ISSN 1990-4789, Journal of Applied and Industrial Mathematics, 2012, Vol. 6, No. 3, pp. 306–317. © Pleiades Publishing, Ltd., 2012.
Original Russian Text © N.A. Kolomeets, 2012, published in Diskretnyi Analiz i Issledovanie Operatsii, 2012, Vol. 19, No. 1, pp. 41–58.

Enumeration of the Bent Functions of Least Deviation from a Quadratic Bent Function

N. A. Kolomeets*

Sobolev Institute of Mathematics, pr. Akad. Koptyuga 4, Novosibirsk, 630090 Russia

Received April 5, 2011; in final form, September 24, 2011

Abstract—We study a construction of the bent functions of least deviation from a quadratic bent function, describe all these bent functions of $2k$ variables, and show that the quantity of them is $2^k(2^1+1)\dots(2^k+1)$. We find some lower bound on the number of the bent functions of least deviation from a bent function of the Maiorana–McFarland class.

DOI: 10.1134/S1990478912030052

Keywords: *bent function, minimum distance, quadratic bent function*

INTRODUCTION

Bent functions are the most distant from the class of affine Boolean functions of an even number of variables. O. Rothuaus was the first to consider bent functions [9]. They have many applications in cryptography, coding theory, and information theory. Nevertheless, there are still many unsolved problems. The most important problem consists in describing all bent functions. In particular, the determination of the structures of bent functions is on the agenda.

In this paper, we consider a construction of the bent functions of least deviation from a quadratic bent function. In [1], it is shown that the two bent functions of $2k$ variables are at distance 2^k (i.e., at the minimum possible distance between two different bent functions) if and only if they differ on an affine subspace of dimension k and are affine on it. We describe all bent functions that are of least deviations from a quadratic bent function (Theorem 1) and also show that the number of these bent functions of $2k$ variables is $2^k(2^1+1)\dots(2^k+1)$ (Theorem 2).

It is known that all quadratic bent functions are affinely equivalent to the function

$$x_1x_{k+1} \oplus x_2x_{k+2} \oplus \dots \oplus x_kx_{2k}$$

which belongs to the Maiorana–McFarland class. Therefore, we further consider the more general problem of finding a lower bound on the number of the bent functions of least deviation from an arbitrary bent function from the Maiyorana–McFarland class (Theorem 3). In conclusion, there are some assertions and a hypothesis of estimating the number of bent functions at distance 2^k from an arbitrary bent function.

1. DEFINITIONS

Let $\mathbb{Z}_2^n$ denote the n-dimensional vector space over $\mathbb{Z}_2$, and let $\oplus$ stand for the modulo-2 addition operation.

The *distance* between two Boolean functions is represented by the Hamming distance (i.e., the number of vectors at which the functions are different). The degree of the algebraic normal form of a Boolean function is called the *algebraic degree* of the function. A Boolean function is called *affine* if its algebraic degree is at most 1, and *quadratic* if its algebraic degree is equal to 2. A set $L \subseteq \mathbb{Z}_2^n$ is called an *affine subspace* if $L = a \oplus U$, where a is a vector of $\mathbb{Z}_2^n$ and U, a linear subspace in $\mathbb{Z}_2^n$. For vectors u and v, we denote their 2-modulo inner sum by $\langle u, v\rangle$. A Boolean function f of n variables is

*E-mail: nkolomeec@gmail.com

called *affine on the set* $D \subseteq \mathbb{Z}_2^n$ if there are $a \in \mathbb{Z}_2^n$ and $c \in \mathbb{Z}_2$ such that $f(x) = \langle a, x\rangle \oplus c$ for all $x \in D$. Recall that

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

is called the *Walsh–Hadamard transform* of f, and the numbers $W_f(v)$, the *Walsh–Hadamard coefficients* of f. A Boolean function f of $2k$ variables is called a *bent function* if all its Walsh–Hadamard coefficients are equal to $\pm 2^k$. The set of all bent functions of $2k$ variables is denoted by $\mathfrak{B}_{2k}$. A survey of papers and results on bent functions can be found, for example, in [4].

Two Boolean functions f and g of n variables are called *affinely equivalent* if there exist some nondegenerate $n \times n$ matrix A, a vector b of length n, and an affine function l of n variables such that

$$g(x) = f(Ax \oplus b) \oplus l(x).$$

Assume that $D \subseteq \mathbb{Z}^n$. Let Ind_D denote the *indicator of* D; i.e., the Boolean function of n variables equal to 1 only at the elements of D. Let $a^{(i)}$ denote the ith column of a matrix A and a_{ij}, the entry of A.

