# The group of automorphisms of the set of self-dual bent functions *

Aleksandr Kutsenko

Mathematical Center in Akademgorodok, Novosibirsk, Russia
Sobolev Institute of Mathematics SB RAS, Novosibirsk, Russia
Novosibirsk State University, Novosibirsk, Russia
Laboratory of Cryptography JetBrains Research, Novosibirsk, Russia

Email: alexandrkutsenko@bk.ru

**Abstract**

A bent function is a Boolean function in even number of variables which is on the maximal Hamming distance from the set of affine Boolean functions. It is called self-dual if it coincides with its dual. It is called anti-self-dual if it is equal to the negation of its dual. A mapping of the set of all Boolean functions in $n$ variables to itself is said to be isometric if it preserves the Hamming distance. In this paper we study isometric mappings which preserve self-duality and anti-self-duality of a Boolean bent function. The complete characterization of these mappings is obtained for $n \geqslant 4$. Based on this result, the set of isometric mappings which preserve the Rayleigh quotient of the Sylvester Hadamard matrix, is characterized. The Rayleigh quotient measures the Hamming distance between bent function and its dual, so as a corollary, all isometric mappings which preserve bentness and the Hamming distance between bent function and its dual are described.

***Keywords*** — Boolean function, Self-dual bent, Isometric mapping, The group of automorphisms, The Rayleigh quotient

## 1 Introduction

The term "bent function" was introduced by Oscar Rothaus in the 1960s [18]. It in known [20], that at the same time Boolean functions with maximal ninlinearity were also studied in the Soviet Union. The term *minimal function*, which is actually a counterpart of a bent function, was proposed by the Soviet scientists Eliseev and Stepchenkov in 1962.

Bent functions have connections with such combinatorial objects as Hadamard matrices and difference sets. Since bent functions have maximum Hamming distance to linear structures and affine functions they deserve attention for practical applications in symmetric cryptography, in particular, for block and stream ciphers. We refer to the survey [3] and monographies of Mesnager [17] and Tokareva [20] for more information concerning known results and open problems related to bent functions.

For each bent function, its dual bent function is uniquely defined. More information about properties of dual bent functions one can find in work [3]. A bent function that coincides with its dual is called self-dual. There are a number of papers devoted to open problems including characterization and description of the class of self-dual bent functions.

All equivalence classes of self-dual bent functions in 2, 4, and 6 variables and all quadratic self-dual bent functions in 8 variables with a respect to a restricted form of affine transformation

*The author was supported by the Russian Foundation for Basic Research (projects No. 18-31-00374, 18-07-01394, 20-31-70043), by the Ministry of Science and Higher Education of the Russian Federation (the 5-100 Excellence Programme and the Project No. 1.13559.2019/13.1), by the program of fundamental scientific researches of the SB RAS No. I.5.1 (project No. 0314-2019-0017), by Mathematical Center in Akademgorodok.

which preserves self-duality were given in [2]. Further, equivalence classes of cubic self-dual bent functions in 8 variables with respect to the mentioned above restricted form of affine transformation one can find in [7]. In [8] a classification of quadratic self-dual bent functions was obtained. The upper bound for the cardinality of the set of self-dual bent functions was given in [9]. New constructions of self-dual bent functions weere presented in [13, 16]. The complete Hamming distance spectrum between self-dual Maiorana–McFarland bent functions was obtained in [11]. Iterative constructions and metrical properties, in particular, sets of Boolean functions which are maximally distant from the sets of self-dual and anti-self-dual bent functions and also the questions concerning metrical regularity of the sets of self-dual and anti-self-dual bent functions, were completely studied in [12].

Study of automorphism groups of mathematical objects deserve attention since these groups are closely connected with the structure of the objects. There exists an essential generally non-trivial question: how groups of automorphisms of two mathematical objects, one of which is embedded to another one, are related.

The group of automorphisms of the set of bent functions was completely characterized by Tokareva in [21]: it was proved that each isometric mapping of the set of Boolean functions in $n$ variables to itself preserving the class of bent functions is a combination of an affine transformation of coordinates and a shift by an affine function. The said group is a semidirect product of the affine group $\mathrm{GA}(n, \mathbb{F}_2)$ and $\mathbb{F}_2^{n+1}$. A natural question arises how the automorphism group of the set of self-dual bent functions is connected with the group of automorphisms of the set of bent functions.

In papers [2, 7] an approach to equivalence of self-dual bent functions based on the restricted form of affine equivalence preserving self-duality, which forms the extended orthogonal group, was proposed. We study a question whether there exist other isometric mappings of Boolean functions to itself which preserve the class of self-dual bent function. In this paper, we prove that there are no other mappings satisfying such a property, thus obtaining a characterization of the group of automorphisms of the set of self-dual bent functions.

In this paper we study isometric mappings of the set of all Boolen functions in $n$ variables to itself which preserve self-duality and anti-self-duality of a Boolean function. The complete characterization of these mappings is obtained. It is proved that every such mapping has form

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x \rangle \oplus d,$$

where $L$ is a $n \times n$ orthogonal binary matrix, $c \in \mathbb{F}_2^n$, $c$ has even Hamming weight, $d \in \mathbb{F}_2$. Based on this result, the set of isometric mappings which preserve the Rayleigh quotient of the Sylvester Hadamard matrix of every Boolean function is obtained. As a corollary all isometric mappings which preserve bentness and the Hamming distance between bent function and its dual are given.

The work has the following structure: basic definitions and notions concerning isometric mappings and groups of automorphisms are in the Sections 2 and 3. In Section 4 required material on sign functions of (anti-)self-dual bent function, which is directly used throughout the paper, is given. In Section 5 we characterize isometric mappings preserving self-duality (Theorem 1) and prove that isometiric mapping preserves self-duality if and only if it preserves anti-self-duality (Proposition 2). In Section 6 isometric mappings which define bijections between the sets of self-dual and anti-self-dual bent functions (Theorem 2) are characterized. Section 7 is devoted to the Rayleigh quotient of a Boolean function and isometric mappings which preserve it (Theorem 3) and change its sign (Theorem 4) for every Boolean function. In Section 8 we summarize results from this paper (Theorems 6 and 7), the group of automorphisms of (anti-)self-dual bent functions is provided in Theorem 8. The conclusion is in Section 9.

## 2 Preliminaries

Let $\mathbb{F}_2^n$ be a set of binary vectors of length $n$.

A *Boolean function* $f$ in $n$ variables is any map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of Boolean functions in $n$ variables is denoted by $\mathcal{F}_n$.

The $(0,1)$-sequence defined by $(f(\mathbf{v}_0), f(\mathbf{v}_1), ..., f(\mathbf{v}_{2^n-1}))$ is called the *truth table* of $f \in \mathcal{F}_n$ , where

$$\begin{aligned}
&\mathbf{v}_0 = (0,0,...,0) \in \mathbb{F}_2^n \\
&\mathbf{v}_1 = (0,0,...,0,1) \in \mathbb{F}_2^n \\
&\vdots \\
&\mathbf{v}_{2^n-1} = (1,1,...,1) \in \mathbb{F}_2^n,
\end{aligned}$$

ordered by lexicographical order.

