UDC 517.7, 519.1

# Description of $k$-bent functions in four variables [1] [2]

Natalia N. Tokareva

A simple description of the class of 2-bent functions in four variables is given. This class consists of 384 quadratic functions with 12 distinct types of the quadratic part. Thus, all $k$-bent functions with not more than four variables are classified.

**Key words.** $k$-Bent functions, $k$-Walsh—Hadamard transform.

## Introduction

A Boolean function $f$ with even number $m$ of variables is called a *bent function*, if it is on the maximal possible Hamming distance from the set of all affine Boolean functions. Equivalently, a bent function $f$ one can define as a function such that all its Walsh—Hadamard coefficients

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

equal $\pm 2^{m/2}$. Bent functions is a classical topic in many areas of discrete mathematics. They have a lot of applications, see e. g. the survey of C. Carlet [2].

There is a well known hard problem: to describe all bent functions for any $m$ or to get good enough lower and upper bounds for the number of them. Indeed, the following fact confirms the hardness of this problem. In spite of the long period of studying bent functions (since 60–70-ties of XX century [9]) and a great interest to them, 6 is still the maximal value of $m$ for which the tight number of bent functions is known (it equals $5\,425\,430\,528 \simeq 2^{32{,}3}$, see [1], [7], and the earlier paper [8]).

$k$-Bent functions were introduced in [10] as a generalization of bent functions. An integer parameter $k$ changes from 1 to $m/2$ and nonlinear properties of bent functions become stronger as $k$ increases. Bent functions and 1-bent functions coincide. There are known constructions of $k$-bent functions for any $k$, see [10], and the fact that by using $k$-bent functions in a block cipher it is possible to make it extremely resistant to the special type quadratic approximations [11].

In the paper we give a simple description of the class of 2-bent functions in four variables. This class consists of 384 quadratic functions with 12 distinct types of the quadratic part. Thus, all $k$-bent functions in $m$ variables, where $m \leqslant 4$, are classified now.

## §1. The main result

[1]The original Russian version will appear soon as *Tokareva N. N. Description of k-bent functions in four variables // Discrete Analysis and Operation Research, 2008. V. 15, N 4. P. ??–?? [in Russian].*
This English translation will be available soon in *J. Applied and Industrial Mathematics.*

[2]This research 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), by the Russian Foundation for Basic Research (projects 07-01-00248, 08-01-00671) and Russian Science Support Foundation.

Let $m$ be integer, $\mathfrak{F}_m$ be the class of all Boolean functions in $m$ variables. Let $\mathbf{v} = (v_1, \ldots, v_m)$, $\mathbf{u} = (u_1, \ldots, u_m)$ be binary vectors of length $m$. For any integer $k$, $1 \leqslant k \leqslant m/2$, in [10] we defined the binary operation $\langle \cdot, \cdot \rangle_k : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_2$ as

$$\langle\, \mathbf{u}, \mathbf{v}\, \rangle_k = \Big( \bigoplus_{i=1}^{k} \bigoplus_{j=i}^{k} (u_{2i-1} \oplus u_{2i})(u_{2j-1} \oplus u_{2j})(v_{2i-1} \oplus v_{2i})(v_{2j-1} \oplus v_{2j}) \Big) \oplus \langle\, \mathbf{u}, \mathbf{v}\, \rangle,$$

where $\langle\, \mathbf{u}, \mathbf{v}\, \rangle = u_1 v_1 \oplus \ldots \oplus u_m v_m$ is the usual inner product of binary vectors and $\oplus$ denotes the addition modulo 2. Operations $\langle \cdot, \cdot \rangle_k$ are tightly connected to nonlinear binary Hadamard-like codes of the special types obtained from $\mathbb{Z}_4$-linear Hadamard-like codes [3], [4]. Properties of the product $\langle \cdot, \cdot \rangle_k$ allow us to consider it as a nonlinear analog of the inner product. The integer-valued function $W_f^{(k)}$ defined on $\mathbb{Z}_2^m$ by

