Math-Net.Ru

Общероссийский математический портал

N. A. Kolomees, Граф минимальных расстояний между булевыми функциями,
Матем. вопр. криптогр., 2016, том 7, выпуск 2, 103–110

DOI: <https://doi.org/10.4213/mvk187>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и
согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.80.181.102

26 апреля 2023 г., 18:15:39

A graph of minimal distances between bent functions

N. A. Kolomeec¹

Sobolev Institute of Mathematics SB RAS, Novosibirsk

Получено 02.III.2015

Abstract. A graph of minimal distances between bent functions is introduced as 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 bent functions). It is shown that its subgraph induced by all functions affine equivalent to the Maiorana–McFarland bent functions is connected.

Key words: Boolean functions, bent functions, the minimal distance

Граф минимальных расстояний между булевыми функциями

Н. А. Коломеец

Институт математики им. С. Л. Соболева СО РАН, Новосибирск

Аннотация. Граф минимальных расстояний между булевыми функциями определяется как неориентированный граф (V, E) , где V — множество всех бент-функций от $2k$ переменных и $(f, g) \in E$, если расстояние Хемминга между f и g равно 2^k (это минимально возможное расстояние между двумя бент-функциями). Показано, что его подграф, индуцированный всеми функциями, которые аффинно эквивалентны бент-функциям Майораны–МакФарланда, связан.

Ключевые слова: булевы функции, бент-функции, минимальное расстояние

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 2, pp. 103–110 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

¹ The author was supported by the Russian Foundation for Basic Research (project no. 15-07-01328) and by Grant NSh-1939.2014.1 of President of Russia for Leading Scientific Schools.

1. Introduction

We consider graphs of minimal distances between bent functions. Bent functions proposed by O. Rothaus [7] are Boolean functions in even number of variables that have maximal possible nonlinearity. Bent functions have a lot of applications in algebra, combinatorics, coding theory, cryptography, see [5, 8, 9]. We prove that if two bent functions f, g are affinely equivalent to Maiorana–McFarland bent functions, then there exist bent functions $f_0, f_1, \dots, f_n$ (all affinely equivalent to Maiorana–McFarland bent functions) such that $f = f_0$, $g = f_n$ and the Hamming distance between f_i and f_{i+1} is the smallest possible. This statement is also true for any bent functions f, g in a small number of variables (2, 4 and 6).

Let us give definitions. A *Boolean function* in n variables is a mapping $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$. Denote by $\mathcal{F}_n$ the set of all Boolean functions in n variables. The *Hamming distance* $\text{dist}(f, g)$ between two Boolean functions f, g in n variables is the number of $x \in \mathbb{F}_2^n$ such that $f(x) \neq g(x)$. Define by $\langle x, y \rangle = x_1y_1 \oplus x_2y_2 \oplus \dots \oplus x_ny_n$ the inner product of two vectors $x, y \in \mathbb{F}_2^n$.

Restriction of a Boolean function $f \in \mathcal{F}_n$ on the set $S \subseteq \mathbb{F}_2^n$ is a mapping $f|_S : S \rightarrow \mathbb{F}_2$ such that $f|_S(x) = f(x)$ for all $x \in S$. A Boolean function is called *affine* if its algebraic degree is 0 or 1 and *quadratic* if its degree is equal to 2.

A *shift* $s \oplus D$ of the set $D \subseteq \mathbb{F}_2^n$ by $s \in \mathbb{F}_2^n$ is the set $\{s \oplus x : x \in D\}$. A shift of a linear subspace of $\mathbb{F}_2^n$ is called an *affine subspace* of $\mathbb{F}_2^n$. *Dimension* of an affine subspace is a dimension of a corresponding linear subspace.

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

Two Boolean functions $f, g \in \mathcal{F}_n$ are called *affinely equivalent* if there exist an invertible $n \times n$ binary matrix A and $b \in \mathbb{F}_2^n$ such that $g(x) = f(xA \oplus b)$ for any $x \in \mathbb{F}_2^n$. Note that $\text{dist}(f, g) = \text{dist}(f(xA \oplus b), g(xA \oplus b))$.

A *bent function* is a Boolean function from $\mathcal{F}_{2k}$ that is at the maximal possible distance from the set of all affine functions in $2k$ variables.

The following functions form the Maiorana–McFarland [6] class of bent functions $\mathcal{M}_{2k} : f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y)$ 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 the *completed* Maiorana–McFarland class). It is obvious that $f \oplus \ell \in \widetilde{\mathcal{M}}_{2k}$ for any $f \in \widetilde{\mathcal{M}}_{2k}$ and any affine function ℓ in $2k$ variables.