The *sign function* $F$ of a Boolean function $f \in \mathcal{F}_n$ is a real-valued function $F(x) = (-1)^{f(x)}$, $x \in \mathbb{F}_2^n$. Obviously, we have $(-1)^{f(x)} = 1 - 2f(x)$ for any $x \in \mathbb{F}_2^n$. We will denote the sign function by $F = (-1)^f$ and refer to it as to a vector $F = \left((-1)^{f(\mathbf{v}_0)}, (-1)^{f(\mathbf{v}_1)}, ..., (-1)^{f(\mathbf{v}_{2^n-1})}\right)$ from the set $\{\pm 1\}^{2^n}$ (it is also known as a $(1,-1)$-*sequence* of the function $f \in \mathcal{F}_n$, see [4]).

Two Boolean functions $f, g \in \mathcal{F}_n$ are said to be *affinely equivalent* if $g(x) = f(Ax \oplus b) \oplus \langle b, x\rangle \oplus d$, where $b, c \in \mathbb{F}_2^n$, $d \in \mathbb{F}_2$ and $A$ is a $n \times n$ nonsingular binary matrix. If no such transformation exists, then $f, g$ are called *inequivalent*.

The *Hamming weight* $\mathrm{wt}(x)$ of the vector $x \in \mathbb{F}_2^n$ is the number of nonzero coordinates of $x$. The *Hamming weight* $\mathrm{wt}(f)$ of the function $f \in \mathcal{F}_n$ is the Hamming weight of its vector of values. The sign $\oplus$ denotes a sum modulo 2. The *Hamming distance* $\mathrm{dist}(f, g)$ between Boolean functions $f, g$ in $n$ variables is a cardinality of the set $\{x \in \mathbb{F}_2^n | f(x) \oplus g(x) = 1\}$. For $x, y \in \mathbb{F}_2^n$ denote $\langle x, y\rangle = \bigoplus_{i=1}^{n} x_i y_i$. The *Walsh-Hadamard transform* (WHT) of the Boolean function $f$ in $n$ variables is an integer function $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, defined as

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

A Boolean function $f$ in an even number $n$ of variables is said to be *bent* if

$$|W_f(y)| = 2^{n/2}$$

for all $y \in \mathbb{F}_2^n$. The set of bent functions in $n$ variables is denoted by $\mathcal{B}_n$.

From the definition above it follows that for any $y \in \mathbb{F}_2^n$ we have

$$W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}$$

for some $\widetilde{f} \in \mathcal{F}_n$.

The Boolean function $\widetilde{f}$ defined above is called the *dual* function of the bent function $f$. The duality of bent functions was introduced by Dillon [6].

Some known properties of dual functions:

- Every dual function is a bent function [1];
- If $\widetilde{f}$ is dual to $f$ and $\widetilde{\widetilde{f}}$ is dual to $\widetilde{f}$, then $\widetilde{\widetilde{f}} = f$ [1];
- The mapping $f \to \widetilde{f}$ which acts on the set of bent functions, preserves the Hamming distance [1].

If bent function $f$ coincides with its dual it is said to be *self-dual bent*. A bent function which coincides with the negation of its dual is called an *anti-self-dual bent*. The set of (anti-)self-dual bent functions in $n$ variables, according to [8], is denoted by $\mathrm{SB}^+(n)$ $\left(\mathrm{SB}^-(n)\right)$.

Let $I_n$ be the identity matrix of size $n$ and $H_n = H_1^{\otimes n}$ be the $n$-fold tensor product of the matrix $H_1$ with itself, where

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

It is known the Hadamard property of this matrix

$$H_n H_n^T = 2^n I_{2^n},$$

where $H_n^T$ is transpose of $H_n$ (it holds $H_n^T = H_n$ by symmetricity of $H_n$).

Denote $\mathcal{H}_n = 2^{-n/2} H_n$, this matrix is symmetric and orthogonal. Since all rows of the matrix $H_n$ correspond to sign functions of all linear functions (see [4] for instance), equivalently, bent function can be defined as a function whose sign function, say $F$, satisfies $\mathcal{H}_n F \in \{\pm 1\}^{2^n}$.

Denote, according to [10], the orthogonal group of index $n$ over the field $\mathbb{F}_2$ as

$$\mathcal{O}_n = \left\{ L \in GL\left(n, \mathbb{F}_2\right) | LL^T = I_n \right\},$$

where $L^T$ denotes the transpose of $L$ and $I_n$ is an identical matrix of order $n$ over the field $\mathbb{F}_2$.

## 3 Isometric mappings and automorphism groups

A mapping $\varphi$ of the set of all Boolean functions in $n$ variables to itself is called *isometric* if it preserves the Hamming distance between functions, that is

$$\mathrm{dist}(\varphi(f), \varphi(g)) = \mathrm{dist}(f, g),$$

for any $f, g \in \mathcal{F}_n$. The set of all isometric mappings of the set of all Boolean functions in $n$ variables to itself is denoted by $\mathcal{I}_n$.

**Example 1.** *Composition of an affine transform of coordinates and an affine shift, that is the mapping of the form*

$$f(x) \longrightarrow f\left(Lx \oplus b\right) \oplus \langle c, x \rangle \oplus d, \tag{1}$$

*where $L$ is a $n \times n$ nonsingular binary matrix, $b, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2$, is an element of $\mathcal{I}_n$.*

The general form of isometric mappings of all Boolean functions in $n$ variables to itself is

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

where $\pi$ is a permutation on the set $\mathbb{F}_2^n$ and $g \in \mathcal{F}_n$ [15]. The mapping of this form is denoted by $\varphi_{\pi,g} \in \mathcal{I}_n$.

There is an one-to-one correspondence between $\mathcal{I}_n$ and the set of monomial matrices of order $2^n \times 2^n$ with elements from the set $\{0, \pm 1\}$. Indeed, consider arbitrary mapping $\varphi_{\pi,g} \in \mathcal{I}_n$. Then for any $f \in \mathcal{F}_n$ and its sign function $F \in \{\pm 1\}^{2^n}$ the sign function $F' \in \{\pm 1\}^{2^n}$ of $f' = \varphi_{\pi,g}(f) \in \mathcal{F}_n$ can be expressed as an action of some linear mapping (operator $\mathbb{R}^n \to \mathbb{R}^n$), namely $F' = AF$, where $A$ is a $2^n \times 2^n$ matrix

$$\begin{array}{c} \\ \mathbf{v}_i \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & \pi(\mathbf{v}_i) & & & \end{array} \\ \begin{pmatrix} & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \dots & 0 & (-1)^{g(\mathbf{v}_i)} & 0 & \dots & 0 \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{pmatrix} \end{array},$$

in which in the row with number $(i+1) \in \{1, 2, ..., 2^n\}$ a nonzero element is in the $(j+1)$-th column, where $j$ is a number with binary representation $\pi(\mathbf{v}_i)$.

The *group of automorphisms* of a fixed subset $M \subseteq \mathcal{F}_n$ is the group of isometric mappings of the set of all Boolean functions in $n$ variables to itself preserving the set $M$. It is denoted by $\mathrm{Aut}(M)$.

