ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Сентябрь—октябрь 2013. Том 20, № 5. С. 45–57

УДК 519.7

КЛАССИФИКАЦИЯ ГРАФОВ КВАДРАТИЧНЫХ БЕНТ-ФУНКЦИЙ ОТ ШЕСТИ ПЕРЕМЕННЫХ

Е. П. Корсакова

Аннотация. Рассматривается задача классификации бент-функций от малого числа переменных. Построена графовая классификация квадратичных бент-функций от 6 переменных. Проведён анализ полученных графов, выявлены новые итеративные конструкции бент-функций.

Ключевые слова: булева функция, нелинейность, бент-функция, алгебраическая нормальная форма (АНФ), графовая эквивалентность, итеративные конструкции.

Введение

Исследование свойств нелинейных булевых функций полезно из-за их широкого приложения в комбинаторике, алгебре, криптографии, теории кодирования и т. д. (см. подробнее [3]). Особенный интерес представляют функции, нелинейные свойства которых экстремальны (при чётном числе переменных — бент-функции), поскольку они крайне плохо приближаются аффинными функциями.

Бент-функции введены в [8], где установлены базовые свойства таких функций и предложены их простейшие конструкции. В настоящее время известны серии конструкций бент-функций, однако задача описания всех бент-функций от n переменных решена лишь при малых значениях n. При $n \geqslant 10$ класс бент-функций не описан, для его мощности не найдена асимптотика и не установлены приемлемые нижние и верхние оценки.

Задача классификации бент-функций от малого числа переменных интересна для выявления общих свойств бент-функций, поиска новых конструкций и общих итеративных способов построения бент-функций.

В нашей работе рассматривается задача классификации бент-функций от малого числа переменных, а именно, введено понятие графовой эквивалентности квадратичных булевых функций и построена графовая классификация квадратичных бент-функций от 6 переменных. Установлено, что существует 37 типов графов, которым соответствует 47 графово неэквивалентных квадратичных бент-функций от 6 переменных.

Проведён анализ полученных графов. Предложены две новые итеративные конструкции бент-функций. Результаты статьи анонсированы в [1].

1. Базовые определения

Пусть $\mathbb{Z}_2^n$ — множество двоичных векторов длины n и $x, y \in \mathbb{Z}_2^n$. Пусть символ $\oplus$ обозначает сложение по модулю два. *Скалярным произведением* двоичных векторов x, y называется число $\langle x, y\rangle = x_1 y_1 \oplus \ldots \oplus x_n y_n$. *Булевой функцией от n переменных* называется функция, действующая из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция W_f, заданная на $\mathbb{Z}_2^n$ равенством

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

Бент-функцией называется булева функция от n переменных (n чётно) такая, что модуль каждого коэффициента Уолша — Адамара этой функции равен $2^{n/2}$.

Каждая булева функция однозначно задаётся своей *алгебраической нормальной формой* (АНФ), т. е. представляется в виде

$$f(x) = \left(\bigoplus_{k=1}^{n} \bigoplus_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k} x_{i_1} \cdot \ldots \cdot x_{i_k} \right) \oplus a_0,$$

где $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и $a_{i_1, \ldots, i_k},\ a_0 \in \mathbb{Z}_2$. *Степенью* $\deg f$ булевой функции f называется число переменных в самом длинном слагаемом её алгебраической нормальной формы. Булева функция называется *квадратичной*, если её степень равна 2. Булевы функции f и g от n переменных *аффинно эквивалентны*, если существуют невырожденная $(n \times n)$-матрица A, векторы b, c длины n и константа $\lambda \in \mathbb{Z}_2$ такие, что

$$g(y) = f(Ay \oplus b) \oplus \langle c, y\rangle \oplus \lambda.$$

2. Графовое описание квадратичных булевых функций

Рассмотрим подробнее классы аффинной эквивалентности квадратичных бент-функций.