Let Ind_D , $D \subseteq \mathbb{F}_2^n$, be a Boolean function in n variables taking value 1 only on the set D . Let $\text{supp}(f)$, $f \in \mathcal{F}_n$, be the set $\{x \in \mathbb{F}_2^n : f(x) = 1\}$.

The minimal possible distance between two bent functions in $2k$ variables is equal to 2^k . There exist a construction of bent functions at the distance 2^k proposed by C. Carlet [1]. Let f be a bent function in $2k$ variables and f be affine on a k -dimensional affine subspace L of $\mathbb{F}_2^{2k}$. Then $f \oplus \text{Ind}_L$ is also a bent function. Any bent function at the distance 2^k from f may be constructed in this way [4].

2. A graph of minimal distances between bent functions

An undirected graph $GB_{2k} = (V, E)$ is called a *graph of minimal distances between bent functions* if V is the set of all bent functions in $2k$ variables and $(f, g) \in E$ if and only if $\text{dist}(f, g) = 2^k$.

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 maximal degree of a vertex is equal to $2^k(2^1 + 1)(2^2 + 1) \cdots (2^k + 1)$, any vertex of the maximal degree is a quadratic bent function. It is true for both GB_{2k} and GM_{2k} , see [3].

▷ Degree of a vertex of GM_{2k} is not smaller than $2^{2k+1} - 2^k$, see Lemma 2.

Next, in Section 3 a subgraph of GB_{2k} induced by all vertices from $\mathcal{M}_{2k}$ is considered. In Section 4 auxiliary results concerning quadratic bent functions are obtained. A proof of the main result is based on properties of quadratic Boolean functions. In Section 5 the main result of this paper is proved: a connectivity of GM_{2k} .

3. Maiorana–McFarland bent functions

First of all, consider bent functions that are at the minimal distance from a Maiorana–McFarland bent function.

Lemma 1. Let $f \in \mathcal{M}_{2k}$, i.e. $f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y)$. Let $g(x, y) = \langle x, \pi'(y) \rangle \oplus \varphi'(y)$, where for some distinct $a, b \in \mathbb{F}_2^k$:

$$\begin{aligned}\pi'(y) &= \pi(y) \text{ for all } y \in \mathbb{F}_2^k, \quad y \neq a, b, \\ \pi'(a) &= \pi(b) \text{ and } \pi'(b) = \pi(a), \\ \varphi'(y) &= \varphi(y) \text{ for all } y \in \mathbb{F}_2^k, \quad y \neq a, b.\end{aligned}$$

Then $g \in \mathcal{M}_{2k}$ and $\text{dist}(f, g) = 2^k$.

Proof. Since π' is a permutation too, $g \in \mathcal{M}_{2k}$. Note that $f(x, y) = g(x, y)$ for all $x, y \in \mathbb{F}_2^k, y \neq a, b$. It means that it is sufficient to calculate distance when $y = a, b$. Let $y = a$. Then $f(x, a) = \langle x, \pi(a) \rangle \oplus \varphi(a)$ and $g(x, a) = \langle x, \pi(b) \rangle \oplus \varphi'(a)$.

Therefore, $f(x, a) \neq g(x, a)$ if and only if

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

Since $\pi(a) \neq \pi(b)$, there are exactly 2^{k-1} distinct $x \in \mathbb{F}_2^k$ such that $f(x, a) \neq g(x, a)$. The case $y = b$ is the same. Thus, $\text{dist}(f, g) = 2^{k-1} + 2^{k-1} = 2^k$. $\square$

So, since the set of all transpositions generates any permutation, a subgraph of GB_{2k} induced by vertices from $\mathcal{M}_{2k}$ is connected.

Lemma 2. *Let $f \in \widetilde{\mathcal{M}}_{2k}$. Then there are at least $2^{2k+1} - 2^k$ bent functions from $\mathcal{M}_{2k}$ that are at the distance 2^k from f .*

Proof. Since a nondegenerate affine transform does not change distance between any two Boolean functions, without loss of generality we can suppose that $f \in \mathcal{M}_{2k}$.

According to Lemma 1 there are at least $4 \cdot 2^k(2^k - 1)/2 = 2^{2k+1} - 2^{k+1}$ bent functions from $\mathcal{M}_{2k}$ that are at the distance 2^k from f .

In addition, if $f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y)$, we can add 2^k functions of the form $g(x, y) = \langle x, \pi(y) \rangle \oplus \varphi'(y)$ where $\text{dist}(\varphi, \varphi') = 1$. $\square$

The following lemma helps us to determine whether a bent function is affinely equivalent to a Maiorana–McFarland bent function.