The group of automorphisms of the set of bent functions was completely characterized by Tokareva in 2010: it was proved that every isometric mapping of the set of all Boolean functions in an even number $n$ of variables to itself that transforms bent functions to bent functions is a combination of an affine transform of coordinates and an affine shift [21], in other words, it is described by (1).

# 4 Sign functions of self-dual bent functions

A non-zero vector $v \in \mathbb{C}^n$ is called an *eigenvector* of a square $n \times n$ matrix $A$ attached to the eigenvalue $\lambda \in \mathbb{C}$ if $Av = \lambda v$. A linear span of eigenvectors attached to the eigenvalue $\lambda$ is called an *eigenspace* associated with $\lambda$.

Consider a linear mapping $\psi : \mathbb{C}^n \to \mathbb{C}^n$ represented by a $n \times n$ complex matrix $A$. A *kernel* of $\psi$ is the set

$$\mathrm{Ker}(\psi) = \{x \in \mathbb{C}^n | Ax = \mathbf{0} \in \mathbb{C}^n\},$$

where $\mathbf{0}$ is a zero element of the space $\mathbb{C}^n$.

Recall an orthogonal decomposition of $\mathbb{R}^{2^n}$ in eigenspaces of $H_n$ from [2] (Lemma 5.2):

$$\mathbb{R}^{2^n} = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right) \oplus \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right),$$

where the symbol $\oplus$ denotes a direct sum of subspaces.

From the definition of self-duality it follows that sign function of any self-dual bent function is the eigenvector of $\mathcal{H}_n$ attached to the eigenvalue 1, that is an element from the subspace $\mathrm{Ker}(\mathcal{H}_n - I_{2^n}) = \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right)$. The same holds for a sign function of any anti-self-dual bent function, which obviously is an eigenvector of $\mathcal{H}_n$ attached to the eigenvalue $(-1)$, that is an element from the subspace $\mathrm{Ker}(\mathcal{H}_n + I_{2^n}) = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)$.

It is known that

$$\dim(\mathrm{Ker}(\mathcal{H}_n + I_{2^n})) = \dim(\mathrm{Ker}(\mathcal{H}_n - I_{2^n})) = 2^{n-1},$$

where $\dim(V)$ is the dimension of the subspace $V \subseteq \mathbb{R}^{2^n}$. Moreover, from symmetricity of $\mathcal{H}_n$ it follows that

$$(\mathrm{Ker}(\mathcal{H}_n + I_{2^n}))^{\perp} = \mathrm{Ker}(\mathcal{H}_n - I_{2^n})$$

and

$$(\mathrm{Ker}(\mathcal{H}_n - I_{2^n}))^{\perp} = \mathrm{Ker}(\mathcal{H}_n + I_{2^n}).$$

In [12] the following result was obtained:

**Proposition 1.** ([12], Theorem 2) *Let $n \geqslant 4$, then the linear span of sign functions of (anti-)self-dual bent functions in $n$ variables has dimension $2^{n-1}$.*

For $n = 2$ there are two self-dual bent functions, namely $x_1x_2$ and $x_1x_2 \oplus 1$, which have sign functions $(1, 1, 1, -1)$ and $(-1, -1, -1, 1)$ respectively. These sign functions are linearly dependent vectors in $\mathbb{R}^4$. The set $\mathrm{SB}^-(2)$ consists of functions $x_1x_2 \oplus x_1 \oplus x_2$ and $x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ with sign functions $(1, -1, -1, -1)$ and $(-1, 1, 1, 1)$ respectively. These sign functions are linearly dependent vectors in $\mathbb{R}^4$ as well.

## 5 Isometric mappings preserving self-duality

In [7] (Theorem 1) it was shown that the mapping

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x\rangle \oplus d,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{F}_2$, preserves self-duality of a bent function. It is obvious that this mapping is an element from $\mathcal{I}_n$ with $\pi(x) = L\left(x \oplus c\right)$ and $g(x) = \langle c, x\rangle \oplus d$, $x \in \mathbb{F}_2^n$. The group which consists of mappings of such form is called an *extended orthogonal group* and denoted by $\overline{\mathcal{O}}_n$ [5, 7]. It holds $\overline{\mathcal{O}}_n \leqslant \mathrm{GL}\left(n+2, \mathbb{F}_2\right)$.

Assume that $n \geqslant 4$ is an even integer. In this section we generalize this result within isometric mappings from the set $\mathcal{I}_n$.

At first the question of how the sets of isometric mapping preserving self-duality and anti-self-duality or, in other words, automorphism groups of the sets $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ are connected.

**Proposition 2.** *For isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ with matrix $A$ the following conditions are equivalent:*

*1) $\varphi_{\pi,g}$ preserves self-duality;*

*2) $\varphi_{\pi,g}$ preserves anti-self-duality;*

*3) $A\mathcal{H}_n = \mathcal{H}_n A$.*

*Proof.* By Proposition 1 for $n \geqslant 4$ within the set $\mathrm{SB}^+(n)$ there exist a subset $\{f_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^+(n)$ with linearly independent sign functions $\{F_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)$ and a subset $\{g_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^-(n)$ with linearly independent sign functions $\{G_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)$.

Prove that from the first assertions of the Proposition the second one follows. Assume $\varphi_{\pi,g}$ preserves self-duality. Since the matrix $A$ is a nonsingular one, the vectors $\{AF_i\}_{i=1}^{2^{n-1}}$ are also linearly independent sign functions of self-dual bent functions $\{\varphi_{\pi,g}\left(f_i\right)\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^+(n)$. Then for any sign function $G \in \mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)$ of $g \in \mathrm{SB}^-(n)$ we have

$$\langle AG, AF_i\rangle = \left\langle A^T AG, F_i\right\rangle = \langle G, F_i\rangle = 0$$

for $i = 1, 2, ..., 2^{n-1}$, hence it holds $AG \in \mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)$ and immediately $\varphi_{\pi,g}\left(g\right) \in \mathrm{SB}^-(n)$. That is, for every anti-self-dual bent function $g$ its image $\varphi_{\pi,g}(g)$ is also an anti-self-dual bent function.

By using the same arguments one can show that from the second assertions the first one follows as well, and we can conclude that the first and the second ones are equivalent.

Now prove the equivalence of the first and the third assertions. If $A\mathcal{H}_n = \mathcal{H}_n A$, then for any sign functions $F$ of $f \in \mathrm{SB}^+(n)$ it holds

$$\mathcal{H}_n\left(AF\right) = A\left(\mathcal{H}_n F\right) = AF,$$

hence the mapping preserves self-duality.

