Designs, Codes and Cryptography (2020) 88:201–222
https://doi.org/10.1007/s10623-019-00678-x

Metrical properties of self-dual bent functions

Aleksandr Kutsenko[1]

Received: 8 July 2018 / Revised: 9 September 2019 / Accepted: 11 September 2019 /
Published online: 26 September 2019

Abstract
In this paper we study metrical properties of Boolean bent functions which coincide with their dual bent functions. We propose an iterative construction of self-dual bent functions in $n+2$ variables through concatenation of two self-dual and two anti-self-dual bent functions in n variables. We prove that minimal Hamming distance between self-dual bent functions in n variables is equal to $2^{n/2}$. It is proved that within the set of sign functions of self-dual bent functions in $n \geqslant 4$ variables there exists a basis of the eigenspace of the Sylvester Hadamard matrix attached to the eigenvalue $2^{n/2}$. Based on this result we prove that the sets of self-dual and anti-self-dual bent functions in $n \geqslant 4$ variables are mutually maximally distant. It is proved that the sets of self-dual and anti-self-dual bent functions in n variables are metrically regular sets.

Keywords Boolean functions · Self-dual bent · Iterative construction · Metrical regularity

Mathematics Subject Classification 06E30 · 15B34 · 94C10

1 Introduction

The term "bent function" was introduced by Oscar Rothaus in the 1960s and published in [22]. At the same time the maximally nonlinear Boolean functions were also under study 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, see [25].

Bent functions have applications in many domains, such as error correcting codes, spreading sequences for CDMA and cryptology. In symmetric cryptography, due to maximal nonlinearity, these functions can be used as building blocks of stream (Grain 2004) and

Communicated by C. Carlet.

The author was supported by the Russian Foundation for Basic Research (Projects No. 18-31-00374, 18-07-01394), by the Ministry of Education and Science of the Russian Federation (the 5-100 Excellence Programme and the Project No. 1.12875.2018/12.1), by the program of fundamental scientific researches of the SB RAS No. I.5.1. (Project No. 0314-2016-0017).

✉ Aleksandr Kutsenko
Alexandrkutsenko@bk.ru

[1] Novosibirsk State University, Novosibirsk, Russia

block (CAST 1997) ciphers in order to increase resistance to some statistical methods of cryptanalysis among which linear and differential cryptanalyses are. Nevertheless, bent functions are not balanced and their algebraic degree is at most $n/2$, that entails vulnerability, in particular, to fast algebraic attacks [29].

There are a number of open problems connected with bent functions: in particular, the problems of classification of these functions and search of new constructions. The exact number of bent functions of n variables is unknown if $n > 8$, only lower and upper bounds of this number are available. The problems concerning the metrical properties of bent functions deserve attention including because they are connected with problems related to the cardinality of the class of bent functions. In [13] one can find other results in this area. Extensive information concerning bent functions can be found in the survey [4] and monographies of Mesnager [18] and Tokareva [25].

For each bent function, its dual Boolean function is uniquely defined. The dual function is also a bent function. More information about properties of dual functions is in work [4]. It is known that the mapping which assigns to every bent function its dual function preserves the Hamming distance, hence it is an isometric mapping of the set of bent functions [2]. The isometric mappings of the set of all Boolean functions in n variables into itself that transform bent functions into bent functions were completely studied in [26].

A bent function that coincides with its dual is called self-dual. Open questions which are relevant to the class of bent functions are also relevant for the self-dual bent functions. A difficult problem is the complete characterization and description of the class of self-dual bent functions and estimation of its cardinality. There are a number of articles which are devoted to these and other problems. In particular, in the article [3] Carlet et al. explored 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 relative to an affine transformation which preserves self-duality are given; it has been proved that the Hamming distance between a self-dual bent function and an anti-self-dual bent function in n variables is exactly 2^{n-1}. Also self-dual bent functions obtained by some primary and secondary constructions have been explored. In [10] the classification of all quadratic self-dual bent functions is presented by Hou. Feulner et al. [9] with a help of computers have determined classes of affine equivalence of quadratic and cubic self-dual bent functions in 8 variables with respect to the mentioned above restricted form of affine transformation. Several new constructions of (anti-)self-dual bent functions were proposed in [16,17]. The upper bound for the cardinality of the set of self-dual bent functions which follows from the exact number of formally self-dual bent functions is presented by Hyun and Lee [11]. In [23] Sok et al. discovered a connection between quaternary self-dual bent functions and self-dual bent Boolean functions. The complete Hamming distance spectrum between self-dual Maiorana–McFarland bent functions was obtained in [14].

In the current work we find necessary and sufficient conditions for self-duality of bent functions constructed via iterative construction of Canteaut and Charpin [1] (2003) in a simplified form which was also discovered by Preneel et al. [21] (1990). This construction allows to obtain a bent function in $n+2$ variables through concatenation of four bent functions in n variables provided their duals satisfy the certain condition. We obtain new iterative construction of self-dual bent functions and provide a lower bound for the cardinality of the set of self-dual bent iterative functions. We use the correspondence of self-dual bent functions to eigenvectors of the Sylvester type Hadamard matrix and prove that within the set of sign functions of self-dual bent functions in $n \geqslant 4$ variables there exists a basis of the eigenspace of the Sylvester Hadamard matrix attached to the eigenvalue $2^{n/2}$. Based on this result we prove that sets of self-dual and anti-self-dual bent functions in $n \geqslant 4$ variables are mutually

maximally distant sets and they are metrically regular for any positive even n. We prove that minimal Hamming distance between self-dual bent functions is equal to $2^{n/2}$. We prove that every bent function in $n \leqslant 6$ variables is affinely equivalent to its dual bent function.

The work has the following structure: basic definitions are in the Sect. 2, and in Sect. 3 some known results are listed and new ones are given. Necessary and sufficient conditions for self-duality of bent iterative functions are found (Theorem 1) and it is proved that within the set of sign functions of self-dual bent functions in $n \geqslant 4$ variables there exists a basis of the eigenspace of the Sylvester Hadamard matrix attached to the eigenvalue $2^{n/2}$ (Theorem 2). New construction of iterative self-dual bent functions is proposed (Corollary 1) and a bound is given for the cardinality of the set of iterative self-dual bent functions (Corollary 2). It is proved that there exist self-dual bent functions of any algebraic degree (Proposition 3). In Sect. 4 metrical properties, in particular, minimal Hamming distance is presented (Proposition 4), metrical complements of the sets of self-dual and anti-self-dual bent functions in $n \geqslant 4$ variables (Theorem 3) and metrical regularity of these sets (Theorem 4) are studied. In Sect. 5 we prove that all bent functions in at most 6 variables are affinely equivalent to their dual bent functions (Proposition 7). The conclusion is in Sect. 6.

2 Notation and definitions

Let $\mathbb{F}_2^n$ be the 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 $(f(\mathbf{v}_0), f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^n-1}))$ is called the *truth table* of $f \in \mathcal{F}_n$, where

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

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 $F = \left((-1)^{f(\mathbf{v}_0)}, (-1)^{f(\mathbf{v}_1)}, \ldots, (-1)^{f(\mathbf{v}_{2^n-1})}\right)$ 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 [6]).

Two Boolean functions in n variables are said to be *affinely equivalent* if there exists an affine transform of coordinates and an affine shift that transform one function into another. 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 the cardinality of the set $\left\{x \in \mathbb{F}_2^n : f(x) \oplus g(x) = 1\right\}$. The *degree* $\deg(f)$ of a Boolean function is the maximal degree of monomials which occur in its algebraic normal form (ANF, Zhegalkin polynomial) with nonzero coefficients. For $x, y \in \mathbb{F}_2^n$, we 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 the 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 $\mathcal{B}_n$.

In other words, the function f is bent if and only if for its sign function F it holds $\mathcal{H}_n F \in \{\pm 1\}^{2^n}$. 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 [8].

Some known properties of dual functions (see [2]):

- 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 $f \longrightarrow \widetilde{f}$ which acts on the set of bent functions, preserves the Hamming distance.

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 [10], 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 $H_n^T = H_n$ since H_n is symmetric).

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 [6] for instance), equivalently, a bent function in n variables can be defined as a Boolean function whose sign function, say F, satisfies $\mathcal{H}_n F \in \{\pm 1\}^{2^n}$.

A non-zero vector $v \in \mathbb{C}^n$ is called an *eigenvector* of a complex 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 $\lambda \in \mathbb{C}$ is called the *eigenspace* associated with λ.

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

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

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

From the definition of self-duality it follows that a sign function of any self-dual bent function is the eigenvector of $\mathcal{H}_n$ attached to the eigenvalue 1 (equivalently, the eigenvector of H_n attached to the eigenvalue $2^{n/2}$), 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 $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n}) = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)$.

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

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

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.

3 Characterization of self-dual bent functions

Further we assume that n is an even positive number.

