ISSN 1990-4789, Journal of Applied and Industrial Mathematics, 2008, Vol. 2, No. 4, pp. 1–21. © Pleiades Publishing, Ltd., 2008.
Original Russian Text © N.N. Tokareva, 2007, published in Diskretnyi Analiz i Issledovanie Operatsii, Ser. 1, 2007, Vol. 14, No. 4, pp. 76–102.

Bent Functions With Stronger Nonlinear Properties: k-Bent Functions

N. N. Tokareva*

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

Received May 11, 2007

Abstract—We introduce the notion of *k-bent function*, i.e., a Boolean function with even number$m$ of variables $v_1, \ldots, v_m$ that can be approximated with all functions of the form $\langle \mathbf{u}, \mathbf{v} \rangle_j \oplus a$ in the equally bad manner, where $\mathbf{u} \in \mathbb{Z}_2^m$, $a \in \mathbb{Z}_2$, and $1 \leqslant j \leqslant k$. Here $\langle \cdot, \cdot \rangle_j$ is an analog of the inner product of vectors; k changes from 1 to $m/2$. The operations $\langle \cdot, \cdot \rangle_k$, $1 \leqslant k \leqslant m/2$, are defined by using the special series of binary Hadamard-like codes A_m^k of length 2^m. Namely, the vectors of values for the functions $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$ are codewords of the code A_m^k. The codes A_m^k are constructed using subcodes of the $\mathbb{Z}_4$-linear Hadamard-like codes of length 2^{m+1}, which were classified by D. S. Krotov (2001). At that the code A_m^1 is linear and $A_m^1, \ldots, A_m^{m/2}$ are pairwise nonequivalent. On the codewords of any code A_m^k we define a group operation $\bullet$ coordinated with the Hamming metric. That is why we can consider k-bent functions as functions that are maximal nonlinear in k distinct senses of linearity at the same time. Bent functions in usual sense coincide with 1-bent functions. For $k > \ell \geqslant 1$, the class of k-bent functions is a proper subclass of the class of ℓ-bent functions. In the paper, we give methods for constructing k-bent functions and study their properties. It is shown that there exist k-bent functions with any algebraic degree d, where $2 \leqslant d \leqslant \max\{2, \frac{m}{2} - k + 1\}$. For an arbitrary k, we define the subset $\mathfrak{F}_m^k$ of the set $\mathfrak{F}_m$ of all Boolean functions in m variables with the following property: on this subset k-bent functions and 1-bent functions coincide.

DOI: 10.1134/S1990478908040017

INTRODUCTION

It is known that one of the most important characteristics of a Boolean function in cryptology is the measure of its nonlinearity. The linearity and some close to it properties of a Boolean function often can allow us to extract a lot of other function's properties. And of course it is hardly desired from the cryptographic point of view. We know *bent functions* as Boolean functions that reach the maximum of nonlinearity. By definition, they are "moved away" from all affine functions on the maximal possible distance. In Russian terminology, instead of *bent function* the term *maximal nonlinear function* is widely used. But there is a small difference: we consider bent functions in m variables for even m only whereas the maximal nonlinear functions in m variables exist for any m. For even m, these two notions coincide. The bent functions were introduced by O. Rothaus in the sixties of XX century although the paper [35] was published only in 1976. J. Dillon [13] and R. L. McFarland [28] considered the bent

*E-mail: tokareva@math.nsc.ru

functions in connection with difference sets. Nowadays there is a lot of constructions for bent functions, see surveys [25] and [14]. Nevertheless, the class of all bent functions in m variables is not described yet. There is no asymptotic for the number of bent functions. Moreover, there are no acceptable lower and upper bounds for this number (to meet some progress in this direction, see [10]). The distinct generalizations of the notion of bent function are known; e.g., see [2, 21, 22, 24, 34]. The objects tightly connected to bent functions are widely studied; for example, the bent sequences [32]. The bent functions play a very important role in coding theory. They are used for constructing Kerdock codes, Preparata and BCH codes. They are interesting also for studying subcodes of the second order Reed–Muller codes, several cyclic and optimal codes (for instance, see [26] and [8, 11, 12, 36]). Among the last studies of bent functions' properties we can mention [6].

In the geometric interpretation, the vectors of values for all affine Boolean functions $\langle \mathbf{u}, \mathbf{v} \rangle \oplus a$ in m variables form the binary *linear Hadamard code* of length 2^m (or *the first order Reed–Muller code*). For bent functions, the vectors of values are on the maximal possible distance $2^{m-1} - 2^{(m/2)-1}$ from this code (if m is even). Informally, every function f from the class of bent functions can be approximated by affine functions too bad as it is only possible. It is this property of Boolean functions used in block ciphers that promotes the extreme rise of cryptographic resistance of these ciphers with respect to linear [27] and differential [3] cryptanalyses (see [29] for details).

We can find in the literature some other classes of approximating functions distinct with the class of affine functions. In 2001, A. Youssef and G. Gong [39] proposed the approximations by *proper monomial functions* (this term was given later in [23]). The authors of [39] considered Boolean functions in m variables as functions from $GF(2^m)$ to $GF(2)$: for any binary vector $\mathbf{v}$ they put into correspondence the appropriate element of the field $GF(2^m)$. Let $tr : GF(2^m) \to GF(2)$ be the trace function, i.e.,

$$tr(\mathbf{v}) = \mathbf{v} + \mathbf{v}^2 + \cdots + \mathbf{v}^{2^{m-1}}, \qquad \mathbf{v} \in GF(2^m).$$

Then each linear function $\langle \mathbf{u}, \mathbf{v} \rangle$ can be presented as $tr(a_{\mathbf{u}}\mathbf{v})$ for a suitable element $a_{\mathbf{u}} \in GF(2^m)$. Functions of the form $tr(a_{\mathbf{u}}\mathbf{v}^s)$, where s is integer such that $1 \leqslant s \leqslant 2^m - 1$ and $\gcd(s, 2^m - 1) = 1$, are called *proper monomial functions*. Authors of [39] by *hyper-bent functions* mean the functions that can be approximated by all proper monomial functions in the worse manner. For every even m, they proved the existence of such hyper-bent functions. C. Carlet and P. Gaborit [9] and independently A. S. Kuzmin, V. T. Markov, A. A. Nechaev, and A. B. Shishkov [23] have shown that the algebraic degree of every hyper-bent function in m variables is equal to $m/2$. The approximations by nonlinear functions are studied, for example, in [18] and [16].

The main idea of this paper is the following: Although a bent function f is badly approximated by linear functions, it may be approximated good enough by nonlinear functions that are "linear" in some "alternative" sense. Then, using such bent functions for instance in a block cipher, we probably may collide with its weakness with respect to the appropriate modifications of linear or some other methods of cryptanalysis. In order to avoid some of such situations, we consider the bent functions with stronger nonlinear properties: bent functions in m variables that are maximal nonlinear in k distinct senses of "linearity" at the same time, where k changes from 1 to $m/2$.

Since the nineties of XX century, in coding theory there are intensively studied the nonlinear codes that can be transformed to some linear codes in other metric spaces via appropriate mappings (as a

rule, one-to-one and isometric), see [4, 5, 7, 15, 19, 20, 30]. Consider $\mathbb{Z}_2$- and $\mathbb{Z}_4$-linear codes with parameters of Hadamard codes (further, briefly *Hadamard-like codes*). It is known that $\mathbb{Z}_2$-linear (i.e., linear in the usual sense) binary Hadamard code of length 2^m is unique up to an equivalence. D. S. Krotov [20] has shown that there exist exactly $\lfloor m/2 \rfloor$ pairwise nonequivalent $\mathbb{Z}_4$-linear Hadamard-like codes of length 2^{m+1} if $m \geqslant 3$. Basing on the classification of all such codes (given by D. S. Krotov [20]), we consider the series of some "alternatively linear" binary Hadamard-like codes A_m^k, $1 \leqslant k \leqslant \lfloor m/2 \rfloor$, of length 2^m. Every code A_m^k in this series is obtained from the linear quaternary code $\mathcal{A}_m^k$ by changing the elements 0 and 1 in every position to 0; and 2, 3, to 1. Here $\mathcal{A}_m^k$ is a subcode of the corresponding linear quaternary Hadamard-like code of the type $4^k 2^{m-2k}$ (see [20]) that consists of all codewords having in the first position only 0 or 2. At that, the code A_m^1 is linear and $A_m^1, \ldots, A_m^{\lfloor m/2 \rfloor}$ are pairwise nonequivalent codes. Every code A_m^k is an Abelian group with respect to operation $\bullet$ produced by operation $+$ of coordinatewise addition over $\mathbb{Z}_4$ defined on $\mathcal{A}_m^k$. The operation $\bullet$ is coordinated with Hamming metric. So, the code A_m^k is "alternatively linear" in this sense.

Let the set $\mathfrak{A}_m^k$ be consisted of all Boolean functions with vectors of values being codewords of the code A_m^k. The class $\mathfrak{A}_m^k$ includes functions of the form $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$, where $a \in \mathbb{Z}_2$ and operation $\langle \cdot, \cdot \rangle_k$ plays the role of the inner product. Further we call such functions *k-affine* in analogy with usual affine functions. These codes A_m^k are chosen for the arising new inner products $\langle \cdot, \cdot \rangle_k$ have many properties of the usual inner product and also for us to be able to develop some constructive ideas on this base. Let $\mathbf{u} = (u_1, \ldots, u_m)$ and $\mathbf{v} = (v_1, \ldots, v_m)$. Then the explicit view of the product $\langle \mathbf{u}, \mathbf{v} \rangle_k$ is

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \Big(\bigoplus_{i=1}^{k} \bigoplus_{j=i}^{k} Y_i Y_j \Big) \oplus \langle \mathbf{u}, \mathbf{v} \rangle,$$

where $Y_i = (u_{2i-1} \oplus u_{2i})(v_{2i-1} \oplus v_{2i})$ for any integer i, $1 \leqslant i \leqslant \lfloor m/2 \rfloor$. Thus, any class $\mathfrak{A}_m^k$ contains exactly $2^{m-k+1}(k+1)$ affine functions and $2^{m-k+1}(2^k - k - 1)$ quadratic functions.

Using the inner product $\langle \cdot, \cdot \rangle_k$, we define *$k$-Walsh–Hadamard transform* $W_f^{(k)}(\cdot)$ and *k-nonlinearity* $N_f^{(k)}$ of a Boolean function f. We call a Boolean function with even number of variables m *maximal k-nonlinear* (*k-bent*), $1 \leqslant k \leqslant m/2$, if the vector of values of this function is on the maximal possible distance $2^{m-1} - 2^{(m/2)-1}$ from the each Hadamard-like code A_m^j, $j = 1, \ldots, k$ (or equivalently, $W_f^{(j)}(\mathbf{v}) = \pm 2^{m/2}$ for any $\mathbf{v} \in \mathbb{Z}_2^m$ and every $j = 1, \ldots, k$). In other words, every k-bent function can be approximated by Boolean functions from the each class $\mathfrak{A}_m^j$, $j = 1, \ldots, k$ in the equally bad manner. Usual bent functions form the class of 1-bent functions $\mathfrak{B}_m^1$. For $k > \ell \geqslant 1$ the class $\mathfrak{B}_m^k$ of k-bent functions is a proper subclass of the class $\mathfrak{B}_m^\ell$ of ℓ-bent functions. In the paper we give methods for constructing k-bent functions for every k, $1 \leqslant k \leqslant m/2$, and study their properties. In particular, it is shown that there exist k-bent functions with any algebraic degree d, where $2 \leqslant d \leqslant \max\{2, \frac{m}{2} - k + 1\}$. For any k we define the subset $\mathfrak{F}_m^k$ of the set $\mathfrak{F}_m$ of all Boolean functions with the following property: on this subset k-bent functions and 1-bent functions coincide.