Denote $B = \mathcal{H}_n A - A\mathcal{H}_n$ and assume that the mapping with matrix $A$ preserves self-duality and, as proved above, anti-self-duality. In particular, for $i = 1, 2, ..., 2^{n-1}$ it holds

$$\mathcal{H}_n\left(AF_i\right) = AF_i$$

and

$$\mathcal{H}_n\left(AG_i\right) = -AG_i.$$

For $i = 1, 2, ..., 2^{n-1}$ we have:

$$\left(\mathcal{H}_n A - A\mathcal{H}_n\right) F_i = \mathcal{H}_n\left(AF_i\right) - A\left(\mathcal{H}_n F_i\right) = \mathcal{H}_n\left(AF_i\right) - AF_i = BF_i.$$

Then $BF_i = \mathbf{0} \in \mathbb{R}^{2^n}$ for every $i = 1, 2, ..., 2^{n-1}$. From the fact that the set $\{F_i\}_{i=1}^{2^{n-1}}$ forms a basis of the subspace $\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$ it follows that all rows of the matrix $B$ are vectors from the subspace $(\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n}))^{\perp} = \mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$.

For $i = 1, 2, ..., 2^{n-1}$ we also have

$$(\mathcal{H}_n A - A\mathcal{H}_n)\, G_i = \mathcal{H}_n\,(AG_i) - A\,(\mathcal{H}_n G_i) = \mathcal{H}_n\,(AG_i) + AG_i = BG_i.$$

In this case $BG_i = \mathbf{0} \in \mathbb{R}^{2^n}$ for every $i = 1, 2, ..., 2^{n-1}$. Since the set $\{G_i\}_{i=1}^{2^{n-1}}$ forms a basis of the subspace $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$ we can conclude that all rows of the matrix $B$ are vectors from the subspace $(\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}))^{\perp} = \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$.

Thus we have proved that all rows of the matrix $B$ lie in $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}) \cap \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$ but the intersection of orthogonal subspaces consists only of the zero element of the space $\mathbb{R}^n$. Therefore the matrix $B$ is zero matrix. □

**Corollary 1.** *It holds*

$$\mathrm{Aut}\left(\mathrm{SB}^{+}(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^{-}(n)\right).$$

From this Proposition it follows that the problem of characterization of isometric mappings with considered properties is directly linked with the problem of enumerating all monomial matrices of order $2^n \times 2^n$ with elements from the set $\{0, \pm 1\}$, which commute with the matrix $\mathcal{H}_n$. The solution of this problem is given by the following

**Theorem 1.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ preserves (anti-)self-duality if and only if*

$$\pi(x) = L\,(x \oplus c)\,,\ x \in \mathbb{F}_2^n,$$

*and*

$$g(x) = \langle c, x\rangle \oplus d,\ x \in \mathbb{F}_2^n,$$

*where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{F}_2$.*

*Proof.* The opposite direction immediately comes from [7] (Theorem 1).

Assume that $A$ is a matrix of the mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ preserving (anti-)self-duality. Let $T_{a,r}$ be a sign function of an affine function $l(x) = \langle a, x\rangle \oplus r$, where $a, x \in \mathbb{F}_2^n, r \in \mathbb{F}_2$. In other words $T_{a,r}$ is equal to some row (column) of the matrix $H_n$ if $r = 0$ or $(-H_n)$ in the case $r = 1$. From Proposition 2 it follows that $A\mathcal{H}_n = \mathcal{H}_n A$ hence

$$\mathcal{H}_n\,(AT_{a,r}) = A\,(\mathcal{H}_n T_{a,r}) = 2^{n/2}\sigma \cdot Ae_k = 2^{n/2}\sigma' \cdot e_{k'},$$

where $k, k' \in \{1, 2, ..., 2^n\}\,, \sigma, \sigma' \in \{\pm 1\}$. Then

$$AT_{a,r} = 2^{n/2}\sigma' \cdot \mathcal{H}_n e_{k'} = T_{a',r'}$$

for some $a' \in \mathbb{F}_2^n, r' \in \mathbb{F}_2$.

Thus, the considered mapping transforms the set of all affine functions in $n$ variables to itself hence it has form

$$f(x) \longrightarrow f\,(Lx \oplus b) \oplus \langle c, x\rangle \oplus d,$$

where $L$ is a $n \times n$ nonsingular binary matrix, $b, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2$, see [14], for example.

Now consider the relation $AH_n = H_n A$ in details. Recall that

$$H_n = \begin{pmatrix} (-1)^{\langle \mathbf{v}_0, \mathbf{v}_0\rangle} & (-1)^{\langle \mathbf{v}_0, \mathbf{v}_1\rangle} & \dots & (-1)^{\langle \mathbf{v}_0, \mathbf{v}_{2^n-1}\rangle} \\ (-1)^{\langle \mathbf{v}_1, \mathbf{v}_0\rangle} & (-1)^{\langle \mathbf{v}_1, \mathbf{v}_1\rangle} & \dots & (-1)^{\langle \mathbf{v}_1, \mathbf{v}_{2^n-1}\rangle} \\ \vdots & \vdots & \ddots & \vdots \\ (-1)^{\langle \mathbf{v}_{2^n-1}, \mathbf{v}_0\rangle} & (-1)^{\langle \mathbf{v}_{2^n-1}, \mathbf{v}_1\rangle} & \dots & (-1)^{\langle \mathbf{v}_{2^n-1}, \mathbf{v}_{2^n-1}\rangle} \end{pmatrix}.$$

and $A$ is the matrix

$$\begin{array}{c} \\ \mathbf{v}_i \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & L\mathbf{v}_i \oplus b & & & \end{array} \\ \begin{pmatrix} & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \dots & 0 & (-1)^{\langle c, \mathbf{v}_i \rangle \oplus d} & 0 & \dots & 0 \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{pmatrix} \end{array},$$

in which in the row with number $(i+1) \in \{1, 2, ..., 2^n\}$ a nonzero element is in the $(j+1)$-th column, where $j$ is a number with binary representation $Lv_i \oplus b$.

Fix arbitrary $i, j \in \{0, 1, ..., 2^n - 1\}$. Write explicitly

$$(AH_n)_{i+1,j+1} = (-1)^{\langle c, \mathbf{v}_i \rangle \oplus \langle L\mathbf{v}_i \oplus b, \mathbf{v}_j \rangle \oplus d}.$$

In order to obtain $(H_n A)_{i+1,j+1}$ rewrite matrix $A$ in the following form

$$\begin{array}{c} \\ L^{-1}(\mathbf{v}_j \oplus b) \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & \mathbf{v}_j & & & \end{array} \\ \begin{pmatrix} & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \dots & 0 & (-1)^{\left\langle c, L^{-1}(\mathbf{v}_j \oplus b) \right\rangle \oplus d} & 0 & \dots & 0 \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{pmatrix} \end{array}.$$

Then it clear that

$$(H_n A)_{i+1,j+1} = (-1)^{\left\langle \mathbf{v}_i, L^{-1}(\mathbf{v}_j \oplus b) \right\rangle \oplus \left\langle c, L^{-1}(\mathbf{v}_j \oplus b) \right\rangle \oplus d}.$$

Since $AH_n = H_n A$ implies $(AH_n)_{i+1,j+1} = (H_n A)_{i+1,j+1}$ for any $i, j \in \{0, 1, ..., 2^n - 1\}$, the following relation must hold

$$(-1)^{\langle c, \mathbf{v}_i \rangle \oplus \langle L\mathbf{v}_i \oplus b, \mathbf{v}_j \rangle \oplus d} = (-1)^{\left\langle \mathbf{v}_i, L^{-1}(\mathbf{v}_j \oplus b) \right\rangle \oplus \left\langle c, L^{-1}(\mathbf{v}_j \oplus b) \right\rangle \oplus d},$$

or, equivalently,

$$\langle c, x \rangle \oplus \langle Lx \oplus b, y \rangle \oplus d = \left\langle x, L^{-1}(y \oplus b) \right\rangle \oplus \left\langle c, L^{-1}(y \oplus b) \right\rangle \oplus d \tag{2}$$

for any $x, y \in \mathbb{F}_2^n$.