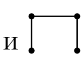
Утверждение 1 [8]. *Все квадратичные бент-функции от n переменных аффинно эквивалентны.*

Введём более сильную эквивалентность, которая позволит разбить множество квадратичных бент-функций на разные классы.

Каждой функции от n переменных сопоставим простой неориентированный граф на n вершинах. *Графом квадратичной булевой функции* $G = \langle V_G, E_G \rangle$ назовём граф, вершины которого V_G отождествлены с переменными функции, рёбрами E_G соединены те вершины, которые образуют слагаемое в квадратичной части АНФ функции. *Тип графа* — упорядоченный по убыванию набор степеней его вершин.

Напомним, что графы $G = \langle V_G, E_G \rangle$ *и* $H = \langle V_H, E_H \rangle$ *изоморфны*, если существует биекция между множествами вершин графов $f : V_G \to V_H$ такая, что любые две вершины u и v графа G смежны, если и только если вершины $f(u)$ и $f(v)$ смежны в графе H. Две квадратичные функции назовём *графово эквивалентными*, если соответствующие им графы изоморфны. Заметим, что это более сильная эквивалентность, чем аффинная.

Пример 1. Функции $f(x) = x_1x_2 \oplus x_3x_4$ и $g(x) = x_1x_2 \oplus x_2x_3 \oplus x_3x_4$ аффинно эквивалентны, так как $g(x) = f(Ax)$, где $A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$,

но не эквивалентны графово: f и  g.

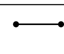
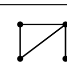
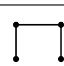
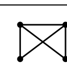
3. Графовая классификация АНФ квадратичных бент-функций

Рассмотрим графовую классификацию квадратичных бент-функций от малого числа переменных.

3.1. Графовая классификация бент-функций от 4 переменных. Графовая классификация функций от 4 переменных получена и описана в [8].

Таблица 1

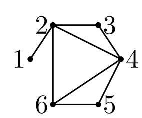
Классификация функций от 4 переменных

N	Тип	Граф	N	Тип	Граф
1	1 1 1 1		3	3 2 2 1	
2	2 2 1 1		4	3 3 3 3	

3.2. Графовая классификация бент-функций от 6 переменных. Рассмотрим задачу графовой классификации квадратичных бент-функций от 6 переменных. Согласно утверждению 1 все они аффинно эквивалентны функции $x_1x_2 \oplus x_3x_4 \oplus x_5x_6$. Поэтому для нахождения графов использовались аффинные преобразования этой функции, заданные невырожденными двоичными матрицами размера 6×6. Была написана программа на C++, которая, перебирая все возможные матрицы данного вида, определяет типы графов.

Теорема 1. *Существует* 37 *различных типов графов квадратичных бент-функций от* 6 *переменных и* 47 *графово неэквивалентных квадратичных бент-функций от* 6 *переменных.*

В табл. 2 представлены все 37 типов графов. В третьем столбце указаны все неизоморфные графы, соответствующие данному типу. Номера конструкций, с помощью которых они могут быть построены, указаны в скобках во втором столбце (номер 2 соответствует конструкции, описанной в теореме 2, номер 3 — конструкции, описанной в теореме 3 из разд. 4). Для 9 графов не удалось найти итеративных способов построения, однако 6 из них (7.2, 11, 15, 20.1, 28.2, 31) могут быть представлены с помощью конструкции Майорана —МакФарланда. Для каждого графа, фиксируя любую нумерацию его вершин, можно построить соответствующую ему бент-функцию.

Пример 2. Возьмём граф 18 из табл. 2 и фиксируем нумерацию его вершин следующим образом:  .

Такие граф и нумерация однозначно определяют квадратичную часть квадратичной бент-функции, равную $x_1x_2 + x_2x_3 + x_2x_4 + x_2x_6 + x_3x_4 + x_4x_5 + x_4x_6 + x_5x_6$. Заметим, что данный граф может быть построен с помощью конструкции, описанной в теореме 2 разд. 4.