Necessary definitions and notation are given in § 1. In § 2 we define binary Hadamard-like codes A_m^k. Then in § 3 we introduce inner products $\langle \cdot, \cdot \rangle_k$ that correspond to codes A_m^k. k-Affine Boolean functions $\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$ and their algebraic normal forms are studied in § 4. The notion of k-bent function and methods of constructing such functions are presented in § 5 and § 6 respectively. In § 7 we consider interrelation between k-bent functions and usual bent functions.

1. NECESSARY DEFINITIONS AND NOTATION

Let $\mathbb{N}$ be the set of natural numbers, $\langle \mathbf{u}, \mathbf{v} \rangle$ be the usual inner product of binary vectors $\mathbf{u} = (u_1, \ldots, u_m)$, $\mathbf{v} = (v_1, \ldots, v_m)$ of length m, i.e.,

$$\langle \mathbf{u}, \mathbf{v} \rangle = \bigoplus_{j=1}^{m} u_j v_j,$$

where $\oplus$ is the addition modulo 2. Denote by $\mathfrak{F}_m$ the set of all Boolean functions in m variables. By $\mathfrak{A}_m$ denote the class of all affine Boolean functions $\langle \mathbf{u}, \mathbf{v} \rangle \oplus a$ in m variables $v_1, \ldots, v_m$. To any Boolean function $f \in \mathfrak{F}_m$ we put into correspondence the binary vector $\mathbf{f}$ of its values. The length of $\mathbf{f}$ equals 2^m. Further we use bold font for vectors and normal font for functions. The *Hamming weight* $wt_H(\mathbf{v})$ of a binary vector $\mathbf{v}$ is the number of its nonzero coordinates. The *Hamming distance* $d_H(\mathbf{u}, \mathbf{v})$ between binary vectors equals the number of coordinates in which they differ. By distance $\mathrm{dist}(f, g)$ between two Boolean functions f and g we mean Hamming distance between their vectors of values. Remember that the integer-valued function W_f defined on $\mathbb{Z}_2^m$ as

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

is called *Walsh–Hadamard transform* (or *discrete Fourier transform*) of a function $f \in \mathfrak{F}_m$. The values $W_f(\mathbf{v})$ are called *Walsh–Hadamard coefficients* of f. For W_f the Parseval's equality holds:

$$\sum_{\mathbf{v} \in \mathbb{Z}_2^m} (W_f(\mathbf{v}))^2 = 2^{2m}.$$

It follows from here that

$$\max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f(\mathbf{v})| \geqslant 2^{m/2}.$$

By *nonlinearity* N_f of a Boolean function f we as usual mean the distance between f and the set of all affine functions, i. e.

$$N_f = \mathrm{dist}(f, \mathfrak{A}_m) = 2^{m-1} - \frac{1}{2} \max_{\mathbf{v} \in \mathbb{Z}_2^m} |W_f(\mathbf{v})|$$

(see details in [25] for example). A function $f \in \mathfrak{F}_m$ is said to be *maximal nonlinear* (m is any), if parameter N_f gets the maximal possible value. A function f is a *bent function* (m is even), if all Walsh–Hadamard coefficients of it are equal to $\pm 2^{m/2}$. For even m, these two definitions coincide. Denote by $\mathfrak{B}_m$ the class of bent functions in m variables.

Let us remind several basic notions of coding theory. Let $\langle \mathbb{Z}_2^n, d_H \rangle$ denote the metric space on the set of all binary vectors of length n equipped with Hamming metric. A nonempty set $C \subseteq \mathbb{Z}_2^n$ of size $|C| = M$ with minimal distance d between its distinct elements is called a *binary* $(n, M, d)_2$*-code* (or a *binary code with parameters* n, M and d). Elements of C are said to be *codewords*. Numbers n and d are *length* and *code distance* of the code respectively. A code is *linear*, if it is a linear subspace of $\mathbb{Z}_2^n$. The *Lee weight* $wt_L(\cdot)$ of a quaternary vector is the sum (in usual sense) of weights for its coordinates, where $wt_L(0) = 0, wt_L(1) = wt_L(3) = 1, wt_L(2) = 2$. The *Lee distance* $d_L(\mathbf{x}, \mathbf{y})$ between quaternary vectors $\mathbf{x}$ and $\mathbf{y}$ of the same lengths is given by $d_L(\mathbf{x}, \mathbf{y}) = wt_L(\mathbf{x} - \mathbf{y})$. Let $\langle \mathbb{Z}_4^n, d_L \rangle$ be the metric space on the set of all quaternary vectors of length n with Lee metric. By $+$ we denote the addition over $\mathbb{Z}_4$. We denote the parameters of a quaternary code by $(n, M, d)_4$. Let $\mathbf{0}, \mathbf{1}, \mathbf{2}$ and $\mathbf{3}$ be vectors with all coordinates equal to $0, 1, 2$ and 3 respectively. Let $\beta, \gamma : \mathbb{Z}_4 \to \mathbb{Z}_2$ be the following maps

c	$\beta(c)$	$\gamma(c)$
0	0	0
1	0	1
2	1	1
3	1	0

Let $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ denote the Gray map:

$$\varphi(c) = (\beta(c), \gamma(c)) \text{ for } c \in \mathbb{Z}_4.$$

Maps β, γ, and φ can be coordinatewise extended to $\beta, \gamma : \mathbb{Z}_4^i \to \mathbb{Z}_2^i$, and $\varphi : \mathbb{Z}_4^i \to \mathbb{Z}_2^{2i}$ for all integer i. Remember that, according to [15], the map φ is an isometry; i.e., for any $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_4^i$, it holds

$$d_L(\mathbf{x}, \mathbf{y}) = d_H(\varphi(\mathbf{x}), \varphi(\mathbf{y})).$$

A code of length n over $\mathbb{Z}_4$ is called *linear*, if it is a subgroup of $\mathbb{Z}_4^n$ (probably, it is more correct to call it a *group code*). A binary code C is $\mathbb{Z}_4$-*linear*, if the code $\varphi^{-1}(C)$ is linear.

2. CODES A_m^k WITH PARAMETERS OF HADAMARD CODES

In this section we define binary Hadamard-like codes A_m^k and group operations on them.

Let $m \in \mathbb{N}$, k be a fixed integer number such that $0 \leqslant k \leqslant m/2$. In what follows let $n = 2^m$. By $\mathbf{G}_m^k$ denote the $(m-k) \times n$-matrix over $\mathbb{Z}_4$ that consists of lexicographically ordered columns $\mathbf{z}^T$, where $\mathbf{z}$ runs through $\mathbb{Z}_4^k \times (2\mathbb{Z}_4)^{m-2k}$. For example,

$$\mathbf{G}_1^0 = \begin{pmatrix} 02 \end{pmatrix}, \mathbf{G}_2^0 = \begin{pmatrix} 0022 \\ 0202 \end{pmatrix}, \mathbf{G}_2^1 = \begin{pmatrix} 0123 \end{pmatrix}, \mathbf{G}_3^0 = \begin{pmatrix} 00002222 \\ 00220022 \\ 02020202 \end{pmatrix},$$

$$\mathbf{G}_3^1 = \begin{pmatrix} 00112233 \\ 02020202 \end{pmatrix}, \mathbf{G}_4^2 = \begin{pmatrix} 0000111122223333 \\ 0123012301230123 \end{pmatrix}.$$

The matrices of this type were first considered by D. S. Krotov for constructing and classifying $\mathbb{Z}_4$-linear Hadamard-like and perfect codes (see [19, 20]). Let the mapping $\varphi_k : \mathbb{Z}_4^k \times \mathbb{Z}_2^{m-2k} \to \mathbb{Z}_2^m$ be given by

$$\varphi_k : (\mathbf{u}', \mathbf{u}'') \to (\varphi(\mathbf{u}'), \mathbf{u}'') \text{ for any vectors } \mathbf{u}' \in \mathbb{Z}_4^k, \mathbf{u}'' \in \mathbb{Z}_2^{m-2k}.$$

In a similar manner as it was done in [5] define the binary operation

$$\star : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2^m$$

by equality

$$\mathbf{u} \star \mathbf{v} = \varphi_k(\varphi_k^{-1}(\mathbf{u}) + \varphi_k^{-1}(\mathbf{v})) \text{ for any vectors } \mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m,$$

where $+$ denotes the addition over $\mathbb{Z}_4$ for the first k coordinates of vectors $\varphi_k^{-1}(\mathbf{u})$, $\varphi_k^{-1}(\mathbf{v})$ and denotes the addition over $\mathbb{Z}_2$ for the rest $m-2k$ coordinates. Let the quaternary vector $\mathbf{h^u}$ of length n be defined as

$$\mathbf{h^u} = \varphi_k^{-1}(\mathbf{u}) \cdot \mathbf{G}_m^k. \tag{1}$$

It is easy to note that, for all vectors $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$, it holds

$$\mathbf{h^u} + \mathbf{h^v} = \mathbf{h^{u \star v}}.$$

Let $\mathbf{C}_m^k = (c_{\mathbf{u},\mathbf{v}}^k)$, $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$, be the $n \times n$-matrix over $\mathbb{Z}_4$ with the rows $\mathbf{h^u}$. We arrange these rows in the lexicographical order of vectors $\varphi_k^{-1}(\mathbf{u})$. We will numerate the columns of $\mathbf{C}_m^k$ by the vectors $\mathbf{v}$ in the lexicographical order of vectors $\varphi_k^{-1}(\mathbf{v})$ too. For instance,

$$\mathbf{C}_1^0 = \begin{pmatrix} 00 \\ 02 \end{pmatrix}, \ \mathbf{C}_2^0 = \begin{pmatrix} 0000 \\ 0202 \\ 0022 \\ 0220 \end{pmatrix}, \ \mathbf{C}_2^1 = \begin{pmatrix} 0000 \\ 0123 \\ 0202 \\ 0321 \end{pmatrix},$$

$$\mathbf{C}_3^0 = \begin{pmatrix} 00000000 \\ 02020202 \\ 00220022 \\ 02200220 \\ 00002222 \\ 02022020 \\ 00222200 \\ 02202002 \end{pmatrix}, \ \mathbf{C}_3^1 = \begin{pmatrix} 00000000 \\ 02020202 \\ 00112233 \\ 02132031 \\ 00220022 \\ 02200220 \\ 00332211 \\ 02312013 \end{pmatrix}.$$

And for example if $m = 2$ we have $c_{(10),(01)}^1 = 3$. Let J_s be the $s \times s$-matrix with all ones. For squarte matrices $A = (a_{i,j})$ and B of orders p and q respectively denote by $A \otimes B$ their Kronecker product

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1p}B \\ \dots & \dots & \dots \\ a_{p1}B & \dots & a_{pp}B \end{pmatrix}.$$

Further we use the following properties of matrices $\mathbf{C}_m^k$.

Proposition 1. *For any integer m, k such that $0 \leqslant k \leqslant m/2$, it holds*

(i) $\mathbf{C}_{m+1}^k = (\mathbf{C}_m^k \otimes J_2) + (J_n \otimes \mathbf{C}_1^0)$;

(ii) $\mathbf{C}^{k+1}_{m+2} = (J_4 \otimes \mathbf{C}^k_m) + (\mathbf{C}^1_2 \otimes J_n)$;

(iii) $(\mathbf{C}^k_m)^T = \mathbf{C}^k_m$.