The minimum possible distance between two different bent functions of $2k$ variables is 2^k. Denote this distance by d_k. In [1], the following is proven:

Proposition 1. *Let $f \in \mathfrak{B}_{2k}$ and $L \subseteq \mathbb{Z}_2^{2k}$. Then $g(x) = f(x) \oplus \mathrm{Ind}_L(x)$ is the bent function at distance d_k from f if and only if L is an affine subspace of dimension k and f is affine on L.*

Proposition 1 gives an approach for constructing bent functions by means of a subspace of dimension k (it can be found in [2, 6]).

In our work, we use this for constructing the bent functions at distance d_k; i.e., we reduce the problem under study to finding in $\mathbb{Z}_2^{2k}$ some affine subspaces of dimension k on which a given bent function is affine.

2. THE BENT FUNCTIONS OF LEAST DEVIATION FROM A QUADRATIC BENT FUNCTION

Let us construct all bent functions at distance d_k from the bent function

$$x_1x_{k+1} \oplus x_2x_{k+2} \oplus \cdots \oplus x_kx_{2k}$$

and calculate their quantity.

Proposition 2 [7]. *Every quadratic bent function of $2k$ variables is affinely equivalent to the bent function*

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

Note that the affine equivalent bent functions have the same number of bent functions at every given distance. Therefore, by Proposition 2, it suffices to count the number of the bent functions at distance d_k from f_0^{2k}. Then, the same will be the number of bent functions at distance d_k from each of the other quadratic bent functions.

For consideration of the bent functions at distance d_k from f_0^{2k}, we present some statements about the affinity of functions in general and f_0^{2k}, in particular, on a subspace (Section 3), consider some convenient bases for representing the subspaces (Section 4), describe the affine subspaces of dimension k on which f_0^{2k} is affine (Section 5), count these subspaces (Section 6), and give some examples in the cases of small dimension (Section 7).

3. AFFINITY OF BOOLEAN FUNCTIONS ON SUBSPACES

We can associate a basis matrix with each linear subspace L and assume that the columns of the matrix present some basis of L. The following allows us to determine whether a Boolean function is affine on a subspace or not:

Proposition 3. *Let g be an arbitrary Boolean function of n variables and B, an $n \times k$ basis matrix for a linear subspace L of dimension k in $\mathbb{Z}_2^n$. Then g is affine on L if and only if $g'(u) = g(Bu)$ of k variables is an affine function.*

The proof of Proposition 3 is trivial.

The following provides a criterion for the affinity of f_0^{2k} on a subspace with a basis matrix B:

Lemma 1. *Let B be an arbitrary $2k \times k$ basis matrix of a linear subspace L of dimension k in $\mathbb{Z}_2^{2k}$, and let the matrices $A = (a_{ij})$ and $Y = (y_{ij})$ be formed by the first k and the last k rows of B, respectively. Then f_0^{2k} is affine on L if and only if*

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

where $a^{(i)}$ and $y^{(i)}$ are the ith columns of A and Y.

Proof. By Proposition 3, f_0^{2k} is affine on L if and only if the function $f'(u) = f_0^{2k}(Bu)$ of k variables is affine.

The function f' has the following algebraic normal form:

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

The degree of f' is obviously at most 2; therefore, for its affinity, it is necessary and sufficient that all coefficients at $u_i u_j$ for $i \neq j$ were equal to 0; i.e.,

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

The proof of Lemma 1 is over. □

Proposition 4. *Let g be an arbitrary function quadratic and affine on a certain affine subspace $u \oplus L$. Then g is also affine on each adjacent class of the subspace L.*

Proof. Note that g is affine on $a \oplus L$ if and only if $g(x \oplus a)$ is affine on L for every vector a. Since g is quadratic, the algebraic normal form of $g(x \oplus a)$ differs from that of g only by its affine part. Therefore, g is affine on L if and only if $g(x \oplus a)$ is affine on L. At the same time, g is affine on $u \oplus L$ by the assumption. Consequently, g is affine on $a \oplus L$ for all a. The proof is over. □

4. REPRESENTATION FOR SUBSPACES

We describe the linear subspace using the basis matrices of Gauss–Jordan type (or GJB-matrices, in short). Note that, in our notation, the basis vectors are the columns of the basis matrix.