Put zero vector $y \in \mathbb{F}_2^n$ in (2). Then

$$\langle c, x \rangle = \left\langle x, L^{-1}b \right\rangle \oplus \left\langle c, L^{-1}b \right\rangle,$$

$$\left\langle x, L^{-1}b \oplus c \right\rangle = \left\langle c, L^{-1}b \right\rangle$$

for any $x \in \mathbb{F}_2^n$. Then

$$\begin{cases} L^{-1}b \oplus c = 0, \\ \left\langle c, L^{-1}b \right\rangle = 0, \end{cases}$$

$$\begin{cases} b = Lc, \\ \mathrm{wt}\,(c) \text{ is even.} \end{cases} \tag{3}$$

Return to (2) and take (3) into account:

$$\langle c, x\rangle \oplus \langle Lx \oplus Lc, y\rangle = \left\langle x, L^{-1}\left(y \oplus Lc\right)\right\rangle \oplus \left\langle c, L^{-1}\left(y \oplus Lc\right)\right\rangle,$$

$$\langle c, x\rangle \oplus \langle Lx, y\rangle \oplus \langle Lc, y\rangle = \left\langle x, L^{-1}y\right\rangle \oplus \langle x, c\rangle \oplus \left\langle c, L^{-1}y\right\rangle \oplus \langle c, c\rangle,$$

$$\langle Lx, y\rangle \oplus \langle Lc, y\rangle = \left\langle x, L^{-1}y\right\rangle \oplus \left\langle c, L^{-1}y\right\rangle,$$

$$\langle L\left(x \oplus c\right), y\rangle = \left\langle \left(L^{-1}\right)^{T}\left(x \oplus c\right), y\right\rangle.$$

for any $x, y \in \mathbb{F}_2^n$. In this case

$$L\left(x \oplus c\right) = \left(L^{-1}\right)^{T}\left(x \oplus c\right)$$

for any $x \in \mathbb{F}_2^n$ that is

$$L(z) = \left(L^{-1}\right)^{T}(z)$$

for any $z \in \mathbb{F}_2^n$. It holds if and only if

$$L = \left(L^{-1}\right)^{T}. \tag{4}$$

Thus, combining (3) and (4) we obtain

$$\begin{cases} L^{-1} = L^{T}, \\ b = Lc, \\ \mathrm{wt}\,(c) \text{ is even.} \end{cases}$$

□

**Corollary 2.** *It holds*

$$\mathrm{Aut}\left(\mathrm{SB}^{+}(n)\right) = \overline{\mathcal{O}}_n.$$

It can be concluded that from Proposition 2 and Theorem 1 it follows that the group of automorphisms of the set of (anti-)self-dual bent functions coincides with the extended orthogonal group, that is

$$\mathrm{Aut}\left(\mathrm{SB}^{+}(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^{-}(n)\right) = \overline{\mathcal{O}}_n.$$

### 5.1 Sets of (anti-)self-dual bent function in two variables

The case $n = 2$ is out of the ordinary, because, in particular, Propositions 1 and 2 do not hold. Indeed, consider isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_2$ with the followong matrix:

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

It transforms sign function $(1, 1, 1, -1)$ of self-dual bent function $f\left(x_1, x_2\right) = x_1x_2$ to its negation $(-1, -1, -1, 1)$ and sign function $(1, -1, -1, -1)$ of anti-self-dual bent function $f\left(x_1, x_2\right) = x_1x_2 \oplus x_1 \oplus x_2$ to itself, that is this isometric mapping preserves both self-duality and anti-self-duality. But we have

$$A\mathcal{H}_n = \begin{pmatrix} -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix}, \quad \mathcal{H}_nA = \begin{pmatrix} -1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1. \end{pmatrix},$$

and $A\mathcal{H}_n \neq \mathcal{H}_n A$.

Consider another isometric mapping $\varphi_{\pi',g'} \in \mathcal{I}_2$ with the followong matrix:

$$A' = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

It transforms sign function $(1,1,1,-1)$ of self-dual bent function $f(x_1,x_2) = x_1x_2$ to itself but sign function $(1,-1,-1,-1)$ of anti-self-dual bent function $f(x_1,x_2) = x_1x_2 \oplus x_1 \oplus x_2$ it transforms to sign function $(-1,1,-1,-1)$ of bent function $f(x_1,x_2) = x_1x_2 \oplus x_2 \oplus 1$ which is neither self-dual nor anti-self-dual, that is this isometric mapping preserves self-duality but does not preserve anti-self-duality.

# 6 Isometric bijections between self-dual and anti-self-dual bent functions

It is known [2] (Theorems 5.1, 5.3) that there exists a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$, based on the decomposition of sign functions of (anti-)self-dual bent functions. Also note that from the existence of such bijection it follows that $\left|\mathrm{SB}^+(n)\right| = \left|\mathrm{SB}^-(n)\right|$.

Namely, let $(Y,Z) \in \{\pm 1\}^{2^n}$, where $Y,Z \in \{\pm 1\}^{2^{n-1}}$, be a sign function for some $f \in \mathrm{SB}^+(n)$. Then a vector $(Z,-Y) \in \{\pm 1\}^{2^n}$ is a sign function for some function from $\mathrm{SB}^-(n)$. In terms of isometric mappings the mentioned transform can be represented as

$$f(x) \longrightarrow f(x \oplus c) \oplus \langle c, x \rangle,$$

where $c = (1,0,0,...,0) \in \mathbb{F}_2^n$.

In paper [8] it was mentioned that the more general form of this mapping

$$f(x) \longrightarrow f(x \oplus c) \oplus \langle c, x \rangle,$$

where $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is odd, is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$. It is obvious that this mapping is an element from $\mathcal{I}_n$.

Assume that $n \geqslant 4$ is an even integer. In this section we generalize these results within isometric mappings from the set $\mathcal{I}_n$.

**Proposition 3.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ with matrix $A$ is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ if and only if $A\mathcal{H}_n = -\mathcal{H}_n A$.*

*Proof.* If $\mathcal{H}_n A = -A\mathcal{H}_n$, then for any sign functions $F, G$ of $f \in \mathrm{SB}^+(n)$ and $g \in \mathrm{SB}^-(n)$ respectively it holds

$$\mathcal{H}_n(AF) = -A(\mathcal{H}_n F) = -AF,$$
$$\mathcal{H}_n(AG) = -A(\mathcal{H}_n G) = AG,$$

hence the mapping is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$.