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

is said to be *$k$-Walsh—Hadamard transform* of a Boolean function $f \in \mathfrak{F}_m$. According to [10] it holds the inversion formula and Parseval's equality for $W_f^{(k)}$. From Parseval's equality it follows

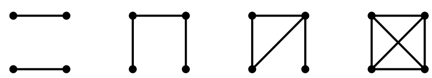
$$\max_{\mathbf{u} \in \mathbb{Z}_2^m} |W_f^{(k)}(\mathbf{u})| \geqslant 2^{m/2}.$$

A Boolean function $f \in \mathfrak{F}_m$ is called *$k$-bent* ($m$ is even), if all coefficients $W_f^{(j)}(\mathbf{u})$, $j = 1, \ldots, k$, equal $\pm 2^{m/2}$. In other words, such functions can be approximated by all functions $\langle\, \mathbf{u}, \mathbf{v}\, \rangle_k$ in the equally bad manner. Let $\mathfrak{B}_m^k$ be the class of all $k$-bent functions in $m$ variables. Then $\mathfrak{B}_m^1$ coincide with the class of usual bent functions as far as $W_f^{(1)}(\mathbf{u}) = W_f(\hat{\mathbf{u}})$ for any $\mathbf{u} \in \mathbb{Z}_2^m$, where $\hat{\mathbf{u}} = (u_2, u_1, u_3, \ldots, u_m)$. The proper inclusions have a place $\mathfrak{B}_m^1 \supset \cdots \supset \mathfrak{B}_m^{m/2}$, and the set $\mathfrak{B}_m^{m/2}$ is nonempty, see [10] for detail.

Consider the small values of $m$.

Let $m = 2$. The class $\mathfrak{B}_2^1$ consists of all functions with vectors of values having an odd weight; $|\mathfrak{B}_2^1| = 8$.

The case $m = 4$. It is known [6] that the set $\mathfrak{B}_4^1$ consists of 896 Boolean functions. Any function in it is quadratic, i. e. of algebraic degree 2. The set $\mathfrak{B}_4^1$ can be divided into 28 classes of 32 functions. Algebraic normal forms (or *Zhegalkin polynomials*[3], and briefly ANFs) of functions from any such class have the same quadratic part, arbitrary linear parts and any free terms. Consider a graph with vertices being variables and edges connecting those variables that form an item in the quadratic part of a function's ANF. Then these 28 types of the quadratic part for bent functions one can collect as



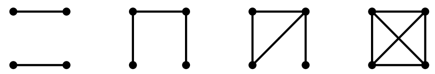
(3) (12) (12) (1)

The number of distinct types presented by a graph is given under it. For example, there are 12 types for the quadratic part consisting of three items and only one type with all six items.

In the paper we give a simple description of $\mathfrak{B}_4^2$ using interpretation on graphs. Consider a graph on four vertices numerated by integers from 1 to 4. Let the vertex $i$ correspond to

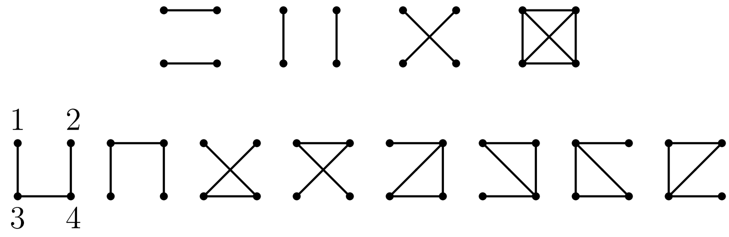
[3]This term is widely used in Russian mathematical literature.

variable $v_i$. Divide vertices into parts $\{1,2\}$ and $\{3,4\}$. Among 28 graphs given above we choose only those for which the number of edges between the parts is even. Then we obtain the series of the following 12 graphs:



(3) (4) (4) (1)

Namely, if we numerate vertices from left to right and up to down, then we get




The main result is the following. The set $\mathfrak{B}_4^2$ is a union of 12 classes of 1-bent functions presented with graphs given above. Functions from any such class can differ only by a linear part and a free term; the number of them is 32. Thus, $|\mathfrak{B}_4^2| = 384$. Let us prove it.

