UDC 519.7 DOI 10.17223/20710410/49/2

METRICAL PROPERTIES OF THE SET OF BENT FUNCTIONS IN VIEW OF DUALITY[1]

A. V. Kutsenko*,**, N. N. Tokareva*

*Sobolev Institute of Mathematics, Novosibirsk, Russia
**Novosibirsk State University, Novosibirsk, Russia

E-mail: alexandrkutsenko@bk.ru, tokareva@math.nsc.ru

In the paper, we give a review of metrical properties of the entire set of bent functions and its significant subclasses of self-dual and anti-self-dual bent functions. We present results for iterative construction of bent functions in $n+2$ variables based on the concatenation of four bent functions and consider related open problem proposed by one of the authors. Criterion of self-duality of such functions is discussed. It is explored that the pair of sets of bent functions and affine functions as well as a pair of sets of self-dual and anti-self-dual bent functions in $n \geqslant 4$ variables is a pair of mutually maximally distant sets that implies metrical duality. Groups of automorphisms of the sets of bent functions and (anti-)self-dual bent functions are discussed. The solution to the problem of preserving bentness and the Hamming distance between bent function and its dual within automorphisms of the set of all Boolean functions in n variables is considered.

Keywords: *Boolean bent function, self-dual bent function, Hamming distance, metrical regularity, automorphism group, iterative construction.*

1. Introduction

How much do we know about some cryptographic objects? One way to measure it is to describe what we can do with them. Otherwise, to characterize groups of automorphisms of these objects — separately for each object or together while they form some special class. The question about the group of automorphisms of a set in the Boolean cube necessarily leads us to metrical properties of this set.

That is why we are very interested in *metrical properties* of distinct cryptographic Boolean functions.

The term "bent function" was introduced by Oscar Rothaus in the 1960s [1]. It is known [2], that at the same time Boolean functions with maximal nonlinearity 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 S. Mesnager [4] and N. Tokareva [2] for more information concerning known results and open problems related to bent functions. Results regarding

[1]The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

the study of metrical properties, in particular, distances between bent functions, one can find in [5].

In this paper we give a review on metrical properties of the entire class of bent function $\mathcal{B}_n$ and its important subclasses — self-dual bent functions $\mathrm{SB}^+(n)$ (i.e. functions such that $f = \widetilde{f}$) and anti-self-dual bent functions $\mathrm{SB}^-(n)$ (i.e. functions such that $f \oplus 1 = \widetilde{f}$), where $\widetilde{f}$ is the dual of f. We suppose that the *keys* to the nontrivial and important properties of the class of bent functions are in understanding how does the *duality mapping* $f \to \widetilde{f}$ operate with bent functions. Recall that $\widetilde{\widetilde{f}} = f$ for every bent function f. It is important to note that the duality mapping is the *unique* known isometric mapping of the bent functions into themselves that can not be extended to a typical isometry of the whole set of all Boolean functions that preserves bent functions.

On the other hand, the essence of bent functions is expressed in their metrical properties, namely in maximizing distances between them and affine functions. Note that this very idea in more general form is realized in the concept of metrical complement and metrically regular sets. Recall that $\widehat{X}$ is the metrical complement of the set of functions X if it contains all Boolean functions that are on the maximal possible distance from X. The set is metrically regular, if $\widehat{\widehat{X}} = X$. There is a some similarity to the self-duality of bent functions, is not it?

Our attention is drawn to automorphism groups of the sets $\mathcal{B}_n$, $\mathcal{A}_n$, $\mathrm{SB}^+(n)$, $\mathrm{SB}^-(n)$ and their metrical properties. Previously, we established that the set of all bent functions $\mathcal{B}_n$ and the set of all affine functions $\mathcal{A}_n$ form a pair of metrically regular sets, i.e. $\widehat{\widehat{\mathcal{B}_n}} = \widehat{\mathcal{A}_n} = \mathcal{B}_n$. Now, we prove the same fact for the classes of self-dual and anti-self-dual functions: they form another such pair of metrically complement functions, i.e. $\widehat{\widehat{\mathrm{SB}^+(n)}} = \widehat{\mathrm{SB}^-(n)} = \mathrm{SB}^+(n)$. In both cases for elements in a pair of metrically regular sets we prove the coincidence of automorphism groups. Thus, $\mathrm{Aut}\,(\mathcal{B}_n) = \mathrm{Aut}\,(\mathcal{A}_n)$ and $\mathrm{Aut}\,\big(\mathrm{SB}^+(n)\big) = \mathrm{Aut}\,\big(\mathrm{SB}^-(n)\big)$. Some other curious properties of bent functions related to their special constructions are discussed.

The paper has the following structure: notation and definitions are in the Section 2. In Section 3, the duality of a bent function is described, including some its important properties and relevant hypothesis proposed by one of the authors (Section 3.1). Some general and metrical properties of the set of bent functions which coincide with their duals, namely self-dual bent functions, are given in Section 3.2. In Section 4, we discuss the iterative construction of bent function in $n+2$ variables based on the concatenation of four bent functions in n variables. The lower bounds on its cardinality and open problem relevant for the set of bent function are in Section 4.1. Criterion of self-duality for bent iterative functions and its corollaries for sign functions together with constructions of self-dual bent functions are discussed in Sections 4.2 and 4.3. In Section 5, the metrical complement of the set of bent functions is studied (Section 5.2) and the results regarding metrical regularity of the set of bent functions and the set of affine functions are given. Metrical complement of the set of (anti-)self-dual bent functions is in Section 5.3. In Section 6, groups of automorphisms of considered sets are studied. The group of automorphisms of the set of bent functions is characterized in Section 6.3 while the (anti-)self-dual case is in Section 6.4. In Section 7, we consider some relations between isometric mappings and the duality of bent function. Isometric mappings which define bijections between the sets of self-dual and anti-self dual bent functions are described in Section 7.1. The Rayleigh quotient of a Boolean function and description of isometric mappings that perserve it or change it for every Boolean function

is given in Section 7.2. The meaning of the Rayleigh quotient in a scope of bent functions is discussed as well.

