a & c \\ a & * & b \\ c & b & * \end{array} \right),$$

где a, b, c — некоторые элементы \mathbb{Z}_2 . Таким образом, получаем 135 линейных подпространств. Посчитав также все смежные классы данных подпространств, получим 1080 аффинных подпространств, на которых f_0^6 аффинна.

В следующей таблице приведено число бент-функций на расстоянии d_k от любой квадратичной бент-функции для малого числа переменных.

| | | | | | | |
|-------|---|----|------|-------|---------|-----------|
| 2k | 2 | 4 | 6 | 8 | 10 | 12 |
| число | 6 | 60 | 1080 | 36720 | 2423520 | 315057600 |

**8. Нижняя оценка числа бент-функций
на минимальном расстоянии от бент-функций
из класса Мэйорана — МакФарланда**

Поскольку бент-функция f_0^{2k} принадлежит классу Мэйорана — МакФарланда, все квадратичные бент-функции аффинно эквивалентны бент-функциям из этого класса. Поэтому рассмотрим более общую задачу нахождения некоторой нижней оценки числа бент-функций на расстоянии d_k от функции из этого класса.

Класс Мэйорана — МакФарланда содержит бент-функции вида

$$f(x, y) = \langle x, \pi(y) \rangle \oplus \psi(y),$$

где $x, y \in \mathbb{Z}_2^k$, ψ — булева функция от k переменных, π — перестановка на \mathbb{Z}_2^k . Обозначим этот класс через \mathcal{M}_{2k} . Более подробную информацию о нём можно получить в [8].

Для нахождения нижней оценки нам потребуются следующие утверждения.

Утверждение 6. Пусть f — булева функция от n переменных, L — линейное подпространство в \mathbb{Z}_2^n , D_1 и D_2 — различные смежные классы из L такие, что $f|_{D_1}(x) = \langle a, x \rangle \oplus c$, $f|_{D_2}(x) = \langle a, x \rangle \oplus c'$ для некоторого вектора $a \in \mathbb{Z}_2^n$ и констант c и c' . Тогда f аффинна на $D_1 \cup D_2$.

ДОКАЗАТЕЛЬСТВО. Без ограничения общности пусть $D_1 = L$. Обозначим D_2 через D . Ясно, что объединение линейного подпространства и его смежного класса будет являться линейным подпространством. Обозначим $L \cup D$ через L' .

Покажем что функция f аффинна на подпространстве L' .

Если $c = c'$, утверждение очевидно. Предположим, что $c' = c \oplus 1$. Тогда $f|_L(x) = \langle a, x \rangle \oplus c$, $f|_D(y) = \langle a, y \rangle \oplus c \oplus 1$. Следовательно, для любого $w \in L^\perp$ и $b = a \oplus w$ выполняется

$$f|_L(x) = (f(x) \oplus \langle w, x \rangle)|_L = \langle b, x \rangle \oplus c.$$

Пусть $v \in D$. Также для любых $x \in L$ и $y \in D$ имеем

$$\begin{aligned} \langle b, y \rangle &= \langle a \oplus w, y \rangle = \langle a, y \rangle \oplus \langle w, y \rangle = \langle a, y \rangle \oplus \langle w, x \oplus v \rangle \\ &= \langle a, y \rangle \oplus \langle w, x \rangle \oplus \langle w, v \rangle = \langle a, y \rangle \oplus \langle w, v \rangle. \end{aligned}$$

Ясно, что существует $w' \in L^\perp$ такой, что $\langle w', v \rangle = 1$. Если это не так, то $v \in L^{\perp\perp} = L$, но L и D различны; противоречие. Отсюда для $b = a \oplus w'$ выполняется $\langle b, y \rangle = \langle a, y \rangle \oplus 1$. Следовательно,

$$f|_D(y) = \langle a, y \rangle \oplus c \oplus 1 = \langle b, y \rangle \oplus c \oplus 1 \oplus 1 = \langle b, y \rangle \oplus c,$$

а также $f|_L(x) = \langle b, x \rangle \oplus c$. Утверждение 6 доказано.

