The graph of minimal distances of bent functions and its properties[*]

Nikolay Kolomeec
Sobolev Institute of Mathematics, Novosibirsk, Russia
Novosibirsk State University, Novosibirsk, Russia

E-mail: nkolomeec@gmail.com

Abstract

A notion of the graph of minimal distances of bent functions is introduced. It is an undirected graph (V, E) where V is the set of all bent functions in $2k$ variables and $(f, g) \in E$ if the Hamming distance between f and g is equal to 2^k (it is the minimal possible distance between two different bent functions). The maximum degree of the graph is obtained and it is shown that all its vertices of maximum degree are quadratic. It is proven that a subgraph of the graph induced by all functions affinely equivalent to Maiorana—McFarland bent functions is connected.

Keywords Boolean functions, bent functions, the minimal distance, affinity

1 Introduction

Bent functions are Boolean functions in even number of variables that have maximal possible nonlinearity. They were proposed by O. Rothaus [17]. Bent functions have a lot of applications in algebra, combinatorics, coding theory, cryptography, see [19]. However, there are still many open questions concerning bent function, for example, see [4].

This work is devoted to the minimal Hamming distance between two bent functions. It is equal to 2^k for bent functions in $2k$ variables. For the given bent function f in $2k$ variables any bent function at the distance 2^k from f can be obtained in the following way: we chose some k-dimensional affine subspace L such that f is affine on it and just invert values of f on L, see [14]. For the first time this approach to construct new bent functions by affine subspaces was proposed in [2].

It seemed some properties can be formulated easier in terms of graph of minimal distances GB_{2k}. It is an undirected graph (V, E) where V is the set of all bent functions in $2k$ variables and $(f, g) \in E$ if the Hamming distance between f and g is equal to 2^k. For example, the number of bent functions at the distance 2^k from the given bent function f is the degree of vertex f in GB_{2k}; an existence of bent functions $h_1, \ldots, h_n$ for two bent functions f, g such that $\mathrm{dist}(f, h_1) = 2^k$, $\mathrm{dist}(h_n, g) = 2^k$ and $\mathrm{dist}(h_i, h_{i+1}) = 2^k$ for $i \in \{1, \ldots, n-1\}$ is just existence of a path between f and g in GB_{2k}.

[*]The author was supported by the Russian Foundation for Basic Research (project no. 15-31-20635).

In this work the maximum degree of GB_{2k} is obtained. It is equal to $2^k(2^1+1)\dots(2^k+1)$. Moreover, it is proven that any vertex of maximum degree is a quadratic bent function. In order to prove that, a notion of completely affinely decomposable Boolean function of order k is introduced. Such function is either affine on each coset of a k-dimensional affine subspace or not affine on any coset; and the function should be affine on at least one k-dimensional affine subspace. It is obtained that completely affinely decomposable functions are either affine or quadratic; their complete classification depending on k is done.

Next, a subgraph GM_{2k} of GB_{2k} induced by all bent functions affinely equivalent to Maiorana—McFarland bent functions is considered. A lower bound of a vertex degree in GM_{2k} is obtained and it is proven that GM_{2k} is connected. As a consequence, GB_2, GB_4, GB_6 are connected too. But in general GB_{2k} is not connected due to existing isolated vertices (starting with $2k=14$), such bent functions were found in [5].

Note that results of the work were announced in [19].

2 Definitions

2.1 Boolean functions

Let us give definitions. *A Boolean function* in n variables is a mapping $f:\mathbb{F}_2^n\to\mathbb{F}_2$. Denote by $\mathcal{F}_n$ the set of all Boolean functions in n variables. *The Hamming distance* $\operatorname{dist}(f,g)$ between two Boolean functions $f,g\in\mathcal{F}_n$ is the number of $x\in\mathbb{F}_2^n$ such that $f(x)\neq g(x)$. Define by $\langle x,y\rangle = x_1y_1\oplus x_2y_2\oplus\ldots\oplus x_ny_n$ inner product of two vectors $x,y\in\mathbb{F}_2^n$. Denote by $\operatorname{supp}(f)$, $f\in\mathcal{F}_n$, the set $\{x \,:\, f(x)=1, x\in\mathbb{F}_2^n\}$. *The weight* $\operatorname{wt}(f)$ of Boolean function $f\in\mathcal{F}_n$ is equal to $|\operatorname{supp}(f)|$. *The restriction* of a Boolean function $f\in\mathcal{F}_n$ on the set $S\subseteq\mathbb{F}_2^n$ is a mapping $f|_S : S\to\mathbb{F}_2$, where $f|_S(x)=f(x)$ for all $x\in S$. *A subfunction* $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}$ of function f is a restriction of f on the *face* $\{x\in\mathbb{F}_2^n \mid x_{i_1}=b_1,\ldots,x_{i_k}=b_k\}$.

A Boolean function $f\in\mathcal{F}_n$ is called *balanced* if $\operatorname{wt}(f)=2^{n-1}$. Balancedness is generalized to the restriction of a Boolean function: $f|_S$ is called *balanced*, where $S\subseteq\mathbb{F}_2^n$ and $|S|$ is even, if $|\{x\in S \mid f|_S(x)=1\}|=|S|/2$.

2.2 Algebraic normal form

Representation of $f\in\mathcal{F}_n$ in the form

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

where $a_0, a_{i_1\ldots i_k}\in\mathbb{F}_2$, is called *algebraic normal form* (*ANF*), $x_{i_1}\ldots x_{i_k}$ is called *a monomial of degree* k, $a_{i_1\ldots i_k}, a_0$ are *coefficients. The degree* $\deg f$ is the length of the longest monomial with nonzero coefficient (and $-\infty$ if all coefficients are zero). There is the only way to represent f in such form.

A Boolean function is called *affine* if its degree is not more than 1, in other words, it is a function of the form

$$\ell_{a,c}(x)=\langle a,x\rangle\oplus c \text{ for some } a\in\mathbb{F}_2^n, c\in\mathbb{F}_2.$$

Denote by $\mathcal{A}_n$ the set of all affine functions in n variables.

A Boolean function is called *quadratic* if its degree is equal to 2.

Derivative function $D_\alpha f$ of $f \in \mathcal{F}_n$ *in the direction* $\alpha \in \mathbb{F}_2^n$ is the function $f(x) \oplus f(x \oplus \alpha)$. Note that if $\deg f \geq 0$, then $\deg D_\alpha f < \deg f$ for any direction $\alpha \in \mathbb{F}_2^n$.

2.3 Affine equivalence

Two Boolean functions $f, g \in \mathcal{F}_n$ are called *affinely equivalent* if there exist an invertible n-by-n binary matrix A, vector $b \in \mathbb{F}_2^n$ and affine function $\ell \in \mathcal{A}_n$ such that

$$f(x) = g(xA \oplus b) \oplus \ell(x) \text{ for all } x \in \mathbb{F}_2^n.$$

Note that $\mathrm{dist}(f, g) = \mathrm{dist}(f(xA \oplus b) \oplus \ell(x), g(xA \oplus b) \oplus \ell(x))$.

The notion of affine equivalence is used with addition of an affine function instead of classic definition $f(x) = g(xA \oplus b)$ since considered transformations form the group of automorphisms of the set of bent functions, see [18]. In these terms some results of the work can be formulated shorter.

It holds *Dickson's theorem* for a quadratic Boolean function: any quadratic $f \in \mathcal{F}_n$ can be reduced by transformation of the form $f(xA)$, where A is an invertible n-by-n binary matrix, to the form

$$x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2t-1}x_{2t} \oplus \ell(x)$$

for some $\ell \in \mathcal{A}_n$ and t, $1 \leq t \leq n/2$.

Thus, any quadratic $f \in \mathcal{F}_n$ is affinely equivalent to the function $g_t(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2t-1}x_{2t}$ for some t, $1 \leq t \leq n/2$.