Proof. Consider $\mathbf{G}^k_m = (\mathbf{z}_1^T, \ldots, \mathbf{z}_n^T)$. Then the matrix $\mathbf{G}^k_{m+1}$ can be presented as

$$\mathbf{G}^k_{m+1} = \begin{pmatrix} \mathbf{z}_1^T & \mathbf{z}_1^T & \ldots & \mathbf{z}_n^T & \mathbf{z}_n^T \\ 0 & 2 & \ldots & 0 & 2 \end{pmatrix}.$$

Let $\mathbf{h}^{\mathbf{u}} = (h_1, \ldots, h_n)$. By definition we have $\mathbf{h}^{(\mathbf{u},a)} = \varphi_k^{-1}(\mathbf{u}, a) \cdot \mathbf{G}^k_{m+1}$. Using the definition of map φ_k^{-1} we get

$$\mathbf{h}^{(\mathbf{u},a)} = (\varphi_k^{-1}(\mathbf{u}), a) \cdot \mathbf{G}^k_{m+1} = (h_1, h_1 + 2a, \ldots, h_n, h_n + 2a)$$

for any $a \in \mathbb{Z}_2$. Thus, in order to obtain the matrix $\mathbf{C}^k_{m+1}$ we should replace any element $c^k_{\mathbf{u},\mathbf{v}}$ of $\mathbf{C}^k_m$ by the matrix $\begin{pmatrix} c^k_{\mathbf{u},\mathbf{v}} & c^k_{\mathbf{u},\mathbf{v}} \\ c^k_{\mathbf{u},\mathbf{v}} & c^k_{\mathbf{u},\mathbf{v}} + 2 \end{pmatrix}$. In other words, we have $\mathbf{C}^k_{m+1} = (\mathbf{C}^k_m \otimes J_2) + (J_n \otimes \mathbf{C}^0_1)$. So, (i) is true.

Let $\delta = \varphi^{-1}(a, b)$, where $a, b \in \mathbb{Z}_2$. According to the presentation

$$\mathbf{G}^{k+1}_{m+2} = \begin{pmatrix} 0\ldots0 & 1\ldots1 & 2\ldots2 & 3\ldots3 \\ \mathbf{G}^k_m & \mathbf{G}^k_m & \mathbf{G}^k_m & \mathbf{G}^k_m \end{pmatrix}$$

we have $\mathbf{h}^{(a,b,\mathbf{u})} = (\delta, \varphi_k^{-1}(\mathbf{u})) \cdot \mathbf{G}^{k+1}_{m+1} = (\mathbf{h}^{\mathbf{u}}, \mathbf{h}^{\mathbf{u}} + \delta\mathbf{1}, \mathbf{h}^{\mathbf{u}} + \delta\mathbf{2}, \mathbf{h}^{\mathbf{u}} + \delta\mathbf{3})$. Now it is easy to get equality (ii).

The equality (iii) follows from (i), (ii) and equality $(A \otimes B)^T = A^T \otimes B^T$. □

Let quaternary code $\mathcal{A}^k_m$ consist of all possible vectors $\mathbf{h}^{\mathbf{u}}$ and $\mathbf{h}^{\mathbf{u}} + \mathbf{2}$ (see (1)).

Proposition 2 [20]. *The quaternary code $\mathcal{A}^k_m$ is linear and has the parameters $(n, 2n, n)_4$.*

Define the following binary codes of lengths n and $2n$ respectively:

$$A^k_m = \beta(\mathcal{A}^k_m), \qquad H^k_m = \varphi(\mathcal{A}^k_m).$$

It is easy to see that sizes of these codes coincide and equal $2n$. It is possible to define the code A^k_m also as $\gamma(\mathcal{A}^k_m)$. Note that according to [20] any $\mathbb{Z}_4$-linear Hadamard-like code of length $2n$ is equivalent to one of the codes $\varphi\left(\mathcal{A}^k_m \cup (\mathcal{A}^k_m + \mathbf{1})\right)$, where k runs trough all the values $1, \ldots, \lfloor m/2 \rfloor$.

The maximal linear subcode $\mathrm{Ker}(C)$ of a binary code C such that $\mathbf{x} \oplus C = C$ for any vector $\mathbf{x} \in \mathrm{Ker}(C)$ is said to be the *kernel* of the code C.

Proposition 3 [20]. *The codes H^0_m, H^1_m are linear. For $k > 1$ it holds $|\mathrm{Ker}(H^k_m)| = 2^{m-k+1}$.*

It is easy to obtain the following fact.

Proposition 4. *For any k, $0 \leqslant k \leqslant m/2$, it is true* $\mathrm{Ker}(A^k_m) = \beta(\varphi^{-1}(\mathrm{Ker}(H^k_m)))$.

Proof. Let $\varphi(\mathbf{x}) \in \mathrm{Ker}(H_m^k)$ for a certain vector $\mathbf{x} \in \mathcal{A}_m^k$. Then $\varphi(\mathbf{x}) \oplus H_m^k = H_m^k$ and hence, $\beta(\mathbf{x}) \oplus A_m^k = A_m^k$. Consequently,

$$\mathrm{Ker}(A_m^k) \supseteq \beta(\varphi^{-1}(\mathrm{Ker}(H_m^k))).$$

Conversely, let $\beta(\mathbf{x}) \in \mathrm{Ker}(A_m^k)$ for some vector $\mathbf{x} \in \mathcal{A}_m^k$. At first show that the vector $\gamma(\mathbf{x})$ belongs to the set $\mathrm{Ker}(A_m^k)$ too. In fact, by linearity of the quaternary code $\mathcal{A}_m^k$ and according to

$$\beta(2\mathbf{x} + \mathcal{A}_m^k) = \beta(2\mathbf{x}) \oplus \mathcal{A}_m^k,$$

we get $\beta(2\mathbf{x}) \in \mathrm{Ker}(A_m^k)$. As far as the binary subcode $\mathrm{Ker}(A_m^k)$ is linear we obtain $\gamma(\mathbf{x}) = \beta(\mathbf{x}) \oplus \beta(2\mathbf{x}) \in \mathrm{Ker}(A_m^k)$. Then from equality $A_m^k = \beta(\mathcal{A}_m^k) = \gamma(\mathcal{A}_m^k)$ and the fact that vectors $\beta(\mathbf{x}), \gamma(\mathbf{x})$ belong to $\mathrm{Ker}(A_m^k)$, we obtain $\varphi(\mathbf{x}) \in \mathrm{Ker}(H_m^k)$. Really, it is sufficient to note that if the equality $\beta(\mathbf{x}) \oplus \beta(\mathbf{y}) = \beta(\mathbf{z})$ holds for some $\mathbf{y}, \mathbf{z}$ then it also holds $\gamma(\mathbf{x}) \oplus \gamma(\mathbf{y}) = \gamma(\mathbf{z})$. Hence, we have $\mathrm{Ker}(A_m^k) \subseteq \beta(\varphi^{-1}(\mathrm{Ker}(H_m^k)))$. □

Recall that binary codes C and C' of length n are *equivalent*, if there exist a binary vector $\mathbf{x} \in \mathbb{Z}_2^n$ and a permutation τ on n elements such that it holds $\mathbf{x} \oplus C = \tau(C')$, where $\tau(C') = \{\, \tau(\mathbf{y}) \mid \mathbf{y} \in C' \,\}$. From Propositions 3 and 4 it follows that codes $A_m^1, \ldots, A_m^{\lfloor m/2 \rfloor}$ are pairwise nonequivalent. Although the map $\beta : \mathbb{Z}_4^{2^m} \to \mathbb{Z}_2^{2^m}$ is not one-to-one, it is possible to inverse it on the set A_m^k (one can easily prove it). On codewords of A_m^k define the binary operation

$$\bullet : A_m^k \times A_m^k \to A_m^k$$

coordinated with $+$ on the set $\mathcal{A}_m^k$. Namely, consider

$$\mathbf{x} \bullet \mathbf{y} = \beta(\beta^{-1}(\mathbf{x}) + \beta^{-1}(\mathbf{y})) \text{ for any vectors } \mathbf{x}, \mathbf{y} \in A_m^k. \tag{2}$$

It is easy to see that $(A_m^k, \bullet)$ is an Abelian group. For a vector $\mathbf{x} \in A_m^k$ let $\mathbf{x}^{-1}$ be the vector such that $\mathbf{x} \bullet \mathbf{x}^{-1} = \mathbf{0}$. It holds $\beta^{-1}(\mathbf{x}^{-1}) = -\beta^{-1}(\mathbf{x})$.

Let us study properties of the operation $\bullet$.

Proposition 5. *For every $\mathbf{x}, \mathbf{y} \in A_m^k$, it is true*

(i) $wt_H(\mathbf{x}) = \frac{1}{2} wt_L(\beta^{-1}(\mathbf{x}))$;

(ii) $d_H(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} \bullet \mathbf{y}^{-1})$;

(iii) $d_H(\mathbf{x}, \mathbf{y}) = \frac{1}{2} d_L(\beta^{-1}(\mathbf{x}), \beta^{-1}(\mathbf{y}))$.

Proof. (i) Let $\mathbf{x}' = \beta^{-1}(\mathbf{x})$ be a codeword of the code $\mathcal{A}_m^k$. Let b_c denote the number of coordinates of $\mathbf{x}'$ that are equal to c, where $c \in \mathbb{Z}_4$. We have

$$wt_L(\mathbf{x}') = b_1 + 2b_2 + b_3, \qquad wt_H(\mathbf{x}) = b_2 + b_3.$$

The matrix $\mathbf{G}_m^k$ is constructed in such a way that for any its column $\mathbf{z}_1^T$ there exist the only column $\mathbf{z}_2^T$ of $\mathbf{G}_m^k$ such that $\mathbf{z}_2^T = 3\mathbf{z}_1^T$ (the case $\mathbf{z}_1^T = \mathbf{z}_2^T$ is possible). It follows from here that for any codeword of $\mathcal{A}_m^k$ the numbers of coordinates that are equal to 1 and 3 respectively coincide. Thus, according to $b_1 = b_3$ we get the required equality.

(ii) Let $\mathbf{x}' = \beta^{-1}(\mathbf{x})$, $\mathbf{y}' = \beta^{-1}(\mathbf{y})$ be codewords of the code $\mathcal{A}_m^k$. Then it is true

$$wt_H(\mathbf{x} \bullet \mathbf{y}^{-1}) = \frac{1}{2} wt_L(\beta^{-1}(\mathbf{x} \bullet \mathbf{y}^{-1})) = \frac{1}{2} wt_L(\mathbf{x}' - \mathbf{y}').$$

Denote by $\mathrm{supp}(\mathbf{v})$ the set of nonzero components of a binary vector $\mathbf{v}$. By I_c we denote the set of all components of the vector $\mathbf{x}' - \mathbf{y}'$ that are equal to c, $c \in \mathbb{Z}_4$. Let $b_c = |I_c|$. Then it holds $wt_L(\mathbf{x}' - \mathbf{y}') = b_1 + 2b_2 + b_3$. According to (2) we have

$$\mathrm{supp}(\mathbf{x} \bullet \mathbf{y}^{-1}) = I_2 \cup I_3,$$

and hence $wt_H(\mathbf{x} \bullet \mathbf{y}^{-1}) = b_2 + b_3$. For any $c \in \mathbb{Z}_4$ define the subset $I_c^{1,3}$ of the set I_c be consisting of all elements $s \in I_c$ such that $y'_s \in \{1, 3\}$. Then using the definition of β we get

$$\mathrm{supp}(\mathbf{x} \oplus \mathbf{y}) = I_1^{1,3} \cup I_2 \cup (I_3 \setminus I_3^{1,3}).$$

Note that the vector $\mathbf{x} \oplus \mathbf{y}$ may not belong to A_m^k in general. Using the foregoing property of matrix $\mathbf{G}_m^k$ (for any column $\mathbf{z}_1^T$ there exists the only column $\mathbf{z}_2^T$ such that $\mathbf{z}_2^T = 3\mathbf{z}_1^T$, see (i)) we derive $|I_1^{1,3}| = |I_3^{1,3}| = r$. Hence,

$$d_H(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} \oplus \mathbf{y}) = r + b_2 + (b_3 - r) = b_2 + b_3 = wt_H(\mathbf{x} \bullet \mathbf{y}^{-1}).$$

From (i) and (ii) the equality (iii) follows easily. □

By Propositions 2 and 5, the code A_m^k has code distance $n/2$. Thus, from Propositions 2, 3, 4, and 5 it follows

Theorem 1. *For any $m \in \mathbb{N}$, any integer k, $0 \leqslant k \leqslant m/2$ it is true:*

(i) *the binary code A_m^k is a Hadamard-like code with parameters $(n, 2n, n/2)_2$;*

(ii) *the operation $\bullet$ defined on A_m^k is coordinated with Hamming metric:*

$$\textit{for any } \mathbf{x}, \mathbf{y} \in A_m^k \textit{ it holds } d_H(\mathbf{x}, \mathbf{y}) = wt_H(\mathbf{x} \bullet \mathbf{y}^{-1});$$

(iii) *codes A_m^0, A_m^1 are linear; for $k \geqslant 2$, it holds $|\mathrm{Ker}(A_m^k)| = 2^{m-k+1}$.*

As far as the cardinalities of kernels for codes $A_m^1, \ldots, A_m^{\lfloor m/2 \rfloor}$ are all distinct, these codes are pairwise nonequivalent.