Definition 1. Let G be a matrix with k columns formed by the nonzero vectors $u^{(1)}, \dots, u^{(k)}$. Let $\ell(u^{(i)}) = \min \{ j \mid u_j^{(i)} \neq 0 \}$. The matrix G is a GJB-*matrix* if the following conditions are met:

$$\text{(i) if } i_1 < i_2 \text{ then } \ell(u^{(i_1)}) < \ell(u^{(i_2)}); \qquad \text{(ii) if } i_1 \neq i_2 \text{ then } u^{(i_1)}_{\ell(u^{(i_2)})} = 0.$$

In this case, we denote the set $\{\ell(u^{(1)}), \dots, \ell(u^{(k)})\}$ by $\ell(G)$. All rows of G with the numbers from $\ell(G)$ will be called the *leading rows*, the remaining, *nonleading*. We denote the subspace with the basis $u^{(1)}, \dots, u^{(k)}$ by L_G. Note that the columns of G actually are the basis vectors of the space L_G, and $G^\top$ is called also the *reduced stepped matrix*.

Example 1. For a subspace of dimension 3 in $\mathbb{Z}_2^6$ with $\ell(G) = \{1, 3, 5\}$, the following is a GJB-matrix:

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

Proposition 5. *Each linear subspace has a unique* GJB-*matrix.*

Proof. Given a linear subspace, we can define its GJB-matrix G as follows: the ith column $u^{(i)}$ of G is a vector of the space L_G which has the most number of junior zeros as well as $u^{(i)}_{\ell(u_j)} = 0$ for all $j > i$. This implies that any subspace L has the GJB-matrix.

Let us prove the uniqueness of such a matrix. Suppose that, for some i, there are two vectors $u^{(i)}$ and $u'^{(i)}$ satisfying the above property. Then $u^{(i)} \oplus u'^{(i)}$ has at least one junior zero more, and the coinciding coordinates of $u^{(i)}$ and $u'^{(i)}$ are zero for their sum.

The proof is complete. □

Thus, all kinds of $n \times k$ GJB-matrices correspond bijectively to all kinds of linear subspaces of dimension k in $\mathbb{Z}_2^n$.

5. CONSTRUCTING THE BENT FUNCTIONS OF LEAST DEVIATION FROM A QUADRATIC BENT FUNCTION

Introduce the definition of admissible GJB-matrix. Let a GJB-matrix G for a subspace of dimension k in $\mathbb{Z}_2^{2k}$ have the form

$$\left(\begin{array}{c|c} A & 0 \\ \hline Z & Y \end{array}\right), \qquad (*)$$

where A and Y are some $k \times t$ and $k \times (k-t)$ matrices. Since G is a GJB-matrix, the following hold:

(i) A and Y are GJB-matrices; (ii) all rows of Z with numbers from $\ell(Y)$ are zero.

Remove from Z and A all rows with the numbers from $\ell(Y)$ and denote the resultants by Z' and A' respectively. Impose the additional conditions on the elements of Z':

(iii) $L_Y = L_A^{\perp}$;

(iv) the elements of Z' are solutions of the system of equations

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

where the matrix M of the system has size $(t(t-1)/2) \times t^2$ (if $t \le 1$ then there is no restrictions on the elements of Z').

If the above conditions are true then G is called an *admissible matrix* of order t.

The following describes all affine subspaces on which the quadratic bent function is affine:

Theorem 1. *Let L be an affine subspace of dimension k in $\mathbb{Z}_2^{2k}$. The bent function f_0^{2k} is affine on L if and only if L is a linear subspace with an admissible GJB-matrix or with an adjacent class of such subspace.*

Proof. By Proposition 4, we can assume without loss of generality that L is a linear subspace.

Let G be a GJB-матрица for the subspace L. Denote the upper half of G by D and its lower part by V. Let $d^{(i)}$ and $v^{(i)}$ be the ith columns of D and V, respectively. By Lemma 1, f_0^{2k} is affine on L if and only if

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

Consider this as a system of equations with respect to the variables $v^{(i)} \in \mathbb{Z}_2^k$ and the coefficients $d^{(i)} \in \mathbb{Z}_2^k$. It is obvious that every GJB-matrix G can be expressed as $(*)$, where, A and Y are some $k \times t$ and $k \times (k-t)$ GJB-matrices with $t \in \{0, \dots, k\}$, respectively. Then, for the columns of Y, the system (2) has the form

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

or simply

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

The equations (2) for the columns of Z can be divided into the two parts:

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

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

However, (3) imply $\langle a^{(j)}, y^{(i-t)} \rangle = 0$. Therefore, (2) are transformed into (3) and (4) for $y^{(i)}$ and $z^{(i)}$ respectively.

