Designs, Codes and Cryptography (2024) 92:113–144
https://doi.org/10.1007/s10623-023-01298-2

Decomposing self-dual bent functions

Aleksandr Kutsenko[1,2]

Received: 28 August 2022 / Revised: 24 August 2023 / Accepted: 26 August 2023 /
Published online: 30 September 2023

Abstract

Bent functions are Boolean functions in even number of variables that have maximal nonlinearity. They have flat Walsh–Hadamard spectrum and are of interest for their applications in algebra, coding theory and cryptography. A bent function is called self-dual if it coincides with its dual bent function. In current work we study the decomposition of the form $\left(f_0, f_1, \ldots, f_{2^k-1}\right)$ of the vector of values of a self-dual bent function, formed by the concatenation of 2^k Boolean functions f_j in $n-k$ variables. We treat the cases $k = 1, 2$. Based on a spectral characterization, we introduce a notion of *self-dual near-bent function* in odd number of variables and prove that there exists a one-to-one correspondence between the notions of self-duality for even and odd number of variables. As a result the characterization for the decomposition (f_0, f_1) is obtained. For the decomposition $f = (f_0, f_1, f_2, f_3)$ we prove that if sign vectors of subfunctions f_j are linearly dependent, then all these subfunctions are bent. We prove that for $n \geq 6$ the converse does not hold, that is the obtained condition is sufficient only. These results are also generalized for the case of an arbitrary bent function. Three new iterative constructions of self-dual bent functions are proposed. One of them allows to build a class of self-dual bent functions which cannot be decomposed into the concatenation of four bent functions. Based on the constructions a new iterative lower bound on the cardinality of the set of self-dual bent functions is obtained.

Keywords Self-dual bent · Rayleigh quotient · Near-bent · Bent-decomposition · Gram matrix

Mathematics Subject Classification 06E30 · 94D10

Communicated by G. Kyureghyan.

✉ Aleksandr Kutsenko
alexandrkutsenko@bk.ru

[1] Sobolev Institute of Mathematics SB RAS, 4 Acad. Koptyug avenue, Novosibirsk, Russia 630090

[2] Novosibirsk State University, 1 Pirogova str., Novosibirsk, Russia 630090

1 Introduction

Bent functions are Boolean functions in even number of variables that have maximal nonlinearity. They were studied in 60th of the previous century in the USA and USSR (see the report [12] and thesis [13] of Dillon, while the research in the Soviet Union was mentioned in historical sections of [24, 41]) and firstly published by Rothaus in [35]. They are mathematical objects of a great interest due to many applications in discrete mathematics, algebra, coding theory, cryptography. Having a property of maximal nonlinearity these functions can be used for obtaining Boolean and vectorial Boolean functions with good cryptographic properties. Another applications use the fact that bent functions and only them have flat Walsh–Hadamard spectrum that is crucial for some approaches within the signals theory, including CDMA technology. More information about them one can find in monographies [29, 41] and survey [7]. For extensive data about cryptographic properties of Boolean functions and other their applications one can refer to the books [6, 10]. Despite the long history of study there are many open problems related to bent functions, in particular, their cardinality is still unknown, their affine classification is completely studied only for small number of variables, obtaining of new constructions is also the goal worth pursuing.

For every bent function it is possible to define its dual Boolean function that defines the signs of its Walsh–Hadamard transform. This function is also bent and, in turn, its dual coincides with the initial function, so bent functions come in pairs. The duality mapping has a great interest in a scope of bent functions since it is the only known isometric mapping of the set of bent functions that is not an element of its group of automorphisms [5]. More information about the duals and the properties of the duality mapping one can find in [7].

Among different classes of bent functions the class of self-dual bent functions is emphasized. Essentially, self-dual are precisely such bent functions that coincide with their duals. They are also important from the perspective of obtaining polyphase sequences (sign vectors for Boolean case) with particular properties. Note that the polyphase sequence of self-dual bent function is the eigenvector of the Sylvester Hadamard matrix that appears in many areas of discrete mathematics and also in quantum computation. So the construction and characterization of self-dual bent functions has strong relation with the problem of description of eigenvectors of the Sylvester–Hadamard matrix, which is a long-standing problem of independent interest from linear algebra [15, 43]. Also self-dual bent functions are the fixed points of the duality mapping. Note that on self-dual bent functions and only on them the Rayleigh quotient of a Boolean function has maximal value for the case of even number of variables.