2. Notation

Let $\mathbb{F}_2^n$ be a space of binary vectors of length n. A *Boolean function* f in n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Its *sign function* is $F(x) = (-1)^{f(x)}$, $x \in \mathbb{F}_2^n$. We will also refer to a sign function as to a vector from the set $\{\pm 1\}^{2^n}$:

$$F = (-1)^f = \left((-1)^{f_0}, (-1)^{f_1}, \ldots, (-1)^{f_{2^n-1}}\right) \in \{\pm 1\}^{2^n},$$

where $(f_0, f_1, \ldots, f_{2^n-1}) \in \mathbb{F}_2^{2^n}$ is a truth-table representation of f with arguments given in the lexicographic order. The set of all Boolean functions in n variables is denoted by $\mathcal{F}_n$.

The *algebraic normal form* (ANF, Zhegalkin polynomial) of a Boolean function $f \in \mathcal{F}_n$ is defined as

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{(i_1, i_2, \ldots, i_n) \in \mathbb{F}_2^n} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n},$$

where $a_z \in \mathbb{F}_2$ for any $z \in \mathbb{F}_2^n$ (with the convention $0^0 = 1$). The *algebraic degree* $\deg(f)$ of a Boolean function f is the maximal degree of monomials which occur in its algebraic normal form with nonzero coefficients.

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 *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 $\langle x, y \rangle = \bigoplus_{i=1}^{n} x_i y_i$. Boolean functions in n variables of the form $f(x) = \langle a, x \rangle \oplus a_0$, $x \in \mathbb{F}_2^n$, where $a_0 \in \mathbb{F}_2$, $a \in \mathbb{F}_2^n$, are called *affine* functions. The set of all affine functions in n variables is denoted by $\mathcal{A}_n$.

The *Walsh – Hadamard transform* (WHT) of a Boolean function f in n variables is an integer valued 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 called *bent* if

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

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

A mapping φ 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 $f, g \in \mathcal{F}_n$.

Denote, following [6], the orthogonal group of index n over the field $\mathbb{F}_2$ as

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

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

3. The dual of a bent function

From the definition of a bent function it follows that there exists such $\widetilde{f} \in \mathcal{F}_n$ that for any $y \in \mathbb{F}_2^n$ we have

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

The Boolean function $\widetilde{f}$ defined above is called the *dual* function of the bent function f. Thus, for any bent function in n variables its dual Boolean function is uniquely defined. The duality of bent functions was introduced by Dillon [7].

3.1. P r o p e r t i e s

Some basic known properties of dual functions are the following [8]:

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

There is the following connection between the algebraic degrees of a bent function and its dual [9]:

$$n/2 - \deg(f) \geqslant \frac{n/2 - \deg\left(\widetilde{f}\right)}{\deg\left(\widetilde{f}\right) - 1}.$$

Some results obtained for dual functions can be used in proving the results concerning bent functions, in particular, the connection between ANF coefficients of a bent function and its dual, see [10]:

$$\sum_{x \preccurlyeq y} f(x) = 2^{\mathrm{wt}(y)} - 2^{n/2-1} + 2^{\mathrm{wt}(y)-n/2} \sum_{x \preccurlyeq y \oplus 1} \widetilde{f}(x).$$

One of the most important problem in bent functions is to find the number of them. A new approach to this problem was introduced in [11], see Section 4.1, and the following hypothesis was formulated.

Hypothesis (Tokareva, 2011). Any Boolean function in n variables of degree not more than $n/2$ can be represented as the sum of two bent functions in n variables, where $n \geqslant 2$ is an even number.

The review of partial results regarding this problem and also in favour of the Hypothesis one can find in [12]. It was also proved in [13] that

Theorem 1 [13]. A bent function in $n \geqslant 4$ variables can be represented as the sum of two bent functions in n variables if and only if its dual bent function does.

So, it follows that the mentioned Hypothesis with the decomposition problem, see Section 4.1, can not be considered separately for a bent function and its dual.

It is worth noting that this Hypothesis is a counterpart of the Goldbach's conjecture in number theory unsolved since 1742: any even number $n > 4$ can be represented as the sum of two prime numbers.

Isometric mappings of the set of all Boolean functions in n variables to itself which preserve bentness and the Hamming distance between every bent function and its dual were characterized in [14], namely it was proved that

Theorem 2 [14]. An isometric mapping φ of the set of all Boolean functions in n variables into itself preserves bentness and the Hamming distance between every bent function and its dual if and only if φ has form

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x\rangle \oplus d, \quad x \in \mathbb{F}_2^n, \tag{1}$$

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

3.2. Self-duality

If a bent function f coincides with its dual it is said to be *self-dual*, that is, $f = \widetilde{f}$. A bent function which coincides with the negation of its dual is called an *anti-self-dual*, that is, $f = \widetilde{f} \oplus 1$. The set of (anti-)self-dual bent functions in n variables, according to [15], is denoted by $\mathrm{SB}^+(n)$ $\left(\mathrm{SB}^-(n)\right)$.

Self-dual bent functions were explored in paper of C. Carlet et al. [16] in 2010, where important properties and constructions were given. 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 respect to a restricted form of an affine transformation (1), which preserves self-duality, were also presented. 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 [17]. In [15], 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 [18]. In [19, 20], one can find new constructions of self-dual bent functions. In papers [21 – 23], several families of self-dual bent functions from involutions were presented. A connection of quaternary self-dual bent functions and self-dual bent Boolean functions was shown in [24]. In [25], it was proved that for $n \geqslant 4$ and any $d \in \{2, 3, \ldots, n/2\}$ there exists a self-dual bent function in n variables of algebraic degree d.

In papers [14, 25, 26], metrical properties of the sets of (anti-)self-dual bent functions in n variables were studied. Below we briefly discuss some of them.

Recall that bent functions in $2k$ variables which have a representation

$$f(x, y) = \langle x, \pi(y)\rangle \oplus g(y), \quad x, y \in \mathbb{F}_2^k,$$

where $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and g is a Boolean function in k variables, form the well known *Maiorana — McFarland class* of bent functions [27]. Necessary and sufficient conditions of (anti-)self-duality of bent functions from Maiorana — McFarland class are known from [16]. Let the denotion $\mathrm{SB}^+_{\mathcal{M}}(n)$ stands for the set of self-dual Maiorana — McFarland bent functions and $\mathrm{SB}^-_{\mathcal{M}}(n)$ for the set of anti-self-dual ones both in n variables. In [26], the set of possible Hamming distance between such self-dual bent functions was found.