Lemma 3 (A. Canteaut et al. [2]). *Let f be a bent function in $2k$ variables. Then $f \in \widetilde{\mathcal{M}}_{2k}$ if and only if there exists a k -dimensional affine subspace L of $\mathbb{F}_2^{2k}$ such that f is affine on $a \oplus L$ for any $a \in \mathbb{F}_2^{2k}$.*

4. Affinity of a quadratic Boolean function on an affine subspace

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

Statement 1. *Let f be a quadratic Boolean function in n variables and f be affine on an affine subspace L of $\mathbb{F}_2^n$. Then function f is affine on $a \oplus L$ for any $a \in \mathbb{F}_2^n$.*

Proof. Note that $f(x \oplus a) = f(x) \oplus (f(x) \oplus f(x \oplus a))$. Since degree of derivative function $f(x) \oplus f(x \oplus a)$ is smaller than that of f (i. e. it is 0 or 1), $f(x \oplus a)$ is affine on L and, therefore, f is affine on $a \oplus L$. $\square$

Statement 2. *Let f be a quadratic Boolean function in n variables and f is affine on a t -dimensional affine subspace L of $\mathbb{F}_2^n$, $t \leq n/2$. Then there exist distinct affine subspaces $a_1 \oplus L, \dots, a_{2^{n-2t}} \oplus L$ such that $f_{a_i \oplus L}(x) = \langle w, x \rangle \oplus c_i$, $i \in \{1, \dots, 2^{n-2t}\}$, for some $w \in \mathbb{F}_2^n$ and $c_1, \dots, c_{2^{n-2t}} \in \mathbb{F}_2$.*

Proof. Denote by S_w the set of all shifts of L such that the function $f(x) \oplus \langle w, x \rangle$ is a constant on it. Note that if $f|_{a \oplus L}(x) = \langle w, x \rangle \oplus c$, then for any $w' \in w \oplus L^\perp$ we have $f|_{a \oplus L}(x) = \langle w', x \rangle \oplus \langle w \oplus w', a \rangle \oplus c$. Thus, $S_w = S_{w \oplus u}$ for $u \in L^\perp$. According to Statement 1 the function f is affine on each of 2^{n-t} distinct shifts of L . Therefore,

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

so, $|S_w| \geq 2^{n-t} 2^{n-t} / 2^n = 2^{n-2t}$ for some $w \in \mathbb{F}_2^n$. $\square$

Statement 3. Let f be a Boolean function in n variables, L be an affine subspace of $\mathbb{F}_2^n$, $a \in \mathbb{F}_2^n$ and for some $w \in \mathbb{F}_2^n$ and $c_1, c_2 \in \mathbb{F}_2$

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

Then f is affine on affine subspace $L \cup (a \oplus L)$.

Proof. Suppose that $a \notin L$, in other case the statement is trivial. It is also clear that $L \cup (a \oplus L)$ is an affine subspace. Consider the function $f'(x) = f(x) \oplus \langle w, x \rangle \oplus c_1$: function f is affine on an affine subspace if and only if f' is affine on it. If $c_1 = c_2$, the statement is obvious. In other way we have $f'|_L = 0$ and $f'|_{a \oplus L} = 1$. Without loss of generality suppose that L is a linear subspace (we can consider affinity of function $f'(x \oplus s)$ on a linear subspace for any $s \in L$). Let $v \in L^\perp$. Then $f'|_L(x) = 0 = \langle v, x \rangle$. Moreover, if $\langle v, a \rangle = 0$ for any v , then $a \in (L^\perp)^\perp = L$, but $a \notin L$. So, $\langle v', a \rangle = 1$ for some $v' \in L^\perp$. Therefore,

$$f'|_{a \oplus L}(x) = 1 + 0 = \langle v', a \rangle \oplus \langle v', a \oplus x \rangle = \langle v', x \rangle$$

because of $a \oplus x \in L$. Thus, $f'|_{L \cup (a \oplus L)}(x) = \langle v', x \rangle$. $\square$

Lemma 4. Let f be a quadratic Boolean function in $2k$ variables and U be a $(2k-1)$ -dimensional affine subspace of $\mathbb{F}_2^{2k}$. Then there exists a k -dimensional affine subspace $L \subseteq U$ such that f is affine on L .