2.4 Affine subspaces

Nonempty set $L \subseteq \mathbb{F}_2^n$ is called *linear subspace* of $\mathbb{F}_2^n$ if for any $a, b \in L$ it is true $a \oplus b \in L$; its *dimension* $\dim L$ is equal to $\log_2 |L|$.

Denote by $s \oplus D$, where $s \in \mathbb{F}_2^n$ and $D \subseteq \mathbb{F}_2^n$, *a shift* of the set D, i. e. $s \oplus D = \{s \oplus x \mid x \in D\}$.

The set $L \subseteq \mathbb{F}_2^n$ is called *affine subspace* of $\mathbb{F}_2^n$ (or briefly *subspace*) if it is a shift of some linear subspace of $\mathbb{F}_2^n$; *the dimension* $\dim L$ is the dimension of corresponding linear subspace. A shift of an affine subspace is also called its *coset*.

Denote by $\mathcal{ASP}_n^k$ the set of all k-dimensional affine subspaces of $\mathbb{F}_2^n$ and by $\mathcal{LSP}_n^k$ the set of all k-dimensional linear subspaces. An affine(linear) subspace L is *a subspace of an affine(linear) subspace* U if $L \subseteq U$ (both $L, U \subseteq \mathbb{F}_2^n$); let

$$\mathcal{ASP}^k(U) = \{L \in \mathcal{ASP}_n^k \mid L \subseteq U\},$$

$$\mathcal{LSP}^k(U) = \{L \in \mathcal{LSP}_n^k \mid L \subseteq U\}.$$

A Boolean function $f \in \mathcal{F}_n$ is *affine on an affine subspace* $L \subseteq \mathbb{F}_2^n$ if $f|_L = \ell_{a,c}|_L$ for some $a \in \mathbb{F}_2^n,\ c \in \mathbb{F}_2$. Denote that by $f|_L(x) = \langle a, x \rangle \oplus c$.

2.5 Walsh—Hadamard transform

Walsh—Hadamard transform of $f \in \mathcal{F}_n$ is the mapping $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ such that

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

the numbers $W_f(y)$ are called *Walsh—Hadamard* coefficients. Walsh—Hadamard transform uniquely determines f. It is true *Parseval's equality*:

$$\sum_{y\in\mathbb{F}_2^n} W_f^2(y) = 2^{2n}.$$

For a function $f \in \mathcal{F}_n$, a linear subspace $L \subseteq \mathbb{F}_2^n$ and $a, b \in \mathbb{F}_2^n$ it is right the following formula:

$$\sum_{x\in a\oplus L} (-1)^{f(x)\oplus\langle b,x\rangle} = 2^{\dim L-n}(-1)^{\langle a,b\rangle} \sum_{y\in b\oplus L^{\perp}} W_f(y)(-1)^{\langle a,y\rangle}. \tag{1}$$

2.6 Bent functions

A *bent* function is a Boolean function $f \in \mathcal{F}_{2k}$ such that $|W_f(y)| = 2^k$ for all $y \in \mathbb{F}_2^{2k}$. Denote by $\mathfrak{B}_{2k}$ the set of all bent functions in $2k$ variables. Note that for $f \in \mathfrak{B}_{2k}$ it holds

$$\mathrm{wt}(f), \mathrm{dist}(f, \ell_{a,c}) \in \{2^{2k-1} \pm 2^{k-1}\} \text{ for any } a \in \mathbb{F}_2^{2k}, c \in \mathbb{F}_2.$$

The *dual* function $\tilde{f}$ can be defined by f in the following way

$$(-1)^{\tilde{f}(y)} = \frac{1}{2^k} W_f(y) \text{ for all } y \in \mathbb{F}_2^{2k}.$$

Function $\tilde{f}$ is a bent function too. For a bent function f formula (1) can be simplified:

$$\sum_{x\in a\oplus L} (-1)^{f(x)\oplus\langle b,x\rangle} = 2^{\dim L-k}(-1)^{\langle a,b\rangle} \sum_{y\in b\oplus L^{\perp}} (-1)^{\tilde{f}(y)\oplus\langle a,y\rangle}, \tag{2}$$

where L is a linear subspace of $\mathbb{F}_2^{2k}$, $a, b \in \mathbb{F}_2^{2k}$. It can be found in [2].

Denote by Ind_D, where $D \subseteq \mathbb{F}_2^n$, the Boolean function in n variables that takes value 1 only on the set D.

For a bent function the following construction is right. Let $f \in \mathfrak{B}_{2k}$, $L \in \mathcal{ASP}_{2k}^k$ and f be affine on L. Then

$$f \oplus Ind_L \text{ is a bent function too.} \tag{3}$$

The construction was proposed by C. Carlet [2].

For $f, g \in \mathfrak{B}_{2k}$, $f \neq g$, it holds $\mathrm{dist}(f, g) \geq 2^k$. In [12] was proven the following criterion.

Proposition 1. *Let $f \in \mathfrak{B}_{2k}$. Then all bent functions at the distance 2^k from f have the form $f \oplus Ind_L$, where $L \in \mathcal{ASP}_{2k}^k$ and f is affine on L.*

The following functions form Maiorana—McFarland [16] class of bent functions $\mathcal{M}_{2k}$:

$$f(x, y) = \langle x, \pi(y)\rangle \oplus \varphi(y), \text{ where}$$

- $x, y \in \mathbb{F}_2^k$,
- π is a permutation on $\mathbb{F}_2^k$ and
- φ is an arbitrary Boolean function in k variables.

Denote by $\widetilde{\mathcal{M}}_{2k}$ the set of all bent functions affinely equivalent to functions from $\mathcal{M}_{2k}$. This class is also called *completed* Maiorana—McFarland class.

More information concerning bent functions can be found in [19], [8], [10], [15] and [7] (Chapters 8 and 9 by C. Carlet).

3 The graph of minimal distances of bent functions

An undirected graph $GB_{2k} = (V, E)$ is called *the graph of minimal distances of bent functions* if

- V is the set of all bent functions in $2k$ variables and
- $(f, g) \in E$ if and only if $\mathrm{dist}(f, g) = 2^k$.

Denote by GM_{2k} a subgraph of GB_{2k} induced by all vertices from $\widetilde{\mathcal{M}}_{2k}$. Summarize known facts in terms of GB_{2k} and GM_{2k}.

- The maximum degree of GB_{2k} and GM_{2k} is equal to $2^k(2^1+1)(2^2+1)\dots(2^k+1)$, any vertex of maximum degree is a quadratic bent function, see section 7.
- Degree of a vertex of GM_{2k} is not less than $2^{2k+1} - 2^k$, see proposition 13.
- GM_{2k} is connected, see section 9.

Describe the structure of the work. In sections 4 and 5 auxiliary results concerning affinity of Boolean functions will be obtained. Section 6 is devoted to a notion of completely affinely decomposable Boolean function. Complete classification of such functions will be done. Then, in section 7 the maximum degree of GB_{2k} will be obtained; due to results of section 6, it will be also proven that all vertices of maximum degree are quadratic. Next, the last two sections are devoted to connectivity of some subgraphs of GB_{2k}. In section 8 a subgraph of GB_{2k} induced by all vertices from $\mathcal{M}_{2k}$ will be considered. Finally, in section 9 connectivity of GM_{2k} will be proven.

4 Affinity of a Boolean function on an affine subspace

There are the following notions concerning affinity of a Boolean function on an affine subspace. A Boolean function $f \in \mathcal{F}_n$ is called *k-normal* (*weakly k-normal*) if it is constant (affine) on some k-dimensional affine subspace of $\mathbb{F}_2^n$. And function f is called *normal* (*weakly normal*) if it is $\lceil n/2 \rceil$-normal (weakly $\lceil n/2 \rceil$-normal). The notion of normality was introduced for even number of variables by H. Dobbertin [9]. Later it was generalized by C. Charpin [6]. There are also notions of *affinity level* and *generalized affinity level* connected with the maximum dimension of a subspace such that f is affine on it [1], [15].