3.1 Some known results

Below we list some known facts which characterize the set of self-dual bent functions and will be used as auxiliary statements throughout the paper.

The next statement shows that there exists a one-to-one correspondence between self-dual and anti-self-dual bent functions.

Proposition 1 ([3], Theorems 5.1, 5.3) *Let n be an even integer and Z be a sign function of some function from $\mathcal{F}_{n-1}$. If $Z + \frac{2H_{n-1}}{2^{n/2}} Z$ is also a sign function of some function from $\mathcal{F}_{n-1}$, then*

- *the vector $\left(Z + \frac{2}{2^{n/2}} H_{n-1} Z, Z\right)$ is the sign function of a self-dual bent function in n variables;*
- *the vector $\left(Z, -Z - \frac{2}{2^{n/2}} H_{n-1} Z\right)$ is the sign function of an anti-self-dual bent function in n variables.*

Moreover sign functions of all self-dual and anti-self-dual bent functions satisfy this decomposition.

Denote, according to [12], the orthogonal group of index n over the field $\mathbb{F}_2$ as

$$\mathcal{O}_n = \left\{ L \in GL(n, 2) | L L^T = I_n \right\},$$

where L^T denotes the transpose of L.

It is known that the following composition of an affine transform of coordinates and an affine shift preserves self-duality of a bent function.

Proposition 2 ([3], Theorem 4.6, [9], Theorem 1) *Let f be a self-dual bent function in n variables. If $L \in \mathcal{O}_n$, $b \in \mathbb{F}_2^n$ with $\mathrm{wt}(b)$ even and $c \in \mathbb{F}_2$ then the function*

$$f(L(x \oplus b)) \oplus \langle b, x \rangle \oplus c$$

is also self-dual bent.

3.2 Bent iterative functions ($\mathcal{BI}$)

In the article [1] the decompositions of bent functions are studied. In particular, the authors have proved that restrictions of a function $f \in \mathcal{B}_n$ to a subspace $V \subseteq \mathbb{F}_2^n$ of codimension 2 and to its cosets are bent if and only if the second derivative of its dual bent function with respect to $V^\perp$ is constant equal to 1. This result can be interpreted as an iterative construction of bent functions. The iterative construction was studied by Tokareva in [27] in a simplified form and a lower bound on its cardinality was introduced.

The necessary and sufficient conditions for the construction of bent function in $n+2$ variables through concatenation of four bent functions in n variables were also found by Preneel et al. [21, Theorem 7, Corollary 2].

Below we present the form of the construction given in [27].

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

$$\begin{aligned} g(00,x) &= f_0(x), \quad g(01,x) = f_1(x),\\ g(10,x) &= f_2(x), \quad g(11,x) = f_3(x), \end{aligned}$$

where $x \in \mathbb{F}_2^n$.

In [27, Theorem 2] (see also [21, Theorem 7, Corollary 2]) it was proved that under condition $f_0, f_1, f_2 \in \mathcal{B}_n$ the function g is bent if and only if $f_3 \in \mathcal{B}_n$ and

$$\widetilde{f_0} \oplus \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3} = 1.$$

Bent functions which are obtained by this construction are called *bent iterative* functions ($\mathcal{BI}$). In the article [5] the comparison of cardinalities of different known iterative constructions of bent functions was presented and the class $\mathcal{BI}$ had the biggest cardinality among them.

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

We will need the following

Lemma 1 *Assume $g \in \mathcal{BI}_{n+2}$ then $g \in \mathrm{SB}^+_{\mathcal{BI}}(n)$ if and only if it holds*

$$\begin{cases} 2\widetilde{f_0} = f_0 + f_1 + f_2 + f_3 - 1,\\ 2\widetilde{f_1} = f_0 - f_1 + f_2 - f_3 + 1,\\ 2\widetilde{f_2} = f_0 + f_1 - f_2 - f_3 + 1,\\ 2\widetilde{f_3} = f_0 - f_1 - f_2 + f_3 + 1. \end{cases}$$

Proof Let F_i be a sign function of the function f_i, $i = 0,1,2,3$. We have $G = (F_0, F_1, F_2, F_3) \in \{\pm 1\}^{2^{n+2}}$. Vector G will be a sign function of self-dual bent function if and only if

$$\begin{aligned} \widetilde{G} = \mathcal{H}_{n+2}G &= \frac{1}{2^{(n+2)/2}} \begin{pmatrix} H_n & H_n & H_n & H_n\\ H_n & -H_n & H_n & -H_n\\ H_n & H_n & -H_n & -H_n\\ H_n & -H_n & -H_n & H_n \end{pmatrix} \begin{pmatrix} F_0\\ F_1\\ F_2\\ F_3 \end{pmatrix}\\ &= \frac{2^{n/2}}{2^{(n+2)/2}} \begin{pmatrix} \widetilde{F_0} + \widetilde{F_1} + \widetilde{F_2} + \widetilde{F_3}\\ \widetilde{F_0} - \widetilde{F_1} + \widetilde{F_2} - \widetilde{F_3}\\ \widetilde{F_0} + \widetilde{F_1} - \widetilde{F_2} - \widetilde{F_3}\\ \widetilde{F_0} - \widetilde{F_1} - \widetilde{F_2} + \widetilde{F_3} \end{pmatrix} = \begin{pmatrix} F_0\\ F_1\\ F_2\\ F_3 \end{pmatrix} = G. \end{aligned}$$

Rewrite this equality by using the fact that for any $f \in \mathcal{F}_n$ and every $x \in \mathbb{F}_2^n$ it is true $(-1)^{f(x)} = 1 - 2f(x)$, the same holds for $\widetilde{F}_i$.

$$\begin{pmatrix} 1-2f_0 \\ 1-2f_1 \\ 1-2f_2 \\ 1-2f_3 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1-2\widetilde{f}_0+1-2\widetilde{f}_1+1-2\widetilde{f}_2+1-2\widetilde{f}_3 \\ 1-2\widetilde{f}_0-1+2\widetilde{f}_1+1-2\widetilde{f}_2-1+2\widetilde{f}_3 \\ 1-2\widetilde{f}_0+1-2\widetilde{f}_1-1+2\widetilde{f}_2-1+2\widetilde{f}_3 \\ 1-2\widetilde{f}_0-1+2\widetilde{f}_1-1+2\widetilde{f}_2+1-2\widetilde{f}_3 \end{pmatrix}$$
$$= \frac{1}{2}\begin{pmatrix} 4-2\widetilde{f}_0-2\widetilde{f}_1-2\widetilde{f}_2-2\widetilde{f}_3 \\ -2\widetilde{f}_0+2\widetilde{f}_1-2\widetilde{f}_2+2\widetilde{f}_3 \\ -2\widetilde{f}_0-2\widetilde{f}_1+2\widetilde{f}_2+2\widetilde{f}_3 \\ -2\widetilde{f}_0+2\widetilde{f}_1+2\widetilde{f}_2-2\widetilde{f}_3 \end{pmatrix} = \begin{pmatrix} 2-\widetilde{f}_0-\widetilde{f}_1-\widetilde{f}_2-\widetilde{f}_3 \\ -\widetilde{f}_0+\widetilde{f}_1-\widetilde{f}_2+\widetilde{f}_3 \\ -\widetilde{f}_0-\widetilde{f}_1+\widetilde{f}_2+\widetilde{f}_3 \\ -\widetilde{f}_0+\widetilde{f}_1+\widetilde{f}_2-\widetilde{f}_3 \end{pmatrix}.$$

In this case we have

$$2\begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{pmatrix} = \begin{pmatrix} \widetilde{f}_0+\widetilde{f}_1+\widetilde{f}_2+\widetilde{f}_3-2 \\ \widetilde{f}_0-\widetilde{f}_1+\widetilde{f}_2-\widetilde{f}_3 \\ \widetilde{f}_0+\widetilde{f}_1-\widetilde{f}_2-\widetilde{f}_3 \\ \widetilde{f}_0-\widetilde{f}_1-\widetilde{f}_2+\widetilde{f}_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = H_2\begin{pmatrix} \widetilde{f}_0 \\ \widetilde{f}_1 \\ \widetilde{f}_2 \\ \widetilde{f}_3 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Then

$$2H_2\begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{pmatrix} = H_2H_2\begin{pmatrix} \widetilde{f}_0 \\ \widetilde{f}_1 \\ \widetilde{f}_2 \\ \widetilde{f}_3 \end{pmatrix} + H_2\begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 4\begin{pmatrix} \widetilde{f}_0 \\ \widetilde{f}_1 \\ \widetilde{f}_2 \\ \widetilde{f}_3 \end{pmatrix} + \begin{pmatrix} 2 \\ -2 \\ -2 \\ -2 \end{pmatrix}.$$