Theorem 3 [26]. Let $n \geqslant 4$ and $f, g \in \mathrm{SB}^+_{\mathcal{M}}(n) \cup \mathrm{SB}^-_{\mathcal{M}}(n)$, then

$$\mathrm{dist}(f, g) \in \left\{2^{n-1}, 2^{n-1}\left(1 \pm \frac{1}{2^r}\right), r = 0, 1, ..., n/2 - 1\right\}.$$

Moreover, if either $f, g \in \mathrm{SB}^+_{\mathcal{M}}(n)$ or $f, g \in \mathrm{SB}^-_{\mathcal{M}}(n)$, then all distances are attainable, and for any pair $f \in \mathrm{SB}^+_{\mathcal{M}}(n)$ and $g \in \mathrm{SB}^-_{\mathcal{M}}(n)$ it holds $\mathrm{dist}(f, g) = 2^{n-1}$.

By analysis of the set of distances from Theorem 3, the minimal Hamming distance between considered functions can be obtained.

Corollary 1. Let $n \geqslant 4$, then the minimal Hamming distance between (anti-)self-dual Maiorana — McFarland bent functions is equal to 2^{n-2}.

Moreover, since the minimal Hamming distance between quadratic Boolean functions in n variables (which correspond to codewords of the $\mathrm{RM}(2,n)$ code) is at least 2^{n-2} [28], the following fact holds.

Corollary 2. Let $n \geqslant 4$, then the minimal Hamming distance between quadratic bent functions can be attained on (anti-)self-dual Maiorana — McFarland bent functions.

It is known that the minimal Hamming distance between bent functions in n variables is $2^{n/2}$ [5]. In [25], it was proved that this extremal value can be attained on (anti-)self-dual bent functions.

Theorem 4 [25]. Let $n \geqslant 4$, then the minimal Hamming distance between distinct (anti-)self-dual bent functions in n variables is equal to $2^{n/2}$.

In the case $n = 2$, there are only two self-dual Maiorana — McFarland bent functions, namely $f_1(x_1, x_2) = x_1x_2$ and $f_2(x_1, x_2) = x_1x_2 \oplus 1$, and two anti-self-dual Maiorana — McFarland bent functions, namely $g_1(x_1, x_2) = x_1x_2 \oplus x_1 \oplus x_2$ and $g_2(x_1, x_2) = x_1x_2 \oplus x_1 \oplus \oplus x_2 \oplus 1$. It is clear that $\mathrm{dist}(f_1, g_1) = \mathrm{dist}(f_2, g_2) = 4 = 2^n$ and $\mathrm{dist}(f_1, g_2) = \mathrm{dist}(f_2, g_1) = = 2 = 2^{n-1}$.

4. Iterative construction $\mathcal{BI}$

Let f_0, f_1, f_2, f_3 be Boolean functions in n variables. Consider a Boolean function g in $n + 2$ variables which is defined as

$$g(00, x) = f_0(x), \quad g(01, x) = f_1(x), \quad g(10, x) = f_2(x), \quad g(11, x) = f_3(x), \quad x \in \mathbb{F}_2^n.$$

It is known (Preneel et al., 1991; see also [11, 29]) that under condition $f_0, f_1, f_2, f_3 \in \mathcal{B}_n$ the mentioned function g is a bent function in $n + 2$ variables if and only if

$$\widetilde{f}_0 \oplus \widetilde{f}_1 \oplus \widetilde{f}_2 \oplus \widetilde{f}_3 = 1,$$

that gives the construction of a bent function in $n + 2$ variables through the concatenation of vectors of values of four bent functions in n variables [30].

Following N. Tokareva [11], we will refer to bent functions obtained by this construction as *bent iterative functions* ($\mathcal{BI}$) and denote the set of such bent functions in n variables by $\mathcal{BI}_n$.

In [31], the comparison of cardinalities of different known iterative constructions of bent functions in $n \leqslant 10$ variables was presented and the class $\mathcal{BI}$ had the biggest cardinality among them.

According to [29], there exist bent functions from Maiorana — McFarland class [27] and from the class $\mathcal{PS}$ (Partial Spreads) [7] that can not be represented as bent iterative functions. Also, from paper [32] on nonnormal bent functions, it follows that there exist bent functions in $\mathcal{BI}_n$ that are nonequivalent to Maiorana — McFarland bent functions.

4.1. Lower bounds on the cardinality and related open problem

In paper [11], some possible methods for calculating the number of bent iterative functions were shown.

Theorem 5 [11]. For any even $n \geqslant 4$

$$|\mathcal{BI}_n| = \sum_{f' \in \mathcal{B}_{n-2}} \sum_{f'' \in \mathcal{B}_{n-2}} |(\mathcal{B}_{n-2} \oplus f') \cap (\mathcal{B}_{n-2} \oplus f'')| .$$

Denote $X_n = \{f \oplus h : f, h \in \mathcal{B}_n\}$ and consider the system $\{C_f : f \in \mathcal{B}_n\}$ of its subsets defined as $C_f = \mathcal{B}_n \oplus f$. So

$$X_n = \bigcup_{f \in \mathcal{B}_n} C_f.$$

Let ψ be an element of X_n. The number of subsets C_f that cover ψ, according to [11], is called *multiplicity* of ψ and is denoted by $m(\psi)$. One can notice that if ψ is covered by C_f, then it is covered by any set $C_{f'}$, where f' is obtained from f by adding an affine function.

In [11], the exact number of bent iterative functions through the multiplicities was obtained.

Theorem 6 [11]. For any even $n \geqslant 2$,

$$|\mathcal{BI}_{n+2}| = \sum_{\psi \in C_f} m^2(\psi).$$

So in order to evaluate $|\mathcal{BI}_{n+2}|$ (and then $|\mathcal{B}_{n+2}|$) we have to study the set X_n and the distribution of multiplicities for its elements. Such an analysis, as shown in [11], gives the following lower bound.