Proof. Note that $\mathbb{F}_2^{2k} = U \cup (c \cup U)$ for some $c \in \mathbb{F}_2^{2k}$, since U is of dimension $2k-1$. We will prove by induction that there exists a t -dimensional affine subspace L of $\mathbb{F}_2^{2k}$, $t \leq k$, such that $L \subseteq U$ and f is affine on L . The base of the induction $t = 0$ is obvious, since such affine subspace contains only one element.

Suppose that the statement is true for some $t < k$. Let's prove that it holds for $t + 1$. By the assumption there exists an affine subspace L of dimension t such that f is affine on L and $L \subseteq U$. By Statement 2 for some $w \in \mathbb{F}_2^{2k}$ there exist distinct $a_1 \oplus L, \dots, a_{2^{2k-2t}} \oplus L$ such that for some $w \in \mathbb{F}_2^{2k}$ it holds that $f|_{a_i \oplus L}(x) = \langle w, x \rangle \oplus c_i$, $c_i \in \mathbb{F}_2$. Since $t < k$, we have $2^{2k-2t} \geq 4$ distinct affine subspaces.

Therefore, there always exist distinct $a \oplus L$, $b \oplus L$, $a, b \in \mathbb{F}_2^{2k}$, among $a_1 \oplus L, \dots, a_{2^{2k-2t}} \oplus L$ such that $a \oplus L, b \oplus L \subseteq U$ or $a \oplus L, b \oplus L \subseteq c \oplus U$. Next, by Statement 3 function f is affine on $L' = (a \oplus L) \cup (b \oplus L)$ of dimension $t + 1$. If $L' \subseteq U$, the lemma is proved. Otherwise $L' \subseteq c \oplus U$. By Statement 1 function f is affine on $c \oplus L'$ and $c \oplus L' \subseteq U$. $\square$

5. Connectivity of GM_{2k}

The following lemma is basic for the connectivity proof of GM_{2k} .

Lemma 5. *Let f be a quadratic bent function in $2k$ variables. Then there is a path in GM_{2k} between f and $f(x_1, \dots, x_{2k-1}, x_{2k} \oplus x_1 \oplus c)$, $c \in \mathbb{F}_2$.*

Proof. Since f is quadratic, represent it as follows:

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

where $w_1, \dots, w_{2k-1}, d \in \mathbb{F}_2$. Then

$$\begin{aligned} g(x_1, \dots, x_{2k}) &\stackrel{\text{def}}{=} f(x_1, \dots, x_{2k-1}, x_{2k} \oplus x_1 \oplus c) = \\ &= f(x) \oplus (w_1 x_1 \oplus \dots \oplus w_{2k-1} x_{2k-1} \oplus d)(x_1 \oplus c). \end{aligned}$$

Let $S = \text{supp}(w_1 x_1 \oplus \dots \oplus w_{2k-1} x_{2k-1} \oplus d)(x_1 \oplus c)$. Note that S is an affine subspace. We prove that there exists a k -dimensional affine subspace L of $\mathbb{F}_2^{2k}$ such that $L \subseteq S$ and f is affine on L . Case $w_1 = \dots = w_{2k-1} = 0$ is impossible, because a bent function $f(x) \oplus dx_k$ must depend on each of its variables. Therefore, there exists $w_t \neq 0$ for some $1 \leq t \leq 2k - 1$. If only $w_1 \neq 0$, then $S = \text{supp}(x_1 \oplus c)(x_1 \oplus d)$. If $c \neq d$, then $f = g$. Otherwise S is a linear subspace of dimension $2k - 1$ and by Lemma 4 there exists required L . If there exists other nonzero w_t , we may suppose that $t = 2k - 1$. Then $f|_{x_{2k-1}=w_1 x_1 \oplus \dots \oplus w_{2k-2} x_{2k-2} \oplus d \oplus 1 \oplus x_{2k}}$ equals to

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

as a function in $2k - 2$ variables. Let $U = \text{supp}(x_1 \oplus c)$. Then by Lemma 4 there exists a $(k - 1)$ -dimensional affine subspace $L' \subseteq U$ of $\mathbb{F}_2^{2k-2}$ such that $f'(x_1, \dots, x_{2k-2}, w_1 x_1 \oplus \dots \oplus w_{2k-2} x_{2k-2} \oplus d \oplus 1)$ is affine on L' .