An idea of affinity on an affine subspaces was applied to construct bent function. For example, big class of normal bent functions was introduced by H. Dobbertin [9]; bent functions that are affine on some t-dimensional affine subspace (face) and on each its coset were considered in [20], [3].

Next, prove auxiliary propositions concerning affinity of a Boolean function on an affine subspace. First of all, prove the main lemma of this section.

Lemma 1. *Let $f \in \mathcal{F}_n$ and $U \in \mathcal{ASP}_n^k$, where $k > 0$. Then f is affine on U if and only if there exists $L \in \mathcal{ASP}^{k-1}(U)$ such that both $f|_L$ and $f|_{a \oplus L}$ are constants, where $a \in U \backslash L$.*

Proof. Without loss of generality it can be supposed that both U and L are linear subspaces, i. e. $U \in \mathcal{LSP}_n^k$, $L \in \mathcal{LSP}^{k-1}(U)$ (otherwise function $f(x \oplus b)$ for $b \in U$ can be considered instead of f).

($\Longrightarrow$) Let f be affine on U. It means that $f|_U(x) = \langle w, x\rangle \oplus c$ for some $w \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. Solve the equation

$$\langle w, x\rangle = 0, \ x \in U.$$

Since U is a linear subspace, the set of all solutions will be either U or some $L \in \mathcal{LSP}_U^{k-1}$. For the second case the set of all solutions of the equation $\langle w, x\rangle = 1, \ x \in U$ will be $a \oplus L$, where $a \in U \backslash L$.

Thus, for both cases there exists $L \in \mathcal{LSP}^{k-1}(U)$ such that both $f|_L$ and $f|_{a\oplus L}$ are constants.

($\Longleftarrow$) Let $f|_L = c_1$ and $f|_{a\oplus L} = c_2$, $c_1, c_2 \in \mathbb{F}_2$. Prove that f is affine on U. Note that $U = L \cup (a \oplus L)$. If $c_1 = c_2$, the statement is obvious. Let $c_1 \neq c_2$, i. e. $c_2 = c_1 \oplus 1$. Consider $L^\perp$. For some $w \in L^\perp$ it is true that $\langle w, a\rangle = 1$ since if $\langle w, a\rangle = 0 \ \forall w \in L^\perp$, then $a \in {L^\perp}^\perp = L$, but $a \notin L$. Therefore, $\langle w, x\rangle|_L = 0$ and $\langle w, x\rangle|_{a\oplus L} = 1$. Thus, $f|_U(x) = \langle w, x\rangle \oplus c_1$. □

Consider corollaries of the lemma.

Proposition 2. *Let $f \in \mathcal{F}_n$ be affine on $L \in \mathcal{ASP}_k^n$. Then $f|_L$ is either constant or balanced.*

Its proof is obvious.

Proposition 3. *Let $f \in \mathcal{F}_n$ and $f|_L$ be constant, where $L \in \mathcal{ASP}_n^k$. Then f is affine on a subspace $L \cup (a \oplus L)$, $a \in \mathbb{F}_2^n$, if and only if $f|_{a\oplus L}$ is constant too.*

The proof obviously follows from lemma 1 and proposition 2.

Proposition 4. *Let $f \in \mathcal{F}_n$ be affine on $L \in \mathcal{ASP}_n^k$, $k > 0$, and $f|_U = c$ for some $U \in \mathcal{ASP}^t(L)$, $c \in \mathbb{F}_2$, where $t < k$. Then there exists an affine subspace $T \in \mathcal{ASP}^{k-1}(L)$ such that $f|_T = c$ and $U \subseteq T$.*

Proof. If $f|_L = c$, any $T \in \mathcal{ASP}^{k-1}(L)$ containing U can be chosen. Otherwise, by lemma 1 there exists $T \in \mathcal{ASP}^{k-1}(L)$ such that both $f|_T$ and $f|_{a\oplus T}$ are constants, where $a \in L \backslash T$. Without loss of generality we can suppose that $f|_T = c$. Since $f|_L$ is not constant, $f|_{a\oplus T} = c \oplus 1$. Thus, $U \subseteq T$. □

Proposition 5. *Let $f \in \mathcal{F}_n$, L be an affine subspace of $\mathbb{F}_2^n$ and $f|_L(x) = \langle w, x\rangle \oplus c$ for some $w \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. Then f is affine on $L \cup (a \oplus L)$, $a \in \mathbb{F}_2^n$, if and only if $f|_{a\oplus L}(x) = \langle w, x\rangle \oplus c'$ for some $c' \in \mathbb{F}_2$.*

Proof. Consider function $f'(x) = f(x) \oplus \langle w, x\rangle \oplus c$. It holds $f'|_L = 0$. Next, the proof is obvious by proposition 3. □

Proposition 6. *Let $f \in \mathcal{F}_n$, $n > 2$ and $L = \{a, b, c, d\}$ be a 2-dimensional affine subspace of $\mathbb{F}_2^n$. Then f is affine on L if and only if $f(a) \oplus f(b) \oplus f(c) \oplus f(d) = 0$.*

The proof is obvious.

5 Affinity of a quadratic Boolean function on an affine subspace

In this section we give auxiliary results concerning affinity of a quadratic Boolean function on an affine subspace.

Proposition 7. *Let $f \in \mathcal{F}_n$, $\deg f \leq 2$ and f be affine on an affine subspace L of $\mathbb{F}_2^n$. Then f is affine on each coset of L.*

Proof. Note that $f(x \oplus a) = f(x) \oplus (f(x) \oplus f(x \oplus a))$, $a \in \mathbb{F}_2^n$. Since the degree of derivative function $f(x) \oplus f(x \oplus a)$ is less than the degree of f (i.e. it is not more than 1), $f(x \oplus a)$ is affine on L and, therefore, f is affine on $a \oplus L$. □

Lemma 2. *Let $f \in \mathcal{F}_n$, f be quadratic and affine on $L \in \mathcal{ASP}_n^t$, $t \leq n/2$. Then there exist different affine subspaces $(a_1 \oplus L), \ldots, (a_{2^{n-2t}} \oplus L)$ such that for some $w \in \mathbb{F}_2^n$ and $c_1, \ldots, c_{2^{n-2t}} \in \mathbb{F}_2$ it is true*

$$f|_{a_i \oplus L}(x) = \langle w, x \rangle \oplus c_i,\ i \in \{1, \ldots, 2^{n-2t}\}.$$

Proof. Denote by S_w the set of all cosets of L such that function $f(x) \oplus \langle w, x \rangle$ is constant on it. Note that if $f|_{a \oplus L}(x) = \langle w, x \rangle \oplus c$, then for any $w' \in w \oplus L^{\perp}$ it holds $f|_{a \oplus L}(x) = \langle w', x \rangle \oplus \langle w \oplus w', a \rangle \oplus c$. Thus, $S_w = S_{w \oplus u}$ for $u \in L^{\perp}$.

According to proposition 7, f is affine on each of 2^{n-t} different shifts of L. Therefore, it is true

$$\frac{1}{|L^{\perp}|} \sum_{w \in \mathbb{F}_2^n} |S_w| = \frac{1}{2^{n-t}} \sum_{w \in \mathbb{F}_2^n} |S_w| \geq 2^{n-t},$$

that is why $|S_w| \geq 2^{n-t} 2^{n-t} / 2^n = 2^{n-2t}$ for some $w \in \mathbb{F}_2^n$. □

Lemma 3. *Let $f \in \mathcal{F}_{2k}$, f be quadratic and $U \in \mathcal{ASP}^{2k-1}(2k)$. Then there exists $L \in \mathcal{ASP}^k(U)$ such that f is affine on L.*

Proof. Since U is of dimension $2k-1$, it holds $\mathbb{F}_2^{2k} = U \cup (c \cup U)$ for some $c \in \mathbb{F}_2^{2k}$. Prove by induction that there exists $L \in \mathcal{ASP}^t(U)$, $t \leq k$, such that f is affine on L.