3. AN ANALOG $\langle \mathbf{u}, \mathbf{v} \rangle_k$ OF INNER PRODUCT

So, let $\mathbf{C}_m^k = (c_{\mathbf{u},\mathbf{v}}^k)$ be given above quaternary matrix of order n, where vectors $\mathbf{u}, \mathbf{v}$ runs trough the space $\mathbb{Z}_2^m$ in lexicographical order of vectors $\varphi_k^{-1}(\mathbf{u})$ and $\varphi_k^{-1}(\mathbf{v})$ respectively. For any integer k, $0 \leqslant k \leqslant m/2$, define a binary operation

$$\langle \cdot, \cdot \rangle_k : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2$$

by the rule:

$$\langle \mathbf{u}, \mathbf{v} \rangle_k = \beta(c_{\mathbf{u},\mathbf{v}}^k) \text{ for any } \mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m.$$

The operation $\langle \cdot, \cdot \rangle_0$ and the usual inner product coincide, i. e. $\langle \mathbf{u}, \mathbf{v} \rangle_0 = \langle \mathbf{u}, \mathbf{v} \rangle$. Further we use both notation.

Let π_k be the permutation $(1, 2)(3, 4) \ldots (2k - 1, 2k)$ on m elements. We present it as a combination of transpositions. In other words, the vector $\pi_k(\mathbf{u})$ one can obtain from $\mathbf{u} \in \mathbb{Z}_2^m$, by changing over two coordinates of $\mathbf{u}$ in the each pair that forms a $\mathbb{Z}_4$-coordinate by an action of φ_k^{-1}. Note that the sum of rows of the matrix $\mathbf{C}_m^k$ that correspond to $\mathbf{u}$ and $\pi_k(\mathbf{u})$ equals the zero vector for any $\mathbf{u} \in \mathbb{Z}_2^m$.

Several properties of the operation $\langle \cdot, \cdot \rangle_k$ are given in the following statement.

Proposition 6. *Let $m \in \mathbb{N}$, k be integer, $0 \leqslant k \leqslant m/2$. Then for any vectors $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{Z}_2^m$ the equalities hold:*

(i) $\langle \mathbf{u}, \mathbf{v} \rangle_k = \langle \mathbf{v}, \mathbf{u} \rangle_k$;

(ii) $\langle a\mathbf{u}, \mathbf{v} \rangle_k = a\langle \mathbf{u}, \mathbf{v} \rangle_k$ *for any* $a \in \mathbb{Z}_2$;

(iii) $$\sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus \langle \mathbf{w}, \mathbf{v} \rangle_k} = \begin{cases} 2^m, & \text{if } \mathbf{u} = \mathbf{w}, \\ 0 & \text{else;} \end{cases}$$

(iv) $\langle (\mathbf{u}, a), (\mathbf{v}, b) \rangle_k = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus ab$ *for arbitrary* $a, b \in \mathbb{Z}_2$;

(v) $\langle (a, a'), (b, b') \rangle_1 = \langle (a', a), (b, b') \rangle_0$ *for any* $a, a', b, b' \in \mathbb{Z}_2$;

(vi) $\langle (a, a', \mathbf{u}), (b, b', \mathbf{v}) \rangle_{k+1} = \langle (a, a'), (b, b') \rangle_\varepsilon \oplus \langle \mathbf{u}, \mathbf{v} \rangle_k$, *for any* $a, a', b, b' \in \mathbb{Z}_2$, *where parameter* $\varepsilon \in \mathbb{Z}_2$ *is given by the equality* $\varepsilon = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{v} \rangle_k \oplus 1$;

(vii) $\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \mathbf{v}, \mathbf{w} \rangle_k = \langle \mathbf{u} \star \mathbf{v}, \mathbf{w} \rangle_k \oplus \Big(\langle \mathbf{u}, \mathbf{w} \rangle_k \oplus \langle \pi_k(\mathbf{u}), \mathbf{w} \rangle_k \Big) \Big(\langle \mathbf{v}, \mathbf{w} \rangle_k \oplus \langle \pi_k(\mathbf{v}), \mathbf{w} \rangle_k \Big)$.

Proof. The relation (i) follows from Proposition 1. By definition of matrix $\mathbf{C}_m^k$ we get equality (ii).

(iii) Note that the left part of the equality is $2^m - 2d_H(\beta(\mathbf{h}^{\mathbf{u}}), \beta(\mathbf{h}^{\mathbf{w}}))$. Hence, by Theorem 1, we get what we need. Indeed, if $\mathbf{u} \neq \mathbf{w}$ then the distance between codewords $\beta(\mathbf{h}^{\mathbf{u}})$ and $\beta(\mathbf{h}^{\mathbf{w}})$ of A_m^k is equal to 2^{m-1}.

(iv) According to Proposition 1, see (i), it holds $c^k_{(\mathbf{u},a),(\mathbf{v},b)} = c^k_{\mathbf{u},\mathbf{v}} + 2ab$ and hence (iv) is true.

(v) It follows from definition of $\langle \cdot, \cdot \rangle_k$, as far as

$\langle \cdot, \cdot \rangle_0$	00	01	10	11
00	0	0	0	0
01	0	1	0	1
10	0	0	1	1
11	0	1	1	0

$\langle \cdot, \cdot \rangle_1$	00	01	10	11
00	0	0	0	0
01	0	0	1	1
10	0	1	0	1
11	0	1	1	0

(vi) By Proposition 1, see (ii), we get

$$c^{k+1}_{(a,a',\mathbf{u}),(b,b',\mathbf{v})} = \varphi^{-1}(a, a') \cdot \varphi^{-1}(b, b') + c^k_{\mathbf{u},\mathbf{v}}.$$

First, by direct check up, we can establish

$$\langle (a, a'), (b, b') \rangle_0 = \gamma(\varphi^{-1}(a, a') \cdot \varphi^{-1}(b, b')),$$

$$\langle (a, a'), (b, b') \rangle_1 = \beta(\varphi^{-1}(a, a') \cdot \varphi^{-1}(b, b')).$$

Really, we obtain these using (v). It is easy that, for all $p, q \in \mathbb{Z}_4$, it is true

$$\beta(p + q) = \beta(p) \oplus \begin{cases} \beta(q), & \text{if } p \text{ equals 0 or 2,} \\ \gamma(q) & \text{in other case.} \end{cases}$$

And now we have

$$\langle (a,a',\mathbf{u}),(b,b',\mathbf{v})\rangle_{k+1} = \beta(c^{k+1}_{(a,a',\mathbf{u}),(b,b',\mathbf{v})}) = \beta(c^k_{\mathbf{u},\mathbf{v}}) \oplus \langle (a,a'),(b,b')\rangle_\varepsilon,$$

where ε equals 1 or 0 if $c^k_{\mathbf{u},\mathbf{v}}$ belongs or not to $\{0,2\}$ respectively. Note that $c^k_{\mathbf{u},\mathbf{v}}$ belongs to $\{0,2\}$ if and only if $\beta(c^k_{\mathbf{u},\mathbf{v}}) = \gamma(c^k_{\mathbf{u},\mathbf{v}})$. From definition of permutation π_k it follows

$$c^k_{\pi_k(\mathbf{u}),\mathbf{v}} = 3c^k_{\mathbf{u},\mathbf{v}}.$$

For any $p \in \mathbb{Z}_4$ one can see that $\beta(3p) = \gamma(p)$. Therefore for parameter ε we obtain

$$\varepsilon \oplus 1 = \beta(c^k_{\mathbf{u},\mathbf{v}}) \oplus \gamma(c^k_{\mathbf{u},\mathbf{v}}) = \beta(c^k_{\mathbf{u},\mathbf{v}}) \oplus \beta(3c^k_{\mathbf{u},\mathbf{v}}) = \langle \mathbf{u},\mathbf{v}\rangle_k \oplus \langle \pi_k(\mathbf{u}),\mathbf{v}\rangle_k.$$

(vii) As soon as it holds $\mathbf{h}^{\mathbf{u}} + \mathbf{h}^{\mathbf{v}} = \mathbf{h}^{\mathbf{u}\star\mathbf{v}}$ we have $c^k_{\mathbf{u},\mathbf{w}} + c^k_{\mathbf{v},\mathbf{w}} = c^k_{\mathbf{u}\star\mathbf{w}}$. Note that for any $p, q \in \mathbb{Z}_4$ the equality $\beta(p) \oplus \beta(q) = \beta(p+q)$ is true if and only if at least one element among p, q is equal to 0 or 2. By (vi) element $c^k_{\mathbf{u},\mathbf{w}}$ belongs to $\{1,3\}$ if and only if

$$\langle \mathbf{u},\mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{u}),\mathbf{w}\rangle_k = 1.$$

And so,

$$\beta(c^k_{\mathbf{u},\mathbf{w}}) \oplus \beta(c^k_{\mathbf{v},\mathbf{w}}) = \beta(c^k_{\mathbf{u}\star\mathbf{v},\mathbf{w}}) \oplus \Big(\langle \mathbf{u},\mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{u}),\mathbf{w}\rangle_k\Big)\Big(\langle \mathbf{v},\mathbf{w}\rangle_k \oplus \langle \pi_k(\mathbf{v}),\mathbf{w}\rangle_k\Big).$$

It is just what we need. □

Let us find the explicit view of the product $\langle \mathbf{u},\mathbf{v}\rangle_k$.

Proposition 7. *Let $m, k \in \mathbb{N}$ be such that $1 \leqslant k \leqslant m/2$. For arbitrary $i \in \mathbb{N}$, $1 \leqslant i \leqslant m/2$, and any $\mathbf{u},\mathbf{v} \in \mathbb{Z}_2^m$ denote $Y_i = (u_{2i-1} \oplus u_{2i})(v_{2i-1} \oplus v_{2i})$. Then*

$$\langle \mathbf{u},\mathbf{v}\rangle_k = \Big(\bigoplus_{i=1}^{k}\bigoplus_{j=i}^{k} Y_iY_j\Big) \oplus \langle \mathbf{u},\mathbf{v}\rangle.$$

Proof. We prove it by the induction on k.

If $k = 1$ then, according to items (iv) and (v) of Proposition 6, we have

$$\langle \mathbf{u},\mathbf{v}\rangle_1 = u_2v_1 \oplus u_1v_2 \oplus \bigoplus_{i=3}^{m} u_iv_i = (u_1 \oplus u_2)(v_1 \oplus v_2) \oplus \langle \mathbf{u},\mathbf{v}\rangle = Y_1 \oplus \langle \mathbf{u},\mathbf{v}\rangle.$$

Note that for any j it holds $Y_j^2 = Y_j$. Hence, we obtain what was to be proved.