It is equal to the condition

$$2\begin{pmatrix} \widetilde{f}_0 \\ \widetilde{f}_1 \\ \widetilde{f}_2 \\ \widetilde{f}_3 \end{pmatrix} = \begin{pmatrix} f_0+f_1+f_2+f_3 \\ f_0-f_1+f_2-f_3 \\ f_0+f_1-f_2-f_3 \\ f_0-f_1-f_2+f_3 \end{pmatrix} + \begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

□

By Proposition 1 for sign functions F_0, F_1, F_2, F_3 we have

$$\begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = \begin{pmatrix} F_2 \\ F_3 \end{pmatrix} + \frac{2}{2^{n/2}}H_{n-1}\begin{pmatrix} F_2 \\ F_3 \end{pmatrix} = \begin{pmatrix} F_2 \\ F_3 \end{pmatrix} + \frac{2}{2^{n/2}}\begin{pmatrix} H_{n-2} & H_{n-2} \\ H_{n-2} & -H_{n-2} \end{pmatrix}\begin{pmatrix} F_2 \\ F_3 \end{pmatrix}$$
$$= \begin{pmatrix} F_2 \\ F_3 \end{pmatrix} + \begin{pmatrix} \mathcal{H}_{n-2} & \mathcal{H}_{n-2} \\ \mathcal{H}_{n-2} & -\mathcal{H}_{n-2} \end{pmatrix}\begin{pmatrix} F_2 \\ F_3 \end{pmatrix} = \begin{pmatrix} F_2+\widetilde{F}_2+\widetilde{F}_3 \\ F_3+\widetilde{F}_2-\widetilde{F}_3 \end{pmatrix},$$

so we obtain two equalities which follow from the system above.

At the same time

$$\begin{pmatrix} \mathcal{H}_{n-2}F_0 \\ \mathcal{H}_{n-2}F_1 \end{pmatrix} = \begin{pmatrix} \widetilde{F}_0 \\ \widetilde{F}_1 \end{pmatrix} = \begin{pmatrix} \widetilde{F}_2+F_2+F_3 \\ \widetilde{F}_3+F_2-F_3 \end{pmatrix},$$

and we obtain two equalities which are derived from the system of equalities

$$2\begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \end{pmatrix} = \begin{pmatrix} \widetilde{F}_0+\widetilde{F}_1+\widetilde{F}_2+\widetilde{F}_3 \\ \widetilde{F}_0-\widetilde{F}_1+\widetilde{F}_2-\widetilde{F}_3 \\ \widetilde{F}_0+\widetilde{F}_1-\widetilde{F}_2-\widetilde{F}_3 \\ \widetilde{F}_0-\widetilde{F}_1-\widetilde{F}_2+\widetilde{F}_3 \end{pmatrix}$$

in the proof of Lemma 1.

Thus the decomposition model from Proposition 1 is considered in Lemma 1.

Theorem 1 *Let $g \in \mathcal{BI}_{n+2}$, then $g \in \mathrm{SB}^{+}_{\mathcal{BI}}(n)$ if and only if there exists such pair of functions $g_1, g_2 \in \mathcal{B}_n$ and a function $h \in \mathcal{F}_n$ that:*

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

Remark 1 It can be proved that the function h is uniquely defined by a pair of bent functions g_1, g_2: $h = g_1 \oplus \widetilde{g}_1 \oplus g_2 \oplus \widetilde{g}_2$.

Proof By the previous lemma we have

$$\begin{cases}
2\widetilde{f}_0 = f_0 + f_1 + f_2 + f_3 - 1,\\
2\widetilde{f}_1 = f_0 - f_1 + f_2 - f_3 + 1,\\
2\widetilde{f}_2 = f_0 + f_1 - f_2 - f_3 + 1,\\
2\widetilde{f}_3 = f_0 - f_1 - f_2 + f_3 + 1.
\end{cases}$$

Denote $h = f_1 \oplus f_2$, i.e. $f_1 = f_2 + h - 2f_2h$, then

$$\begin{cases}
2\widetilde{f}_0 = f_0 + f_2 + h - 2f_2h + f_2 + f_3 - 1,\\
2\widetilde{f}_1 = f_0 - f_2 - h + 2f_2h + f_2 - f_3 + 1,\\
2\widetilde{f}_2 = f_0 + f_2 + h - 2f_2h - f_2 - f_3 + 1,\\
2\widetilde{f}_3 = f_0 - f_2 - h + 2f_2h - f_2 + f_3 + 1.
\end{cases}$$

and hence,

$$\begin{cases}
2\widetilde{f}_0 = f_0 + 2f_2 + h - 2f_2h + f_3 - 1,\\
2\widetilde{f}_1 = f_0 - h + 2f_2h - f_3 + 1,\\
2\widetilde{f}_2 = f_0 + h - 2f_2h - f_3 + 1,\\
2\widetilde{f}_3 = f_0 - 2f_2 - h + 2f_2h + f_3 + 1.
\end{cases}$$

Consider these equalities with respect to the function h:

– for any $x \in \mathbb{F}_2^n$ such that $h(x) = 0$ we have

$$\begin{cases}
2\widetilde{f}_0 = f_0 + 2f_2 + f_3 - 1,\\
2\widetilde{f}_1 = f_0 - f_3 + 1,\\
2\widetilde{f}_2 = f_0 - f_3 + 1,\\
2\widetilde{f}_3 = f_0 - 2f_2 + f_3 + 1,
\end{cases}$$

i.e., in this case it holds

$$f_0 = f_3 \oplus 1, \quad f_2 = \widetilde{f}_0, \quad \widetilde{f}_3 = \widetilde{f}_0 \oplus 1,$$

– for any $x \in \mathbb{F}_2^n$ such that $h(x) = 1$ we have

$$\begin{cases}
2\widetilde{f}_0 = f_0 + f_3,\\
2\widetilde{f}_1 = f_0 + 2f_2 - f_3,\\
2\widetilde{f}_2 = f_0 - 2f_2 - f_3 + 2,\\
2\widetilde{f}_3 = f_0 + f_3.
\end{cases}$$

i.e., in this case it holds

$$f_0 = f_3, \quad f_2 = \widetilde{f}_1, \quad \widetilde{f}_2 = f_2 \oplus 1.$$

Investigation of these constraints yields

$$\begin{aligned} f_3 &= hf_0 \oplus (h \oplus 1)(f_0 \oplus 1) = f_0 \oplus h \oplus 1, \\ f_2 &= h\left(\widetilde{f}_2 \oplus 1\right) \oplus (h \oplus 1)\widetilde{f}_0 = h\left(\widetilde{f}_2 \oplus \widetilde{f}_0\right) \oplus \widetilde{f}_0 \oplus h, \\ f_1 &= f_2 \oplus h = h\left(\widetilde{f}_2 \oplus \widetilde{f}_0\right) \oplus \widetilde{f}_0. \end{aligned}$$

Rewrite these expressions in $\mathbb{R}$

$$\begin{aligned} f_3 &= 1 - f_0 - h + 2hf_0, \\ f_2 &= \widetilde{f}_0 - h\widetilde{f}_0 - h\widetilde{f}_2 + h, \\ f_1 &= \widetilde{f}_0 - h\widetilde{f}_0 + h\widetilde{f}_2 \end{aligned}$$

and substitute to the initial system:

$$\begin{cases} 2\widetilde{f}_0 = f_0 + \left(\widetilde{f}_0 - h\widetilde{f}_0 + h\widetilde{f}_2\right) + \left(\widetilde{f}_0 - h\widetilde{f}_0 - h\widetilde{f}_2 + h\right) + (1 - f_0 - h + 2hf_0) - 1, \\ 2\widetilde{f}_1 = f_0 - \left(\widetilde{f}_0 - h\widetilde{f}_0 + h\widetilde{f}_2\right) + \left(\widetilde{f}_0 - h\widetilde{f}_0 - h\widetilde{f}_2 + h\right) - (1 - f_0 - h + 2hf_0) + 1, \\ 2\widetilde{f}_2 = f_0 + \left(\widetilde{f}_0 - h\widetilde{f}_0 + h\widetilde{f}_2\right) - \left(\widetilde{f}_0 - h\widetilde{f}_0 - h\widetilde{f}_2 + h\right) - (1 - f_0 - h + 2hf_0) + 1, \\ 2\widetilde{f}_3 = f_0 - \left(\widetilde{f}_0 - h\widetilde{f}_0 + h\widetilde{f}_2\right) - \left(\widetilde{f}_0 - h\widetilde{f}_0 - h\widetilde{f}_2 + h\right) + (1 - f_0 - h + 2hf_0) + 1. \end{cases}$$