Theorem 7 [11]. For any even $n \geqslant 2$,

$$\frac{|\mathcal{B}_{n+2}|^4}{|X_n|} \leqslant |\mathcal{BI}_{n+2}| \leqslant |\mathcal{B}_{n+2}|.$$

Thus, for calculating the exact number of bent iterative functions, one has to study the structure of the set X_n. So we come to a new problem statement.

Open problem: bent sum decomposition (Tokareva, 2011). What Boolean functions can be represented as the sum of two bent functions in n variables? How many such representations does a Boolean function admit?

The related Hypothesis was previuosly mentioned in the Section 3.1.

4.2. Self-dual bent iterative functions

The set of (anti-)self-dual bent functions from $\mathcal{BI}_n$ is further denoted by $\mathrm{SB}^{+}_{\mathcal{BI}}(n)$ $\left(\mathrm{SB}^{-}_{\mathcal{BI}}(n)\right)$.

In paper [25], the necessary and sufficient conditions of self-duality of bent iterative functions were studied, namely, the following result was obtained: taking constant function h, we can obtain two constructions of self-dual bent iterative functions in $n+2$ variables.

Theorem 8 [25]. Let $g \in \mathcal{BI}_{n+2}$. Then g is self-dual bent if and only if there exists such pair of functions $g_1, g_2 \in \mathcal{B}_n$, that

$$\begin{aligned}
f_0 &= (g_1 \oplus g_2)\, h \oplus g_1 = \widetilde{g}_2,\\
f_1 &= (g_1 \oplus g_2)\, h \oplus g_2 = \widetilde{g_1 \oplus h},\\
f_2 &= (g_1 \oplus g_2)\, h \oplus g_2 \oplus h = \widetilde{g}_1,\\
f_3 &= (g_1 \oplus g_2)\, h \oplus g_1 \oplus h \oplus 1 = \widetilde{g_2 \oplus h} \oplus 1,
\end{aligned}$$

where the function $h \in \mathcal{F}_n$ is uniquely defined by a pair of bent functions g_1, g_2, namely:

$$h = g_1 \oplus \widetilde{g}_1 \oplus g_2 \oplus \widetilde{g}_2.$$

Two iterative constructions of self-dual bent functions immeditely follow from Theorem 8, as it was shown in [25].

Corollary 3. Functions

$$f'(y_1, y_2, x) = (y_1 \oplus y_2)\left(f(x) \oplus \widetilde{f}(x)\right) \oplus f(x) \oplus y_1 y_2,$$
$$f''(y_1, y_2, x) = (y_1 \oplus y_2)(\varphi(x) \oplus \omega(x)) \oplus \varphi(x) \oplus \alpha_1 y_1 \oplus \alpha_2 y_2 \oplus y_1 y_2,$$

where $y_1, y_2, \alpha_1, \alpha_2 \in \mathbb{F}_2$, $\alpha_1 \oplus \alpha_2 = 1$, $x \in \mathbb{F}_2^n$, $f \in \mathcal{B}_n$, $\varphi \in \mathrm{SB}^+(n)$, $\omega \in \mathrm{SB}^-(n)$, are self-dual bent functions in $n+2$ variables.

The first construction (for f') was earlier presented in [16] as an example of the construction which uses the indirect sum of bent functions, see [8]. It is worth noting that the second construction (for f'') can also be obtained from indirect sum of bent functions.

Since these constructions do not intersect, the sum of their cardinalities provides a lower bound for the cardinality of the set of self-dual bent iterative functions [25].

Corollary 4. $|\mathcal{B}_{n-2}| + \left|\mathrm{SB}^+(n-2)\right|^2 \leqslant \left|\mathrm{SB}^+_{\mathcal{BI}}(n)\right| \leqslant |\mathcal{B}_{n-2}|^2$.

4.3. The dimension of linear span of sign functions of self-dual bent functions

Let $H_n = H_1^{\otimes n}$ 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:

$$H_n H_n^{\mathrm{T}} = 2^n I_{2^n}.$$

Denote $\mathcal{H}_n = 2^{-n/2} H_n$. In terms of sign functions, the function $f \in \mathcal{F}_n$ is bent if for its sign function F it holds $\mathcal{H}_n F \in \{\pm 1\}^{2^n}$.

Recall that 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 λ is called an *eigenspace* associated with λ. Consider a linear mapping $\psi : \mathbb{C}^n \to \mathbb{C}^n$ represented by a $n \times n$ complex matrix A. A *kernel* of ψ 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 $\mathbb{C}^n$.

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 $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}) = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)$.

In [16], an orthogonal decomposition of $\mathbb{R}^{2^n}$ in eigenspaces of H_n was given:

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

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

It is known that

$$\dim\left(\mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)\right) = \dim\left(\mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right)\right) = 2^{n-1},$$

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 the subspaces $\mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right)$ and $\mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)$ are mutually orthogonal.

In [25], it was proved that

Theorem 9 [25]. If $n \geqslant 4$, then:

— among sign functions of self-dual bent functions in n variables there exists a basis of the eigenspace of the matrix H_n attached to the eigenvalues 1, that is, the subspace $\mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right)$;

— among sign functions of anti-self-dual bent functions in n variables there exists a basis of the eigenspace of the matrix H_n attached to the eigenvalues (-1), that is, the subspace $\mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)$.

It is worth notice that there exists an example of basis which consists of sign functions of self-dual bent iterative functions provided by two constructions of self-dual bent iterative functions obtained by Theorem 8. Given the basis for self-dual case, the basis for anti-self-dual case can be obtained by using one of bijections from Theorem 20.

5. Metrical complement and regularity

In this section, we give results regarding notable metrical property of a subset of Boolean cube called metrical regularity. The sets of affine Boolean functions and bent functions possess it. The sets of self-dual and anti-self-dual bent functions in $n \geqslant 4$ variables are also mutually maximally distant. That implies metrical *duality*, in some sence, between the considered pairs of subsets of Boolean functions.