Base of the induction $t = 0$ is obvious.

Suppose that the statement is true for t, $t < k$. Prove that it is true for $t+1$. By the induction there exists $L \in \mathcal{ASP}^t(U)$ such that f is affine on L. By lemma 2 for some $w \in \mathbb{F}_2^{2k}$ there exist different $a_1 \oplus L, \ldots, a_{2^{2k-2t}} \oplus L$ such that for some $w \in \mathbb{F}_2^{2k}$ it holds $f|_{a_i \oplus L}(x) = \langle w, x \rangle \oplus c_i$, $c_i \in \mathbb{F}_2$. As long as $t < k$, we have $2^{2k-2t} \geq 4$ different affine subspaces.

Since $L \subseteq U$, there always exist different $a \oplus L$ and $b \oplus L$, $a, b \in \mathbb{F}_2^{2k}$, among $(a_1 \oplus L), \ldots, (a_{2^{2k-2t}} \oplus L)$ such that either $a \oplus L, b \oplus L \subseteq U$ or $a \oplus L, b \oplus L \subseteq c \oplus U$. Next, by proposition 5 function f is affine on $L' = (a \oplus L) \cup (b \oplus L)$ of dimension $t+1$. If $L' \subseteq U$, the lemma is proven. Otherwise $L' \subseteq c \oplus U$. By proposition 7 function f is affine on $c \oplus L'$ and $c \oplus L' \subseteq U$. □

6 Completely affinely decomposable Boolean functions

In this section the notion of *completely affinely decomposable* Boolean function is introduced. It will be showed that any such function is either quadratic or affine.

Definition 1. *Boolean function $f \in \mathcal{F}_n$ is called* completely affinely decomposable *of order k, $2 \leq k \leq n$, if the following conditions hold:*

- *f is affine on some subspace from $\mathcal{ASP}_n^k$;*
- *if f is affine on a subspace $L \in \mathcal{ASP}_n^k$, then f is affine on each coset of L.*

There is no sense to consider orders 0 and 1, since all Boolean functions would satisfy the definition.

Denote by $\mathcal{AD}_n^k$ the set of all completely affinely decomposable functions of order k in n variables. It is simple to prove the following proposition.

Proposition 8. *Let $f, g \in \mathcal{F}_n$ be affinely equivalent. Then $f \in \mathcal{AD}_n^k$ if and only if $g \in \mathcal{AD}_n^k$.*

Show that $\mathcal{AD}_n^k$ contains only affine and quadratic functions. Firstly, it holds

Proposition 9. $\mathcal{AD}_n^k \subseteq \mathcal{AD}_n^{k-1} \subseteq \ldots \subseteq \mathcal{AD}_n^2$.

To prove the proposition it is sufficient to use the following lemma.

Lemma 4. *Let $f \in \mathcal{AD}_n^k$ and f be affine on some linear subspace $U \in \mathcal{LSP}_n^t$, $t < k$. Then there exists linear subspace $L \in \mathcal{LSP}_n^k$ such that $U \subseteq L$ and f is affine on L.*

Proof. Prove the lemma using induction by dimension of U. Base of induction $\dim U = 0$ obviously follows from the lemma condition.

Suppose that for all linear subspaces of dimension less than t, $t \leq k-1$, the statement is true. Prove that it is true for affine subspace U of dimension $t+1$.

Represent U as $U' \cup (a \oplus U')$, where $U' \in \mathcal{LSP}^t(U)$ and $a \in U$. Then by induction there exists $L \in \mathcal{LSP}_n^k$, $U' \subseteq L$ and f is affine on L. Without loss of generality it can be supposed that $f|_L = 0$ thanks to transformations of the form $f \oplus \ell_{w,c}$. Next, by proposition 3 it is true $f|_{a \oplus U'} = c$ for some $c \in \mathbb{Z}_2$. Since by the lemma condition f is affine on $a \oplus L$, by proposition 4 there exists $(a \oplus T) \in \mathcal{ASP}^{k-1}(a \oplus L)$ such that $f|_{a \oplus T} = c$ and $a \oplus U' \subseteq a \oplus T \subset a \oplus L$ (therefore, it holds $U' \subseteq T \subset L$ too). As long as $f|_T = 0$ due to $T \subset L$, by proposition 3 function f is affine on k-dimensional linear subspace $T \cup (a \oplus T)$ that contains U. □

Next, show that $\mathcal{AD}_n^2$ can contain only affine and quadratic functions.

Lemma 5. *Let $f \in \mathcal{F}_n$, $n > 2$. Then there exists $L \in \mathcal{ASP}_n^2$ such that f is affine on L.*

Proof. Prove that f is affine on some $L \in \mathcal{ASP}_n^2$ when $n = 3$. It is sufficient for proving the lemma. ANF of f can contain 4 monomials of degree 2 or 3: $x_1x_2x_3$, x_1x_2, x_1x_3 x_2x_3. Consider two cases.

Case 1. Monomial $x_1x_2x_3$ does not belong to the ANF. There are two subcases.

1. Monomials x_1x_2, x_1x_3 and x_2x_3 belong to the ANF. Note that $x_1x_2 \oplus x_1x_3 \oplus x_2x_3 = x_1(x_2 \oplus x_3) \oplus x_2x_3$, that is why f is affine on 2-dimensional affine subspace $D = \{(x_1, x_2, x_3) \mid x_2 \oplus x_3 = 1, x_1, x_2, x_3 \in \mathbb{F}_2\}$.

2. Otherwise all monimials of degree 2 from the ANF contain common variable x_i, $1 \leq i \leq 3$. Therefore, f_i^0 is affine.

Case 2. Monomial $x_1x_2x_3$ belongs to the ANF. There are also two subcases.

1. There are no minomials of degree 2 in the ANF. Then it is obvious that f_1^0 is affine.

2. Otherwise without loss of generality suppose that the ANF contains x_1x_2. Then f_3^1 is affine since $x_1x_2x_3$, x_1x_2 cancel out and x_1x_3 and x_2x_3 contains $x_3 = 1$.

□

Lemma 6. *Let $f \in \mathcal{AD}_n^2$. Then f is either affine or quadratic.*

Proof. Prove the lemma using induction by the variable number. It is obvious that any Boolean function in 2 variables is either affine or quadratic. Suppose that if $g \in \mathcal{AD}_k^2$, $k < n$, then $\deg g \leq 2$. Prove that $\deg f \leq 2$.