Since G is a GJB-matrix, the rows of Z with the numbers from $\ell(Y)$ are zero. Consequently, (4) can be written as

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

where $a'^{(i)}$ and $z'^{(j)}$ are the columns of A' and Z', respectively, obtained from A and Z by deleting the rows with numbers from $\ell(Y)$.

Thus, f_0^{2k} is affine on L if and only if the relations (3) and (6) hold.

All elements of $L_A^\perp$ are the solutions $y^{(j)}$ of (3). However, Y is the GJB-matrix; and so, it is uniquely determined by A as the GJB-matrix for $L_A^\perp$.

Equations (6) can be written in the form of the system (1) of linear equations considering

$$({z'^{(1)}}^\top, \dots, {z'^{(t)}}^\top)^\top$$

as the column of variables. Consequently, (2) is satisfied if and only if the matrix G is admissible.

The proof of Theorem 1 is complete. □

Here are some extreme cases: for $t = 0$, there is the unique admissible GJB-matrix $B = \left(\frac{0}{E}\right)$; and, for $t = k$, the admissible GJB-matrices have the form $B = \left(\frac{E}{T}\right)$, where T is an arbitrary symmetric matrix. There are $2^{k(k+1)/2}$ of such matrices.

Consider the example of constructing a linear subspace on which $f_0^8(x)$ is affine; i.e., let $k = 4$. The general form of the basis matrix B is defined by $(*)$. Take as A the following matrix of rank 2, obtain one of the basis matrices of the subspace L_Y, and choose the GJB-matrix Y for the subspace L_Y (here $\ell(Y) = \{1, 2\}$):

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

Hence, $A' = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, and then $M = \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix}$. Thus, Z' has the form $Z' = \begin{pmatrix} c_1 \oplus c_2 & c_3 \\ c_1 & c_2 \end{pmatrix}$.

For example, for $c_1, c_2, c_3 = 1$, we obtain the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

In result, we arrive at the GJB-matrix B for L_B on which the function $x_1x_5 \oplus x_2x_6 \oplus x_3x_7 \oplus x_4x_8$ is affine:

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

6. COUNTING THE NUMBER OF BENT FUNCTIONS OF LEAST DEVIATION FROM A QUADRATIC BENT FUNCTION

We proceed to counting the number of bent functions at distance d_k from an arbitrary quadratic bent function:

Lemma 2. *The rows of the matrix M of form* (1) *are linearly independent.*

Proof. Let the matrix Y' be formed by all nonleading rows of Y. Note that Y' has size $t \times t$. We show that the vectors $a'^{(1)}, \ldots, a'^{(t)}$ are linearly independent. Note also that this implies the linear independence of the rows of M.

Assume that there are some distinguished $i_1, \ldots, i_p$ such that

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

Then, for all $j = 1, \ldots, k - t$,

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

Also, for all $q = 1, \ldots, p$,

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

Since $L_Y = L_A^{\perp}$, we have $\langle y^{(j)}, a^{(i_q)} \rangle = 0$ and, therefore,

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

The elements $a_{\ell(y^{(j)})i_q}$ are all those deleted from the columns with numbers $i_1, \ldots, i_p$. Hence, we obtain

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

but the vectors $a^{(1)}, \ldots, a^{(t)}$ are linearly independent. We arrive at a contradiction. Hence, $a'^{(1)}, \ldots, a'^{(t)}$ are linearly independent. The proof of Lemma 2 is complete. □

Let S_k^t denote the number of linear subspaces of dimension t in $\mathbb{Z}_2^k$. Note that S_k^t can be calculated as follows:

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

which can be found, for example, in [3].

Lemma 3. *For arbitrary $k > 0$ and $0 < t < k$, $S_k^t = S_{k-1}^t + 2^{k-t} S_{k-1}^{t-1}$.*

To prove Lemma 3, it suffices to use the above formula.

Theorem 2. *Every quadratic bent function of $2k$ variables has exactly*

$$2^k \cdot (2^1 + 1) \cdots (2^k + 1)$$

bent functions at distance d_k.