Let the proposition be right for some k, $1 \leqslant k \leqslant (m-2)/2$. Show that it takes a place for $k+1$ too. From (vi) of Proposition 6 it follows

$$\langle \mathbf{u},\mathbf{v}\rangle_{k+1} = \langle (u_1,u_2),(v_1,v_2)\rangle_\varepsilon \oplus \langle (u_3,\ldots,u_m),(v_3,\ldots,v_m)\rangle_k, \tag{3}$$

where

$$\varepsilon = \langle (u_3,\ldots,u_m),(v_3,\ldots,v_m)\rangle_k \oplus \langle \pi_k(u_3,\ldots,u_m),(v_3,\ldots,v_m)\rangle_k \oplus 1.$$

By the inductive hypothesis, we have

$$\langle (u_3,\ldots,u_m),(v_3,\ldots,v_m)\rangle_k = \Big(\bigoplus_{i=2}^{k+1}\bigoplus_{j=i}^{k+1} Y_iY_j\Big) \oplus \bigoplus_{s=3}^{m} u_sv_s.$$

As one can easily see, it holds

$$\langle \pi_k(u_3,\dots,u_m),(v_3,\dots,v_m)\rangle_k = \Big(\bigoplus_{i=2}^{k+1}\bigoplus_{j=i}^{k+1} Y_iY_j\Big)\oplus\bigoplus_{j=2}^{k+1}\big(u_{2j}v_{2j-1}\oplus u_{2j-1}v_{2j}\big)\oplus\bigoplus_{s=2k+3}^{m} u_sv_s.$$

From these two facts it follows

$$\varepsilon = \Big(\bigoplus_{j=2}^{k+1} Y_j\Big)\oplus 1.$$

Then the first item in the right part of equality (3), according to (v) of Proposition 6, can be presented as

$$\langle (u_1,u_2),(v_1,v_2)\rangle_\varepsilon = (\varepsilon\oplus 1)(u_1v_1\oplus u_2v_2)\oplus\varepsilon(u_2v_1\oplus u_1v_2) = \varepsilon Y_1\oplus u_1v_1\oplus u_2v_2.$$

Now we substitute the expression for ε and use equality $Y_1^2 = Y_1$ in order to obtain

$$\langle (u_1,u_2),(v_1,v_2)\rangle_\varepsilon = \Big(\bigoplus_{j=1}^{k+1} Y_1Y_j\Big)\oplus u_1v_1\oplus u_2v_2.$$

Thus, for $\langle \mathbf{u},\mathbf{v}\rangle_{k+1}$ we get the expression

$$\langle \mathbf{u},\mathbf{v}\rangle_{k+1} = \left(\Big(\bigoplus_{j=1}^{k+1} Y_1Y_j\Big)\oplus u_1v_1\oplus u_2v_2\right)\oplus\left(\Big(\bigoplus_{i=2}^{k+1}\bigoplus_{j=i}^{k+1} Y_iY_j\Big)\oplus\bigoplus_{s=3}^{m} u_sv_s\right).$$

And hence,

$$\langle \mathbf{u},\mathbf{v}\rangle_{k+1} = \left(\bigoplus_{i=1}^{k+1}\bigoplus_{j=i}^{k+1} Y_iY_j\right)\oplus\langle \mathbf{u},\mathbf{v}\rangle.$$

□

Corollary 1. *For any vectors $\mathbf{u},\mathbf{v}\in\mathbb{Z}_2^m$ and any k, $1\leqslant k\leqslant m/2$, it holds*

$$\langle \mathbf{u},\mathbf{v}\rangle_k\oplus\langle \pi_k(\mathbf{u}),\mathbf{v}\rangle_k = \bigoplus_{i=1}^{k} Y_i.$$

Corollary 2. *For all $\mathbf{u},\mathbf{v}\in\mathbb{Z}_2^m$ and every k, $1\leqslant k\leqslant (m-2)/2$, it is true*

$$\langle \mathbf{u},\mathbf{v}\rangle_{k+1} = \langle \mathbf{u},\mathbf{v}\rangle_k\oplus Y_{k+1}\Big(\bigoplus_{i=1}^{k+1} Y_i\Big).$$

4. NOTION OF k-AFFINE FUNCTION

Consider $m\in\mathbb{N}$, k be integer, $0\leqslant k\leqslant m/2$. To every vector from the code A_m^k we put into correspondence a Boolean function $g\in\mathfrak{F}_m$: let this vector be a vector of values for g. It means that for some $\mathbf{u}\in\mathbb{Z}_2^m$, $a\in\mathbb{Z}_2$ and arbitrary $\mathbf{v}\in\mathbb{Z}_2^m$ the following equality holds $g(\mathbf{v}) = \langle \mathbf{u},\mathbf{v}\rangle_k\oplus a$. We call such functions *k-affine* and the set of all of them denote by $\mathfrak{A}_m^k$. It is clear that $|\mathfrak{A}_m^k| = 2^{m+1}$. From Proposition 7 it follows

Theorem 2. *For integer m, k, such that $0\leqslant k\leqslant m/2$, the class $\mathfrak{A}_m^k$ consists of functions*

$$g(\mathbf{v}) = \Big(\bigoplus_{i=1}^{k}\bigoplus_{j=i}^{k}(u_{2i-1}\oplus u_{2i})(u_{2j-1}\oplus u_{2j})(v_{2i-1}\oplus v_{2i})(v_{2j-1}\oplus v_{2j})\Big)\oplus\Big(\bigoplus_{s=1}^{m} u_sv_s\Big)\oplus a, \quad (4)$$

where vector $\mathbf{u}$ *runs through* $\mathbb{Z}_2^m$ *and* a *is an element of* $\mathbb{Z}_2$.

For instance, any function $g \in \mathfrak{A}_4^2$ is uniquely determined by a binary vector (u_1, u_2, u_3, u_4) and an element $a \in \mathbb{Z}_2$:

$$g(v_1, v_2, v_3, v_4) = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \oplus u_2v_1 \oplus u_1v_2 \oplus u_4v_3 \oplus u_3v_4 \oplus a.$$

The class $\mathfrak{A}_4^2$ consists of 24 affine and 8 quadratic functions. Quadratic functions are given by vectors $\mathbf{u} \in \{\,(0101), (0110), (1001), (1010)\,\}$ and arbitrary a.

Let f be a Boolean function. Recall that the number of variables in the longest item of its algebraic normal form (or Zhegalkin polynomial) is called the *algebraic degree* (or briefly *degree*) of the function f. We denote it by $\deg f$.

From Theorem 2 it follows that degree of a function from any class $\mathfrak{A}_m^k$ is less or equal than 2. It is true

Proposition 8. *For any* $m \in \mathbb{N}$ *and integer* k, $0 \leqslant k \leqslant m/2$, *the class* $\mathfrak{A}_m^k$ *consists of* $2^{m-k+1}(k+1)$ *affine functions and* $2^{m-k+1}(2^k - k - 1)$ *quadratic functions.*

Proof. According to Theorem 2, a function $g(\mathbf{v}) = \langle \mathbf{u}, \mathbf{v} \rangle_k \oplus a$ is affine if and only if for vector $\mathbf{u}$ it holds one of the following two conditions:

1) for all j, $1 \leqslant j \leqslant k$, it is true $u_{2j-1} = u_{2j}$;

2) there exists the unique number j, $1 \leqslant j \leqslant k$, such that $u_{2j-1} \neq u_{2j}$.

The numbers of vectors $\mathbf{u}$ of the first and the second types are 2^{m-k} and $k2^{m-k}$ respectively. Thus, the number of affine functions in $\mathfrak{A}_m^k$ is equal to $2^{m-k+1}(k+1)$. We get the number of quadratic functions in this class as $2^{m+1} - 2^{m-k+1}(k+1)$. □

It is not hard to prove

Corollary 3. *The part of affine functions in the class* $\mathfrak{A}_m^{m/2}$ *tends to zero as* m *grows up.*

5. NOTION OF k-BENT FUNCTION

For any $m \in \mathbb{N}$ and integer k, $0 \leqslant k \leqslant m/2$, let the integer-valued function $W_f^{(k)}$ be defined on the set $\mathbb{Z}_2^m$ by the equality

$$W_f^{(k)}(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_k \oplus f(\mathbf{u})} \text{ for any } \mathbf{v} \in \mathbb{Z}_2^m.$$

We call it *k-Walsh–Hadamard transform* of a Boolean function $f \in \mathfrak{F}_m$.

Note that $W_f^{(0)}$ is the usual Walsh–Hadamard transform W_f. The matrix $\beta(\mathbf{C}_m^k)$ after replacing any its element c by $(-1)^c$ becomes a Hadamard matrix (thanks to Theorem 1). That is why for $W_f^{(k)}$ an analog of Parseval's equality holds (see, e. g. [25], ch. 6]). For completeness of the text we give the proof of this fact.

Theorem 3. (The Parseval equality for $W_f^{(k)}$). *For any* $m \in \mathbb{N}$ *and integer* k, $0 \leqslant k \leqslant m/2$, *for any function* $f \in \mathfrak{F}_m$ *it holds*

$$\sum_{\mathbf{v} \in \mathbb{Z}_2^m} \left(W_f^{(k)}(\mathbf{v}) \right)^2 = 2^{2m}.$$

Proof. By definition of $W_f^{(k)}$, we have

$$\sum_{\mathbf{v}\in\mathbb{Z}_2^m}(W_f^{(k)}(\mathbf{v}))^2=\sum_{\mathbf{v}\in\mathbb{Z}_2^m}\Big(\sum_{\mathbf{u}\in\mathbb{Z}_2^m}(-1)^{\langle\mathbf{u},\mathbf{v}\rangle_k\oplus f(\mathbf{u})}\Big)^2=\sum_{\mathbf{v}\in\mathbb{Z}_2^m}\sum_{\mathbf{u},\mathbf{w}\in\mathbb{Z}_2^m}(-1)^{\langle\mathbf{u},\mathbf{v}\rangle_k\oplus f(\mathbf{u})\oplus\langle\mathbf{w},\mathbf{v}\rangle_k\oplus f(\mathbf{w})}=$$

(we interchange sums and then, using (iii) of Proposition 6, get)

$$=\sum_{\mathbf{u},\mathbf{w}\in\mathbb{Z}_2^m}(-1)^{f(\mathbf{u})\oplus f(\mathbf{w})}\sum_{\mathbf{v}\in\mathbb{Z}_2^m}(-1)^{\langle\mathbf{u},\mathbf{v}\rangle_k\oplus\langle\mathbf{w},\mathbf{v}\rangle_k}=\sum_{\mathbf{u}\in\mathbb{Z}_2^m}2^m=2^{2m}.$$

□

By *k-nonlinearity* of a function $f\in\mathfrak{F}_m$ we mean the distance between f and the class $\mathfrak{A}_m^k$. Denote this parameter by $N_f^{(k)}$.

Proposition 9. *It is true* $N_f^{(k)}=2^{m-1}-\frac{1}{2}\max\limits_{\mathbf{v}\in\mathbb{Z}_2^m}|W_f^{(k)}(\mathbf{v})|$.

Proof. Let a binary vector $\mathbf{g}^{\mathbf{v}}$ be given by $\mathbf{g}^{\mathbf{v}}=\beta(\mathbf{h}^{\mathbf{v}})$, where $\mathbf{h}^{\mathbf{v}}$ is the row of matrix $\mathbf{C}_m^k$ that corresponds to a vector $\mathbf{v}\in\mathbb{Z}_2^m$. We have $g^{\mathbf{v}}(\mathbf{u})=\langle\mathbf{v},\mathbf{u}\rangle_k$. Then

$$N_f^{(k)}=\min_{g\in\mathfrak{A}_m^k}\operatorname{dist}(f,g)=\min_{\mathbf{v}\in\mathbb{Z}_2^m}\{\,d_H(\mathbf{f},\mathbf{g}^{\mathbf{v}}),d_H(\mathbf{f},\mathbf{g}^{\mathbf{v}}\oplus\mathbf{1})\,\}.$$

From definition of $W_f^{(k)}$ and according to (i) of Proposition 6, we can obtain the equalities

$$d_H(\mathbf{f},\mathbf{g}^{\mathbf{v}})=2^{m-1}-\frac{1}{2}W_f^{(k)}(\mathbf{v}),\qquad d_H(\mathbf{f},\mathbf{g}^{\mathbf{v}}\oplus\mathbf{1})=2^{m-1}+\frac{1}{2}W_f^{(k)}(\mathbf{v}).$$

Using them we get

$$N_f^{(k)}=\min_{\mathbf{v}\in\mathbb{Z}_2^m}\Big(2^{m-1}-\frac{1}{2}|W_f^{(k)}(\mathbf{v})|\Big)=2^{m-1}-\frac{1}{2}\max_{\mathbf{v}\in\mathbb{Z}_2^m}|W_f^{(k)}(\mathbf{v})|.$$

□

From Theorem 3 it follows

$$\max_{\mathbf{v}\in\mathbb{Z}_2^m}|W_f^{(k)}(\mathbf{v})|\geqslant 2^{m/2}.$$

Hence, the k-nonlinearity of a function f does not exceed the number $2^{m-1}-2^{(m/2)-1}$. By analogy with notions of a maximal nonlinear function and a bent function we give the following definitions.