Consider the linear subspace

$$L = \{(\mathbf{0}, 0, 0), (\mathbf{0}, 0, 1), (\mathbf{0}, 1, 0), (\mathbf{0}, 1, 1)\} \subseteq \mathbb{F}_2^n.$$

Then any coset of L can be represented in the following way:

$$\{(\mathbf{x}, 0, 0), (\mathbf{x}, 0, 1), (\mathbf{x}, 1, 0), (\mathbf{x}, 1, 1)\},\ \mathbf{x} \in \mathbb{F}_2^{n-2}.$$

Since $f \in \mathcal{AD}_n^2$, function f is either affine on each coset of L or not affine on any coset of L at all. That is why by proposition 6 for some constant $c \in \mathbb{F}_2$ it is true

$$f(\mathbf{x}, 0, 0) \oplus f(\mathbf{x}, 0, 1) \oplus f(\mathbf{x}, 1, 0) \oplus f(\mathbf{x}, 1, 1) = c\ \forall \mathbf{x} \in \mathbb{F}_2^{n-2}.$$

Decompose f by two last variables.

$$f(\mathbf{x}, y, z) = (y \oplus 1)(z \oplus 1) f(\mathbf{x}, 0, 0) \oplus (y \oplus 1) z f(\mathbf{x}, 0, 1) \oplus \\ y(z \oplus 1) f(\mathbf{x}, 1, 0) \oplus yz f(\mathbf{x}, 1, 1).$$

In other words,

$$f(\mathbf{x}, y, z) = (f(\mathbf{x}, 0, 0) \oplus f(\mathbf{x}, 0, 1) \oplus f(\mathbf{x}, 1, 0) \oplus f(\mathbf{x}, 1, 1)) yz \oplus \\ (f(\mathbf{x}, 0, 0) \oplus f(\mathbf{x}, 1, 0)) y \oplus (f(\mathbf{x}, 0, 0) \oplus f(\mathbf{x}, 0, 1)) z \oplus f(\mathbf{x}, 0, 0).$$

Let $f'(\mathbf{x}, y) = f(\mathbf{x}, y, 0)$ and $f''(\mathbf{x}, y) = f(\mathbf{x}, 0, y)$, i. e. they are subfunctions of f; and $\alpha = (\mathbf{0}, 1) \in \mathbb{F}_2^{n-1}$. Then

$$f(\mathbf{x}, y, z) = c \cdot yz \oplus y D_\alpha f'(x) \oplus z D_\alpha f''(x) \oplus f(\mathbf{x}, 0, 0). \tag{4}$$

Let h be any of f', f'' or $f(\mathbf{x}, 0, 0)$; and let m be the number of variables of h, $m < n$. Prove that $\deg h \leq 2$. If $m < 3$ it is obvious. Otherwise, by lemma 5 function h is affine on some 2-dimensional affine subspace. In view of h is a subfunction of f, it is right $h \in \mathcal{AD}_m^2$. Thus, by the induction $\deg h \leq 2$.

Therefore,

$$\deg f(\mathbf{x}, 0, 0) \leq 2 \text{ and } \deg D_\alpha f', \deg D_\alpha f'' \leq 1.$$

By equality (4) it is true $\deg f \leq 2$. The lemma is proven. □

The next lemma can be also found in [2]. To completeness, prove it too.

Lemma 7. *A bent function $f \in \mathfrak{B}_{2k}$ can not be affine on an affine subspace of dimension more than k.*

Proof. Let $f|_L(x) = \langle w, x \rangle \oplus c$, $L \in \mathcal{ASP}_{2k}^{k+1}$. Then for bent function $f'(x) = f(x) \oplus \langle w, x \rangle \oplus c$ it is true $f'|_L = 0$. Since the dimension of L more than k, there exist two different subspace U and $a \oplus U$ such that $U \subseteq L$ and $(a \oplus U) \subseteq L$. Then $g = f' \oplus Ind_U \oplus Ind_{a \oplus U}$ is also bent function by construction (3), at the same time $\mathrm{wt}(g) = \mathrm{wt}(f') + 2^{k+1}$. It is a contradiction because the weight of a bent function is equal to $2^{2k-1} \pm 2^{k-1}$. □

The following theorem gives complete classification of completely affinely decomposable Boolean functions.

Theorem 1. *Let $f \in \mathcal{F}_n$. The following statements are right.*

(i) Function $f \in \mathcal{AD}_n^k$, where $2 \leq k \leq \lceil n/2 \rceil$, if and only if f is either affine or quadratic.

(ii) Function $f \in \mathcal{AD}_n^k$, where $\lceil n/2 \rceil \leq k < n$, and $f \notin \mathcal{AD}_n^{k+1}$ if and only if f is affinely equivalent to the function

$$g_{n-k}(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2n-2k-1}x_{2n-2k}$$

(iii) Function $f \in \mathcal{AD}_n^n$ if and only if f is affine.

Proof. Note that if $f \in \mathcal{AD}_n^k$, then it is either affine or quadratic: it follows from the proposition 9 and lemma 6.

As for affine and quadratic Boolean functions there is proposition 7, it is sufficient to prove existence of an affine subspace such that the function is affine on it. Point (iii) is obvious.

By Dickson's theorem any quadratic Boolean function is affine equivalent to $g_t(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2t-1}x_{2t}$ for some t, $1 \leq t \leq n/2$. So, g_t is affine on affine subspace $\{x \in \mathbb{F}_2^n \mid x_2 = x_4 = \ldots = x_{2t} = 0\}$ of dimension $n-t$, i. e. point (i) is proven. To prove the point (ii) it is sufficient to use that function $h(x_1, \ldots, x_{2n-2k}) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2n-2k-1}x_{2n-2k}$ in $2n-2k$ variables is a bent function and by lemma 7 it can not be affine on an affine subspace of dimension more than $n-k$: then function g can not be affine on an affine subspace of dimension more than $n-k+(n-(2n-2k)) = k$. □

Thus, among bent function only quadratic bent functions can be completely affinely decomposable.

A particular case of completely affinely decomposable functions was considered in [13]: it was proven that $f \in \mathcal{F}_n$ is completely affinely decomposable of order $\lceil n/2 \rceil$ if and only if it is either affine or quadratic.

7 The maximum degree of GB_{2k}

Here we prove that the maximum degree of GB_{2k} is equal to $2^k(2^1+1)(2^2+1)\ldots(2^k+1)$. Note that results of the section were published in [11] (in Russian). Now these results are formulated in other terms, and, to completeness, they are given with proofs.

Recall that the number of bent functions at the distance 2^k from f is equal to the number of k-dimensional affine subspaces of $\mathbb{F}_2^{2k}$ such that f is affine on each of them.

Since any $U \in \mathcal{ASP}_n^k$, $k > 0$, can be represented as $U = L \cup (a \oplus L)$, where $L \in \mathcal{ASP}^{k-1}(U)$ and $a \in U \backslash L$, proposition 5 gives us a condition that allows to increase subspace dimension by 1, keeping affinity of a function.

Next, appreciate the number of ways to increase subspace dimension by 1 using the condition. In order to do that, recall the following notion. Let $f \in \mathcal{F}_n$, $S \subseteq \mathbb{F}_2^n$. *Incomplete Walsh—Hadamard transform* of function $f|_S$ is the mapping

$$W_{f_S}(y) = \sum_{x \in S} (-1)^{f(x) \oplus \langle y, x \rangle}, \ y \in \mathbb{F}_2^n.$$

It holds an analogue of Parseval's equality:

$$\sum_{y \in \mathbb{F}_2^n} W_{f_S}^2(y) = \sum_{y \in \mathbb{F}_2^n} \sum_{u \in S} \sum_{v \in S} (-1)^{f(u) \oplus f(v) \oplus \langle u \oplus v, y \rangle} =$$

$$\sum_{u \in S} \sum_{v \in S} (-1)^{f(u) \oplus f(v)} \sum_{y \in \mathbb{F}_2^n} (-1)^{\langle u \oplus v, y \rangle} = \sum_{u \in S} (-1)^{f(u) \oplus f(u)} 2^n = 2^n |S|.$$

More information concerning incomplete Walsh—Hadamard transform can be found in [15].

Lemma 8. *Let f be bent function in $2k$ variables, $L \in \mathcal{ASP}^t_{2k}$, $t \leq k$ and $a_1 \oplus L, \ldots, a_n \oplus L$ be different cosets of L. Let for some $w \in \mathbb{F}_2^{2k}$ it hold*

$$f|_{a_i \oplus L}(x) = \langle w, x\rangle \oplus c_i,\ c_i \in \mathbb{F}_2 \text{ for all } i \in \{1, \ldots, n\}.$$

Then $n \leq 2^{2k-2t}$. Moreover, if $n = 2^{2k-2t}$, function $(f(x) \oplus \langle w, x\rangle)|_{a \oplus L}$ is balanced for any $a \notin (a_1 \oplus L) \cup \ldots \cup (a_n \oplus L)$.