Proof. By Proposition 2, every quadratic bent function of $2k$ variables is affinely equivalent to f_0^{2k}. We show that this bent function is affine exactly on $\sum_{t=0}^{k} 2^{t(t+1)/2} S_k^t$ linear subspaces of dimension k. Then, there will be 2^k more affine subspaces; and, hence, we obtain the number of bent functions at distance d_k by Proposition 1.

By Theorem 1, it suffices to calculate the number of the admissible $2k \times k$ GJB-matrices since the different GJB-matrices correspond to different linear subspaces. For an admissible GJB-matrix of size t, we consider the corresponding matrices A, Y, and Z. The matrix A of rank t can be chosen in S_k^t ways. Then Y is uniquely determined. For a fixed matrix A, by Theorem 1 and Lemma 2, we can chose $2^{t(t+1)/2}$ matrices Z. Thus, every affine quadratic function is affine on exactly

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

linear subspaces. Let us simplify this formula.

We prove now that, for $k > 0$, $C_k = (2^k + 1) C_{k-1}$. By Lemma 3, $S_k^t = S_{k-1}^t + 2^{k-t} S_{k-1}^{t-1}$ for each t such that $0 < t < k$. Note that, for the extreme values of t, we have $S_k^0 = S_{k-1}^0$ and $S_k^k = 2^{k-k} S_{k-1}^{k-1}$. Hence,

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

The first sum is equal to C_{k-1}. In the second sum, we replace t with $i + 1$ and obtain

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

Since $k - (i+1) + (i+1)(i+2)/2 = k + i(i+1)/2$, we have

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

as well as $C_1 = 3$. Hence, $C_k = (2^1 + 1) \cdots (2^k + 1)$.

The proof of Theorem 2 is complete. □

It is easy that

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

Therefore, more than a third of bent functions at distance d_k from a quadratic bent function are rather simple to obtain, namely, by means of admissible GJB-matrices of the form $G = \left(\frac{E}{T}\right)$, where T is an arbitrary symmetric $k \times k$ matrix.

Also note that all bent functions at distance d_k from an arbitrary quadratic bent function are affinely equivalent to the bent functions of the Maiorana–McFarland class.

7. SOME EXAMPLE IN THE CASE OF SMALL DIMENSION

Denote an arbitrary element of $\mathbb{Z}_2$ by $*$. Then,for $k = 2$, all admissible GJB-matrices are as follows (the leading elements are highlighted):

for $t =$, we have the only matrix

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

for $t = 1$, we obtain $3 \cdot 2 = 6$ matrices of the form

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

and, for $t = 2$, there are $1 \cdot 2^3 = 8$ matrices of the form

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

where a is some element of $\mathbb{Z}_2$. We obtain eventually fifteen linear subspaces. Also taking all adjacent classes of the subspaces with the above basis matrices, we have sixty affine subspaces on which f_0^4 is affine.

For $k = 3$, the function f_0^6 is affine on the linear subspaces with the following admissible GJB-matrices:

for $t = 0$, there is the only matrix a matrix

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

for $t = 1$, we obtain $7 \cdot 2 = 14$ matrices of the form

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

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

for $t = 2$, we have $7 \cdot 2^3 = 56$ matrices of the form

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

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

and, for $t = 3$, we obtain $1 \cdot 2^6 = 64$ matrices of the form

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

where a, b, and c are some elements of $\mathbb{Z}_2$. Thus, we find 135 linear subspaces. Accounting also for all adjacent classes of the given subspaces, we obtain 1080 affine subspaces on which f_0^6 is affine.

The following table presents the number of bent functions at distance d_k from every quadratic bent function for small number of variables:

2k	2	4	6	8	10	12
Number	6	60	1080	36720	2423520	315057600

8. A LOWER ESTIMATE OF BENT FUNCTIONS OF LEAST DEVIATION FROM BENT FUNCTIONS OF THE MAIORANA–McFARLAND CLASS

Since f_0^{2k} belongs to the Maiorana–McFarland class, all quadratic bent functions are affinely equivalent to the bent functions of this class. Therefore, we consider the more general problem of finding a lower bound on the number of bent functions at the distance d_k from the functions of this class.

The Maiorana–McFarland class contains the bent function of the form

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

where $x, y \in \mathbb{Z}_2^k$, ψ is a Boolean function of k variables, and π is a permutation on $\mathbb{Z}_2^k$. We denote this class by $\mathcal{M}_{2k}$. More detailed information on it can be obtained in [8].