Take $\{f_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^+(n)$ with linearly independent sign functions $\{F_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}(\mathcal{H}_n - I_{2^n})$ and $\{g_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{SB}^-(n)$ with linearly independent sign functions $\{G_i\}_{i=1}^{2^{n-1}} \subseteq \mathrm{Ker}(H_n + I_{2^n})$ from the proof of the Proposition 2. Denote $B = \mathcal{H}_n A + A\mathcal{H}_n$ and assume that the mapping with matrix $A$ is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$. In particular, for $i = 1,2,...,2^{n-1}$ it holds

$$\mathcal{H}_n(AF_i) = -AF_i$$

and

$$\mathcal{H}_n(AG_i) = AG_i.$$

For $i = 1, 2, ..., 2^{n-1}$ we have

$$(\mathcal{H}_n A + A\mathcal{H}_n) F_i = \mathcal{H}_n (AF_i) + A (\mathcal{H}_n F_i) = \mathcal{H}_n (AF_i) + AF_i = BF_i.$$

Then $BF_i = \mathbf{0} \in \mathbb{R}^{2^n}$ for every $i = 1, 2, ..., 2^{n-1}$. Since the set $\{F_i\}_{i=1}^{2^{n-1}}$ forms a basis of the subspace $\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$, it can be deduced that all rows of the matrix $B$ are vectors from the subspace $(\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n}))^{\perp} = \mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$.

For $i = 1, 2, ..., 2^{n-1}$ we also have:

$$(\mathcal{H}_n A + A\mathcal{H}_n) G_i = \mathcal{H}_n (AF_i) + A (\mathcal{H}_n G_i) = \mathcal{H}_n (AG_i) - AG_i = BG_i.$$

In this case $BG_i = \mathbf{0} \in \mathbb{R}^{2^n}$ for every $i = 1, 2, ..., 2^{n-1}$. Since the set $\{G_i\}_{i=1}^{2^{n-1}}$ forms a basis of the subspace $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$ we can conclude that all rows of the matrix $B$ are vectors from the subspace $(\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}))^{\perp} = \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$.

Thus we have proved that all rows of the matrix $B$ lie in $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}) \cap \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$ but the intersection of orthogonal subspaces consists only of the zero element of the space $\mathbb{R}^n$. Therefore the matrix $B$ is zero matrix. □

**Theorem 2.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ if and only if*

$$\pi(x) = L(x \oplus c), \ x \in \mathbb{F}_2^n,$$

*and*

$$g(x) = \langle c, x \rangle \oplus d, \ x \in \mathbb{F}_2^n,$$

*where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is odd, $d \in \mathbb{F}_2$.*

*Proof.* Let $f \in \mathrm{SB}^+(n) \cup \mathrm{SB}^-(n)$ that is $\widetilde{f} = f \oplus \varepsilon$ for some $\varepsilon \in \mathbb{F}_2$. Consider a function $g(x) = f(L(x \oplus c)) \oplus \langle c, x \rangle \oplus d$, where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is odd, $d \in \mathbb{F}_2$. Its Walsh-Hadamard transform is

$$\begin{aligned} W_g(y) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,y \rangle \oplus g(x)} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x,y \rangle \oplus f(L(x \oplus c)) \oplus \langle c,x \rangle \oplus d} = \\ &= (-1)^d \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x, y \oplus c \rangle \oplus f(L(x \oplus c))} = (-1)^d \sum_{z \in \mathbb{F}_2^n} (-1)^{\langle L^{-1} z \oplus c, y \oplus c \rangle \oplus f(z)} = \\ &= (-1)^{d \oplus \langle c,y \rangle \oplus \langle c,c \rangle} \sum_{z \in \mathbb{F}_2^n} (-1)^{\langle z, L(y \oplus c) \rangle \oplus f(z)} = \\ &= (-1)^{d \oplus \langle c,y \rangle \oplus 1} 2^{n/2} (-1)^{\widetilde{f}(L(y \oplus c))} = 2^{n/2} (-1)^{f(L(y \oplus c)) \oplus \langle c,y \rangle \oplus d \oplus \varepsilon \oplus 1} = \\ &= 2^{n/2} (-1)^{g(y) \oplus \varepsilon \oplus 1} = 2^{n/2} (-1)^{\widetilde{g}(y)}, \end{aligned}$$

hence $\widetilde{g}(y) = g(y) \oplus \varepsilon \oplus 1$ for any $y \in \mathbb{F}_2^n$. The opposite direction has been proved.

By using the same arguments as in the proof of the Theorem 1 it can be deduced that the considered isometric mapping preserves affinity of a Boolean function and therefore has form

$$f(x) \longrightarrow f(Lx \oplus b) \oplus \langle c, x \rangle \oplus d,$$

where $L$ is a $n \times n$ nonsingular binary matrix, $b, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2$.

From Proposition 3 it follows that $AH_n = -H_n A$. Recall from the proof of the Theorem 1 that

$$(AH_n)_{i+1,j+1} = (-1)^{\langle c, \mathbf{v}_i \rangle \oplus \langle L\mathbf{v}_i \oplus b, \mathbf{v}_j \rangle \oplus d},$$

$$(H_n A)_{i+1,j+1} = (-1)^{\langle \mathbf{v}_i, L^{-1}(\mathbf{v}_j \oplus b) \rangle \oplus \langle c, L^{-1}(\mathbf{v}_j \oplus b) \rangle \oplus d}$$

for any $i, j \in \{0, 1, ..., 2^n - 1\}$.

Since $AH_n = -H_nA$ implies $(AH_n)_{i+1,j+1} = -(H_nA)_{i+1,j+1}$ for any $i, j \in \{0, 1, ..., 2^n - 1\}$, the following relation must hold

$$(-1)^{\langle c, \mathbf{v}_i \rangle \oplus \langle L\mathbf{v}_i \oplus b, \mathbf{v}_j \rangle \oplus d} = (-1)^{\left\langle \mathbf{v}_i, L^{-1}(\mathbf{v}_j \oplus b) \right\rangle \oplus \left\langle c, L^{-1}(\mathbf{v}_j \oplus b) \right\rangle \oplus d \oplus 1},$$

or, equivalently,

$$\langle c, x \rangle \oplus \langle Lx \oplus b, y \rangle \oplus d = \left\langle x, L^{-1}(y \oplus b) \right\rangle \oplus \left\langle c, L^{-1}(y \oplus b) \right\rangle \oplus d \oplus 1 \tag{5}$$

for any $x, y \in \mathbb{F}_2^n$.