Лемма 4. Бент-функция $f \in \mathfrak{B}_{2k}$ не может быть аффинна на аффинном подпространстве размерности больше k .

Данную лемму можно найти в [6]. Для её доказательства достаточно предположить обратное и применить несколько раз утверждение 1.

Утверждение 7. Пусть $f \in \mathfrak{B}_{2k}$ — бент-функция и L — подпространство размерности l в \mathbb{Z}_2^{2k} такое, что f аффинна на любом его смежном классе. Тогда для любого смежного класса $a \oplus L$ существует ровно 2^{2k-l} векторов w таких, что $f|_{a \oplus L}(x) = \langle w, x \rangle \oplus c_w$ для некоторой константы c_w .

Для ДОКАЗАТЕЛЬСТВА УТВЕРЖДЕНИЯ 7 достаточно решить систему уравнений $\langle w \oplus w_0, x \rangle = \text{const}$, $x \in a \oplus L$, относительно w .

Лемма 5. Пусть $f \in \mathfrak{B}_{2k}$ и L — линейное подпространство размерности k в \mathbb{Z}_2^{2k} такое, что бент-функция f аффинна на любом его смежном классе. Тогда для любого $w \in \mathbb{Z}_2^{2k}$ существует $u \in \mathbb{Z}_2^{2k}$ такой, что

$$f|_{u \oplus L}(x) = \langle w, x \rangle \oplus c$$

для некоторой константы c .

ДОКАЗАТЕЛЬСТВО. Предположим, что существуют два различных смежных класса D_1 и D_2 для подпространства L и вектор w такие, что

$$f|_{D_1}(x) = \langle w, x \rangle \oplus c_1, \quad f|_{D_2}(x) = \langle w, x \rangle \oplus c_2.$$

Тогда по утверждению 6 бент-функция f аффинна на аффинном подпространстве $D_1 \cup D_2$ размерности больше k . Получаем противоречие с леммой 4. Далее используем утверждение 7. Лемма 5 доказана.

Теорема 3. Пусть f — бент-функция от $2k$ переменных из класса Мэйорана — МакФарланда. Тогда число бент-функций на расстоянии d_k от неё не меньше $2^{2k+1} - 2^k$.

ДОКАЗАТЕЛЬСТВО. Используя утверждение 1, достаточно подсчитать аффинные подпространства размерности k , на которых f аффинна. Пусть $L = \{(x, 0, \dots, 0) \mid x \in \mathbb{Z}_2^k\} \subseteq \mathbb{Z}_2^{2k}$. Очевидно, что L — линейное подпространство. Также любая функция из класса Мэйорана — МакФарланда аффинна на нём и любом его смежном классе. Будем подсчитывать смежные классы тех подпространств, которые пересекаются с L по 2^{k-1} элементам.

Подпространство L содержит ровно $2^k - 1$ различных линейных подпространств U размерности $k - 1$. Таким образом, аффинное подпространство $u \oplus U$ можно выбрать ровно $2^{k+1} \cdot (2^k - 1)$ способами. Также очевидно, что аффинное подпространство $u \oplus U$ содержится в множестве $u \oplus L$.

Используя утверждение 7, получаем, что существует ровно 2^{k+1} векторов w_1 таких, что $f|_{u \oplus U}(x) = \langle w_1, x \rangle \oplus c_{w_1}$. Но для любого $u \oplus L$ существует ровно 2^k векторов w_2 таких, что $f|_{u \oplus L}(x) = \langle w_2, x \rangle \oplus c_{w_2}$. Поэтому в силу леммы 5 существует смежный класс $v \oplus L$, отличный от $u \oplus L$, такой, что для некоторого вектора w и констант c_1, c_2 выполняется

$$f|_{u \oplus U}(x) = \langle w, x \rangle \oplus c_1, \quad f|_{v \oplus L}(x) = \langle w, x \rangle \oplus c_2.$$