In terms of ANFs our statement sounds in this way.

**Proposition.** *Let $i_1, i_2, i_3$ and $i_4$ get distinct values from 1 to 4. Then the set $\mathfrak{B}_4^2$ consists of all functions of degree 2 with quadratic parts:*

$v_{i_1}v_{i_2} \oplus v_{i_3}v_{i_4}$ (3 *types*);
$v_{i_1}v_{i_2} \oplus v_{i_1}v_{i_3} \oplus v_{i_2}v_{i_4},$ *if* $\{i_1, i_2\} = \{1,2\}$ *or* $\{3,4\}$ (4 *types*);
$v_{i_1}v_{i_2} \oplus v_{i_2}v_{i_3} \oplus v_{i_3}v_{i_4} \oplus v_{i_1}v_{i_3},$ *if* $\{i_1, i_2\} = \{1,2\}$ *or* $\{3,4\}$ (4 *types*);
$v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$ (1 *type*).

**Proof.** It is obvious that $\mathfrak{B}_4^2$ contains only quadratic functions. Note that if a function $f$ belongs to $\mathfrak{B}_4^2$, then $f \oplus 1$ also belongs to it. Consider a quadratic function $f_{\mathbf{w}} \in \mathfrak{B}_4^1$ of the form $f_{\mathbf{w}}(\mathbf{v}) = f(\mathbf{v}) \oplus \langle \mathbf{w}, \mathbf{v} \rangle$, where $\mathbf{w}$ is a fixed vector and $f(\cdot)$ denotes the quadratic part of the function. Determine when the function $f_{\mathbf{w}}$ is 2-bent, i. e. when all its 2-Walsh—Hadamard coefficients equal $\pm 4$. Consider a coefficient $W^{(2)}_{f_{\mathbf{w}}}(\mathbf{u})$ for any vector $\mathbf{u} = (u_1, u_2, u_3, u_4)$.

Let $\mathbb{Z}_2^4 = V_0 \cup V_1$, where the set $V_1$ is given by

$$V_1 = \{\,(1010), (1001), (0110), (0101)\,\},$$

and the set $V_0$ contains all other vectors of length 4. Note that for any vector $\mathbf{u} \in V_\delta$ it holds $(u_1 \oplus u_2)(u_3 \oplus u_4) = \delta$, where $\delta \in \mathbb{Z}_2$. By definition we have

$$\langle \mathbf{u}, \mathbf{v} \rangle_2 = (u_1 \oplus u_2)(u_3 \oplus u_4)(v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \oplus \\ u_2v_1 \oplus u_1v_2 \oplus u_4v_3 \oplus u_3v_4.$$

Then for any vector $\mathbf{u} \in V_0$ it is true

$$W^{(2)}_{f_{\mathbf{w}}}(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \mathbf{u}, \mathbf{v} \rangle_2 \oplus f_{\mathbf{w}}(\mathbf{v})} = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \tilde{\mathbf{u}}, \mathbf{v} \rangle \oplus f_{\mathbf{w}}(\mathbf{v})} = W_{f_{\mathbf{w}}}(\tilde{\mathbf{u}}),$$

where $\tilde{\mathbf{u}} = (u_2, u_1, u_4, u_3)$, and hence $W^{(2)}_{f_{\mathbf{w}}}(\mathbf{u}) = \pm 4$, since $f_{\mathbf{w}}$ is a 1-bent function.