Regarding that, some essential and intriguing questions arise: for instance, are there any pairs of metrically regular subsets inside the metrically regular set of bent functions in n variables? If additionally, in order to exclude some trivial cases, we consider only the subsets which include functions together with their negations, the maximal Hamming distance from the considered sets is at most 2^{n-1}. Are there any pairs of metrically regular subsets with additional mentioned requirement such that the distance between them is exactly 2^{n-1}, that is, they would be extreme?

5.1. Definitions

Let $X \subseteq \mathbb{F}_2^n$ be an arbitrary set and let $y \in \mathbb{F}_2^n$ be an arbitrary vector. Define the *distance* between y and X as $\mathrm{dist}(y, X) = \min\limits_{x \in X} \mathrm{dist}(y, x)$. The *maximal distance* from the set X is

$$\mathrm{d}(X) = \max_{y \in \mathbb{F}_2^n} \mathrm{dist}(y, X).$$

In coding theory this number is also known as the *covering radius* of the set X. A vector $z \in \mathbb{F}_2^n$ is called *maximally distant* from a set X if $\mathrm{dist}(z, X) = \mathrm{d}(X)$. The set of all maximally distant vectors from the set X is called the *metrical complement* of the set X and is denoted by $\widehat{X}$ [33]. A set X is said to be *metrically regular* if $\widehat{\widehat{X}} = X$. Define, following N. Tokareva [2], a subset of Boolean functions to be *metrically regular* if the set of corresponding vectors of values is metrically regular.

Sets of functions which have maximum distance from partition set functions were studied in [34], it was shown that partition set functions defined by some partition are mutually maximally distant sets. Lower bound on size of the largest metrically regular subset of the Boolean cube was studied in [35].

5.2. The set of bent functions

Let $\mathrm{GA}(n)$ denote an affine group.

Proposition 1. Any isometric mapping of the form

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

where $A \in \mathrm{GL}(n)$, $b, c \in \mathbb{F}_2^n$, $d \in \mathbb{F}_2$, preserves bentness.

In [36], the following theorem was proved.

Theorem 10 [36]. For each non-affine Boolean function $h \in \mathcal{F}_n$, there exists a bent function $f \in \mathcal{B}_n$ such that $f \oplus h$ is not bent.

From Proposition 1 and Theorem 10 it follows that the set of bent functions is closed under addition of affine Boolean functions only. This fact implies that the affine functions are precisely all Boolean functions which are at the maximum distance from the class of bent functions. Namely, in [36] it was shown that

Theorem 11 [36]. A Boolean function in n variables is

— a bent function if and only if it has the maximal possible distance $2^{n-1} - 2^{n/2-1}$ to the set of all affine functions, that is it is an element of $\widehat{\mathcal{A}_n}$;

— an affine function if and only if it has the maximal possible distance $2^{n-1} - 2^{n/2-1}$ to the set of all bent functions, that is it is an element of $\widehat{\mathcal{B}_n}$.

Thus, from the results given in [36], it follows that there exists a *duality*, in some sense, between the definitions of bent functions and affine functions. In particular, we obtain metrical regularity of the sets of affine functions and bent functions.

Corollary 5.

1) The set $\mathcal{A}_n$ of all affine Boolean functions in n variables is metrically regular.
2) The set $\mathcal{B}_n$ of all bent functions in n variables is metrically regular.

5.3. The set of (anti-)self-dual bent functions

For any (anti-)self-dual bent function $f \in \mathrm{SB}^+(n)$ its negation $f \oplus 1$ is also (anti-)self-dual bent [16, 17]. Moreover, from the results presented in [14], it follows the counterpart of Theorem 10 for the (anti-)self-dual case, namely:

Theorem 12. For each non-constant Boolean function $h \in \mathcal{F}_n$ there exists a self-dual bent function $f \in \mathrm{SB}^+(n)$ such that $f \oplus h$ is not self-dual bent. Anti-self-dual bent functions possess the same property.

Thus, it follows that the set of (anti-)self-dual bent functions is closed only under addition of 1, that is, taking the negation of the function.

From the fact that considered set is closed under addition of 1, it follows that the maximal Hamming distance from the set $\mathrm{SB}^+(n)$ is at most 2^{n-1}. It was proved by Carlet et al. in [16] that the Hamming distance between any pair of self-dual and anti-self-dual bent functions, both in n variables, is equal to 2^{n-1}. So we have

$$\mathrm{d}\left(\mathrm{SB}^+(n)\right) = 2^{n-1},$$

and all anti-self-dual bent functions in n variables belong to the metrical complement of the set of self-dual bent functions in n variables.

In paper [25], the metrical complement of the set of (anti-)self-dual bent functions in $n \geqslant 4$ variables was completely characterized by using the orthogonal decomposition (2) and existence of the basis provided by the Theorem 9.

Theorem 13 [25]. Let $n \geqslant 4$, then a Boolean function in n variables is:

— self-dual bent if and only if it has the maximal possible distance 2^{n-1} to the set of all anti-self-dual bent functions, that is, it is an element of $\widehat{\mathrm{SB}^-(n)}$;

— anti-self-dual bent if and only if it has the maximal possible distance 2^{n-1} to the set of all self-dual bent functions, that is, it is an element of $\widehat{\mathrm{SB}^+(n)}$.

As for the pair of the sets of bent functions and affine functions, it follows that there also exists a *duality* between the sets of self-dual and anti-self-dual bent functions in $n \geqslant 4$ variables.

The case $n = 2$ was considered explicitly and it appeared that both $\mathrm{SB}^+(2)$ and $\mathrm{SB}^-(2)$ are metrically regular sets. From that and the Theorem 13 it follows

Corollary 6.

1) The set $\mathrm{SB}^+(n)$ of all self-dual bent functions in n variables is metrically regular.
2) The set $\mathrm{SB}^-(n)$ of all anti-self-dual bent functions in n variables is metrically regular.

6. The group of automorphisms

Study of automorphism groups of mathematical objects deserves attention since these groups are closely connected with the structure of the objects. There exists a natural question: how groups of automorphisms of two mathematical objects, one of which is embedded to another one, are related.

An example of such a problem statement is the set of bent functions in n variables and one of its significant subclasses which consisits of self-dual bent functions in n variables.