Definition 1. For any $m,k\in\mathbb{N}$, $1\leqslant k\leqslant m/2$, we call a Boolean function $f\in\mathfrak{F}_m$ *maximal k-nonlinear*, if any parameter $N_f^{(j)}$, $j=1,\ldots,k$, gets the maximal possible value.

In other words, vector of values of maximal k-nonlinear function $f\in\mathfrak{F}_m$ is «moved away» of codes $A_m^1,\ldots,A_m^k$ on maximal possible distances.

Definition 2. For any $m,k\in\mathbb{N}$, such that m is even and $1\leqslant k\leqslant m/2$, we call a function $f\in\mathfrak{F}_m$ *k-bent*, if all coefficients $W_f^{(j)}(\mathbf{v})$, $j=1,\ldots,k$ are equal to $\pm 2^{m/2}$.

If m is even these definitions are equivalent (as we will see later). Denote by $\mathfrak{B}_m^k$ the class of all k-bent functions in m variables. From items (iv) and (v) of Proposition 6 it follows

$$W_f^{(1)}(v_1,v_2,v_3,\ldots,v_m)=W_f(v_2,v_1,v_3,\ldots,v_m).$$

Therefore the class $\mathfrak{B}_m^1$ is the set $\mathfrak{B}_m$ of all usual bent functions. Thus,

$$\mathfrak{B}_m=\mathfrak{B}_m^1\supseteq\cdots\supseteq\mathfrak{B}_m^{m/2},$$

and as we will see too, any inclusion here is proper and $\mathfrak{B}_m^{m/2}$ is nonempty.

6. CONSTRUCTIONS FOR k-BENT FUNCTIONS

Study at first the small values of $m \in \mathbb{N}$.

Let $m = 2$. The class $\mathfrak{B}_2^1$ consists of all functions $f \in \mathfrak{F}_2$ with vectors of values having an odd weight. It is clear that $|\mathfrak{B}_2^1| = 8$.

The case $m = 4$. Using computer, we obtained

$$|\mathfrak{B}_4^1| = 896, \qquad |\mathfrak{B}_4^2| = 384.$$

Let us give an example of $\xi \in \mathfrak{F}_4$ such that $\xi \in \mathfrak{B}_4^1 \setminus \mathfrak{B}_4^2$:

$$\xi(u_1, u_2, u_3, u_4) = u_1u_2 \oplus u_2u_3 \oplus u_3u_4.$$

Using Propositions 6 and 7, consider the corresponding collections of coefficients $W_\xi^{(1)}(\mathbf{v})$ and $W_\xi^{(2)}(\mathbf{v})$ in the lexicographical order of $\mathbf{v} \in \mathbb{Z}_2^4$:

$$W_\xi^{(1)} = (4, 4, 4, -4, 4, -4, 4, 4, 4, 4, 4, -4, -4, 4, -4, -4),$$
$$W_\xi^{(2)} = (4, 4, 4, -4, 4, 0, 0, 4, 4, 8, 0, -4, -4, -4, 4, -4).$$

For instance, look at the computations of $W_\xi^{(1)}(0101)$ and $W_\xi^{(2)}(0101)$ in detail. We have

$$W_\xi^{(k)}(0101) = \sum_{u_1,u_2} \Big(\sum_{u_3,u_4} (-1)^{\langle \mathbf{u}, 0101\rangle_k \oplus \xi(\mathbf{u})} \Big) \text{ for } k = 1, 2.$$

According to Proposition 7 it is true

$$\langle \mathbf{u}, 0101\rangle_1 = u_1 \oplus u_4,$$

$$\langle \mathbf{u}, 0101\rangle_2 = u_1u_3 \oplus u_1u_4 \oplus u_2u_3 \oplus u_2u_4 \oplus u_1 \oplus u_3.$$

And hence

$$W_\xi^{(1)}(0101) = \underbrace{(1 - 1 + 1 + 1)}_{(u_1,u_2)=(00)} + \underbrace{(1 - 1 - 1 - 1)}_{(u_1,u_2)=(01)} + \underbrace{(-1 + 1 - 1 - 1)}_{(u_1,u_2)=(10)} + \underbrace{(1 - 1 - 1 - 1)}_{(u_1,u_2)=(11)} = -4,$$
$$W_\xi^{(2)}(0101) = (1 + 1 - 1 + 1) + (1 - 1 - 1 - 1) + (-1 + 1 - 1 - 1) + (1 + 1 + 1 - 1) = 0.$$

Thus, $\xi \in \mathfrak{B}_4^1 \setminus \mathfrak{B}_4^2$.

Now, given a k-bent function, we construct k-bent and $(k+1)$-bent functions in more variables (see respectively Propositions 10 and 11):

Proposition 10. *Let $m, r \in \mathbb{N}$ be even, $k \in \mathbb{N}$ be such that $1 \leqslant k \leqslant m/2$, and let a function $f \in \mathfrak{F}_{m+r}$ be represented in the form*

$$f(\mathbf{u}', \mathbf{u}'') = p(\mathbf{u}') \oplus q(\mathbf{u}'') \ \textit{ for any } \ \mathbf{u}' \in \mathbb{Z}_2^m,\ \mathbf{u}'' \in \mathbb{Z}_2^r,$$

where $p \in \mathfrak{F}_m$ and $q \in \mathfrak{F}_r$ are functions with nonintersecting sets of variables. Then f belongs to the class $\mathfrak{B}_{m+r}^k$ if and only if $p \in \mathfrak{B}_m^k$ and $q \in \mathfrak{B}_r^1$.

Proof. For arbitrary $\mathbf{v}' \in \mathbb{Z}_2^m$, $\mathbf{v}'' \in \mathbb{Z}_2^r$ and any $\ell = 1, \ldots, k$, consider the coefficient $W_f^{(\ell)}(\mathbf{v}', \mathbf{v}'')$. Using (iv) of Proposition 6, we easy get

$$\langle (\mathbf{u}', \mathbf{u}''), (\mathbf{v}', \mathbf{v}'')\rangle_\ell = \langle \mathbf{u}', \mathbf{v}'\rangle_\ell \oplus \langle \mathbf{u}'', \mathbf{v}''\rangle.$$

Then, because of $f(\mathbf{u}', \mathbf{u}'') = p(\mathbf{u}') \oplus q(\mathbf{u}'')$ we obtain

$$W_f^{(\ell)}(\mathbf{v}', \mathbf{v}'') = W_p^{(\ell)}(\mathbf{v}') \cdot W_q(\mathbf{v}'').$$

If $p \in \mathfrak{B}_m^k$ and $q \in \mathfrak{B}_r^1 = \mathfrak{B}_r$ then it is obvious that

$$|W_f^{(\ell)}(\mathbf{v}', \mathbf{v}'')| = 2^{m/2} \cdot 2^{r/2} = 2^{(m+r)/2}$$

for any ℓ, $1 \leqslant \ell \leqslant k$; and, hence, f belongs to $\mathfrak{B}_{m+r}^k$. From the other side, let $f \in \mathfrak{B}_{m+r}^k$. For every ℓ, $1 \leqslant \ell \leqslant k$, we take the vectors $\mathbf{v}'_\ell$, $\mathbf{v}''$ such that the values $|W_p^{(\ell)}(\mathbf{v}'_\ell)|$ and $|W_q(\mathbf{v}'')|$ are maximal. Then from the corresponding Parseval equalities we get

$$|W_p^{(\ell)}(\mathbf{v}'_\ell)| \geqslant 2^{m/2}, \ |W_q(\mathbf{v}'')| \geqslant 2^{r/2}.$$

Applying the fact $|W_f^{(\ell)}(\mathbf{v}'_\ell, \mathbf{v}'')| = 2^{(m+r)/2}$, we obtain $|W_p^{(\ell)}(\mathbf{v}'_\ell)| = 2^{m/2}$ and $|W_q(\mathbf{v}'')| = 2^{r/2}$ for each ℓ, $1 \leqslant \ell \leqslant k$. But it holds if and only if $p \in \mathfrak{B}_m^k$ and $q \in \mathfrak{B}_r = \mathfrak{B}_r^1$. □

Recall that a Boolean function is *symmetric*, if it is constant on any set of vectors with the same weight. The set of all such functions in two variables denote by $\mathfrak{F}_2^1$ (later we explain the sense of this notation).

Proposition 11. *Let m be even, k be integer, $1 \leqslant k \leqslant m/2$. Let a function $f \in \mathfrak{F}_{m+2}$ be represented in the form*

$$f(a, a', \mathbf{u}) = s(a, a') \oplus p(\mathbf{u}) \quad \textit{for any } \ a, a' \in \mathbb{Z}_2, \ \mathbf{u} \in \mathbb{Z}_2^m,$$

where $s \in \mathfrak{F}_2^1$, $p \in \mathfrak{F}_m$ are functions with nonintersecting sets of variables. Then $f \in \mathfrak{B}_{m+2}^{k+1}$ if and only if $s \in \mathfrak{B}_2^1$, $p \in \mathfrak{B}_m^k$.

Proof. Consider a coefficient $W_f^{(\ell+1)}(b, b', \mathbf{v})$, where $\ell \in \mathbb{N}$, $1 \leqslant \ell \leqslant k$, and elements $b, b' \in \mathbb{Z}_2$, $\mathbf{v} \in \mathbb{Z}_2^m$ are arbitrary. By the equality $f(a, a', \mathbf{u}) = s(a, a') \oplus p(\mathbf{u})$, we have

$$W_f^{(\ell+1)}(b, b', \mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{p(\mathbf{u})} \sum_{a, a' \in \mathbb{Z}_2} (-1)^{\langle (a, a', \mathbf{u}), (b, b', \mathbf{v}) \rangle_{\ell+1} \oplus s(a, a')}.$$

Let for any pair of vectors $\mathbf{u}, \mathbf{v}$ the parameter $\varepsilon \in \mathbb{Z}_2$ be uniquely determined by $\varepsilon = \langle \mathbf{u}, \mathbf{v} \rangle_\ell \oplus \langle \pi_\ell(\mathbf{u}), \mathbf{v} \rangle_\ell \oplus 1$. According to (vi) of Proposition 6, it holds

$$\langle (a, a', \mathbf{u}), (b, b', \mathbf{v}) \rangle_{\ell+1} = \langle \mathbf{u}, \mathbf{v} \rangle_\ell \oplus \langle (a, a'), (b, b') \rangle_\varepsilon,$$

and hence,

$$W_f^{(\ell+1)}(b, b', \mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_\ell \oplus p(\mathbf{u})} \cdot W_s^{(\varepsilon)}(b, b').$$

As far as the function s is symmetric, it is easy to check that for any $b, b' \in \mathbb{Z}_2$ and any ε it is true $W_s^{(\varepsilon(b,b'))} = W_s(b, b')$. Thus, for every ℓ, $1 \leqslant \ell \leqslant k$ it holds

$$W_f^{(\ell+1)}(b, b', \mathbf{v}) = W_s(b, b') \cdot W_p^{(\ell)}(\mathbf{v}).$$

Further we argue in the same manner as in the proof of Proposition 10 and get in this way what is required. □

Summarizing Propositions 10 and 11, we have

Theorem 4. *Let $m, r \geqslant 0$ be even, $j, k \geqslant 0$ be integer, $1 \leqslant k \leqslant m/2$. Let a function $f \in \mathfrak{F}_{2j+m+r}$ be represented in the form*

$$f(a_1, a'_1, \ldots, a_j, a'_j, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^{j} s_i(a_i, a'_i) \right) \oplus p(\mathbf{u}') \oplus q(\mathbf{u}''),$$

where $s_1, \ldots, s_j \in \mathfrak{F}_2^1, p \in \mathfrak{F}_m$ and $q \in \mathfrak{F}_r$ are functions with nonintersecting sets of variables. Then $f \in \mathfrak{B}_{2j+m+r}^{j+k}$ if and only if $s_1, \ldots, s_j \in \mathfrak{B}_2^1$, $p \in \mathfrak{B}_m^k$ and $q \in \mathfrak{B}_r^1$.