Consider the case $\mathbf{u} \in V_1$. We have

$$W^{(2)}_{f_{\mathbf{w}}}(\mathbf{u}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^m} (-1)^{\langle \tilde{\mathbf{u}}, \mathbf{v} \rangle \oplus g_{\mathbf{w}}(\mathbf{v})} = W_{g_{\mathbf{w}}}(\tilde{\mathbf{u}}), \tag{1}$$

where the function $g_{\mathbf{w}}$ is given by $g_{\mathbf{w}}(\mathbf{v}) = g(\mathbf{v}) \oplus \langle \mathbf{w}, \mathbf{v} \rangle$ and

$$g(\mathbf{v}) = (v_1v_3 \oplus v_1v_4 \oplus v_2v_3 \oplus v_2v_4) \oplus f(\mathbf{v}).$$

Find out the conditions under which the following four coefficients

$$W^{(2)}_{f_{\mathbf{w}}}(1010),\ W^{(2)}_{f_{\mathbf{w}}}(1001),\ W^{(2)}_{f_{\mathbf{w}}}(0110),\ W^{(2)}_{f_{\mathbf{w}}}(0101), \tag{2}$$

equal $\pm 4$. There are 28 possible variants for the function $f$. It is easy to see that $g$ is 1-bent only for 12 variants among them. These 12 quadratic functions $f$ are given in the Proposition. We list them here together with the corresponding functions $g$:

| $f(\mathbf{v})$ | $g(\mathbf{v})$ |
|---|---|
| $v_1v_2 \oplus v_3v_4$ | $v_1v_2 \oplus \ldots \oplus v_3v_4$ |
| $v_1v_3 \oplus v_2v_4$ | $v_1v_4 \oplus v_2v_3$ |
| $v_1v_4 \oplus v_2v_3$ | $v_1v_3 \oplus v_2v_4$ |
| $v_1v_2 \oplus \ldots \oplus v_3v_4$ | $v_1v_2 \oplus v_3v_4$ |
| $v_1v_3 \oplus v_2v_4 \oplus v_3v_4$ | $v_1v_4 \oplus v_2v_3 \oplus v_3v_4$ |
| $v_1v_2 \oplus v_1v_3 \oplus v_2v_4$ | $v_1v_2 \oplus v_1v_4 \oplus v_2v_3$ |
| $v_1v_4 \oplus v_2v_3 \oplus v_3v_4$ | $v_1v_3 \oplus v_2v_4 \oplus v_3v_4$ |
| $v_1v_2 \oplus v_1v_4 \oplus v_2v_3$ | $v_1v_2 \oplus v_1v_3 \oplus v_2v_4$ |
| $v_1v_2 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$ | $v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_3v_4$ |
| $v_1v_2 \oplus v_1v_4 \oplus v_2v_4 \oplus v_3v_4$ | $v_1v_2 \oplus v_1v_3 \oplus v_2v_3 \oplus v_3v_4$ |
| $v_1v_2 \oplus v_1v_3 \oplus v_1v_4 \oplus v_3v_4$ | $v_1v_2 \oplus v_2v_3 \oplus v_2v_4 \oplus v_3v_4$ |
| $v_1v_2 \oplus v_1v_3 \oplus v_2v_3 \oplus v_3v_4$ | $v_1v_2 \oplus v_1v_4 \oplus v_2v_4 \oplus v_3v_4$ |

In any of these twelve cases we have $W^{(2)}_{f_{\mathbf{w}}}(\mathbf{u}) = W_{g_{\mathbf{w}}}(\tilde{\mathbf{u}}) = \pm 4$ as far as $g$ (and hence $g_{\mathbf{w}}$) is 1-bent. So, $f_{\mathbf{w}}$ is 2-bent for any vector $\mathbf{w}$. Thus, we have shown that the class $\mathfrak{B}^2_4$ contains not less than $12 \times 32 = 384$ functions. Check that if $g$ is not 1-bent, then the absolute value of at least one coefficient among (2) is always different with 4 and therefore $f_{\mathbf{w}}$ is not 2-bent in this case. We will examine the first coefficient.