Proof. It is known that for bent function f, linear subspace L, $a, w \in \mathbb{F}_2^{2k}$ it holds formula (2):

$$\sum_{x \in a \oplus L} (-1)^{f(x) \oplus \langle w,x\rangle} = 2^{\dim L - k}(-1)^{\langle a,w\rangle} \sum_{y \in w \oplus L^{\perp}} (-1)^{\tilde{f}(y) \oplus \langle a,y\rangle}. \tag{5}$$

Let $S = w \oplus L^{\perp}$, consider incomplete Walsh—Hadamard transform of $\tilde{f}|_S$:

$$W_{\tilde{f}_S}(u) = \sum_{y \in S} (-1)^{\tilde{f}(y) \oplus \langle u,y\rangle},\ u \in \mathbb{F}_2^{2k}.$$

Next, according to equality (5)

$$W_{\tilde{f}_S}(u) = 2^{k-t}(-1)^{\langle u,w\rangle} \sum_{x \in u \oplus L} (-1)^{f(x) \oplus \langle w,x\rangle}. \tag{6}$$

Let $V = (a_1 \oplus L) \cup \ldots \cup (a_n \oplus L)$. Then by equality (6) and the lemma condition it follows that for all $u \in V$ it is true $|W_{\tilde{f}_S}(u)| = 2^{k-t}2^t = 2^k$. According to analogue of Parseval's equality for $\tilde{f}|_S$, $|S| = 2^{2k-t}$ and $|V| = n2^t$, it is obtained

$$\sum_{u \in \mathbb{F}_2^{2k}} W^2_{\tilde{f}_S}(u) = \sum_{u \in V} W^2_{\tilde{f}_S}(u) + \sum_{u \notin V} W^2_{\tilde{f}_S}(u) = n2^t2^{2k} + \sum_{u \notin V} W^2_{\tilde{f}_S}(u) = 2^{2k}2^{2k-t}.$$

Therefore, $n \leq 2^{2k-2t}$.

If $n = 2^{2k-2t}$, then $W_{\tilde{f}_S}(u) = 0$ for any $u \notin V$. In this case by equality (6) it is obtained that $\sum_{x \in u \oplus L} (-1)^{f(x) \oplus \langle w,x\rangle} = 0$ for any $u \notin V$. The lemma is proven. □

Formulate the case $n = 2^{2k-2t}$ from the previous lemma separately.

Proposition 10. *Let $f \in \mathfrak{B}_{2k}$ be constant on each of 2^{2k-2t} different cosets of $L \in \mathcal{ASP}^t_{2k}$, $t \leq k$. Then f is balanced on each of the other cosets of L.*

It is a generalization of the proposition proven by C. Carlet.

Proposition 11 (C. Carlet, 1994, [2])**.** *Let $f \in \mathfrak{B}_{2k}$ and $f|_L$ be constant, where $L \in \mathcal{ASP}^k_{2k}$. Then f is balanced on each coset of L except L.*

Next, formulate the main result of the section.

Theorem 2. *The maximum degree of GB_{2k} is equal to $2^k(2^1 + 1) \cdot \ldots \cdot (2^k + 1)$. Any vertex of maximum degree is a quadratic bent function.*

Proof. Denote by h an arbitrary quadratic bent function in $2k$ variables. Define the following set:

$$D^t(f) = \{L \mid L \in \mathcal{ASP}^t_{2k} \text{ and } f \text{ is affine on } L\},\ 0 \le t \le k.$$

By proposition 1 the number of bent functions that are at the distance 2^k from f is equal to $|D^k(f)|$. Prove that $|D^k(f)| \le |D^k(h)|$.

Show that $|D^t(f)| \le |D^t(h)|$ using induction by t, $0 \le t \le k$. For $t = 0$ it is obvious that $|D^0(f)| = |D^0(h)| = 2^{2k}$.

Let for $t < k$ it hold $|D^t(f)| \le |D^t(h)|$. Prove that $|D^{t+1}(f)| \le |D^{t+1}(h)|$. Let $N_f(L) = \{U \in D^{t+1}(f) \mid L \subset U\}$, where $L \in D^t(f)$. Note that any $U \in N_f(L)$ can be represented as $U = L \cup (a \oplus L)$ for any $a \in U \backslash L$. Then

$$|D^{t+1}(f)| = \frac{1}{2(2^{t+1}-1)} \sum_{L \in D^t(f)} |N_f(L)|, \tag{7}$$

since $|\mathcal{ASP}^t(U)| = 2(2^{t+1}-1)$. By proposition 5 and by lemmas 8 and 2 for any $L \in D^t(f)$ and $L' \in D^t(h)$ it holds $|N_f(L)| \le |N_h(L')| = 2^{2k-2t} - 1$. Therefore, $|D^{t+1}(f)| \le |D^{t+1}(h)|$.

Thus, $|D^k(f)| \le |D^k(h)|$. Since $|N_h(L')| = 2^{2k-2\dim L'} - 1$, it is true

$$|D^k(h)| = 2^{2k} \prod_{t=0}^{k-1} \frac{2^{2k-2t}-1}{2(2^{t+1}-1)} = 2^k \prod_{t=1}^{k} \frac{2^{2t}-1}{2^t-1} = 2^k(2^1+1)\cdot \ldots \cdot (2^k+1).$$

Note that this formula for a quadratic bent function was calculated in [12].

Prove that the bound is reached only on quadratic bent functions. Let f be not quadratic and $|D^k(f)| \ne 0$, note that in this case it holds $k > 2$. Then by theorem 1 function f is not completely affinely decomposable of order k. It means that f is affine on some $L \in \mathcal{ASP}^k_{2k}$ and not affine on some its coset.

Without loss of generality it can be supposed that L is a linear subspace and $f|_L = 0$ thanks to transformations of the form $f(x \oplus a) \oplus \langle w, x\rangle \oplus c$. By proposition 10 function f is balanced on each coset of L except L.

Let $L' \in \mathcal{LSP}^{k-1}(L)$, so, $f|_{L'} = 0$. Let $N_f(L') > 1$, i. e. f is affine on $L' \cup (a \oplus L')$ for some $a \notin L$. Then by lemma 3 $f|_{a\oplus L'} = c$ for some $c \in \mathbb{F}_2$. Since $f|_{a\oplus L}$ is balanced, it holds $f|_{(a\oplus L)\backslash(a\oplus L')} = c \oplus 1$ and by lemma 3 function f is affine on $a \oplus L$.

At the same time if $L', L'' \in \mathcal{LSP}^{k-1}(L)$ are different, function f can not be affine on both $L' \cup (a \oplus L')$ and $L'' \cup (a \oplus L'')$ due to balancedness of $f|_{a\oplus L}$. Note that $|\mathcal{LSP}^{k-1}(L)| = 2^k - 1$ and $|\{a \oplus L \mid a \in \mathbb{F}_2^{2k}\backslash L\}| = 2^k - 1$. Thus, if $N_f(L') > 1$ for any $L' \in \mathcal{LSP}^{k-1}(L)$, then f is affine on each coset of L. It is a contradiction, therefore, $N_f(L') = 1$ for some $L' \in \mathcal{LSP}^{k-1}(L)$. At the same time $N_h(U) = 3$ for any $U \in D^{k-1}(h)$, that is why $D^k(f) < D^k(h)$ by equality (7). The theorem is proven. □

8 Bent functions at the minimal distance from a Maiorana—McFarland bent function

In this section bent functions at the minimal distance from a Maiorana—McFarland bent function are considered.