Т а б л и ц а 2

Классификация функций от 6 переменных

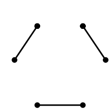
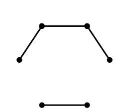
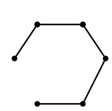
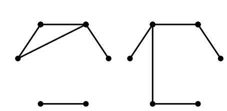
N	Тип	Граф	N	Тип	Граф
1	1 1 1 1 1 1 (2,3)		2	2 2 1 1 1 1 (2,3)	
3	2 2 2 2 1 1 (2)		4	3 2 2 1 1 1 (2,3), (2)	

Таблица 2

Классификация функций от 6 переменных (продолжение)

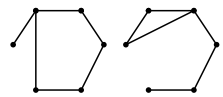
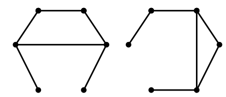
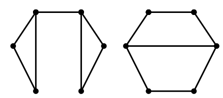
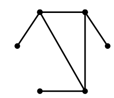
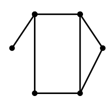
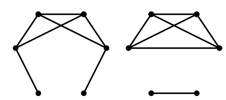
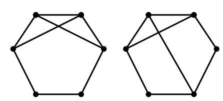
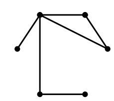
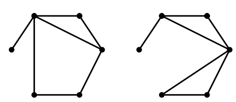
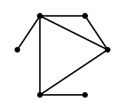
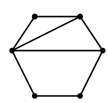
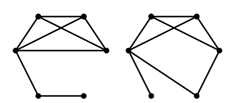
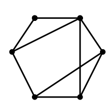
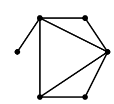
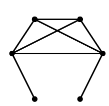
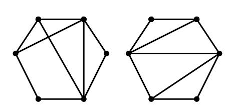
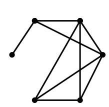
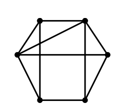
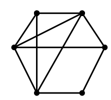
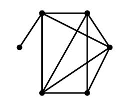
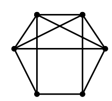
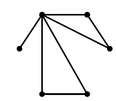
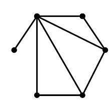
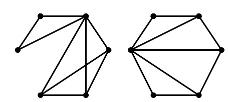
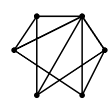
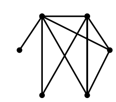
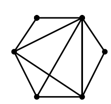
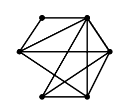
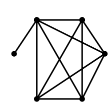
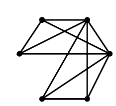
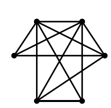
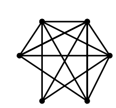
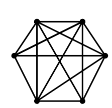
5	3 2 2 2 2 1 (2), (2,3)		6	3 3 2 2 1 1 (2), (2)	
7	3 3 2 2 2 2 (3), (–)		8	3 3 3 1 1 1 (2)	
9	3 3 3 2 2 1 (2)		10	3 3 3 3 1 1 (2,3), (2,3)	
11	3 3 3 3 2 2 (3), (–)		12	4 2 2 2 1 1 (2,3)	
13	4 3 2 2 2 1 (2), (2,3)		14	4 3 3 2 1 1 (2)	
15	4 3 3 2 2 2 (–)		16	4 3 3 3 2 1 (2,3), (2,3)	
17	4 3 3 3 3 2 (3)		18	4 4 3 2 2 1 (2)	
19	4 4 3 3 1 1 (2,3)		20	4 4 3 3 2 2 (–), (–)	
21	4 4 3 3 3 1 (2,3)		22	4 4 3 3 3 3 (–)	

Таблица 2

Классификация функций от 6 переменных (продолжение)

23	4 4 4 3 3 2 (3)	
24	4 4 4 4 3 1 (2,3)	
25	4 4 4 4 3 3 (3)	
26	5 2 2 2 2 1 (2,3)	
27	5 3 3 2 2 1 (2)	
28	5 3 3 3 2 2 (3), (–)	
29	5 3 3 3 3 3 (–)	
30	5 4 3 3 2 1 (2,3)	
31	5 4 4 3 2 2 (–)	
32	5 4 4 4 3 2 (3)	
33	5 4 4 4 4 1 (2,3)	
34	5 5 3 3 3 3 (3)	
35	5 5 4 4 3 3 (3)	
36	5 5 5 4 4 3 (3)	
37	5 5 5 5 5 5 (3)	

3.3. Анализ графов АНФ квадратичных бент-функций. Докажем некоторые свойства графов АНФ квадратичных бент-функций.