It is also worth mentioning that the complexity of classification of combinatorial objects depends on generality of the approach. Consequently, the question "*if the common approach to classify* (*self-dual*) *bent functions is the most general within automorphisms of the set of Boolean functions*", arises naturally.

6.1. Isometric mappings and automorphism groups

Recall that a mapping φ of the set of all Boolean functions in n variables to itself is called *isometric* if it preserves the Hamming distance between functions. Following [14], denote the set of all isometric mappings of the set of all Boolean functions in n variables to itself by $\mathcal{I}_n$.

It is known (A. A. Markov, 1956) that every isometric mapping of all Boolean functions in n variables to itself has the unique representation of the form

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x), \tag{3}$$

where π is a permutation on the set $\mathbb{F}_2^n$ and $g \in \mathcal{F}_n$ [37]. The mapping of this form is denoted by $\varphi_{\pi,g} \in \mathcal{I}_n$.

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 $\mathrm{Aut}\,(M)$.

6.2. Matrix representation

For the number $k \in \{0, 1, \ldots, 2^n - 1\}$, denote by $\mathbf{v}_k \in \mathbb{F}_2^n$ its binary representation.

Recall that a square matrix is called *monomial* (or *generalized permutation matrix*) if it has exactly one nonzero entry in each row and each column.

The following one-to-one correspondence between the set $\mathcal{I}_n$ and the set of monomial matrices of order 2^n with nonzero elements from the set $\{\pm 1\}$ was used in [14]. In more

detail, let $\varphi_{\pi,g} \in \mathcal{I}_n$ be an arbitrary isometric mapping. Then, for any $f \in \mathcal{F}_n$ and its sign function

$$F = \left((-1)^{f(\mathbf{v}_0)}, (-1)^{f(\mathbf{v}_1)}, \ldots, (-1)^{f(\mathbf{v}_{2^n-1})}\right) \in \{\pm 1\}^{2^n},$$

the sign function

$$F' = \left((-1)^{f'(\mathbf{v}_0)}, (-1)^{f'(\mathbf{v}_1)}, \ldots, (-1)^{f'(\mathbf{v}_{2^n-1})}\right) \in \{\pm 1\}^{2^n}$$

of $f' = \varphi_{\pi,g}(f) \in \mathcal{F}_n$ can be expressed as $F' = AF$, where A is the $2^n \times 2^n$ monomial matrix, constructed by the permutation π and the function g:

$$i \begin{pmatrix} & & & & j & & & \\ & & & & \vdots & & & \\ & & & & 0 & & & \\ & & & & \vdots & & & \\ \ldots & 0 & \ldots & & (-1)^{g(\mathbf{v}_{i-1})} & \ldots & 0 & \ldots \\ & & & & \vdots & & & \\ & & & & 0 & & & \\ & & & & \vdots & & & \end{pmatrix},$$

in which in the i-th row a nonzero element $(-1)^{g(\mathbf{v}_{i-1})}$ is in the j-th column, where $(j-1)$ is a number with binary representation $\pi(\mathbf{v}_{i-1})$. So the i-th component of $F' = AF$ is equal to

$$(-1)^{f'(\mathbf{v}_{i-1})} = (-1)^{f(\pi(\mathbf{v}_{i-1}))}(-1)^{g(\mathbf{v}_{i-1})} = (-1)^{f(\pi(\mathbf{v}_{i-1}))\oplus g(\mathbf{v}_{i-1})}$$

for any $i \in \{1, 2, \ldots, 2^n\}$, that is, equivalent to $f'(x) = f(\pi(x)) \oplus g(x)$, $x \in \mathbb{F}_2^n$.

6.3. The group of automorphisms of the set of bent functions

Some attempts to determine the automorphism group of a given bent function were undertaken by U. Dempwolff in 2006 [38]. Results were presented in terms of elementary Abelian Hadamard difference sets (equivalently, bent functions).

A natural question whether there exist isometric mappings of Boolean functions into itself, distinct from those mentioned in Proposition 1, which preserve the class of bent function, was completely solved in paper [39]. It was proved that there were no other mappings possessing such a property. Namely, by using the Theorem 11 in view of the duality, the following coincidence was shown.

Theorem 14 [39]. $\mathrm{Aut}(\mathcal{B}_n) = \mathrm{Aut}(\mathcal{A}_n)$.

The group of automorphisms of the set of all affine functions in n variables consists, as it is well known, of mappings of the form (3) with affine permutation π and affine shift g, see, for example, [28]. Note that the set of all affine functions in n variables forms a group isomorphic to $\mathbb{F}_2^{n+1}$. Let the symbol $\ltimes$ stands for the semidirect product, then the result is formulated as follows.

Theorem 15 [39]. $\mathrm{Aut}(\mathcal{B}_n) = \mathrm{GA}(n) \ltimes \mathbb{F}_2^{n+1}$.

These results imply the non-existence of a more general approach to equivalence of bent functions than that on the base of isometric mappings.

6.4. The group of automorphisms of the set of (anti-)self-dual bent functions

In [16], the following problem was pointed.

Open question (Carlet, Danielson, Parker, Solé, 2010): to find mappings preserving self-duality, distinct from the known ones, or give a proof that there are no more.

In [14], this question was resolved within isometric mappings of the set of all Boolean functions in $n \geqslant 4$ variables into itself.

First, there is the problem of how the sets of isometric mapping preserving self-duality and anti-self-duality or, in other words, groups of automorphisms of the sets $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ are related. This problem was solved in [14], where with a use of the orthogonal decomposition (2) and the basis from the Theorem 9 it was proved

Theorem 16 [14]. If $n \geqslant 4$, then $\mathrm{Aut}\left(\mathrm{SB}^+(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^-(n)\right)$.

In [14], the criterion of preserving self-duality was also presented.