Lemma 9. *Let $f, g \in \mathcal{M}_{2k}$, i. e. $f(x,y) = \langle x, \pi(y)\rangle \oplus \varphi(y)$, Let $g(x,y) = \langle x, \pi'(y)\rangle \oplus \varphi'(y)$. Then $dist(f,g) = 2^k$ if and only if one of the following conditions holds*

- *$\pi = \pi'$ and $dist(\varphi, \varphi') = 1$;*
- *$\pi' = \pi \circ \tau_{a,b}$ and $\varphi'(y) = \varphi(y)$ for all $y \in \mathbb{F}_2^k \backslash \{a, b\}$, where $\tau_{a,b}$ is a transposition that swaps two different $a, b \in \mathbb{F}_2^k$.*

Proof. Let $S = \{y \in \mathbb{F}_2^k \mid \pi(y) \neq \pi'(y)\}$. Then

$$\mathrm{dist}(f,g) = 2^k \sum_{t \in \mathbb{F}_2^k \backslash S} (\varphi(t) \oplus \varphi'(t)) + \sum_{s \in S} \mathrm{dist}(f(x,s), g(x,s)).$$

Consider the second part of the sum: $\mathrm{dist}(f(x,s), g(x,s))$ is equal to the number of solutions of

$$\langle x, \pi(s) \oplus \pi'(s)\rangle \oplus \varphi(s) \oplus \varphi'(s) = 1.$$

Since $\pi(s) \neq \pi'(s)$, there are exactly 2^{k-1} different $x \in \mathbb{F}_2^k$ on which $f(x,s) \neq g(x,s)$. Thus,

$$\mathrm{dist}(f,g) = 2^k \sum_{t \in \mathbb{F}_2^k \backslash S} (\varphi(t) \oplus \varphi'(t)) + 2^{k-1}|S|.$$

It means that $\mathrm{dist}(f,g) = 2^k$ if and only if either $|S| = 0$, $\mathrm{dist}(\varphi, \varphi') = 1$ or $|S| = 2$, $\varphi'(y) = \varphi(y)$ for all $y \in \mathbb{F}_2^k \backslash S$. □

Since the set of all transpositions generates any permutation, the following proposition holds.

Proposition 12. *A subgraph of GB_{2k} induced by vertices from $\mathcal{M}_{2k}$ is a regular connected graph.*

Now the minimum degree of GM_{2k} can be estimated.

Proposition 13. *Let $f \in \widetilde{\mathcal{M}}_{2k}$. Then the degree of vertex f in GM_{2k} is not less than $2^{2k+1} - 2^k$.*

Proof. Since an affine transform does not change distance between any two Boolean functions, without loss of generality we can suppose that $f \in \mathcal{M}_{2k}$. By lemma 9 there are $4 \cdot 2^k(2^k - 1)/2 + 2^k = 2^{2k+1} - 2^k$ bent functions from $\mathcal{M}_{2k}$ that are at the distance 2^k from f. □

It is not difficult to prove the following statement that helps us to determine whether a bent function is affinely equivalent to a Maiorana—McFarland bent function.

Proposition 14 (A. Canteaut et al. [5])**.** *Let $f \in \mathfrak{B}_{2k}$. Then $f \in \widetilde{\mathcal{M}}_{2k}$ if and only if there exists $L \in \mathcal{ASP}_{2k}^k$ such that f is affine on each coset of L.*

9 Connectivity of GM_{2k}

The main idea of proving connectivity of GM_{2k} is to prove that there exists a path in GM_{2k} between any two quadratic bent functions, since there always exists a path between $f \in \widetilde{\mathcal{M}}_{2k}$ and some quadratic bent function by proposition 12. Describe a way to find a path in GM_{2k}.

Lemma 10. *Let $f \in \mathfrak{B}_{2k}$, f be quadratic and $g = f \oplus Ind_U$, where U is an affine subspace of $\mathbb{F}_2^k$. Let $L \in \mathcal{ASP}^k(U)$ and f be affine on L. Then $g \in \widetilde{\mathcal{M}}_{2k}$ and there is a path in GM_{2k} between f and g.*

Proof. As long as $L \in \mathcal{ASP}^k(U)$, it holds

$$U = (a_1 \oplus L) \cup (a_2 \oplus L) \cup \ldots \cup (a_m \oplus L),\ m = 2^{\dim U - k},$$

where all $a_i \oplus L$ are different cosets of L. Function f is quadratic, that is why it is affine on each coset of L. Next, let

$$f_0 = f \text{ and } f_i = f_{i-1} \oplus Ind_{a_i \oplus L},\ 1 \leq i \leq m.$$

It is obvious that $f_m = g$ and $\mathrm{dist}(f_i, f_{i+1}) = 2^k$. Since $a_1 \oplus L, \ldots, a_m \oplus L$ are not intersected, each f_i is affine on each coset of L like f. Thus, each f_i is a bent function by construction 3 and $f_0, \ldots, f_m \in \widetilde{\mathcal{M}}_{2k}$ by proposition 14. □

It is not difficult to prove the following lemma.

Lemma 11. *Let $f \in \mathfrak{B}_{2k}$ and f be quadratic. Then there is a path in GM_{2k} between f and $f \oplus \ell_{a,c}$ for any $a \in \mathbb{F}_2^{2k}$ and $c \in \mathbb{F}_2$.*

Proof. Consider $U = \mathrm{supp}(\ell_{a,c})$. It is obvious that either $U \in \mathcal{ASP}_{2k}^{2k-1}$ or $U = \mathbb{F}_2^{2k}$ or U is empty. For the third case the proof is obvious. Otherwise by lemma 3 there exists $L \in \mathcal{ASP}^k(U)$ such that f is affine on L. Finally, by lemma 10 there exists a path between f and $f \oplus \ell_{a,c}$. □

The following lemma is the main step for proving existence of a path in GM_{2k} between any two quadratic bent functions.

Lemma 12. *Let $f \in \mathfrak{B}_{2k}$ and f be quadratic. Then there is a path in GM_{2k} between f and $f(x_1, \ldots, x_{2k-1}, x_{2k} \oplus x_1)$.*

Proof. Since f is quadratic, represent it as the following:

$$\begin{aligned} f(x_1, \ldots, x_{2k}) = f'(x_1, \ldots, x_{2k-1}) \oplus \\ (w_1 x_1 \oplus \ldots \oplus w_{2k-1} x_{2k-1} \oplus d) x_{2k}, \end{aligned}$$

where $w_1, \ldots, w_{2k-1}, d \in \mathbb{F}_2$. Then for $g(x_1, \ldots, x_{2k}) = f(x_1, \ldots, x_{2k-1}, x_{2k} \oplus x_1)$ it holds

$$g(x) = f(x) \oplus (w_1 x_1 \oplus \ldots \oplus w_{2k-1} x_{2k-1} \oplus d) x_1.$$

Consider $S = \mathrm{supp}((w_1 x_1 \oplus \ldots \oplus w_{2k-1} x_{2k-1} \oplus d) x_1)$. Note that S is an affine subspace. Prove that there exists $L \in \mathcal{ASP}^k(S)$ such that f is affine on L.

Case $w_1 = \ldots = w_{2k-1} = 0$ is impossible, because of bent function $f(x) \oplus dx_k$ must depend on each its variable. Therefore, there exists $w_t \neq 0$ for some $1 \leq t \leq 2k-1$.

If only w_1 is nonzero, then $S = \mathrm{supp}(x_1(x_1 \oplus d))$. If $d = 1$, functions f and g are the same. Otherwise S is an affine subspace of dimension $2k-1$ and by lemma 3 there exists required L.

If there exists other nonzero w_t, without loss of generality suppose that $t = 2k-1$. Consider $f|_{x_{2k-1} = w_1 x_1 \oplus \ldots \oplus w_{2k-2} x_{2k-2} \oplus d \oplus 1} \oplus x_{2k}$ which is equal to

$$f'(x_1, \ldots, x_{2k-2}, w_1 x_1 \oplus \ldots \oplus w_{2k-2} x_{2k-2} \oplus d \oplus 1)$$

as a function in $2k-2$ variables. Let $U = \{x \in \mathbb{F}_2^{2k-2} \mid x_1 = 1\} = \mathrm{supp}(x_1)$. Then by lemma 3 there exists a $(k-1)$-dimensional affine subspace L' of $\mathbb{F}_2^{2k-2}$ that $L' \subseteq U$ and $f'(x_1, \ldots, x_{2k-2}, w_1 x_1 \oplus \ldots \oplus w_{2k-2} x_{2k-2} \oplus d \oplus 1)$ is affine on L'.