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

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

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

To complete the proof, note that, due to choosing of L , we have

$$S = (a_1 \oplus L) \cup \cdots \cup (a_m \oplus L) \quad \text{for some } a_1, \dots, a_m \in \mathbb{F}_2^{2k},$$

$m = 2^{\dim S - \dim L}$. And since f is quadratic, it is affine on each $a_i \oplus L$ too. Next, let $f_0 = f$ and $f_i = f_{i-1} \oplus \text{Ind}_{a_i \oplus L}$, $1 \leq i \leq m$. Then $f_m = g$ and each f_i is a bent function because $a_1 \oplus L, \dots, a_m \oplus L$ do not intersect. Moreover, each f_i is affine on $a \oplus L$ for any $a \in \mathbb{F}_2^{2k}$. Thus, all $f_i \in \widetilde{\mathcal{M}}_{2k}$ by Lemma 3. $\square$

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

Proof. According to Lemma 1 for any bent function $f_0 \in \mathcal{M}_{2k}$ there exist n and $f_1, \dots, f_n \in \mathcal{M}_{2k}$ such that $\text{dist}(f_i, f_{i+1}) = 2^k$ and $f_n(x, y) = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ky_k$. Therefore, for any bent function $f_0 \in \widetilde{\mathcal{M}}_{2k}$ there exist n and $f_1, \dots, f_n \in \widetilde{\mathcal{M}}_{2k}$ such that $\text{dist}(f_i, f_{i+1}) = 2^k$ and f_n is a quadratic bent function, i.e. there exists a path in GM_{2k} between any $f_0 \in \widetilde{\mathcal{M}}_{2k}$ and some quadratic bent function. Thus, it remains to prove the existence of a path in GM_{2k} between any two quadratic bent functions.

According to Dickson's theorem, any two quadratic bent functions are affinely equivalent, i.e. for any two quadratic bent functions f, g in $2k$ variables there exist an invertible $2k \times 2k$ binary matrix A and $b \in \mathbb{F}_2^{2k}$ such that $g(x) = f(xA \oplus b)$ for any $x \in \mathbb{F}_2^{2k}$. At the same time by Lemma 5 there exists a path in GM_{2k} between any quadratic function f and $f(x_1, \dots, x_{2k-1}, x_{2k} \oplus x_1 \oplus c)$. On the one hand, we can extend Lemma 5 (using permutations on variable numbers) to transformations of the form

$$x'_l = x_l \quad \text{for all } l \in \{1, \dots, 2k\} \setminus \{i\}, \quad x'_i = x_i \oplus x_j \oplus c$$

for any $i, j \in \{1, \dots, 2k\}$, $i \neq j$ and $c \in \mathbb{F}_2$. On the other hand, the set of all these transformations generates any invertible affine transform $xA \oplus b$. The theorem is proved. $\square$

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

It follows from the Theorem because all bent functions in 2, 4 and 6 variables are affinely equivalent to Maiorana–McFarland bent functions.

6. Conclusion

In general, GB_{2k} is not connected starting with $k = 7$ due to the existence of isolated vertices, i.e. such bent functions for which there are no bent functions at the distance 2^k from them. Such bent functions are called *non-weakly normal*, they were constructed in [2]. Connectivity of GB_{2k} without isolated vertices is an open question.

References

- [1] Carlet C., “Two new classes of bent functions”. In: “*Advances in Cryptology—EURO-CRYPT’93*”, Lect. Notes Comput. Sci., **765** 1994, 77–101.
- [2] Canteaut A., Daum M., Dobbertin H., Leander G., “Finding nonnormal bent functions”, *Discrete Appl. Math.*, **154**:2 (2006), 202–218.
- [3] 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”, *Prikl. Diskretn. Matem. (Appl. Discrete Math.)*, **3** (25) (2014), 28–39 (in Russian).
- [4] Kolomeec N. A., Pavlov A. V., “Properties of bent functions at the minimal distance”, *Prikl. Diskretn. Matem. (Appl. Discrete Math.)*, **4** (6) (2009), 5–20 (in Russian).
- [5] Logachev O. A., Sal’nikov A. A., Smyshlyaev S. V., Yashenko V. V., *Boolean functions in coding theory and cryptography*, Moscow: MCCME, 2012 (in Russian), 584 pp.
- [6] McFarland R. L., “A family of difference sets in non-cyclic groups”, *J. Combin. Theory, Ser. A*, **15**:1 (1973), 1–10.
- [7] Rothaus O., “On bent functions”, *J. Combin. Theory, Ser. A*, **20**:3 (1976), 300–305.
- [8] Tokareva N. N., “Bent functions: results and applications. A survey”, *Prikl. Diskretn. Matem. (Appl. Discrete Math.)*, № 1 (3) (2009), 15–37 (in Russian).
- [9] Tokareva N., *Bent Functions, Results and Applications to Cryptography*, N. Y./Amsterdam etc.: Academic Press/Elsevier, 2015, 220 pp.