Put zero vector $y \in \mathbb{F}_2^n$ in (5). Then

$$\langle c, x \rangle = \left\langle x, L^{-1}b \right\rangle \oplus \left\langle c, L^{-1}b \right\rangle \oplus 1,$$

$$\left\langle x, L^{-1}b \oplus c \right\rangle = \left\langle c, L^{-1}b \right\rangle \oplus 1$$

for any $x \in \mathbb{F}_2^n$. Then

$$\begin{cases} L^{-1}b \oplus c = 0, \\ \left\langle c, L^{-1}b \right\rangle = 1, \end{cases}$$

$$\begin{cases} b = Lc, \\ \mathrm{wt}(c) \text{ is odd.} \end{cases} \tag{6}$$

Return to (5) and take (6) into account:

$$\langle c, x \rangle \oplus \langle Lx \oplus Lc, y \rangle = \left\langle x, L^{-1}(y \oplus Lc) \right\rangle \oplus \left\langle c, L^{-1}(y \oplus Lc) \right\rangle \oplus 1,$$

$$\langle c, x \rangle \oplus \langle Lx, y \rangle \oplus \langle Lc, y \rangle = \left\langle x, L^{-1}y \right\rangle \oplus \langle x, c \rangle \oplus \left\langle c, L^{-1}y \right\rangle \oplus \langle c, c \rangle \oplus 1,$$

$$\langle Lx, y \rangle \oplus \langle Lc, y \rangle = \left\langle x, L^{-1}y \right\rangle \oplus \left\langle c, L^{-1}y \right\rangle,$$

$$\langle L(x \oplus c), y \rangle = \left\langle \left(L^{-1}\right)^T (x \oplus c), y \right\rangle$$

for any $x, y \in \mathbb{F}_2^n$. It holds if and only if

$$L = \left(L^{-1}\right)^T. \tag{7}$$

Thus, combining (6) and (7) we obtain

$$\begin{cases} L^{-1} = L^T, \\ b = Lc, \\ \mathrm{wt}(c) \text{ is odd.} \end{cases}$$

□

# 7 Isometric mappings and the Rayleigh quotient of the Sylvester Hadamard matrix

In this section isometric mappings from the set $\mathcal{I}_n$, which preserve and change the sign of the Rayleigh quotient (Rayleigh ratio) of the Sylvester Hadamard matrix defined for every Boolean function in $n$ variables, are studied.

## 7.1 Definition and characterization

In [2] the *Rayleigh quotient* $S_f$ of a Boolean function $f \in \mathcal{F}_n$ was defined as

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

For any $f \in \mathcal{B}_n$ the *normalized Rayleigh quotient* $N_f$ is a number

$$N_f = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \widetilde{f}(x)} = 2^{-n/2} S_f.$$

In [2] (Theorem 3.1) it was proved that for any $f \in \mathcal{F}_n$ the absolute value of $S_f$ is at most $2^{3n/2}$ with equality if and only if $f$ is self-dual $\left(+2^{3n/2}\right)$ and anti-self-dual $\left(-2^{3n/2}\right)$ bent function.

In the article [5] the operations on Boolean functions that preserve bentness and the Rayleigh quotient were given. Namely, it was proved that for any $f \in \mathcal{B}_n, L \in \mathcal{O}_n, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2$ the functions $g, h \in \mathcal{B}_n$ defined as $g(x) = f(Lx) \oplus d$ and $h(x) = f(x \oplus c) \oplus \langle c, x \rangle$ provide $N_g = N_f$ and $N_h = (-1)^{\langle c,c \rangle} N_f$.

One can notice that the mentioned operations are isometric mappings from $\mathcal{I}_n$.

Assume that $n \geqslant 4$ is an even integer. In the following subsections we generalize these results within isometric mappings from the set $\mathcal{I}_n$.

## 7.2 Isometric mappings preserving the Rayleigh quotient

**Theorem 3.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ preserves the Rayleigh quotient if and only if it preserves self-duality.*

*Proof.* For straight direction it is enough to mention that $S_f = +2^{3n/2}$ if and only if $f \in \mathrm{SB}^+(n)$ ([2], Theorem 3.1).

Assume that the mapping $\varphi_{\pi,g}$ preserves self-duality. Let $A$ be its matrix. Then by Proposition 2 we have $AH_n = H_n A$. Take arbitrary $f \in \mathcal{F}_n$ and rewrite the Rayleigh quotient in the following form:

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

where $F$ is a sign function of $f$. The mapping preserves the Rayleigh quotient if

$$S_{\varphi_{\pi,g}(f)} = \langle AF, H_n(AF) \rangle = \langle F, H_n F \rangle = S_f.$$

Consider

$$\langle AF, H_n(AF) \rangle = \langle AF, A(H_n F) \rangle = \left\langle A^T AF, H_n F \right\rangle = \langle F, H_n F \rangle,$$

therefore $\varphi_{\pi,g}$ preserves the Rayleigh quotient. □

**Corollary 3.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ preserves the Rayleigh quotient if and only if*

$$\pi(x) = L(x \oplus c), \ x \in \mathbb{F}_2^n,$$

*and*

$$g(x) = \langle c, x \rangle \oplus d, \ x \in \mathbb{F}_2^n,$$

*where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{F}_2$.*

### 7.3 Isometric mappings changing the sign of the Rayleigh quotient

**Theorem 4.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ changes the sign of the Rayleigh quotient if and only if it is a bijection between* $\mathrm{SB}^+(n)$ *and* $\mathrm{SB}^-(n)$.

*Proof.* For straight direction it is enough to mention that $S_f = +2^{3n/2}$ if and only if $f \in \mathrm{SB}^+(n)$ and $S_f = -2^{3n/2}$ if and only if $f \in \mathrm{SB}^-(n)$ ([2], Theorem 3.1).

Assume that the mapping $\varphi_{\pi,g}$ is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$. Let $A$ be its matrix. Then by Proposition 3 we have $AH_n + H_nA = 0$. Take arbitrary $f \in \mathcal{F}_n$ and rewrite the Rayleigh quotient in the following form:

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

where $F$ is a sign function of $f$. The mapping changes the sign of the Rayleight quotient if

$$S_{\varphi_{\pi,g}(f)} = \langle AF, H_n (AF) \rangle = - \langle F, H_n F \rangle = -S_f.$$

Consider

$$\langle AF, H_n (AF) \rangle = \langle AF, -A (H_n F) \rangle = - \left\langle A^T AF, H_n F \right\rangle = - \langle F, H_n F \rangle ,$$

therefore $\varphi_{\pi,g}$ changes the sign of the Rayleigh quotient. □

**Corollary 4.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ changes the sign of the Rayleigh quotient if and only if*

$$\pi(x) = L (x \oplus c) , \ x \in \mathbb{F}_2^n,$$

*and*

$$g(x) = \langle c, x \rangle \oplus d, \ x \in \mathbb{F}_2^n,$$

*where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is odd, $d \in \mathbb{F}_2$.*

From Theorems 3 and 4 it follows

**Corollary 5.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$, which preserves the Rayleigh quotient or changes the sign of the Rayleigh quotient, also preserves bentness.*

### 7.4 Isometric mappings preserving the Hamming distance between bent function and its dual

The Rayleigh quotient characterizes the Hamming distance between a bent-function and its dual. Indeed, let $f \in \mathcal{B}_n$, then

$$\mathrm{dist}\left(f, \widetilde{f}\right) = 2^{n-1} - \frac{1}{2^{n/2+1}} S_f = 2^{n-1} - \frac{1}{2} N_f.$$

**Theorem 5.** *Isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ preserves bentness and the Hamming distance between any bent function in $n$ variables and its dual if and only if it preserves (anti-)self-duality.*

*Proof.* If $\varphi_{\pi,g}$ preserves the Hamming distance between any bent function in $n$ variables and its dual then it preserves (anti-)self-duality.