Then we obtain

$$\begin{cases} h\widetilde{f}_0 = hf_0, \\ \widetilde{f}_1 = f_0 + h - h\widetilde{f}_2 - hf_0, \\ \widetilde{f}_2 = f_0 - hf_0 + h\widetilde{f}_2, \\ \widetilde{f}_3 = 1 - \widetilde{f}_0 - h + 2h\widetilde{f}_0. \end{cases}$$

and therefore

$$\begin{cases} h\widetilde{f}_0 = hf_0, \\ \widetilde{f}_1 = h\left(\widetilde{f}_2 \oplus 1\right) \oplus (h \oplus 1)f_0, \\ \widetilde{f}_2(h \oplus 1) = f_0(h \oplus 1), \\ \widetilde{f}_3 = \widetilde{f}_0 \oplus h \oplus 1. \end{cases}$$

Rewrite the third equality in the form:

$$f_0 = hf_0 \oplus \widetilde{f}_2(h \oplus 1) = h\widetilde{f}_2 \oplus \widetilde{f}_2 \oplus h\widetilde{f}_0.$$

Then the second equality will be

$$\begin{aligned} \widetilde{f}_1 &= h\left(\widetilde{f}_2 \oplus 1\right) \oplus (h \oplus 1)f_0 = h\left(\widetilde{f}_2 \oplus 1\right) \oplus (h \oplus 1)\left(h\widetilde{f}_2 \oplus \widetilde{f}_2 \oplus h\widetilde{f}_0\right) \\ &= h\widetilde{f}_2 \oplus h \oplus h\widetilde{f}_2 \oplus h\widetilde{f}_2 \oplus h\widetilde{f}_0 \oplus h\widetilde{f}_2 \oplus \widetilde{f}_2 \oplus h\widetilde{f}_0 = \widetilde{f}_2 \oplus h. \end{aligned}$$

Denote $g_1 = \widetilde{f}_2$ and $g_2 = \widetilde{f}_0$ then the result follows. □

Corollary 1 *Functions*

$$\begin{aligned} f(y_1, y_2, x) &= (y_1 \oplus y_2)\left(f(x) \oplus \widetilde{f}(x)\right) \oplus f(x) \oplus y_1y_2, \\ f'(y_1, y_2, x) &= (y_1 \oplus y_2)(\varphi(x) \oplus \omega(x)) \oplus \varphi(x) \oplus \alpha_1y_1 \oplus \alpha_2y_2 \oplus y_1y_2, \end{aligned}$$

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.

Proof We obtain the first one for the case $g_1 \oplus \widetilde{g}_1 = g_2 \oplus \widetilde{g}_2$ and hence, $h = 0$. Then a sign function is equal to $(G_1, G_2, G_2, -G_1)$, where G_1 and G_2 are sign functions of functions g_1 and g_2 respectively. The second construction occurs when $g_1 \oplus \widetilde{g}_1 = g_2 \oplus \widetilde{g}_2 \oplus 1$, and therefore $h = 1$. In this case a sign function is equal to $(G_2, G_1, -G_1, G_2)$. Also conditions $\widetilde{g}_2 = g_2 \oplus 1$ and $\widetilde{g}_1 = g_1$ hold. □

Remark 2 The first construction from those listed above (for f) was presented in [3] as an example of the construction which uses the indirect sum of bent functions, see [4]. It is worth noting that the second construction (for f') can also be obtained from indirect sum of bent functions.

Corollary 2 *It holds*

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

Proof Constructions of self-dual functions mentioned in Corollary 1 form two disjoint sets of self-dual bent functions (see the proof of Corollary 1), hence

$$\left|\mathrm{SB}^+_{\mathcal{BI}}(n)\right| \geqslant |\mathcal{B}_{n-2}| + \left|\mathrm{SB}^+(n-2)\right| \cdot \left|\mathrm{SB}^-(n-2)\right|,$$

but since by Proposition 1 there exists the correspondence between self-dual and anti-self-dual bent function, the mentioned lower bound follows.

The upper bound follows from Proposition 1 or the notion that the function h is uniquely defined by the functions g_1, g_2. □

3.3 Algebraic degree

Bent functions in $2k$ variables which have a representation

$$f(x, y) = \langle x, \pi(y)\rangle \oplus g(y),$$

where $x, y \in \mathbb{F}_2^k$, $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and g is a Boolean function in k variables, form the *Maiorana–McFarland* class of bent functions, denoted by $\mathcal{M}_{2k}$. A dual of a Maiorana–McFarland bent function $f(x, y)$ is equal to

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

(Carlet [2]).

From this construction it is clear that if $n \geqslant 4$ then for any number $d \in \{2, 3, \ldots, n/2\}$ there exists a bent function in n variables of degree d. We will prove that this statement holds within self-dual bent functions.

Proposition 3 *For any even $n \geqslant 4$ and number $d \in \{2, 3, \ldots, n/2\}$ there exists a self-dual bent function in n variables of degree d.*

Proof The statement is obvious for $d = 2$ because

$$f(x) = \bigoplus_{i=1}^{n/2} x_{2i-1}x_{2i}, \quad x \in \mathbb{F}_2^n,$$

is a quadratic self-dual bent function for any even n.

Assume $d \geqslant 3$. Denote $k = (n-2)/2$. Consider the function $f \in \mathcal{M}_{2k}$:

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

where the mapping $\pi(y) = (\pi_1(y), \pi_2(y), \ldots, \pi_k(y))$ has the following coordinate functions: for any $y \in \mathbb{F}_2^k$

$$\pi_{d-1}(y) = y_{d-1} \oplus \prod_{j=1}^{d-2} y_j,$$
$$\pi_i(y) = y_i, \quad i \in \{1, 2, \ldots, k\} \setminus \{d-1\}.$$

All non-trivial component functions of π are balanced hence it is indeed a permutation. Moreover it is clear that $\pi = \pi^{-1}$.

Thus we have

$$f(x, y) = \bigoplus_{i=1}^{k} x_i y_i \oplus x_{d-1} \prod_{j=1}^{d-2} y_j, \quad x, y \in \mathbb{F}_2^k,$$
$$\widetilde{f}(x, y) = \bigoplus_{i=1}^{k} x_i y_i \oplus y_{d-1} \prod_{j=1}^{d-2} x_j, \quad x, y \in \mathbb{F}_2^k,$$

then

$$f(x, y) \oplus \widetilde{f}(x, y) = x_{d-1} \prod_{i=1}^{d-2} y_i \oplus y_{d-1} \prod_{j=1}^{d-2} x_j, \quad x, y \in \mathbb{F}_2^k.$$

Consider a Boolean function g in $2k+2$ variables:

$$\begin{aligned} g(u, v, x, y) &= (u \oplus v)\left(f(x, y) \oplus \widetilde{f}(x, y)\right) \oplus f(x, y) \oplus uv \\ &= (u \oplus v)\left(x_{d-1} \prod_{i=1}^{d-2} y_i \oplus y_{d-1} \prod_{j=1}^{d-2} x_j\right) \oplus \left(\bigoplus_{i=1}^{k} x_i y_i \oplus x_{d-1} \prod_{j=1}^{d-2} y_j\right) \oplus uv, \end{aligned}$$

where $u, v \in \mathbb{F}_2$, $x, y \in \mathbb{F}_2^k$. This function has algebraic degree d and by Corollary 1 it is self-dual. □

3.4 Dimension of linear span of the set of sign functions of (anti-)self-dual bent functions

It is known that

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

where $\dim(V)$ is the dimension of the subspace $V \subseteq \mathbb{R}^{2^n}$. Moreover, since the matrix $\mathcal{H}_n$ is symmetric, it holds that the subspaces $\mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)$ and $\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)$ are mutually orthogonal.

Recall a linear algebra lemma from [3]

Lemma 2 ([3], Lemma 5.2) *The spectrum of $\mathcal{H}_n$ consists of the eigenvalues* 1 *and* (-1) *and each of them has the same multiplicity* 2^{n-1}. *A basis of the eigenspace corresponding to* 1 *is formed from the rows of the matrix* $\left(H_{n-1} + 2^{n/2} I_{2^{n-1}},\ H_{n-1}\right)$. *An orthogonal decomposition of* $\mathbb{R}^{2^n}$ *in eigenspaces of* H_n *is*

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

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

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.

The next result shows that for $n \geqslant 4$ it is possible to find 2^{n-1} (anti-)self-dual bent functions in n variables with linearly independent sign functions. Since the dimension of $\mathrm{Ker}\,(\mathcal{H}_n \pm I_{2^n})$ is equal to 2^{n-1}, the found subset will be an example of the basis of the subspace $\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$.

Theorem 2 *The linear span of sign functions of (anti-)self-dual bent functions in* $n \geqslant 4$ *variables has dimension* 2^{n-1}.

Proof Notice that if the statement holds for self-dual bent functions it also holds for anti-self-dual bent functions by the correspondence between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$.

We are to find a subset of 2^{n-1} self-dual bent functions in n variables with linearly independent sign functions. The proof will be led by the induction.