Утверждение 2. *Граф АНФ любой квадратичной бент-функции от n переменных не имеет изолированных вершин.*

Доказательство. От противного. Пусть квадратичная бент-функция $f(x)$ не содержит переменной x_n в квадратичной части АНФ. Известно, что бент-функция существенно зависит от всех своих переменных. Тогда АНФ функции $f(x)$ можно представить в виде

$$f(x) = \sum_{1\leqslant i<j\leqslant n-1} a_{ij}x_ix_j \oplus \sum_{i=1}^{n-1} a_ix_i \oplus x_n \oplus a_0.$$

Поскольку добавление аффинной функции не меняет свойства максимальной удалённости от класса аффинннных функций,

$$g(x) = f(x) \oplus x_n = \sum_{1\leqslant i<j\leqslant n-1} a_{ij}x_ix_j \oplus \sum_{i=1}^{n-1} a_ix_i \oplus a_0$$

тоже является бент-функцией. Но $g(x)$ не зависит от переменной x_n, что противоречит существенной зависимости бент-функций от всех переменных. Утверждение 2 доказано.

Пусть дан граф $G = (V, E)$. *Паросочетанием* M в G называется множество попарно не смежных рёбер, т. е. рёбер, не имеющих общих вершин. *Совершенным* называется паросочетание такое, что любая вершина графа инцидентна некоторому ребру этого паросочетания.

Утверждение 3. *В графе любой квадратичной бент-функции от n переменных существует совершенное паросочетание.*

Доказательство. Известно, что любая квадратичная бент-функция от n переменных эквивалентна функции $x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{n-1}x_n$. Очевидно, что у графа такой бент-функции существует совершенное паросочетание, в явном виде оно выглядит так:

$$M = \{(x_1, x_2), (x_3, x_4), \ldots, (x_{n-1}, x_n)\}.$$

Заметим, что любое аффинное преобразование можно породить элементарными преобразованиями вида

$$(x_1, \ldots, x_i, \ldots, x_n) \to (x_1, \ldots, x_i \oplus x_j, \ldots, x_n).$$

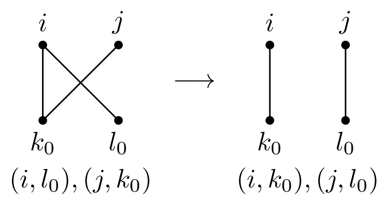
Пусть функция g порождается из f таким преобразованием для некоторых i и j. Обозначим через $G = (V, E)$ граф функции f, через $G' = (V', E')$ — граф функции g. Обозначим через V_k и V'_k множества всех вершин, инцидентных вершине k в G и G' соответственно. Докажем, что если в G существует совершенное паросочетание, то и в G' также существует совершенное паросочетание.

Заметим, что для любой вершины k, не равной j, $V'_k = V_k$, а $V'_j = V_i \cup V_j \setminus (V_i \cap V_j) = V_i \vartriangle V_j$. Пусть граф G обладает совершенным паросочетанием M. Тогда в графе G найдётся некоторая вершина l, инцидентная вершине k, такая, что ребро (k, l) принадлежит M. Построим паросочетание M' в графе G'.

Пусть $k \neq i, j$ и $l \neq i, j$, тогда $(k, l) \in E'$, включаем (k, l) в M'. Поскольку M совершенное, найдётся вершина k_0 такая, что (j, k_0) принадлежит M.

Случай 1. Если $k_0 = i$, то $(i, j) \in E'$, включаем (i, j) в M'.