If $\varphi_{\pi,g}$ preserves (anti-)self-duality then by Theorem 3 it preserves the Rayleigh quotient and from Theorem 1 it follows that this mapping preserves bentness. The characterization of the Hamming distance between bent function and its dual in terms of the Rayleigh quotient yields the result. □

The form of such mappings is described by Theorem 1.

# 8 Summary

In this section we summarize and group results from the paper.

Assume that $n \geqslant 4$ is an even integer.

Let $\varphi_{\pi,g}$ be an isometric mapping of the set of all Boolean functions in $n$ variables to itself with matrix $A$, namely

$$\varphi_{\pi,g} : f(x) \longrightarrow f\left(\pi(x)\right) \oplus g(x),$$

where $\pi$ is a permutation in $\mathbb{F}_2^n$ and $g \in \mathcal{F}_n$. The matrix $A$ is the following

$$\begin{array}{c} \\ \mathbf{v}_i \end{array} \begin{array}{c} \pi\left(\mathbf{v}_i\right) \\ \left( \begin{array}{ccccccc} & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \\ 0 & \ldots & 0 & (-1)^{g(\mathbf{v}_i)} & 0 & \ldots & 0 \\ & & & 0 & & & \\ & & & \vdots & & & \\ & & & 0 & & & \end{array} \right) \end{array},$$

where in the row with number $(i+1) \in \{1, 2, ..., 2^n\}$ a nonzero element is in the $(j+1)$-th column, where $j$ is a number with binary representation $\pi\left(\mathbf{v}_i\right)$.

**Theorem 6.** *The following conditions are equivalent:*

*1)* $\varphi_{\pi,g}$ *preserves self-duality;*

*2)* $\varphi_{\pi,g}$ *preserves anti-self-duality;*

*3)* $\varphi_{\pi,g}$ *preserves the Rayleigh quotient of every Boolean function;*

*4)* $\varphi_{\pi,g}$ *preserves bentness and the Hamming distance between any bent function and its dual;*

*5)* $\pi(x) = L\left(x \oplus c\right), g(x) = \langle c, x\rangle \oplus d$, *where* $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ *is even,* $d \in \mathbb{F}_2$;

*6)* $A\mathcal{H}_n = \mathcal{H}_n A$.

**Theorem 7.** *The following conditions are equivalent:*

*1)* $\varphi_{\pi,g}$ *is a bijection between* $\mathrm{SB}^+(n)$ *and* $\mathrm{SB}^-(n)$;

*2)* $\varphi_{\pi,g}$ *changes sign of the Rayleigh quotient of every Boolean function;*

*3)* $\pi(x) = L\left(x \oplus c\right), g(x) = \langle c, x\rangle \oplus d$, *where* $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ *is odd,* $d \in \mathbb{F}_2$;

*4)* $A\mathcal{H}_n = -\mathcal{H}_n A$.

Recall that the extended orthogonal group $\overline{\mathcal{O}}_n$ consists of mappings of all Boolean functions in $n$ variables to itself which have form

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x\rangle \oplus d,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{F}_2$.

The group of automorphisms of (anti-)self-dual bent functions is characterized by the following

**Theorem 8.** *It holds*

$$\mathrm{Aut}\left(\mathrm{SB}^+(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^-(n)\right) = \overline{\mathcal{O}}_n.$$

From the obtained results it follows that an approach to equivalence of self-dual bent functions in $n \geqslant 4$ variables based on the restricted form of affine equivalence proposed in articles [2, 7] is the most general within isometric mappings of the set of all Boolean functions in $n$ variables to itself.

## 9 Conclusion

In current paper isometric mappings of all Boolean functions in $n \geqslant 4$ variables to itself preserving self-duality and anti-self-duality of Boolean bent function were completely studied. The obtained results were used to determine isometric mappings preserving the Rayleigh quotient of a Boolean function and isometric mappings preserving bentness and the Hamming distance between any bent function and its dual. The group of automorphisms of the set of (anti-)self-dual bent functions is obtained.

An interesting open problem is to characterize isometric mappings preserving self-duality which are not necessarily isometric mappings of the set of all Boolean functions.

## References


[1] Carlet C. Boolean functions for cryptography and error correcting code. In: Crama Y., Hammer P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. p. 257–397. Cambridge University Press, Cambridge (2010).

[2] Carlet C., Danielson L.E., Parker M.G., Solé P., Self-dual bent functions, Int. J. Inform. Coding Theory, **1**, 384–399 (2010).

[3] Carlet C., Mesnager S., Four decades of research on bent functions. In Journal Des. Codes Cryptogr., Springer, **78**(1), 5–50 (2016).

[4] Cusick T.W., Stănică P., Cryptographic Boolean functions and applications, Acad. Press, London, 2017, 288 pp.

[5] Danielsen L.E., Parker M.G., Solé P., The Rayleigh quotient of bent functions, Springer Lect. Notes in Comp. Sci. 5921, pp. 418–432. Springer, Berlin (2009).

[6] Dillon J., Elementary Hadamard Difference Sets, PhD. dissertation, Univ. Maryland, College Park (1974).

[7] Feulner T., Sok L., Solé P., Wassermann A. Towards the Classification of Self-Dual Bent Functions in Eight Variables. Des. Codes Cryptogr. **68**(1), 395–406 (2013).

[8] Hou X.-D., Classification of self dual quadratic bent functions, Des. Codes Cryptogr. **63**(2), 183–198 (2012).

[9] Hyun J.Y., Lee H., Lee Y., MacWilliams duality and Gleason-type theorem on self-dual bent functions, Des. Codes Cryptogr., **63**(3), 295–304 (2012).

[10] Janusz G.J., Parametrization of self-dual codes by orthogonal matrices, Finite Fields Appl., **13**(3), 450–491 (2007).

[11] Kutsenko A.V., The Hamming Distance Spectrum Between Self-Dual Maiorana–McFarland Bent Functions, Journal of Applied and Industrial Mathematics, **12**(1), 112–125 (2018).

[12] Kutsenko A.V., On metrical properties of self-dual bent functions, Des. Codes Cryptogr. (2019). https://doi.org/10.1007/s10623-019-00678-x.

[13] Luo G., Cao X., Mesnager S. Several new classes of self-dual bent functions derived from involutions, Cryptogr. Commun., (2019). https://doi.org/10.1007/s12095-019-00371-9

[14] MacWilliams F.J., Sloane N.J.A, The Theory of Error Correcting Codes, Amsterdam:North-Holland, 1977.

[15] Markov A. A. On transformations without error propagation, in: Selected Works, Vol. II: Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Informatics and Related Topics, p. 70–93, MTsNMO, Moscow (2003) [Russian].

[16] Mesnager S., Several New Infinite Families of Bent Functions and Their Duals, IEEE Trans. Inf. Theory, **60**(7), 4397–4407 (2014).

[17] Mesnager S., Bent Functions: Fundamentals and Results, 544 p., Springer, Berlin (2016).

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

[19] Sok L., Shi M., Solé. P., Classification and Construction of quaternary self-dual bent functions, Cryptogr. Commun., **10**(2), 277–289 (2017).

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

[21] Tokareva N.N., The group of automorphisms of the set of bent functions, Discrete Mathematics and Applications, **20**(5), 655–664 (2010).