Base of induction: For $n = 4$ we have 10 self-dual bent functions having value 0 on the vector $(0, 0, 0, 0) \in \mathbb{F}_2^4$ and 10 their negations. Sign functions of the first 8 of them (according to the lexicographical order of their vectors of values) yield a matrix

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\
1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\
1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

which has a rank equal to $8 = 2^{n-1}$.

Induction step: Let the statement hold for any even $n \in [4, n_0]$ for some $n_0 \geqslant 4$. Assume that $n = n_0 + 2$. Then by induction assumption we have $2^{(n-2)-1} = 2^{n-3}$ self-dual bent functions $f_1^{n-2}, f_2^{n-2}, \ldots, f_{2^{n-3}}^{n-2}$ in $n - 2$ variables with linearly independent sign functions $F_1^{n-2}, F_2^{n-2}, \ldots, F_{2^{n-3}}^{n-2}$ respectively. By using the correspondence between self-dual and anti-self-dual bent functions we can obtain 2^{n-3} anti-self-dual bent functions $g_1^{n-2}, g_2^{n-2}, \ldots, g_{2^{n-3}}^{n-2}$ in $n - 2$ variables with linearly independent sign functions $G_1^{n-2}, G_2^{n-2}, \ldots, G_{2^{n-3}}^{n-2}$ respectively.

Now recall iterative constructions of self-dual bent functions from the Corollary 1. Let F and G be sign functions of any self-dual and anti-self-dual bent functions in $n - 2$ variables respectively, then the following sign functions

$$\begin{aligned}\mathbf{F} &= (F, F, F, -F),\\ \mathbf{G} &= (G, -G, -G, -G),\\ \mathbf{FG} &= (F, -G, G, F),\end{aligned}$$

will be sign functions of self-dual bent functions in n variables. By using first two constructions applied to the mentioned sets of self-dual and anti-self-dual bent functions we obtain 2^{n-3} sign functions of self-dual bent functions of the form

$$\mathbf{F}_i^n = \left(F_i^{n-2}, F_i^{n-2}, F_i^{n-2}, -F_i^{n-2}\right),$$

and 2^{n-3} ones of the form

$$\mathbf{G}_j^n = \left(G_j^{n-2}, -G_j^{n-2}, -G_j^{n-2}, -G_j^{n-2}\right),$$

where $i, j = 1, 2, \ldots, 2^{n-3}$. Note that sets $S_{\mathbf{F}} = \left\{\mathbf{F}_i^n\right\}_{i=1}^{2^{n-3}}$ and $S_{\mathbf{G}} = \left\{\mathbf{G}_i^n\right\}_{i=1}^{2^{n-3}}$ both consist of linearly independent vectors by the choice of the base functions, moreover for any pair we have

$$\langle \mathbf{F}, \mathbf{G}\rangle = \langle F, G\rangle - \langle F, G\rangle - \langle F, G\rangle + \langle F, G\rangle = 0,$$

therefore linear spans of the sets $S_{\mathbf{F}}$ and $S_{\mathbf{G}}$ intersect only in zero element of $\mathbb{R}^{2^n}$, that is $(S_{\mathbf{F}} \cup S_{\mathbf{G}})$ consists of $2^{n-3} + 2^{n-3} = 2^{n-2}$ linearly independent vectors.

Use the third construction and consider 2^{n-2} self-dual bent functions in n variables with sign functions

$$\begin{aligned}(\mathbf{FG})_1^n &= \left(F_1^{n-2}, -G_1^{n-2}, G_1^{n-2}, F_1^{n-2}\right),\\ (\mathbf{FG})_2^n &= \left(F_2^{n-2}, -G_1^{n-2}, G_1^{n-2}, F_2^{n-2}\right),\\ &\vdots\\ (\mathbf{FG})_{2^{n-3}}^n &= \left(F_{2^{n-3}}^{n-2}, -G_1^{n-2}, G_1^{n-2}, F_{2^{n-3}}^{n-2}\right),\\ (\mathbf{FG})_{2^{n-3}+1}^n &= \left(F, -G_1^{n-2}, G_1^{n-2}, F\right),\\ (\mathbf{FG})_{2^{n-3}+2}^n &= \left(F_{2^{n-3}}^{n-2}, -G_2^{n-2}, G_2^{n-2}, F_{2^{n-3}}^{n-2}\right),\\ (\mathbf{FG})_{2^{n-3}+3}^n &= \left(F_{2^{n-3}}^{n-2}, -G_3^{n-2}, G_3^{n-2}, F_{2^{n-3}}^{n-2}\right),\\ &\vdots\\ (\mathbf{FG})_{2^{n-2}}^n &= \left(F_{2^{n-3}}^{n-2}, -G_{2^{n-3}}^{n-2}, G_{2^{n-3}}^{n-2}, F_{2^{n-3}}^{n-2}\right),\end{aligned}$$

where $F = \beta_1 F_1^{n-2} + \beta_2 F_2^{n-2} + \cdots + \beta_{2^{n-3}} F_{2^{n-3}}^{n-2}$ for some $\beta \in \mathbb{R}^{2^{n-3}}$ such that $\sum\limits_{i=1}^{2^{n-3}} \beta_i \neq 1$, e.g. $\beta_1 = -1$ and $\beta_2 = \beta_3 = \cdots = \beta_{2^{n-3}} = 0$.

Now prove that these vectors are linearly independent. Assume that there exists such non-trivial $\lambda \in \mathbb{R}^{2^{n-2}}$ that

$$\sum_{i=1}^{2^{n-2}} \lambda_i \, (\mathbf{FG})_i^n = \mathbf{0} \in \mathbb{R}^{2^n}.$$

It is easy to see that coefficients $\lambda_{2^{n-3}+2}, \lambda_{2^{n-3}+3}, \ldots, \lambda_{2^{n-2}}$ must be equal to zero by linear independence of $S_{\mathbf{G}}$. Then if $\lambda_{2^{n-3}+1} = 0$ we must put zeros for the rest of the coefficients by linear independence of $S_{\mathbf{F}}$, that implies a contradiction with non-triviality of $\lambda \in \mathbb{R}^{2^{n-2}}$. So, $\lambda_{2^{n-3}+1} \neq 0$ and we have

$$\sum_{i=1}^{2^{n-3}} \lambda_i F_i^{n-2} + \lambda_{2^{n-3}+1} F = \sum_{i=1}^{2^{n-3}} \lambda_i F_i^{n-2} + \lambda_{2^{n-3}+1} \left(\sum_{i=1}^{2^{n-3}} \beta_i F_i^{n-2} \right) = \mathbf{0} \in \mathbb{R}^{2^{n-2}},$$

therefore

$$\lambda_i = -\lambda_{2^{n-3}+1} \beta_i,$$

for $i = 1, 2, \ldots, 2^{n-3}$. But then

$$\sum_{i=1}^{2^{n-3}} \lambda_i G_1^{n-2} + \lambda_{2^{n-3}+1} G_1^{n-2} = -\sum_{i=1}^{2^{n-3}} \lambda_{2^{n-3}+1} \beta_i G_1^{n-2} + \lambda_{2^{n-3}+1} G_1^{n-2}$$
$$= \lambda_{2^{n-3}+1} \left(1 - \sum_{i=1}^{2^{n-3}} \beta_i \right) G_1^{n-2} = \mathbf{0} \in \mathbb{R}^{2^{n-2}},$$

that does not hold for $\sum_{i=1}^{2^{n-3}} \beta_i \neq 1$ since $\lambda_{2^{n-3}+1} \neq 0$ and $\left|\left| G_1^{n-2} \right|\right| > 0$.

Thus the set $S_{\mathbf{FG}} = \left\{ (\mathbf{FG})_i^n \right\}_{i=1}^{2^{n-2}}$ consists of 2^{n-2} linearly independent vectors. It remains to note that

$$\langle \mathbf{AB}, \mathbf{F} \rangle = \langle A, F \rangle - \langle B, F \rangle + \langle B, F \rangle - \langle A, F \rangle = 0,$$
$$\langle \mathbf{AB}, \mathbf{G} \rangle = \langle A, G \rangle + \langle B, G \rangle - \langle B, G \rangle - \langle A, G \rangle = 0,$$

that is linear spans of the sets $S_{\mathbf{F}} \cup S_{\mathbf{G}}$ and $S_{\mathbf{FG}}$ intersect only in the zero element of $\mathbb{R}^{2^n}$, hence the set $(S_{\mathbf{F}} \cup S_{\mathbf{G}} \cup S_{\mathbf{FG}})$ consists of $2^{n-3} + 2^{n-3} + 2^{n-2} = 2^{n-1}$ linearly independent vectors. □

Corollary 3 *Let* $f \in \left(\mathrm{SB}^+(n) \cup \mathrm{SB}^-(n) \right)$ *and* $F = (F_0, F_1, F_2, F_3) \in \{\pm 1\}^{2^n}$ *be its sign function, where* $F_0, F_1, F_2, F_3 \in \{\pm 1\}^{2^{n-2}}$. *Then*

$$\langle F_0, F_1 \rangle + \langle F_2, F_3 \rangle = 0,$$
$$\langle F_0, F_2 \rangle + \langle F_1, F_3 \rangle = 0.$$