Therefore, f is affine on a k-dimensional affine subspace $L \subseteq \mathbb{F}_2^{2k}$,

$$L = \{(y, w_1y_1 \oplus \ldots \oplus w_{2k-2}y_{2k-2} \oplus d \oplus 1, z) \ : \ y \in L', z \in \mathbb{F}_2\},$$

and at the same time $L \subseteq S$, because of $(w_1x_1 \oplus \ldots \oplus w_{2k-1}x_{2k-1} \oplus d)x_1$ does not depend on x_{2k}, $w_1x_1 \oplus \ldots \oplus w_{2k-1}x_{2k-1} \oplus d = 1$ for any $x \in L$ and $x_1 = 1$ due to choosing L'. Required L has been found.

Finally, thanks to S to be an affine subspace and $L \in \mathcal{ASP}^k(S)$, by lemma 10 there exists a path between f and g. □

The next theorem is the main result concerning connectivity of subgraphs of GB_{2k}.

Theorem 3. *Graph GM_{2k} is connected for all $k \geq 1$.*

Proof. According to lemma 9, for any bent function $f_0 \in \mathcal{M}_{2k}$ there are $f_1, \ldots, f_n \in \mathcal{M}_{2k}$ for some n where $\mathrm{dist}(f_i, f_{i+1}) = 2^k$ and $f_n(x, y) = x_1y_1 \oplus x_2y_2 \oplus \ldots \oplus x_ky_k$.

Therefore, for any bent function $f_0 \in \widetilde{\mathcal{M}}_{2k}$ there are $f_1, \ldots, f_n \in \widetilde{\mathcal{M}}_{2k}$ for some n where $\mathrm{dist}(f_i, f_{i+1}) = 2^k$ and f_n is a quadratic bent function, i.e. there is a path in GM_{2k} between any $f_0 \in \widetilde{\mathcal{M}}_{2k}$ and some quadratic bent function.

Thus, it is enough to prove that there is a path in GM_{2k} between any two quadratic bent functions.

According to Dickson's theorem, for any two quadratic bent functions f, g in $2k$ variables there exist an invertible $2k \times 2k$ binary matrix A and affine function $\ell \in \mathcal{A}_{2k}$ such that $g(x) = f(xA) \oplus \ell(x)$ for any $x \in \mathbb{F}_2^{2k}$.

At the same time by lemma 12 there is a path in GM_{2k} between any quadratic f and $f(x_1, \ldots, x_{2k-1}, x_{2k} \oplus x_1)$. On one hand, we can easily extend lemma 12 (using permutations on variable numbers) to transformations of the form

$$\begin{aligned} x'_l &= x_l \text{ for all } l \in \{1, \ldots, 2k\}\backslash\{i\}, \\ x'_i &= x_i \oplus x_j \end{aligned}$$

for any $i, j \in \{1, \ldots, 2k\}$, $i \neq j$. On the other hand, the set of all these transformations generates any invertible transform xA. In view of lemma 11, the theorem is proven. □

Corollary 1. *Graphs GB_2, GB_4 and GB_6 are connected.*

It follows from all bent functions in 2, 4 and 6 variables are affinely equivalent to Maiorana—McFarland bent functions (according to affine classification of bent function in small number of variables [17], $\mathfrak{B}_2$ and $\mathfrak{B}_4$ consist of the only class of affine equivalence; $\mathfrak{B}_6$ consists of four classes; all class representatives are affinely equivalent to Maiorana—McFarland bent functions).

10 Conclusion

Note that there are many open questions concerning GB_{2k} and GM_{2k}. For example, the minimum degree of GM_{2k} and an exact lower bound of a vertex degree in GB_{2k} when the vertex belongs to $\widetilde{\mathcal{M}}_{2k}$ are still unknown.

There are also open questions concerning connectivity of GB_{2k}. In general, GB_{2k} is not connected starting with $k = 7$ due to existing isolated vertices, i.e. such bent functions that there are no bent functions at the distance 2^k from them. Such bent functions are called *non-weakly normal*, they were constructed in [5]. At the same time it is an open question whether GB_8, GB_{10} and GB_{12} are connected as well as whether GB_{2k} without isolated vertices is connected.

References

[1] Buryakov M.L., Logachev O.A. On the affinity level of Boolean functions, Discrete Mathematics and Applications, **15**(5), 479-488 (2005).

[2] Carlet C., Two new classes of bent functions, EUROCRYPT'93. LNCS. **765**, 77–101 (1994).

[3] Carlet C., On the confusion and diffusion properties of Maiorana—McFarlands and extended Maiorana—McFarlands functions, J. Complexity, **20**, 182–204 (2004).

[4] Carlet C., Open problems on binary bent functions, Proceedings of the conference "Open problems in mathematical and computational sciences" (Istanbul, Turkey, September 18–20) (2013).

[5] Canteaut A., Daum M., Dobbertin H., Leander G., Finding nonnormal bent functions, Discrete Appl. Math. **154**(2), 202–218 (2006).

[6] Charpin P., Normal Boolean functions, J. Complexity, **20**, 245-265 (2004).

[7] Crama C., Hammer P.L., Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, New York (2010).

[8] Cusick T.W., Stanica P., Cryptographic Boolean functions and applications. Acad. Press. Elsevier (2009).

[9] Dobbertin H., Construction of bent functions and balanced Boolean functions with high nonlinearity, Fast Software Encryption Int. Workshop (Leuven, Belgium, December 14–16, 1994). LNCS. **1008**, 61–74 (1995).

[10] Helleseth T., Kholosha A., Bent functions and their connections to combinatorics, Survey in Combinatorics, 91–126 (2013).

[11] Kolomeec N.A., An upper bound for the number of bent functions at the distance 2^k from an arbitrary bent function in $2k$ variables, Prikladnaya Diskretnaya Matematika, 3, 28–39 (2014) (in Russian).

[12] Kolomeets N.A., Enumeration of the bent functions of least deviation from a quadratic bent function, Journal of Applied and Industrial Mathematics, **6**(3), 306-317 (2012).

[13] Kolomeec N.A., A threshold property of quadratic Boolean functions, Journal of Applied and Industrial Mathematics, **9**(1), 83–87 (2015).

[14] Kolomeec N.A., Pavlov A.V., Bent functions on the minimal distance, Proceedings of IEEE Region 8 International Conference on Computational Technologies in Electrical and Electronics Engineering (SIBIRCON), 11-15 July 2010, 145–149.

[15] Logachev O.A., Sal'nikov A.A., Yashenko V.V., Boolean functions in coding theory and cryptography, Moscow center of uninterrupted mathematical education, Moscow (2004). Translated in English by AMS in series "Translations of Mathematics Monographs" (2012).

[16] McFarland R.L., A family of difference sets in non-cyclic groups, J. Combin. Theory, Ser. A, **15**, 1–10 (1973).

[17] Rothaus O., On bent functions, J. Combin. Theory, Ser. A, **20**(3), 300–305 (1976).

[18] Tokareva N.N., The group of automorphisms of the set of bent functions, Discrete Mathematics and Applications, **20**(5), 655-664 (2011).

[19] Tokareva N., Bent Functions, Results and Applications to Cryptography, 230 p., Acad. Press. Elsevier (2015).

[20] Yashenko V.V., On the Propagation Criterion for Boolean Functions and on Bent Functions, Probl. Peredachi Inf. **33**(1), 75–86 (1997) (in Russian).