Случай 2. Если $k_0 \neq i$, то найдётся вершина l_0 такая, что $(i, l_0) \in M$, тогда $(i, k_0) \in E'$ и $(j, l_0) \in E'$, включаем (i, k_0) и (j, l_0) в M'.



Заметим, что построенное таким образом паросочетание M' является совершенным для графа G'. Утверждение 3 доказано.

Булева симметрическая матрица с нулевой главной диагональю называется *симплектической*.

Утверждение 4 [2, с. 140]. *Ранг симплектической матрицы чётен.*

Утверждение 5. *У каждой невырожденной симплектической матрицы размера $n \times n$ существует невырожденная симплектическая подматрица размера $(n-2) \times (n-2)$.*

Доказательство. Пусть $M = (m_{i,j})_{i,j \in \{1,\ldots,n\}}$ — симплектическая матрица ранга n. Представим M в виде $M = \begin{pmatrix} M' & x \\ x^\top & 0 \end{pmatrix}$, где $x \in \mathbb{Z}_2^{n-1}$. Заметим, что матрица M' симплектическая размера $(n-1) \times (n-1)$. По утверждению 4 ранг M' равен $n-2$. Значит, найдётся номер j такой, что строка $(m_{j,1}, m_{j,2}, \ldots, m_{j,n-1})$ представляется в виде линейной комбинации остальных строк матрицы M'. Значит, удаляя j-ю строку и j-й столбец из матрицы M', получим симплектическую матрицу M'', причём $\operatorname{rank} M'' = \operatorname{rank} M' = n-2$, т. е. M'' — невырожденная подматрица M размера $(n-2) \times (n-2)$. Утверждение 5 доказано.

Каждой квадратичной булевой функции

$$f(x) = \bigoplus_{1\leqslant i<j\leqslant n} a_{ij}x_ix_j \oplus h(x),$$

где h аффинна, $a_{ij} \in \mathbb{Z}_2$, сопоставим симплектическую матрицу $M = (m_{i,j})_{i,j\in\{1,\ldots,n\}}$ над $\mathbb{Z}_2$ следующим образом: $m_{i,i} = 0$, $m_{i,j} = m_{j,i} = a_{ij}$, если $i > j$.

Утверждение 6 [5, с. 67]. *Квадратичная булева функция f является бент-функцией тогда и только тогда, когда соответствующая ей симплектическая матрица невырожденна.*

Следствие 1. *Для каждой квадратичной бент-функции f от n переменных ($n \geqslant 6$) найдутся $i, j \in \{1, \ldots n\}$ такие, что $f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)$ является бент-функцией от $n-2$ переменных.*

Заметим, что можно рассматривать симплектическую матрицу как матрицу смежности графа квадратичной булевой функции.

Подграфом $G' = (V', E')$ графа $G = (V, E)$ называется граф G', для которого $V' \subseteq V$, $E' \subseteq E$.

Порождённым подграфом $G' = (V', E')$ графа $G = (V, E)$ называется подграф, состоящий из подмножества вершин V' множества вершин исходного графа и всех таких рёбер графа G, у которых конечные и начальные вершины принадлежат подмножеству V'.

Следствие 2. *Для любого графа квадратичной бент-функции от n переменных найдётся порождённый подграф на $n-2$ вершинах, являющийся графом квадратичной бент-функции от $n-2$ переменных.*

4. Итеративные конструкции

Если проанализировать полученные графы, то можно выявить некоторые общие способы построения бент-функций от $n+2$ переменных из бент-функций от n переменных. Пусть $x = (x_1, \ldots, x_n)$, а x_{n+1}, x_{n+2} — новые переменные.

Теорема 2. *Если f — произвольная бент-функция от n переменных, то при любых $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_2$ функция*

$$g(x, x_{n+1}, x_{n+2}) = f(x) \oplus \left(\bigoplus_{i=1}^{n} \alpha_i \cdot x_i x_{n+1}\right) \oplus x_{n+1}x_{n+2}$$

является бент-функцией от $n+2$ переменных.