Proof Assume that $f \in \mathrm{SB}^+(n)$. Then there exist such $\alpha, \beta \in \mathbb{R}^{2^{n-3}}$ and $\gamma \in \mathbb{R}^{2^{n-2}}$ that

$$F = \sum_{i=1}^{2^{n-3}} \alpha_i \mathbf{F}_i^n + \sum_{j=1}^{2^{n-3}} \beta_j \mathbf{G}_j^n + \sum_{k=1}^{2^{n-2}} \gamma_k (\mathbf{FG})_k^n,$$

where sets $S_{\mathbf{F}} = \left\{ \mathbf{F}_i^n \right\}_{i=1}^{2^{n-3}}$, $S_{\mathbf{G}} = \left\{ \mathbf{G}_j^n \right\}_{j=1}^{2^{n-3}}$ and $S_{\mathbf{FG}} = \left\{ (\mathbf{FG})_k^n \right\}_{k=1}^{2^{n-2}}$ are defined as in the proof of the Theorem 2. It is enough to notice that the mentioned above relations hold for every function from the set $(S_{\mathbf{F}} \cup S_{\mathbf{G}} \cup S_{\mathbf{FG}})$.

The case $f \in \mathrm{SB}^-(n)$ follows from the correspondence between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$.

□

4 Metrical properties

In the following section we study minimal Hamming distance between (anti-)self-dual bent functions and investigate metrical complements of the sets of self-dual and anti-self-dual bent functions.

4.1 Minimal Hamming distance

It is known in [13] that the minimal Hamming distance between distinct bent functions is equal $2^{n/2}$. We prove that this bound is tight both for self-dual and anti-self-dual bent functions.

Proposition 4 *Let $n \geqslant 4$, then the minimal Hamming distance between distinct self-dual bent functions in n variables is equal to $2^{n/2}$.*

Proof For $n = 4$ consider two functions from $\mathrm{SB}^+(n)$:

$$f_4(x) = x_1x_2 \oplus x_3x_4, \quad g_4(x) = f_4(Ax) = x_1x_4 \oplus x_2x_3,$$

where

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

It is clear that

$$f_4(x) \oplus g_4(x) = (x_1 \oplus x_3)(x_2 \oplus x_4),$$

hence, $\mathrm{dist}(f_4, g_4) = 4 = 2^{n/2}$.

For every even $n \geqslant 6$ construct a pair of self-dual bent functions $f_n, g_n \in \mathrm{SB}^+(n)$ with sign functions

$$F_n = (F_{n-2}, -R_{n-2}, R_{n-2}, F_{n-2}),$$

and

$$G_n = (G_{n-2}, -R_{n-2}, R_{n-2}, G_{n-2}),$$

respectively, where F_{n-2} and G_{n-2} are sign functions of bent functions $f_{n-2} \in \mathrm{SB}^+(n-2)$ and $g_{n-2} \in \mathrm{SB}^+(n-2)$.

The vector R_{2m} is a sign function of anti-self-dual bent function $r \in \mathrm{SB}^-(2m)$:

$$r(x) = \bigoplus_{i=1}^{m} x_{2i-1}x_{2i} \oplus x_{2m-1} \oplus x_{2m}, \quad x \in \mathbb{F}_2^{2m}.$$

Thus we have

$$\begin{aligned} \mathrm{dist}(f_n, g_n) &= 2 \cdot \mathrm{dist}(f_{n-2}, g_{n-2}) = 2^2 \cdot \mathrm{dist}(f_{n-4}, g_{n-4}) = \cdots \\ &= 2^k \cdot \mathrm{dist}(f_{n-2k}, g_{n-2k}) = \cdots = 2^{(n-4)/2} \cdot \mathrm{dist}(f_4, g_4) = 2^{n/2}. \end{aligned}$$

□

Corollary 4 *For $n \geqslant 4$ the minimal Hamming distance between distinct anti-self-dual bent functions in n variables is equal to $2^{n/2}$.*

Proof The result follows by using the correspondence between self-dual and anti-self-dual bent functions (Proposition 1). □

4.2 Metrical complement and regularity

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* [19] of the set X and denoted by $\widehat{X}$. A set X is said to be *metrically regular* if $\widehat{\widehat{X}} = X$. Define, following Tokareva, a subset of Boolean functions to be *metrically regular* if the set of corresponding vectors of values is metrically regular [25].

Example 1 In [28] it was proved that affine function can be defined as a Boolean function that is at the maximal possible distance from the set of all bent functions. Since bent functions are precisely such functions that are maximally distant from affine functions, it can be concluded that sets of affine functions and bent functions in n variables are metrically regular.

Sets of functions which have maximum distance from partition set functions were studied in [24], it was shown that partition set functions defined by some partition are mutually maximally distant sets.

The Hamming distance between self-dual and anti-self-dual bent functions is characterized by the following statement.

Proposition 5 ([3], Proposition 3.2) *The Hamming distance between any pair of bent functions f, g, where $f \in \mathrm{SB}^+(n)$ and $g \in \mathrm{SB}^-(n)$, is equal 2^{n-1}.*

Since for any $f \in \mathrm{SB}^+(n)$ its negation $f \oplus 1$ is also a self-dual bent function by Proposition 2, the covering radius of $\mathrm{SB}^+(n)$ is at most 2^{n-1} and from the Proposition 5 it follows that the covering radius of $\mathrm{SB}^+(n)$ is exactly 2^{n-1}.

In the following theorem we investigate Boolean functions which are maximally distant from the the sets $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$, thus obtaining a metrical complement of the set of (anti-)self-dual bent functions.

Theorem 3 *Let $n \geqslant 4$, then the following statements hold:*

- *The metrical complement of the set of self-dual bent functions is the set of anti-self-dual bent functions;*
- *The metrical complement of the set of anti-self-dual bent functions is the set of self-dual bent functions.*

Proof From Proposition 5 it follows the inclusion

$$\mathrm{SB}^-(n) \subseteq \widehat{\mathrm{SB}^+(n)}. \tag{1}$$

By Theorem 2 among sign functions of self-dual bent functions in n variables there exists a subset of 2^{n-1} linearly independent vectors. Denote these vectors by $F_1^+, F_2^+, \ldots, F_{2^{n-1}}^+$ and corresponding self-dual bent functions in n variables by $f_1^+, f_2^+, \ldots, f_{2^{n-1}}^+$.

Now let $f \in \mathcal{F}_n$ be an arbitrary function from $\widehat{\mathrm{SB}^+(n)}$, i.e. such one, that $\mathrm{dist}\left(f, \mathrm{SB}^+(n)\right) = 2^{n-1}$, from which it follows that $\mathrm{dist}(f, g) = 2^{n-1}$ for any $g \in \mathrm{SB}^+(n)$. By using Lemma 2 consider the decomposition for the sign function F of f, $F = F^+ + F^-$, where $F^\pm \in \mathrm{Ker}\,(\mathcal{H}_n \mp I_{2^n})$, see also [7]. The vectors F^+ and F^- are orthogonal since they correspond to distinct eigenvalues of the real symmetric matrix $\mathcal{H}_n$. Then it holds $\langle F, F\rangle = \langle F^+, F^+\rangle + \langle F^-, F^-\rangle$. Since $F^+ \in \mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$, for some $\alpha \in \mathbb{R}^{2^{n-1}}$ we have $F^+ = \sum_{i=1}^{2^{n-1}} \alpha_i F_i^+$. Then we obtain

$$\langle F, F\rangle = \left\langle F, \sum_{i=1}^{2^{n-1}} \alpha_i F_i^+ \right\rangle + \left\langle F, F^-\right\rangle = \sum_{i=1}^{2^{n-1}} \alpha_i \underbrace{\left\langle F, F_i^+\right\rangle}_{=0} + \left\langle F, F^-\right\rangle$$
$$= \left\langle F, F^-\right\rangle = \left\langle F^+ + F^-, F^-\right\rangle = \left\langle F^-, F^-\right\rangle,$$

therefore $\left\langle F^+, F^+\right\rangle = 0$ that is F^+ is a zero vector. Then $F = F^- \in \mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$ and immediately $f \in \mathrm{SB}^-(n)$.