As soon as it holds

$$g_{\mathbf{w}}(\mathbf{v}) = \begin{cases} f_{\mathbf{w}}(\mathbf{v}), & \text{if } \mathbf{v} \in V_0 \\ f_{\mathbf{w}}(\mathbf{v}) \oplus 1, & \text{if } \mathbf{v} \in V_1, \end{cases}$$

the coefficient $W^{(2)}_{f_{\mathbf{w}}}(1010)$ can be represented according to (1) in the form

$$W^{(2)}_{f_{\mathbf{w}}}(1010) = W_{g_{\mathbf{w}}}(0101) = S_0 - S_1,$$

where

$$S_\delta = \sum_{\mathbf{v} \in V_\delta} (-1)^{\langle (0101), \mathbf{v} \rangle \oplus f_{\mathbf{w}}(\mathbf{v})}, \text{ when } \delta = 0, 1.$$

Since $f_{\mathbf{w}}$ is 1-bent we have

$$W_{f_{\mathbf{w}}}(0101) = S_0 + S_1 = \pm 4.$$

And hence for the equality $S_0 - S_1 = \pm 4$ to be right the value of $S_1$ should equal $\pm 4$ or 0. Transforming $S_1$, we get

$$\begin{aligned} S_1 = (-1)^{w_1} &\left((-1)^{w_3 \oplus f(1010)} + (-1)^{w_4 \oplus f(1001)}\right) + \\ &(-1)^{w_2} \left((-1)^{w_3 \oplus f(0110)} + (-1)^{w_4 \oplus f(0101)}\right). \end{aligned}$$

Then the necessary condition for $S_1 \in \{\pm 4, 0\}$ is the following: on the set $V_1$ the function $f$ gets value 1 for an even number of times. But if $f$ is one of the residuary sixteen quadratic functions, then its ANF contains an odd number of monomials from the set

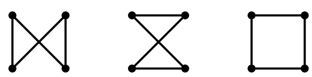
$$\{v_1 v_3, v_1 v_4, v_2 v_3, v_2 v_4\}.$$

Equivalently, in the corresponding graph there is an odd number of edges between parts $\{1, 2\}$ and $\{3, 4\}$. So, on the set $V_1$ every such function $f$ gets value 1 for an odd number of times. Thus, the necessary condition for $W^{(2)}_{f_{\mathbf{w}}}(1010) = \pm 4$ is not satisfied. That is why the function $f_{\mathbf{w}}$ is not 2-bent for any vector $\mathbf{w}$ in this case. $\square$

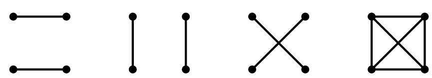
## §2. Remarks

As an interesting corollary of Proposition we have the fact that the class of 2-bent functions in four variables is closed under adding affine functions. We think that the so-called «effect of small parameters» accounts for it. We conjecture that this property will not have a place if $m > 4$.

Note that for definition of $k$-bent functions the manner of dividing variables into pairs and the order of these pairs are essential. One can consider more general approach if study approximations of Boolean functions by all the functions $\langle \mathbf{u}, \pi(\mathbf{v}) \rangle_k$, where $\pi$ is an arbitrary permutation on $m$ elements. In this case the restrictions mentioned above are removed. From Proposition it follows that a function $f \in \mathfrak{B}_4^1$ is 2-bent for any permutation of variables if and only if the intersection of the graph for its quadratic part and every graph among



contains an even number of edges. It is easy to see that all functions with quadratic parts



satisfy this condition. The number of them is 128. Now we conclude that the set of 28 graphs for the quadratic parts of 1-bent functions can be divided into four groups. One group consists of 4 graphs given above and corresponds to 2-bent functions for any permutation of variables. Three other groups (each of 8 graphs) answer to 2-bent functions for three distinct ways of

dividing variables into pairs separately. So, for any division variables into pairs we have $4+8=12$ possible variants for quadratic part of a 2-bent function.