Corollary 4. *The class $\mathfrak{B}_m^k$ is nonempty for any even m and any integer k, $1 \leqslant k \leqslant m/2$.*

Proof. Consider any functions $s_1, \ldots, s_{m/2}$ from $\mathfrak{F}_2^1 \cap \mathfrak{B}_2^1$. It is easy to see that the set $\mathfrak{F}_2^1 \cap \mathfrak{B}_2^1$ consists of the following four functions in variables v_1, v_2:

$$v_1 v_2,\ v_1 v_2 \oplus 1,\ v_1 v_2 \oplus v_1 \oplus v_2,\ v_1 v_2 \oplus v_1 \oplus v_2 \oplus 1.$$

Then the function $f \in \mathfrak{F}_m$ such that

$$f(a_1, a'_1, \ldots, a_{m/2}, a'_{m/2}) = \bigoplus_{i=1}^{m/2} s_i(a_i, a'_i)$$

belongs to $\mathfrak{B}_m^{m/2}$ according to Theorem 4. Hence f belongs to any class $\mathfrak{B}_m^k$. □

Let C be a binary code. The maximal possible distance between a binary vector and the code C is called the *covering radius* of C. The general problem of determining the covering radius of a binary Hadamard-like code of length 2^m is open. It is open even in the case of usual linear Hadamard code if m is odd, see soome results in this direction in [17, 25]. Note that, by Corollary 4, the covering radius of any code A_m^k is equal to $2^{m-1} - 2^{(m/2)-1}$.

Corollary 5. *For any even $m \geqslant 4$ the proper inclusions have places*

$$\mathfrak{B}_m^1 \supset \mathfrak{B}_m^2 \supset \cdots \supset \mathfrak{B}_m^{m/2}.$$

Proof. For any k, $1 \leqslant k \leqslant (m-2)/2$, let us show that the set $\mathfrak{B}_m^k \setminus \mathfrak{B}_m^{k+1}$ is nonempty. Take any function $\psi \in \mathfrak{B}_4^1 \setminus \mathfrak{B}_4^2$ (by the example given above such functions do exist). Let $k = 1$. Then for arbitrary function $q \in \mathfrak{B}_{m-4}^1$ a function $f \in \mathfrak{F}_m$, such that $f(\mathbf{u}', \mathbf{u}'') = \psi(\mathbf{u}') \oplus q(\mathbf{u}'')$, belongs to $\mathfrak{B}_m^1 \setminus \mathfrak{B}_m^2$ according to Theorem 4. Let further $k > 1$. We take any functions $s_1, \ldots, s_{k-1}$ from $\mathfrak{F}_2^1 \cap \mathfrak{B}_2^1$ and a function q from $\mathfrak{B}_{m-2k-2}^1$. Then the function $f \in \mathfrak{F}_m$ such that

$$f(a_1, a'_1, \ldots, a_{k-1}, a'_{k-1}, \mathbf{u}', \mathbf{u}'') = \left(\bigoplus_{i=1}^{k-1} s_i(a_i, a'_i) \right) \oplus \psi(\mathbf{u}') \oplus q(\mathbf{u}'')$$

is k-bent but it does not belong to the class $\mathfrak{B}_m^{k+1}$. □

Let $m \geqslant 4$. It is known (e.g., see [25]) that algebraic degree of a bent function in m variables is less or equal to $m/2$. And for any d, $2 \leqslant d \leqslant m/2$, there exists a bent function $f \in \mathfrak{B}_m$ such that $\deg f = d$. For k-bent functions it holds

Corollary 6. *For even m, $m \geqslant 4$, and any $k \in \mathbb{N}$, $1 \leqslant k \leqslant m/2$, there exist k-bent functions with any algebraic degree d such that $2 \leqslant d \leqslant \max\{2, \frac{m}{2} - k + 1\}$.*

Proof. For $k = 1$ we have usual bent functions and do not consider them. Let $2 \leqslant k \leqslant (m-2)/2$. For any d, $2 \leqslant d \leqslant \frac{m}{2} - k + 1$, there exists a function $p \in \mathfrak{B}^1_{m-2k+2}$ such that $\deg p = d$. Let $s_1, \ldots, s_{k-1}$ be arbitrary functions from $\mathfrak{F}^1_2 \cap \mathfrak{B}^1_2$. Then according to Theorem 4 the function $f \in \mathfrak{F}_m$ given by equality

$$f(a_1, a'_1, \ldots, a_{k-1}, a'_{k-1}, \mathbf{u}) = \left(\bigoplus_{i=1}^{k-1} s_i(a_i, a'_i) \right) \oplus p(\mathbf{u})$$

is k-bent. Moreover it holds $\deg f = d$. For $k = m/2$ the function $\bigoplus_{i=1}^{m/2} s_i(a_i, a'_i)$, where $s_i \in \mathfrak{F}^1_2 \cap \mathfrak{B}^1_2$, $i = 1, \ldots, m/2$, is an example of $m/2$-bent function of degree 2. □

Do k-bent functions of degree more than $\frac{m}{2} - k + 1$ exist? The question is open. Using Corollary 2, we can prove that the known class $\mathcal{HB}_m$ of hyper-bent functions [39] does not coincide with $\mathfrak{B}^k_m$ for every $1 \leqslant k \leqslant m/2$. It follows from the fact that degree of a hyper-bent function in m variables is always equal to $m/2$, see [9, 23].

As we mentioned above, size of the class $\mathfrak{B}^1_m$ of all bent functions in m variables is unknown. Directly from Theorem 4 for k-bent functions we have

Corollary 7. *For even m and any k, $1 \leqslant k \leqslant m/2$, the following inequality holds*

$$|\mathfrak{B}^k_m| \geqslant 2^{2k-2} |\mathfrak{B}^1_{m-2k+2}|.$$

For instance, if $m = 8$ then

$|\mathfrak{B}^1_8| > 2^{70.4}$ (according to [1]),

$|\mathfrak{B}^2_8| > 2^{34}$ (as it follows from [33], where it is proven that $|\mathfrak{B}^1_6| > 2^{32}$),

$|\mathfrak{B}^3_8| \geqslant 7 \cdot 2^{11}$ (in the beginning of the section it was mentioned that $|\mathfrak{B}^1_4| = 896$),

$|\mathfrak{B}^4_8| \geqslant 2^9$ (as far as $|\mathfrak{B}^1_2| = 8$).

But even for $m = 4$ the bound of Corollary 7 is very rough: we have $|\mathfrak{B}^2_4| \geqslant 32$, although the tight value of $|\mathfrak{B}^2_4|$ is 384.

7. CORRELATION BETWEEN k-BENT FUNCTIONS AND 1-BENT FUNCTIONS

Let S_m be the symmetric group on m elements. Denote by $S_{m,k}$ the subgroup of S_m generated by all transpositions $(1,2)$, $(3,4)$, …, $(2k-1, 2k)$. It is obvious that groups $S_{m,k}$ and $\mathbb{Z}^k_2$ are isomorphic. For arbitrary vector $\mathbf{w} \in \mathbb{Z}^k_2$ let us define a permutation $\sigma^{\mathbf{w}}_k$ on m coordinates by the equality

$$\sigma^{\mathbf{w}}_k = (1,2)^{w_1} \cdot (3,4)^{w_2} \cdot \ldots \cdot (2k-1, 2k)^{w_k},$$

where $(i,j)^0$ denotes the identical permutation. Note that $\pi_k \equiv \sigma^{\mathbf{1}}_k$. Let $\mathfrak{F}^k_m$ be the set of all Boolean functions from $\mathfrak{F}_m$ that are constant on the each orbit of $\mathbb{Z}^m_2$ by an action of $S_{m,k}$. The number of such orbits is equal to $3^k 2^{m-2k}$, and hence we have $|\mathfrak{F}^k_m| = 2^{3^k 2^{m-2k}} = 2^{2^{m-k \log_2 \frac{4}{3}}}$. Let us show that k-bent functions and bent functions coincide if they belong to $\mathfrak{F}^k_m$. Namely, it has place the following theorem–criterion for checking a bent function on being k-bent for any k.

Theorem 5. *For even m and integer k, $1 \leqslant k \leqslant m/2$, it holds $\mathfrak{F}^k_m \cap \mathfrak{B}^k_m = \mathfrak{F}^k_m \cap \mathfrak{B}^1_m$.*

Proof. Using Proposition 6, we find the following representation for the product $\langle \mathbf{u}, \mathbf{v}\rangle_\ell$, where $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^m$ are arbitrary vectors and ℓ is such that $1 \leqslant \ell \leqslant k$. Define the vector $\mathbf{w} \in \mathbb{Z}_2^\ell$ that depends on the chosen vectors $\mathbf{u}, \mathbf{v}$. Let, for any $i = 1, \ldots, \ell$,

$$w_i = \langle (u_{2i+1}, \ldots, u_m), (v_{2i+1}, \ldots, v_m)\rangle_{\ell-i} \oplus \langle \pi_{\ell-i}(\,(u_{2i+1}, \ldots, u_m)\,), (v_{2i+1}, \ldots, v_m)\rangle_{\ell-i} \oplus 1,$$

if $i < \ell$, and let $w_\ell = 1$. Then according to (vi) of Proposition 6 it holds

$$\langle \mathbf{u}, \mathbf{v}\rangle_\ell = \left(\bigoplus_{i=1}^{\ell} \langle (u_{2i-1}, u_{2i}), (v_{2i-1}, v_{2i})\rangle_{w_i} \right) \oplus \langle (u_{2\ell+1}, \ldots, u_m), (v_{2\ell+1}, \ldots, v_m)\rangle$$

(here assume that if $\ell = m/2$ then the last item is absent). Hence, using (iv) and (v) of Proposition 6, we get

$$\langle \mathbf{u}, \mathbf{v}\rangle_\ell = \langle \sigma_\ell^{\mathbf{w}}(\mathbf{u}), \mathbf{v}\rangle.$$

Note that if the vector $\mathbf{v} \in \mathbb{Z}_2^m$ is fixed, and the vector $\mathbf{u}$ runs through the space $\mathbb{Z}_2^m$, then the vector $\sigma_\ell^{\mathbf{w}}(\mathbf{u})$ also gets all possible values in $\mathbb{Z}_2^m$. In fact assume the converse. Let vectors $\mathbf{u}, \mathbf{u}' \in \mathbb{Z}_2^m$ be distinct and let $\mathbf{w}, \mathbf{w}'$ be corresponding to them vectors from $\mathbb{Z}_2^\ell$. Suppose $\sigma_\ell^{\mathbf{w}}(\mathbf{u}) = \sigma_\ell^{\mathbf{w}'}(\mathbf{u}')$. It is obvious that vectors $\mathbf{u}, \mathbf{u}'$ can differ only in the first 2ℓ coordinates. Denote by j, $1 \leqslant j \leqslant \ell$, the number of the last pair of coordinates $(2j-1, 2j)$ such that vectors $\mathbf{u}, \mathbf{u}'$ differ at least in one coordinate from this pair (actually, in both coordinates). Note that it is always $j < m/2$. Then according to the assumption it holds $w_j \neq w_j'$. But it is impossible as far as $u_{2j+1} = u'_{2j+1}, \ldots, u_m = u'_m$. Thus, from the inequality $\mathbf{u} \neq \mathbf{u}'$ it follows $\sigma_\ell^{\mathbf{w}}(\mathbf{u}) \neq \sigma_\ell^{\mathbf{w}'}(\mathbf{u}')$.