To find a lower bound, we need the following assertions:

Proposition 6. *Let f be a Boolean function of n variables, let L be a linear subspace in $\mathbb{Z}_2^n$, and let D_1 and D_2 be various adjacent classes from L such that*

$$f|_{D_1}(x) = \langle a, x\rangle \oplus c, \qquad f|_{D_2}(x) = \langle a, x\rangle \oplus c'$$

for some vector $a \in \mathbb{Z}_2^n$ and constants c and c'. Then f is affine on $D_1 \cup D_2$.

Proof. Without loss of generality, assume that $D_1 = L$ and denote D_2 by D. Clearly, the union of a linear subspace and its adjacent class is a linear subspace. We denote $L \cup D$ by L'.

Show that f is affine on L'.

If $c = c'$ then the assertion is obvious. Assume that $c' = c \oplus 1$. Then $f|_L(x) = \langle a, x\rangle \oplus c$ and $f|_D(y) = \langle a, y\rangle \oplus c \oplus 1$. Hence, for all $w \in L^\perp$ and $b = a \oplus w$,

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

Let $v \in D$. Also, for every $x \in L$ and $y \in D$, we have

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

It is clear that there exists $w' \in L^{\perp}$ such that $\langle w', v\rangle = 1$. If it is not the case then $v \in L^{\perp\perp} = L$. However, L and D are distinguished; a contradiction. Hence, for $b = a \oplus w'$, we have $\langle b, y\rangle = \langle a, y\rangle \oplus 1$. Consequently,

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

as well as $f|_L(x) = \langle b, x\rangle \oplus c$. The proof of Proposition 6 is complete. □

Lemma 4. *A bent function $f \in \mathfrak{B}_{2k}$ cannot be affine on an affine subspace of dimension greater than k.*

This can be found in [6]. To prove the lemma, it suffices to assume the converse and apply Proposition 1 several times.

Proposition 7. *Let $f \in \mathfrak{B}_{2k}$ be a bent function and let L be as subspace of dimension l in $\mathbb{Z}_2^{2k}$ such that f is affine on every adjacent class of it. Then, for each adjacent class $a \oplus L$, there exist exactly 2^{2k-l} vectors w such that $f|_{a\oplus L}(x) = \langle w, x\rangle \oplus c_w$ for some constant c_w.*

To prove Proposition 7, it suffices, for $x \in a \oplus L$, to solve the equations $\langle w \oplus w_0, x\rangle = \text{const}$ with respect to w.

Lemma 5. *Let $f \in \mathfrak{B}_{2k}$ and let L be a linear subspace of dimension k in $\mathbb{Z}_2^{2k}$ such that the bent function f is affine on every adjacent class of it. Then, for $w \in \mathbb{Z}_2^{2k}$, there is $u \in \mathbb{Z}_2^{2k}$ such that, for some constant c,*

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

Proof. Assume that there are two different adjacent classes D_1 and D_2 for the subspace L and a vector w such that

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

Then, by Proposition 6, f is affine on the affine subspace $D_1 \cup D_2$ of dimension greater than k; a contradiction with Lemma 4. Next, we use Proposition 7. The proof is over. □

Theorem 3. *Let f be a bent function of $2k$ variables of the Maiorana–McFarland class. Then the number of bent functions at distance d_k from f is at least $2^{2k+1} - 2^k$.*

Proof. By Proposition 1, it suffices to calculate the affine subspace of dimension k on which f is affine. Let

$$L = \{(x, 0, \ldots, 0) \mid x \in \mathbb{Z}_2^k\} \subseteq \mathbb{Z}_2^{2k}.$$

Obviously, L is a linear subspace. Also, every function of the Maiorana–McFarland class is affine on L and each its adjacent class. Let us count the adjacent classes of the subspaces that intersect L on 2^{k-1} elements.

The subspace L contains exactly $2^k - 1$ different linear subspaces U of dimension $k - 1$. Thus, the affine subspace $u \oplus U$ can be selected by exactly $2^{k+1} \cdot (2^k - 1)$ ways. It is also clear that $u \oplus U$ is contained in $u \oplus L$.