Finally, we give the information (not great for the present time) about the number of $k$-bent functions for small values of $m$. Results on 1-bent functions and bounds for the number of them for any $m$ one can find in [5] and [2].

| $m$ | $k$ | Information about classes $\mathfrak{B}_m^k$ |
|---|---|---|
| 2 | 1 | $\lvert\mathfrak{B}_2^1\rvert = 8$ |
| 4 | 1, 2 | $\lvert\mathfrak{B}_4^1\rvert = 896$, see description in [6];<br>$\lvert\mathfrak{B}_4^2\rvert = 384$, description is given in this paper;<br>the number is calculated in [10]; |
| 6 | 1, 2, 3 | $\lvert\mathfrak{B}_6^1\rvert = 5\,425\,430\,528 \simeq 2^{32{,}3}$, see [1], [7], [8];<br>$\lvert\mathfrak{B}_6^2\rvert \geqslant 4 \cdot 896 = 3\,584$, it follows from [10];<br>$\lvert\mathfrak{B}_6^3\rvert \geqslant 4 \cdot 384 = 1\,536$, it follows from [10]; |
| 8 | 1, 2, 3, 4 | $\lvert\mathfrak{B}_8^1\rvert \geqslant 1\,559\,994\,535\,674\,013\,286\,400 \simeq 2^{70{,}4}$, see [1];<br>$\lvert\mathfrak{B}_8^2\rvert > 2^{34{,}3}$, obtain from [1], [7], [8] and [10];<br>$\lvert\mathfrak{B}_8^3\rvert \geqslant 16 \cdot 896 = 14\,336$, it follows from [10];<br>$\lvert\mathfrak{B}_8^4\rvert \geqslant 16 \cdot 384 = 6\,144$, it follows from [10]; |

# References


[1] *Agievich S. V.* On the representation of bent-functions by bent-rectangles // Fifth Int. Petrozavodsk conf. on probabilistic methods in discrete mathematics (Petrozavodsk, Russia. June 1–6, 2000). Proc. Boston: VSP, 2000. P. 121–135. Is available at `http://arxiv.org/abs/math/0502087v1`.

[2] *Carlet C.* Boolean Functions for Cryptography and Error Correcting Codes // chapter of the monograph «Boolean methods and models», Cambridge Univ. Press (P. Hammer, Y. Crama eds.), to appear. Prelim. version is available at `www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf`.

[3] *Krotov D. S.* $\mathbb{Z}_4$-linear perfect codes // Discrete Analysis and Operation Research. 2000. V. 7. N. 4. P. 78–90 [in Russian]. English translation is available at `http://arxiv.org/abs/0710.0198`.

[4] *Krotov D. S.* $\mathbb{Z}_4$-linear Hadamard and extended perfect codes // Proc. of the Int. Workshop on Coding and Cryptography (Paris, France. January 8–12, 2001). P. 329–334.

[5] *Logachev O. A., Sal'nikov A. A., Yashenko V. V.* Boolean functions in coding theory and cryptology // Moscow center for the uninterrupted mathematical education, 2004 [in Russian].

[6] *MacWilliams F. J., Sloane N. J. A.* Theory of error correcting codes. North-Holland: Amsterdam, 1977.

[7] *Meng Q., Yang M. C., Zhang H.* A novel algorithm enumerating bent functions // is available at `http://eprint.iacr.org`, 2004/274.

[8] *Preneel B.* Analysis and design of cryptographic hash functions // Ph. D. thesis, Katholieke Universiteit Leuven, 3001 Leuven, Belgium. 1993, 338 p.

[9] *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. N 3. P. 300–305.

[10] *Tokareva N. N.* Bent functions with stronger nonlinear properties: $k$-bent functions // Discrete Analysis and Operation Research, 2007. V. 14, N 4. P. 76–102 [in Russian]. Engl. trans. is available at `www.math.nsc.ru/∼tokareva` and will appear soon in J. Applied and Industrial Mathematics, 2008.

[11] *Tokareva N. N.* On quadratic approximations in block ciphers // Problems of Information Transmission. 2008. V. 44. N. 3. P. 105–127.

Address:

The paper was send
March 14, 2008

Sobolev Institute of Mathematics
Siberian Branch of the Russian Academy of Sciences
4 Acad. Koptyug avenue,
630090 Novosibirsk, Russia.
E-mail: `tokareva@math.nsc.ru`
Web: `www.math.nsc.ru/∼tokareva`