Доказательство. Покажем, что g — бент-функция. Для этого рассмотрим преобразование Уолша — Адамара функции g на векторе (y, y_{n+1}, y_{n+2}), где $y = (y_1, \dots, y_n)$. Имеем

$$W_g(y, y_{n+1}, y_{n+2}) = \sum_{(x,x_{n+1},x_{n+2})\in\mathbb{Z}_2^{n+2}} (-1)^{\langle x,y\rangle\oplus x_{n+1}y_{n+1}\oplus x_{n+2}y_{n+2}\oplus g(x,x_{n+1},x_{n+2})}.$$

Подставляя выражение для g, получаем

$$\begin{aligned}W_g(y, y_{n+1}, y_{n+2}) &= \sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle\oplus f(x)} \\ &+ \sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle\oplus f(x)\oplus y_{n+1}\oplus(\bigoplus_{i=1}^n \alpha_i\cdot x_i)} + \sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle\oplus f(x)\oplus y_{n+2}} \\ &+ \sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle\oplus f(x)\oplus y_{n+1}\oplus y_{n+2}\oplus(\bigoplus_{i=1}^n \alpha_i\cdot x_i)\oplus 1} \\ &= \sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle\oplus f(x)}\cdot(1+(-1)^{y_{n+2}}) \\ &+ \sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle\oplus f(x)\oplus y_{n+1}\oplus(\bigoplus_{i=1}^n x_i)}\cdot(1-(-1)^{y_{n+2}}).\end{aligned}$$

Поскольку f — бент-функция, $h(x) = f(x)\oplus y_{n+1}\oplus\left(\bigoplus_{i=1}^n x_i\right)$ также является бент-функцией, следовательно, $|W_f(y)| = 2^{n/2}$ и $|W_h(y)| = 2^{n/2}$, значит,

$$\begin{cases} \Big|\sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle\oplus f(x)}\Big| = |W_f(y)| = 2^{n/2}, \\ \Big|\sum_{x\in\mathbb{Z}_2^n} (-1)^{\langle x,y\rangle\oplus f(x)\oplus y_{n+1}\oplus(\bigoplus_{i=1}^n x_i)}\Big| = |W_h(y)| = 2^{n/2}, \end{cases}$$

и для каждого фиксированного y_{n+2} либо

$$1+(-1)^{y_{n+2}} = 0, \quad 1-(-1)^{y_{n+2}} = 2,$$

либо

$$1+(-1)^{y_{n+2}} = 2, \quad 1-(-1)^{y_{n+2}} = 0.$$

Итак, $|W_g(y, y_{n+1}, y_{n+2})| = 2^{n/2} \cdot 2 + 2^{n/2} \cdot 0 = 2^{(n+2)/2}$. Тем самым $g(x, x_{n+1}, x_{n+2})$ является бент-функцией от $n+2$ переменных. Теорема 2 доказана.

Теорема 3. *Если f — произвольная бент-функция от n переменных, то при любых $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_2$ функция*

$$g(x, x_{n+1}, x_{n+2}) = f(x) \oplus \left(\bigoplus_{i=1}^{n} \alpha_i \cdot x_i (x_{n+1} + x_{n+2}) \right) \oplus x_{n+1} x_{n+2}$$

является бент-функцией от $n+2$ переменных.

Доказательство. Докажем, что g — бент-функция. Для этого рассмотрим преобразование Уолша — Адамара функции g на векторе (y, y_{n+1}, y_{n+2}), где $y = (y_1, \ldots, y_n)$. Имеем

$$W_g(y, y_{n+1}, y_{n+2}) = \sum_{(x, x_{n+1}, x_{n+2}) \in \mathbb{Z}_2^{n+2}} (-1)^{\langle x, y \rangle \oplus x_{n+1} y_{n+1} \oplus x_{n+2} y_{n+2} \oplus g(x, x_{n+1}, x_{n+2})}.$$