В множестве $v \oplus L$ содержится ровно 2 различных смежных класса подпространства U , обозначим их через $a \oplus U$ и $b \oplus U$. Таким образом, по утверждению 6 функция f аффинна на аффинных подпространствах $(u \oplus U) \cup (a \oplus U)$ и $(u \oplus U) \cup (b \oplus U)$ размерности k . С учётом того, что мы выбираем неупорядоченную пару смежных классов, получаем

$$((2^k - 1) \cdot 2^{k+1} \cdot 2)/2 = 2^{2k+1} - 2^{k+1}$$

различных аффинных подпространств размерности k , на которых функция f аффинна. Также f аффинна на всех смежных классах подпространства L . Теорема 3 доказана.

9. Другие оценки и гипотезы

Рассмотрим тривиальную верхнюю оценку числа бент-функций на расстоянии d_k от заданной бент-функции.

Утверждение 8. Пусть $f \in \mathfrak{B}_{2k}$. Тогда число бент-функций на расстоянии d_k от неё меньше 2^{k^2+2k} .

Это утверждение получено с помощью оценки сверху числа аффинных подпространств нужной размерности с использованием формулы для S_k^t . Таким образом, число бент-функций на расстоянии d_k от любой квадратичной бент-функции больше, чем корень из тривиальной верхней оценки.

Рассмотрим гипотезу о максимальном числе бент-функций на расстоянии d_k от заданной бент-функции.

Гипотеза. Любая квадратичная бент-функция имеет максимально возможное число бент-функций на расстоянии d_k , т. е. верхняя оценка

числа бент-функций на расстоянии d_k от произвольной бент-функции равна $2^k(2^1 + 1) \dots (2^k + 1)$.

Заметим, что нижняя оценка числа бент-функций на расстоянии d_k от заданной бент-функции равна нулю, так как существуют бент-функции, не имеющие бент-функций на расстоянии d_k . Проблема существования бент-функций на расстоянии d_k от заданной связана с понятиями нормальной и ненормальной бент-функций. В частности, из [5] следует, что существуют бент-функции от $2k$ переменных, которые не являются аффинными ни на одном аффинном подпространстве размерности k . Таким образом, не для всех бент-функций возможно построить бент-функцию на расстоянии d_k .

ПРИМЕР 2 [5]. Для любого чётного $n \geq 14$ бент-функция

$$\text{tr}(\alpha(x_1, \dots, x_{14})^{57}) \oplus x_{15}x_{16} \oplus x_{17}x_{18} \oplus \dots \oplus x_{n-1}x_n$$

не имеет бент-функций на расстоянии d_k . Здесь через $\text{tr}(\cdot)$ обозначается след из $GF(2^{14})$ в $GF(2)$, α — подходящий элемент \mathbb{Z}^2 , вектор (x_1, \dots, x_{14}) также рассматривается как элемент $GF(2^{14})$.

ЛИТЕРАТУРА

1. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикл. дискрет. математика. — 2009. — № 4. — С. 5–21.
2. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 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. Нелинейные булевы функции: бент-функции и их обобщения // Saarbrücken, Germany: Lambert Acad. Publ., 2011. — 180 с.
5. Canteaut A., Daum M., Dobbertin H., Leander G. Finding nonnormal bent functions // Discrete Appl. Math. — 2006. — Vol. 154, N 2. — P. 202–218.
6. Carlet C. Boolean functions for cryptography and error correcting codes. Chapter of the monograph // Boolean methods and models, to appear. Prelim. version is available at <http://www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf>.
7. Dillon J. F. A survey of bent functions // The NSA Techn. J. — 1972. — P. 191–215.
8. McFarland R. L. A family of difference sets in non-cyclic groups // J. Comb. Theory, Ser. A. — 1973. — Vol. 15, N 1. — P. 1–10.

- 9. Rothaus O.** On bent functions // J. Comb. Theory, Ser. A. — 1976. — Vol. 20, N 3. — P. 300–305.

Коломеец Николай Александрович,
e-mail: nkolomeec@gmail.com

Статья поступила
5 апреля 2011 г.
Переработанный вариант —
24 сентября 2011 г.