Thus we have an inclusion

$$\widehat{\mathrm{SB}^+(n)} \subseteq \mathrm{SB}^-(n). \tag{2}$$

Both inclusions 1 and 2 yield the result

$$\widehat{\mathrm{SB}^+(n)} = \mathrm{SB}^-(n).$$

The second statement of the Theorem follows from the correspondence between self-dual and anti-self-dual bent functions (Proposition 1). □

For $n = 2$ the Boolean function $x_1x_2 \oplus x_1$ is at the distance $2 = 2^{n-1}$ from the set $\mathrm{SB}^+(2)$ but it is not an anti-self-dual bent, hence $\mathrm{SB}^-(2) \subset \widehat{\mathrm{SB}^+(2)}$ that is $\widehat{\mathrm{SB}^+(2)} \neq \mathrm{SB}^-(2)$. It is clear that $\widehat{\mathrm{SB}^-(2)} \neq \mathrm{SB}^+(2)$ as well. Then $\mathrm{SB}^+(2)$ and $\mathrm{SB}^-(2)$ are not metrical complements of each other.

Theorem 4 *The sets* $\mathrm{SB}^+(n)$, $\mathrm{SB}^-(n)$ *are metrically regular sets, both with covering radius* 2^{n-1}.

Proof For the case $n = 2$ denote

$$M = \{x_1x_2 \oplus x_1, x_1x_2 \oplus x_2, x_1x_2 \oplus x_1 \oplus 1, x_1x_2 \oplus x_2 \oplus 1\} \subset \mathcal{F}_2.$$

Recall that

$$\mathrm{SB}^+(2) = \{x_1x_2, x_1x_2 \oplus 1\}$$

and

$$\mathrm{SB}^-(2) = \{x_1x_2 \oplus x_1 \oplus x_2, x_1x_2 \oplus x_1 \oplus x_2 \oplus 1\}.$$

Obviously, we have

$$\mathrm{dist}\left(\mathrm{SB}^+(2), M\right) = \mathrm{dist}\left(\mathrm{SB}^-(2), M\right) = 2 = 2^{n-1},$$
$$\widehat{M} = \mathrm{SB}^+(2) \cup \mathrm{SB}^-(2).$$

It holds

$$\widehat{\mathrm{SB}^+(2)} = M \cup \mathrm{SB}^-(2),$$

Metrical complement of the set $M \cup \mathrm{SB}^-(2)$ coincides with $\mathrm{SB}^+(2)$, therefore $\mathrm{SB}^+(2)$ is a metrically regular set.

Furthermore, it holds

$$\widehat{\mathrm{SB}^-(2)} = M \cup \mathrm{SB}^+(2),$$

Metrical complement of the set $M \cup \mathrm{SB}^+(2)$ coincides with $\mathrm{SB}^-(2)$, hence $\mathrm{SB}^-(2)$ is a metrically regular set as well.

The case $n \geqslant 4$ follows from the Theorem 3. □

Let $X \subseteq \mathbb{F}_2^n$ be a metrically regular set with covering radius r. Then, according to [20], sets $X, \hat{X}$ are said to be *strongly metrically regular*, if for any $y \in \mathbb{F}_2^n$ it holds

$$\mathrm{dist}\,(y, X) + \mathrm{dist}\left(y, \hat{X}\right) = r.$$

Define, as before, a pair of sets of Boolean functions to be a pair of *strongly metrically regular* sets if the sets of corresponding vectors of values are strongly metrically regular.

Proposition 6 *For $n \geqslant 4$ the sets $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ are not strongly metrically regular.*

Proof Consider the linear function $f(x) \equiv 0$. It holds

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

hence

$$\mathrm{dist}\left(f, \mathrm{SB}^+(n)\right) + \mathrm{dist}\left(f, \mathrm{SB}^-(n)\right) = 2^n - 2^{n/2} > 2^{n-1}$$

for $n > 2$. □

4.3 Bounds on the Hamming distance from self-dual bent functions

In this section we study bounds on the maximal Hamming distance from the sets $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$ that is

$$\max_{f \in \mathcal{F}_n \setminus \mathrm{SB}^-(n)} \mathrm{dist}\left(f, \mathrm{SB}^+(n)\right)$$

and

$$\max_{f \in \mathcal{F}_n \setminus \mathrm{SB}^+(n)} \mathrm{dist}\left(f, \mathrm{SB}^-(n)\right).$$

Lemma 3 *A function $f \in \mathcal{B}_n$ is (anti-)self-dual if and only if for any constant $y \in \mathbb{F}_2^n$ and for the function $F_y \in \mathcal{F}_n$, defined as*

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

it holds $\mathrm{wt}\left(F_y\right) = 2^{n-1} - 2^{n/2-1}$ $\left(2^{n-1} + 2^{n/2-1}\right.$ *respectively*$\left.\right)$.

Proof Let $f \in \mathrm{SB}^+(n)$. Then for any $y \in \mathbb{F}_2^n$ we have

$$\begin{aligned}(-1)^{f(y)} 2^{n/2} &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x, y \rangle \oplus f(x) \oplus f(y) \oplus f(y)} \\ &= (-1)^{f(y)} \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle x, y \rangle \oplus f(x) \oplus f(y)} = (-1)^{f(y)} \sum_{x \in \mathbb{F}_2^n} (-1)^{F_y(x)}.\end{aligned}$$

Hence wt $\left(F_y\right) = 2^{n-1} - 2^{n/2-1}$, where $F_y(x) = f(x) \oplus \langle x, y\rangle \oplus f(y)$.

Now assume that wt $\left(F_y\right) = 2^{n-1} - 2^{n/2-1}$ for any $y \in \mathbb{F}_2^n$.

$$\sum_{y\in\mathbb{F}_2^n} (-1)^{f(y)\oplus\widetilde{f}(y)} = 2^{-n/2} \sum_{y\in\mathbb{F}_2^n} W_f(y)(-1)^{f(y)}$$

$$= 2^{-n/2} \sum_{y\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{F_y(x)} \right) = 2^{-n/2} \sum_{y\in\mathbb{F}_2^n} 2^{n/2} = 2^n.$$

Thus $f \in \mathrm{SB}^+(n)$. The proof for anti-self-dual case is similar and is omitted. □

Theorem 5 *It holds*

$$\max_{f\in\mathcal{F}_n\setminus\mathrm{SB}^-(n)} \mathrm{dist}\left(f, \mathrm{SB}^+(n)\right) \geqslant 2^{n-1} - 2^{n/2-1} + 1.$$

Proof Consider the function

$$f(x) = (x_1 \oplus 1)(x_2 \oplus 1) \cdot \cdots \cdot (x_n \oplus 1), \ x \in \mathbb{F}_2^n.$$

Its vector of values is equal to $(1, 0, 0, \ldots, 0) \in \mathbb{F}_2^{2^n}$. Let $g \in \mathrm{SB}^+(n)$, then by Lemma 3 the Hamming weight of a function $g(x) \oplus g(\mathbf{v}_0)$, $x \in \mathbb{F}_2^n$, is equal to $2^{n-1} - 2^{n/2-1}$. That is $\mathrm{wt}(g) = 2^{n-1} - (-1)^{g(\mathbf{v}_0)} 2^{n/2-1}$.

Thus for any $g \in \mathrm{SB}^+(n)$ such that $g(\mathbf{v}_0) = 0$ it holds

$$\mathrm{dist}(f, g) = 2^{n-1} - 2^{n/2-1} + 1,$$

and for any $g \in \mathrm{SB}^+(n)$ such that $g(\mathbf{v}_0) = 1$ it holds

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

As a result we have

$$\mathrm{dist}\left(f, \mathrm{SB}^+(n)\right) = \min_{g\in\mathrm{SB}^+(n)} \mathrm{dist}(f, g) =$$

$$= \min(2^{n-1} - 2^{n/2-1} + 1, 2^{n-1} + 2^{n/2-1} - 1) = 2^{n-1} - 2^{n/2-1} + 1.$$

□

Corollary 5

$$\max_{f\in\mathcal{F}_n\setminus\mathrm{SB}^+(n)} \mathrm{dist}\left(f, \mathrm{SB}^-(n)\right) \geqslant 2^{n-1} - 2^{n/2-1} + 1.$$

Proof The statement follows from the correspondence between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$. □

5 Affine equivalence of bent function in small number of variables and its dual

In this section we state some connections between known isometric mappings of the set of bent functions in the case of small number of variables.

Let $\varphi : A \to \mathcal{F}_n$, where $A \subseteq \mathcal{F}_n$.

A mapping φ is said to be *isometric* mapping of the set $A \subseteq \mathcal{F}_n$ if it preserves the Hamming distance between functions from the set A, that is for any $f, g \in A$ it holds

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

It is known [26] that every isometric mapping of the set of all Boolean functions to itself that transforms the set of bent functions to itself is a combination of an affine transformation of coordinates and a shift by an affine function. The mapping $f \to \widetilde{f}$ defined on the set of bent functions, preserves the Hamming distance [2] that is it is an isometric mapping of the set $\mathcal{B}_n$.

Langevin et al. in [15] mentioned that the problem of checking the equivalence of bent function and its dual is not a trivial one. The general problem of determining whether two Boolean functions are equivalent or inequivalent was arisen by Dillon in [8].