Let $f \in \mathfrak{F}_m^k \cap \mathfrak{B}_m^1$. Consider the coefficient $W_f^{(\ell)}(\mathbf{v})$ for arbitrary $\mathbf{v} \in \mathbb{Z}_2^m$. Taking into account the remarks given above we obtain

$$W_f^{(\ell)}(\mathbf{v}) = \sum_{\mathbf{u} \in \mathbb{Z}_2^m} (-1)^{\langle \sigma_\ell^{\mathbf{w}}(\mathbf{u}), \mathbf{v}\rangle \oplus f(\mathbf{u})}.$$

As far as $f(\mathbf{u}) = f(\sigma_\ell^{\mathbf{w}}(\mathbf{u}))$ for any $\mathbf{u}, \mathbf{w}$, we have

$$W_f^{(\ell)}(\mathbf{v}) = \sum_{\mathbf{u}' \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}', \mathbf{v}\rangle \oplus f(\mathbf{u}')}, \text{ where } \mathbf{u}' = \sigma_\ell^{\mathbf{w}}(\mathbf{u}),$$

and hence $W_f^{(\ell)}(\mathbf{v}) = W_f(\mathbf{v})$ for the each $\ell = 1, \ldots, k$. □

One can show that the class $\mathfrak{B}_m^k$ is not exhausted by functions from $\mathfrak{F}_m^k \cap \mathfrak{B}_m^1$. It seems to be interesting to study known bent functions in order to determine their "k-bentness." In other words how much nonlinear (in our sense) they are?

The results of the paper were partially announced in [37] and [38].

ACKNOWLEDGMENTS

The author was supported by the Siberian Branch of the Russian Academy of Sciences (Integration Project "Tree-Like Catalogue of Mathematical Internet Resources Mathtree.ru" no. 35), the Russian Foundation for Basic Research (projects nos. 07-01-00248 and 08-01-00671), and Russian Science Support Foundation.

REFERENCES

1. S. V. Agievich, "On the Representation of Bent-Functions by Bent-Rectangles," in *Proceedings of the Fifth International Petrozavodsk Conference on Probabilistic Methods in Discrete Mathematics (Petrozavodsk, Russia. June 1–6, 2000)* (VSP, Boston, 2000), pp. 121–135.
2. A. S. Ambrosimov, "Properties of Bent Functions of q-Valued Logic Over Finite Fields," Diskretn. Mat. (1994) **6** (3), 50–60 [Discrete Math. Appl. **4** (4), 341–350 (1994)].
3. Biham E., Shamir A. "Differential Cryptanalysis of DES-Like Cryptosystems," J. Cryptology **4** (1), 3–72 (1991).
4. J. Borges, C. Fernandez, and K. T. Phelps, "Quaternary Reed-Muller Codes," IEEE Trans. Inform. Theory **51** (7), 2686–2691 (2005).
5. J. Borges, K. T. Phelps, J. Rifa, and V. A. Zinoviev, "On $\mathbb{Z}_4$-Linear Preparata-Like and Kerdock-Like Codes," IEEE Trans. Inform. Theory **49** (11), 2834–2843 (2003).
6. A. Canteaut, M Daum, H. Dobbertin, and G. Leander, "Finding Nonnormal Bent Functions," Discrete Appl. Math. **154** (2), 202–218 (2006).
7. C. Carlet, "$\mathbb{Z}_{2^k}$-Linear Codes," IEEE Trans. Inform. Theory **44** (4), 1543–1547 (1998).
8. C. Carlet, P. Charpin, and Zinoviev V., "Codes, Bent Functions and Permutations Suitable for DES-Like Cryptosystems," Designs, Codes and Cryptography **15** (2), 125–156 (1998).
9. Carlet C., Gaborit P., "Hyper-Bent Functions and Cyclic Codes," J. Combin. Theory, Ser. A **113** (3), 466–482 (2006).
10. Carlet C., Klapper A., "Upper Bounds on the Numbers of Resilient Functions and of Bent Functions," in *Proceedings of the 23rd Symposium on Information Theory* (Benelux, Belgium, 2002) pp. 307-314.
11. E. R. van Dam and D. G. Fon-Der-Flaass, "Uniformly Packed Codes and More Distance Regular Graphs from Crooked Functions," J. Algebraic Combinatorics **12** (2), 115–121 (2000).
12. E. R. van Dam and D. G. Fon-Der-Flaass, "Codes, Graphs, and Schemes from Nonlinear Functions," European J. Combin. **24** (1), 85–98 (2003).
13. J. F. Dillon, "A Survey of Bent Functions," The NSA Technical J., Special Issue, 191–215 (1972).
14. H. Dobbertin and G. Leander, "A Survey of Some Recent Results on Bent Functions," iin *Lecture Notes in Computer Sciences* Vol. 3486: *Sequences and their applications—SETA 2004. Third International Conference* (*Seul, Korea, October 24–28, 2004*) (Springer, Berlin, 2005), pp. 1–29.
15. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, "The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes," IEEE Trans. Inform. Theory **40** (2), 301–319 (1994).
16. A. V. Ivanov, "The Use of the Reduced Representation of the Boolean Functions in Their Nonlinear Approximations' Construction," in *Bulletin of Tomsk State University*, Supplement. Vol. 23: *Sixth Siberian Scientific School "Computer security and cryptography"—SIBECRYPT'2007 (Gorno-Altaisk, Russia, September, 4–7. 2007)* (Tomsk. Gos. Univ., Tomsk, 2007), pp. 31–35.
17. S. Kavut, S. Maitra, and M. D. Yucel, "Search for Boolean Functions with Excellent Profiles in the Rotation Symmetric Class," IEEE Trans. Inform. Theory **53** (5), 1743–1751 (2007).
18. L. R. Knudsen and M. J. B. Robshaw, "Non-Linear Approximation in Linear Cryptanalysis," in *Lecture Notes in Computer Sciences*, Vol. 1070: *Advances in Cryptology – EUROCRYPT'96. Workshop on the Theory and Application of Cryptographic Techniques* (*Saragossa, Spain. May 12–16, 1996*) (Springer, Berlin, 1996), PP. 224–236.
19. D. S. Krotov, "$\mathbb{Z}_4$-Linear Perfect Codes," Discrete Analysis and Oper. Res. (2000) **7** (4), 78–90 [English translation is available at `http://arxiv.org/abs/0710.0198`].
20. D. S. Krotov, "$\mathbb{Z}_4$-Linear Hadamard and Extended Perfect Codes," in *Proceedings of the International Workshop on Coding and Cryptography (Paris, France, January 8–12, 2001)* (Paris, 2001), pp. 329–334.

21. P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized Bent Functions and Their Properties," J. Combin. Theory, Ser. A, **40** (1), 90–107 (1985).
22. A. S. Kuzmin, V. T. Markov, A. A. Nechaev, V. A. Shishkin, and A. B. Shishkov, "Bent- and Hyperbent-Functions over a Field of 2^ℓ Elements," in *Tenth International Workshop "Algebraic and Combinatorial Coding Theory" (Zvenigorod, Russia. September 3–9, 2006)* (Zvenigorod, 2006), pp. 178–181.
23. A. S. Kuzmin, V. T. Markov, A. A. Nechaev, and A. B. Shishkov, "Approximation of Boolean Functions by Monomial Functions," Diskretn. Mat. **18** (1), 9–29 (2006) [Discrete Math. Appl. **16** (1), 7–28 (2006)].
24. O. A. Logachev, A. A. Sal'nikov, and V. V. Yashenko, "Bent Functions on a Finite Abelian Group," Diskretn. Mat. **9** (4), 3–20 (1997) [Discrete Math. Appl. **7** (6), 547–564 (1997)].
25. O. A. Logachev, A. A. Sal'nikov, and V. V. Yashenko, *Boolean Functions in Coding Theory and Cryptology* (Moscow Center for the Uninterrupted Mathematical Education, Moscow, 2004) [in Russian].
26. F. J. MacWilliams and N. J. A. Sloane, *Theory of Error Correcting Codes* (North-Holland, Amsterdam, 1977).
27. M. Matsui, "Linear Cryptanalysis Method for DES Cipher," in *Lecture Notes in Computer Sciences*, Vol. 765: *Advances in Cryptology – EUROCRYPT'93. Workshop on the Theory and Application of Cryptographic Techniques* (*Lofthus, Norway. May 23–27, 1993*) (Springer, Berlin, 1994), PP. 386–397.
28. R. L. McFarland, "A Family of Difference Sets in Non-Cyclic Groups," J. Combin. Theory, Ser. A **15** (1), 1–10 (1973).
29. A. A. Moldovyan, N. A. Moldovyan, N. D. Gutz, and B. V. Izotov, *Cryptography: High-Speed Ciphers* (BHV-Petersburg, St. Petersburg, 2002) [in Russian].
30. A. A. Nechaev, "Kerdock Code in a Cycled Form," Diskretn. Mat. **1** (4), 123–139 (1989) [Discrete Math. Appl. **1** (4), 365–384 (1991)].
31. K. Nyberg, "New Bent Mappings Suitable for Fast Implementation," in *Lecture Notes in Computer Sciences*, Vol. 809: *Fast Software Encryption'93 (Cambridge, December 9–11, 1993)* (Springer, Berlin, 1994), pp. 179–184.
32. J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-Function Sequences," IEEE Trans. Inform. Theory **28** (6), 858–864 (1982).
33. B. Preneel, *Analysis and Design of Cryptographic Hash Functions*, PhD thesis (Katholieke Universiteit Leuven, Leuven, Belgium, 1993).
34. C. Qu, J. Seberry, and J. Pieprzyk, "Homogeneous Bent Functions," Discrete Appl. Math. **102** (1–2), 133–139 (2000).
35. O. Rothaus, "On Bent Functions," J. Combin. Theory, Ser. A **20** (3), 300–305 (1976).
36. Yu. Tarannikov, "On Some Connections Between Codes and Cryptographic Properties of Boolean Functions," in *Seventh International Workshop "Algebraic and Combinatorial Coding Theory" (Bansko, Bulgaria. June 18–24, 2000)* (Bansko, 2000), pp. 299–304.
37. N. N. Tokareva, "The Hierarchy of Classes of Bent Functions with Multiple Nonlinearity," in *Sixth Scientific School on Discrete Mathematics and its Applications. Proceedings*, Part III (Keldysh Institute of Applied Mathematics, Moscow, 2007), pp. 5-11.
38. N. N. Tokareva, "On k-Bent Functions," in *Bulletin of Tomsk State University*, Suppl. Vol. 23: *Sixth Siberian Scientific School "Computer security and cryptography"—SIBECRYPT'2007 (Gorno-Altaisk, Russia, September 4–7, 2007)* (Tomsk. Gos. Univ., Tomsk, 2007), pp. 74–76.
39. A. Youssef and G. Gong, "Hyper-Bent Functions," in *Lecture Notes in Computer Sciences*, Vol. 2045: *Advances in Cryptology—EUROCRYPT'2001. International Conference on the Theory and Application of Cryptographic Techniques* (*Innsbruk, Austria. May 6–10, 2001*) (Berlin, Springer, 2001), PP. 406–419.