Theorem 17 [14]. If $n \geqslant 4$, then isometric mapping $\varphi_{\pi,g}$ belongs to $\mathrm{Aut}\left(\mathrm{SB}^+(n)\right)$ if and only if, for any $x, y \in \mathbb{F}_2^n$, it holds

$$\langle \pi(x), y\rangle \oplus g(x) = \left\langle x, \pi^{-1}(y)\right\rangle \oplus g\left(\pi^{-1}(y)\right).$$

In matrix terms the criterion can be formulated as $A\mathcal{H}_n = \mathcal{H}_n A$, where A is the matrix which represents the mapping $\varphi_{\pi,g}$.

The problem of characterization mappings which preserve self-duality was studied in [16, 17], where it was shown that the mapping (1) preserves self-duality of a bent function, in other words, it is an element of $\mathrm{Aut}\left(\mathrm{SB}^+(n)\right)$. It is obvious that this mapping is isometric and corresponds to $\varphi_{\pi,g} \in \mathcal{I}_n$ with

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

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{F}_2$. The group which consists of mappings of such form is called an *extended orthogonal group* and denoted by $\overline{\mathcal{O}}_n$ [17, 40]. It is known that this group is a subgroup of $\mathrm{GL}\left(n+2, \mathbb{F}_2\right)$ [17].

In paper [14], known results were generalized within isometric mappings from the set $\mathcal{I}_n$ for $n \geqslant 4$. Namely, by using the criterion from Theorem 17 and the matrix representation of isometric mappings (see Section 6.2), it was proved that the desired group of automorphisms coincides with the extended orthogonal group.

Theorem 18 [14]. For $n \geqslant 4$,

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

It follows that the classification of self-dual bent functions in $n \geqslant 4$ variables based on the restricted form of affine equivalence proposed in [16, 17] is the most general isometric mapping of the set of all Boolean functions in n variables into itself.

7. Isometric mappings and duality

In this Section, we discuss results from [14] on characterization of isometric mappings which define bijections between self-dual and anti-self dual bent functions, and description of isometric mappings which preserve or change the sign of the Rayleigh quotient of a Boolean function.

7.1. Isometric bijections between self-dual and anti-self-dual bent functions

It is known [16] 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, this transformation can be represented as

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

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

In [15], it was mentioned that the more general form of this mapping

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

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 $\mathcal{I}_n$.

In [14], these results were generalized within isometric mappings from the set $\mathcal{I}_n$ for $n \geqslant 4$.

The criterion of bijectivity between self-dual and anti-self-dual bent functions was obtained in [14] with a use of the orthogonal decomposition (2) and the basis from the Theorem 9.

Theorem 19 [14]. Let $n \geqslant 4$, then isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ if and only if, for any $x, y \in \mathbb{F}_2^n$, it holds

$$\langle \pi(x), y \rangle \oplus g(x) = \left\langle x, \pi^{-1}(y) \right\rangle \oplus g\left(\pi^{-1}(y)\right) \oplus 1.$$

By using this criterion, in [14] the general form of considered isometric bijections was found.

Theorem 20 [14]. For $n \geqslant 4$, isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ if and only if

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

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

Thus, from Theorems 18 and 20 we can conclude that if we take a mapping from the group $\overline{\mathcal{O}}_n$ and replace the vector $c \in \mathbb{F}_2^n$ by a binary vector of length n with an odd Hamming weight, then we switch the mapping from the "automorphism mode" to the "bijection mode" between the sets $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$.

7.2. Isometric mappings and the Rayleigh quotient

In [16], the *Rayleigh quotient* S_f of a Boolean function $f \in \mathcal{F}_n$ was defined as

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

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

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

In [16], 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. That is, the maximum (minimum) value of the Rayleigh quotient of a Boolean function in an even number of variables is attainable on self-dual (anti-self-dual) bent functions and only them, thus providing a criterion for (anti-)self-duality in terms of the Rayleigh quotient values.

In [40], 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 $N_h = (-1)^{\langle c,c \rangle} N_f$.

The mentioned operations are isometric mappings from $\mathcal{I}_n$. The complete characterization of isometric mappings that preserve the Rayleigh quotient as well as change it was given in [14].

Theorem 21 [14]. If $n \geqslant 4$, then isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ preserves the Rayleigh quotient of every Boolean function in n variables if and only if $\varphi_{\pi,g} \in \mathrm{Aut}\left(\mathrm{SB}^+(n)\right)$.

Theorem 22 [14]. If $n \geqslant 4$, then isometric mapping $\varphi_{\pi,g} \in \mathcal{I}_n$ changes the sign of the Rayleigh quotient of every Boolean function in n variables if and only if it is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$.

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

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

So from Theorem 21 we immediately have that general form of isometric mappings preserving the Hamming distance between every bent function and its dual is described by the extended orthogonal group $\overline{\mathcal{O}}_n$ (see Theorem 2).

8. Conclusion

In this paper, we have given a review of metrical properties of the set of bent functions and its subset of functions which coincide with their duals. The group of automorphisms and metrical complements of these sets are described. We also reviewed some general metrical properties of the set of self-dual bent functions and considered an iterative construction of bent functions. Some relevant open problems and hypothesis on bent functions were discussed.

An interesting question is the characterization of isometric mappings preserving bentness and self-duality, that are beyond the automorphisms of the set of all Boolean functions.

The solution of the problems, that were considered in this review, with regard to different generalizations of bent functions that is study of metrical properties and the duality as well as self-duality in this scope, is a goal worth pursuing.

REFERENCES

1. *Rothaus O. S.* On bent functions. J. Combin. Theory. Ser. A, 1976, vol. 20, no. 3, pp. 300–305.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, Elsevier, 2015. 230 p.
3. *Carlet C. and Mesnager S.* Four decades of research on bent functions. Des. Codes Cryptogr., 2016, vol. 78, no. 1, pp. 5–50.
4. *Mesnager S.* Bent Functions: Fundamentals and Results. Berlin, Springer, 2016. 544 p.