Подставляя выражение для g, получаем

$$\begin{aligned} W_g(y, y_{n+1}, y_{n+2}) &= \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x, y \rangle \oplus f(x)} \\ &\quad + \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x, y \rangle \oplus f(x) \oplus y_{n+1} \oplus \left(\bigoplus_{i=1}^{n} \alpha_i \cdot x_i \right)} \\ + \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x, y \rangle \oplus f(x) \oplus y_{n+2} \oplus \left(\bigoplus_{i=1}^{n} \alpha_i \cdot x_i \right)} &+ \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x, y \rangle \oplus f(x) \oplus y_{n+1} \oplus y_{n+2} \oplus 1} \\ &= \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x, y \rangle \oplus f(x)} \cdot (1 - (-1)^{y_{n+1} + y_{n+2}}) \\ &\quad + \sum_{x \in \mathbb{Z}_2^n} (-1)^{\langle x, y \rangle \oplus f(x) \oplus y_{n+1} \oplus \left(\bigoplus_{i=1}^{n} x_i \right)} \cdot (1 + (-1)^{y_{n+1} + y_{n+2}}). \end{aligned}$$

Поскольку f — бент-функция, $h(x) = f(x) \oplus y_{n+1} \oplus \left(\bigoplus_{i=1}^{n} x_i \right)$ также является бент-функцией, следовательно, $|W_f(y)| = 2^{n/2}$ и $|W_h(y)| = 2^{n/2}$, значит,

$$\begin{cases} \Big|\sum\limits_{x\in\mathbb{Z}_2^n}(-1)^{\langle x,y\rangle\oplus f(x)}\Big| = |W_f(y)| = 2^{n/2}, \\ \Big|\sum\limits_{x\in\mathbb{Z}_2^n}(-1)^{\langle x,y\rangle\oplus f(x)\oplus y_{n+1}\oplus\big(\bigoplus\limits_{i=1}^{n} x_i\big)}\Big| = |W_h(y)| = 2^{n/2}, \end{cases}$$

и для каждого фиксированного y_{n+2} либо

$$1+(-1)^{y_{n+1}+y_{n+2}} = 0, \quad 1-(-1)^{y_{n+1}+y_{n+2}} = 2,$$

либо

$$1+(-1)^{y_{n+1}+y_{n+2}} = 2, \quad 1-(-1)^{y_{n+1}+y_{n+2}} = 0.$$

Итак, $|W_g(y, y_{n+1}, y_{n+2})| = 2^{n/2}\cdot 2 + 2^{n/2}\cdot 0 = 2^{(n+2)/2}$. Тем самым $g(x, x_{n+1}, x_{n+2})$ является бент-функцией от $n+2$ переменных. Теорема 3 доказана.

Выражаю благодарность научному руководителю Н. Н. Токаревой и С. В. Августиновичу за полезные советы.

ЛИТЕРАТУРА

1. **Корсакова Е. П.** Классификация графов АНФ квадратичных бент-функций от шести переменных // Прикл. дискрет. математика. Приложение. — 2011. — № 4. — С. 13–14.
2. **Логачев О. А., Сальников А. А., Ященко В. В.** Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.
3. **Токарева Н. Н.** Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken, Germany: LAP LAMBERT Acad. Publ., 2011. — 180 с.
4. **Carlet C.** On the confusion and diffusion properties of Maiorana — McFarland's and extended Maiorana — McFarland's functions // J. Complexity. — 2004. — Vol. 20. — P. 182–204.
5. **Carlet C.** Boolean functions for cryptography and error correcting codes // Boolean methods and models. Cambridge Univ. Press (P. Hammer, Y. Crama, eds.), to appear. `www-rocq.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts.pdf`
6. **Dillon J. F.** Elementary Hadamard difference sets // Thes. . . . doct. phylosophy (mathematics). Univ. Maryland, College Park, 1974. — 118 p.
7. **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.

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

Корсакова Екатерина Павловна,
e-mail: korsakova.katerina@gmail.com

Статья поступила
27 сентября 2012 г.

Переработанный вариант —
19 декабря 2012 г.