We study the problem for small number of variables.

Proposition 7 *Any bent function in at most* 6 *variables is affinely equivalent to its dual bent function.*

Proof For each of cases $n = 2, 4$ there exists only one class of affine equivalence with representative x_1x_2 and $x_1x_2 \oplus x_3x_4$ respectively, that is every bent function in 2 and 4 variables is affinely equivalent to its dual.

In the case $n = 6$ there are four classes $C_i, i = 1, 2, 3, 4$, of affine equivalence with the following representatives [22]:

$$f_1(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6,$$
$$f_2(x) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6,$$
$$f_3(x) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5,$$
$$f_4(x) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6,$$

where $x \in \mathbb{F}_2^6$.

Assume that in some class of affine equivalence, say C, there exists a bent function f' which is affinely equivalent to its dual bent function. Every bent function f from this class is affinely equivalent to the bent function f', then bent functions $\widetilde{f}$ and $\widetilde{f'}$ are also affinely equivalent since affine equivalence of two bent functions implies affine equivalence of their duals. In this case $\widetilde{f}$ also belongs to the class C, therefore every bent function from the class C is affinely equivalent to its dual bent function.

Thus it is enough to show that in every equivalence class of bent functions in 6 variables there exists a bent function which is affinely equivalent to its dual bent function.

1. The function $f_1(x) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6$ is self-dual bent [3, Table 3];
2. Consider the binary matrix

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

and Maiorana–McFarland bent function

$$\begin{aligned} f(x) &= f_2(Ax) = \langle (x_1, x_2, x_3), (x_4, x_5, x_6) \rangle \oplus x_4x_5x_6 \\ &= \langle (x_1, x_2, x_3), \pi(x_4, x_5, x_6) \rangle \oplus g(x_4, x_5, x_6), \end{aligned}$$

where $\pi : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ is the identity permutation and $g(y) = y_1y_2y_3$ for any $y \in \mathbb{F}_2^3$. By using the form of the dual to the bent function from the Maiorana–McFarland class we obtain

$$\widetilde{f}(x) = \left\langle \pi^{-1}(x_1, x_2, x_3), (x_4, x_5, x_6) \right\rangle \oplus g\left(\pi^{-1}(x_1, x_2, x_3)\right)$$
$$= x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_1x_2x_3 = f_2(x);$$

3. Consider the binary matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad c = (0, 1, 0, 0, 0, 0) \in \mathbb{F}_2^6$$

and the function

$$f(x) = f_3(Ax) \oplus \langle c, x \rangle = x_4(x_1 \oplus x_2)x_3 \oplus (x_1 \oplus x_2)x_6x_5 \oplus x_4(x_1 \oplus x_2) \oplus$$
$$\oplus x_4x_6 \oplus (x_1 \oplus x_2)(x_2 \oplus x_4) \oplus x_3x_5 \oplus x_6x_5 \oplus x_2$$
$$= (x_1 \oplus x_2)x_3x_4 \oplus (x_1 \oplus x_2)x_5x_6 \oplus x_1x_4 \oplus$$
$$x_2x_4 \oplus x_4x_6 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_2 \oplus x_2x_4 \oplus x_3x_5 \oplus x_6x_5 \oplus x_2$$
$$= (x_1 \oplus x_2)x_3x_4 \oplus (x_1 \oplus x_2)x_5x_6 \oplus x_1x_2 \oplus x_3x_5 \oplus x_4x_6 \oplus x_5x_6.$$

This bent function is a self-dual bent [3, Table 3].

4. Suppose that in the class C_4 there exists a bent function f which is not affinely equivalent to $\widetilde{f}$, it means that $\widetilde{f} \in C_1 \cup C_2 \cup C_3$. But in this case, due to the previous considerations, it holds $\widetilde{\widetilde{f}} = f \in C_1 \cup C_2 \cup C_3$. Since $C_4 \cap (C_1 \cup C_2 \cup C_3) = \emptyset$, there is a contradiction. Hence every bent function f from the class C_4 is affinely equivalent to its dual bent function $\widetilde{f}$. □

In fact, the graph whose vertices correspond to classes of affine equivalence of bent functions in n variables and an edge between two vertices v and v', which correspond to affine equivalence classes C and C' respectively, exists if and only if for any $f \in C$ it holds $\widetilde{f} \in C'$. It is clear that this graph has the following properties:

- There are isolated vertices, for instance that ones which include self-dual or anti-self-dual bent functions;
- The rest of the vertices have degree 1, thus the corresponding edges form a matching.

6 Conclusion

In this work we study metrical properties of bent functions which coincide with their duals and bent functions which coincide with negations of their duals namely minimal Hamming distance and metrical regularity of the sets of self-dual and anti-self-dual bent functions.

It is interesting to continue the study of iterative self-dual bent functions and obtain new constructions in addition to those mentioned in Corollary 1.

References

1. Canteaut A., Charpin P.: Decomposing bent functions. IEEE Trans. Inf. Theory **49**(8), 2004–2019 (2003).
2. 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, pp. 257–397. Cambridge University Press, Cambridge (2010).

3. Carlet C., Danielson L.E., Parker M.G., Solé P.: Self-dual bent functions. Int. J. Inform. Coding Theory **1**, 384–399 (2010).
4. Carlet C., Mesnager S.: Four decades of research on bent functions. J. Des. Codes Cryptogr. **78**(1), 5–50 (2016).
5. Climent J.-J., Garcia F.J., Requena V.: A construction of bent functions of $n + 2$ variables from a bent function of n variables and its cyclic shifts. Algebra. https://doi.org/10.1155/2014/701298 (2014).
6. Cusick T.W., Stănică P.: Cryptographic Boolean Functions and Applications. Academic Press, London (2017).
7. Danielsen L.E., Parker M.G., Solé P.: The Rayleigh Quotient of Bent Functions. Springer Lecture Notes in Computer Science, vol. 5921, pp. 418–432. Springer, Berlin (2009).
8. Dillon J.: Elementary Hadamard difference sets. PhD. dissertation, Univ. Maryland, College Park (1974).
9. 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).
10. Hou X.-D.: Classification of self dual quadratic bent functions. Des. Codes Cryptogr. **63**(2), 183–198 (2012).
11. 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).
12. Janusz G.J.: Parametrization of self-dual codes by orthogonal matrices. Finite Fields Appl. **13**(3), 450–491 (2007).
13. Kolomeec N.A.: The graph of minimal distances of bent functions and its properties. Des. Codes Cryptogr. **85**(3), 1–16 (2017).
14. Kutsenko A.V.: The Hamming distance spectrum between self-dual Maiorana–McFarland bent functions. J. Appl. Ind. Math. **12**(1), 112–125 (2018).
15. Langevin P., Leander G., McGuire G.: Kasami bent function are not equivalent to their duals. Finite Fields Appl. **461**, 187–197 (2008).
16. Luo G., Cao X., Mesnager S.: Several new classes of self-dual bent functions derived from involutions. Cryptogr. Commun. https://doi.org/10.1007/s12095-019-00371-9 (2019).
17. Mesnager S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inf. Theory **60**(7), 4397–4407 (2014).
18. Mesnager S.: Bent Functions: Fundamentals and Results, p. 544. Springer, Berlin (2016).
19. Oblaukhov A.K.: Metric complements to subspaces in the Boolean cube. J. Appl. Ind. Math. **10**(3), 397–403 (2016).
20. Oblaukhov A.K.: A lower bound on the size of the largest metrically regular subset of the Boolean cube. Cryptogr. Commun. **11**(4), 777–791 (2019).
21. Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandewalle J.: Propagation characteristics of Boolean functions. In: Advances in Cryptology-EUROCRYPT. Lecture Notes in Computer Science, vol. 473, pp. 161–173. Springer, Berlin (1990).
22. Rothaus O.S.: On bent functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976).
23. Sok L., Shi M., Solé P.: Classification and construction of quaternary self-dual bent functions. Cryptogr. Commun. **10**(2), 277–289 (2017).
24. Stănică P., Sasao T., Butler J.T.: Distance duality on some classes of Boolean functions. J. Comb. Math. Comb. Comput. **107**, 181–198 (2018).
25. Tokareva N.: Bent Functions, Results and Applications to Cryptography. Academic Press, London (2015).
26. Tokareva N.N.: The group of automorphisms of the set of bent functions. Discret. Math. Appl. **20**(5), 655–664 (2010).
27. Tokareva N.N.: On the number of bent functions from iterative constructions: lower bounds and hypotheses. Adv. Math. Commun. **5**(4), 609–621 (2011).
28. Tokareva N.: Duality between bent functions and affine functions. Discret. Math. **312**, 666–670 (2012).
29. Wang Q., Johansson T.: A note on fast algebraic attacks and higher order nonlinearities. In: International Conference on Information Security and Cryptology, Inscrypt 2010, pp. 404–414 (2010).