5. *Kolomeec N.* The graph of minimal distances of bent functions and its properties. Des. Codes Cryptogr., 2017, vol. 85, no. 3, pp. 1–16.
6. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices. Finite Fields Appl., 2007, vol. 13, no. 3, pp. 450–491.
7. *Dillon J.* Elementary Hadamard Difference Sets. PhD.dissertation, Univ. Maryland, College Park, 1974.
8. *Carlet C.* Boolean functions for cryptography and error correcting codes. Y. Crama and P. L. Hammer (eds.). Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, Cambridge University Press, 2010, pp. 257–397.
9. *Hou X.-D.* New constructions of bent functions. Proc. Intern. Conf. Combinatorics, Inform. Theory and Statistics. J. Combin. Inform. System Sci., 2000, vol. 25, no. 1–4, pp. 173–189.
10. *Cusick T. W. and Stănică P.* Cryptographic Boolean Functions and Applications. London, Acad. Press, 2017. 288 p.
11. *Tokareva N. N.* On the number of bent functions from iterative constructions: lower bounds. Adv. Math. Commun., 2011, vol. 5, no. 4, pp. 609–621.
12. *Tokareva N. N.* On decomposition of a Boolean function into sum of bent functions. Siberian Electronic Math. Reports, 2014, vol. 11, pp. 745–751.
13. *Tokareva N. N.* O razlozhenii dual'noy bent-funktsii v summu dvukh bent-funktsiy [On decomposition of a dual bent function into sum of two bent functions. Prikladnaya Diskretnaya Matematika, 2014, no. 4(26), pp. 59–61. (in Russian)
14. *Kutsenko A.* The group of automorphisms of the set of self-dual bent functions. Cryptogr. Commun., 2020, vol. 12, no. 5, pp. 881–898.
15. *Hou X.-D.* Classification of self dual quadratic bent functions. Des. Codes Cryptogr., 2012, vol. 63, no. 2, pp. 183–198.
16. *Carlet C., Danielson L. E., Parker M. G., and Solé P.* Self-dual bent functions. Int. J. Inform. Coding Theory, 2010, vol. 1, pp. 384–399.
17. *Feulner T., Sok L., Solé P. and Wassermann A.* Towards the classification of self-dual bent functions in eight variables. Des. Codes Cryptogr., 2013, vol. 68, no. 1, pp. 395–406.
18. *Hyun J. Y., Lee H., and Lee Y.* MacWilliams duality and Gleason-type theorem on self-dual bent functions. Des. Codes Cryptogr., 2012, vol. 63, no. 3, pp. 295–304.
19. *Mesnager S.* Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory, 2014, vol. 60, no. 7, pp. 4397–4407.
20. *Rifà J. and Zinoviev V. A.* On binary quadratic symmetric bent and almost bent functions. 2019, arXiv:1211.5257v3.
21. *Mesnager S.* On constructions of bent functions from involutions. Proc. ISIT, 2016, pp. 110–114.
22. *Coulter R. and Mesnager S.* Bent functions from involutions over $\mathbb{F}_{2^n}$. IEEE Trans. Inf. Theory, 2018, vol. 64, no. 4, pp. 2979–2986.
23. *Luo G., Cao X., and Mesnager S.* Several new classes of self-dual bent functions derived from involutions. Cryptogr. Commun., 2019, vol. 11, no. 6, pp. 1261–1273.
24. *Sok L., Shi M., and Solé. P.* Classification and construction of quaternary self-dual bent functions. Cryptogr. Commun., 2018, vol. 10, no. 2, pp. 277–289.
25. *Kutsenko A.* Metrical properties of self-dual bent functions. Des. Codes Cryptogr., 2020, vol. 88, no. 1, pp. 201–222.
26. *Kutsenko A. V.* The Hamming distance spectrum between self-dual Maiorana-McFarland bent functions. J. Appl. Industr. Math., 2018, vol. 12, no. 1, pp. 112–125.
27. *McFarland R. L.* A family of difference sets in non-cyclic groups. J. Combin. Theory. Ser. A, 1973, vol. 15, no. 1, pp. 1–10.

28. *MacWilliams F. J. and Sloane N. J. A.* The Theory of Error-Correcting Codes. Amsterdam, New York, Oxford, North-Holland, 1983. 782 p.
29. *Canteaut A. and Charpin P.* Decomposing bent functions. IEEE Trans. Inform. Theory, 2003, vol. 49, no. 8, pp. 2004–2019.
30. *Preneel B., Van Leekwijck W., Van Linden L., et al.* Propagation characteristics of Boolean functions. Advances in Cryptology-EUROCRYPT, LNCS, 1990, vol. 473, pp. 161–173.
31. *Climent J.-J., Garcia F. J., and Requena V.* A construction of bent functions of $n+2$ variables from a bent function of n variables and its cyclic shifts. Algebra, 2014, vol. 2014, Article ID 701298. 11 p.
32. *Canteaut A., Daum M., Dobertin H., and Leander G.* Finding nonnormal bent functions. Discrete Appl. Math., 2006, vol. 154, no. 2, pp. 202–218.
33. *Oblaukhov A. K.* Metric complements to subspaces in the Boolean Cube. J. Appl. Industr. Math., 2016, vol. 10, no. 3, pp. 397–403.
34. *Stănică P., Sasao T., and Butler J. T.* Distance duality on some classes of Boolean functions. J. Combin. Math. Combin. Computing, 2018, vol. 107, pp. 181–198.
35. *Oblaukhov A.* A lower bound on the size of the largest metrically regular subset of the Boolean cube. Cryptogr. Commun., 2019, vol. 11, no. 4, pp. 777–791.
36. *Tokareva N.* Duality between bent functions and affine functions. Discrete Math., 2012, vol. 312, no. 3, pp. 666–670.
37. *Markov A. A.* O preobrazovaniyakh, ne rasprostranyayushchikh iskazheniya [On transformations without error propagation]. Selected Works, vol. II: Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Informatics and Related Topics, Moscow, MTsNMO Publ., 2003, pp. 70–93. (in Russian)
38. *Dempwolff U.* Automorphisms and equivalence of bent functions and of difference sets in elementary Abelian 2-groups. Commun. Algebra, 2006, vol. 34, no. 3, pp. 1077–1131.
39. *Tokareva N. N.* The group of automorphisms of the set of bent functions. Discrete Math. Appl., 2010, vol. 20, no. 5–6, pp. 655–664.
40. *Danielsen L. E., Parker M. G., and Solé P.* The Rayleigh quotient of bent functions. LNCS, 2009, vol. 5921, pp. 418–432.