By Proposition 7, there are exactly 2^{k+1} vectors w_1 such that $f|_{u\oplus U}(x) = \langle w_1, x\rangle \oplus c_{w_1}$. However, for $u \oplus L$, there exist exactly 2^k vectors w_2 such that $f|_{u\oplus L}(x) = \langle w_2, x\rangle \oplus c_{w_2}$. Therefore, by Lemma 5, there exists an adjacent class $v \oplus L$ different from $u \oplus L$ and such that, for some vector w and constants c_1 and c_2, we have

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

The set $v \oplus L$ contains exactly two different adjacent classes of the subspace U. We denote them by $a \oplus U$ and $b \oplus U$. Thus, by Proposition 6, f is affine on the affine subspaces $(u \oplus U) \cup (a \oplus U)$ and $(u \oplus U) \cup (b \oplus U)$ of dimension k. Since we choose an unordered pair of the adjacent classes, we obtain

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

different affine subspaces of dimension k on which f is affine. Also, f is affine on all adjacent classes of the subspace L.

The proof of Theorem 3 is complete. □

9. OTHER ESTIMATES AND HYPOTHESES

Consider a trivial upper estimate on the number of bent functions at distance d_k from some given bent function.

Proposition 8. *Let $f \in \mathfrak{B}_{2k}$. Then the number of bent functions at distance d_k from f is at least 2^{k^2+2k}.*

This result was obtained by an upper estimate on the number of affine subspaces of the required dimension using the formula for S_k^t. Thus, the number of the bent functions at distance d_k from a quadratic bent function is greater than the square root of the trivial upper estimate.

Consider a hypothesis about maximum number of the bent functions at distance d_k from a given bent function:

Hypothesis. *Each quadratic bent function has the maximum possible number of bent functions at distance d_k; i.e., the upper bound on the number of bent functions at distance d_k from an arbitrary bent function is $2^k(2^1+1)\cdots(2^k+1)$.*

Note that the lower bound on the number of bent functions at distance d_k from a given bent function is zero, because there are bent functions which have no bent functions at distance d_k. The problem of the existence of bent functions at distance d_k from a given function is related with the concepts of the normal and abnormal bent functions. In particular, from [5] it follows that there are some bent functions of $2k$ variables that are not affine on any affine subspace of dimension k. Thus, not for all bent functions we can construct a bent function at distance d_k.

Example 2 [5]. For even $n \geqslant 14$, the bent function

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

has no bent functions at distance d_k. Here, by $\mathrm{tr}(\cdot)$ is denoted the trace of $GF(2^{14})$ into $GF(2)$, and by α, a corresponding element $\mathbb{Z}^2$. The vector $(x_1,\ldots,x_{14})$ is also considered as an element of $GF(2^{14})$.

ACKNOWLEDGMENTS

The author was supported by the Russian Foundation for Basic Research (project no. 11–01–00997) and the Federal Target Program "Scientific and Scientific-Pedagogical Personnel of Innovative Russia" for 2009–2013 (State contract no. 02.740.11.0362).

REFERENCES

1. N. A. Kolomeets and A. V. Pavlov, "Properties of the Bent Functions Being at Minimum Distance from Each Other," Prikl. Diskret. Mat. No. 4, 5–21 (2009).
2. O. A. Logachev, A. A. Sal'nikov, and V. V. Yashchenko, *Boolean Functions in Coding Theory and Cryptology* (MTsNMO, Moscow, 2004) [in Russian].
3. F. J. MacWilliams and N. J. A. Sloane, *Theory of Error Correcting Codes* (Amsterdam, North-Holland, 1977; Svyaz', Moscow, 1979).
4. N. N. Tokareva, *Nonlinear Boolean Functions*: *Bent Functions and Their Generalizations* (Lambert Acad. Publ., Saarbrucken, 2011).
5. A. Canteaut, M. Daum, H. Dobbertin, and G. Leander, "Finding Nonnormal Bent Functions," Discrete Appl. Math. **154** (2), 202–218 (2006).
6. C. Carlet, "Boolean Functions for Cryptography and Error Correcting Codes," in *Boolean Methods and Models* (to appear) [Prelim. version is available at http://www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf].
7. J. F. Dillon, "A Survey of Bent Functions," The NSA Techn. J., pp. 191–215 (1972).
8. R. L. McFarland, "A Family of Difference Sets in Noncyclic Groups," J. Combin. Theory Ser. A, **15** (1), 1–10 (1973).
9. O. Rothaus, "On Bent Functions," J. Combin. Theory Ser. A, **20** (3), 300–305 (1976).