The notion of *dual* and *anti-dual* (precisely self-dual and anti-self-dual) bent functions in terms of sign vectors was initially considered by Preneel et al. [33], whereas more general definition of a self-dual bent function on a finite group was intriduced by Logachev, Sal'nikov and Yashchenko in [26]. The first deep study of self-dual Boolean bent function was made by Carlet et al. in paper [8], where several constructions and properties were obtained. From that time there appeared a number of papers devoted to the study and characterization of self-dual bent functions. In particular, the classification of quadratic self-dual bent functions was provided by Hou in [18]. The classification of qubic self-dual bent functions in 8 variables was done in paper [14], while the bounds for the cardinality of this class were deduced in [19]. A number of combinatorial and algebraic constructions one can find in [25, 27, 31, 34, 38]. Some combinatorial questions and open problems related to anti-self-dual bent functions were considered and solved in [39]. Metrical properties of self-dual bent functions were studied in papers [20–23]. Self-dual bent sequences, having connection with sign vectors of self-dual bent functions, were recently studied in [36, 37].

In current work we study the decompositions of vector of values of self-dual bent functions in n variables of the form $\left(f_0, f_1, \ldots, f_{2^k-1}\right)$, where f_j are Boolean functions in $n-k$ variables. These functions are subfunctions obtained by fixing first k variables. We consider the cases $k=1,2$. The properties of such subfunctions and some relations comprising them are treated. Note that the best known for today lower and upper bounds on the cardinality of the set of self-dual bent functions are based on the analysis of such decompositions. For details, these decompositions were considered in papers [8] (case $k=1$) from the perspective of generating all self-dual bent functions and [21] (case $k=2$) for the conditions when all f_j are bent.

The structure of the work is following. Necessary notation is given in Sect. 2. In Sect. 3 we introduce the concept of self-duality on near-bent functions in odd number of variables and prove that there is a one-to-one correspondence between self-dual bent function in n variables and near-bent functions in $n-1$ variables having particular value of the Rayleigh quotient (Theorem 1). Note that this value coincides with the best known for today bound for the maximal value of the Rayleigh quotient for the case of odd number of variables. Further, in Sect. 4.2 we study the Gram matrix obtained via sign vectors of subfunctions obtained by fixing two variables of bent function. The general form of this matrix is deduced (Theorem 6). We use it for obtaining metrical relations between subfunctions of every bent function (Corollary 1). The Rayleigh quotients of subfunctions are characterized in Sect. 4.3 and their general form is obtained (Proposition 2). The form of the Gram matrix is explicitly used in Sect. 4.4, where we prove that given a self-dual bent function with linearly dependent sign vectors of subfunctions, all these functions are neccesarily bent (Theorem 3, Corollary 2). The converse of Theorem 3 is considered in Sect. 5. New constructions and a lower bound on the number of self-dual bent functions are presented in Sect. 6. In Sect. 7 we study the properties of the Gram matrix of decomposition for the general case, taking an arbitrary bent function. The Conclusion is in Sect. 8.

2 Notation

Let $\mathbb{F}_2^n$ be a set of binary vectors of length n. For $x, y \in \mathbb{F}_2^n$ denote $\langle x, y\rangle = \bigoplus_{i=1}^{n} x_i y_i$, where sign $\oplus$ denotes a sum modulo 2.

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 $\mathcal{F}_n$. A *sign* vector (also known as polyphase vector or $\{\pm 1\}$-sequence) of $f \in \mathcal{F}_n$ is an integer vector $\left((-1)^{f_0}, (-1)^{f_1}, \ldots, (-1)^{f_{2^n-1}}\right)$ of length 2^n, where $(f_0, f_1, \ldots, f_{2^n-1})$ is a vector of values (truth table) of the function f. Any Boolean function in n variables can be uniquely represented via the multivariate polynomial over $\mathbb{F}_2$:

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

where $a_z \in \mathbb{F}_2$ for all $z \in \mathbb{F}_2^n$. Here we use the agreement $0^0 = 1$. This representation is called the *algebraic normal form* (ANF) of the Boolean function f. The *degree* $\deg(f)$ of the function f is the maximal degree (number of terms) of the monimial from its algebraic normal form that has nonzero coefficient. If $\deg(f) \leq 1$, the function is called *affine*. If $\deg(f) = 2$, the function is said to be *quadratic*.

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 distance* $\mathrm{dist}(f, g)$ between Boolean functions f, g in n variables is the cardinality of the set $\left\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\right\}$.

The Walsh–Hadamard transform of the function $f \in \mathcal{F}_n$ is the integer function

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

For this functions the *Parseval's identity* holds

$$\sum_{y \in \mathbb{F}_2^n} W_f^2(y) = 2^{2n}.$$

A Boolean function f in an odd number m of variables is said to be *near-bent* if

$$W_f(y) \in \left\{0, \pm 2^{(m+1)/2}\right\}, \quad y \in \mathbb{F}_2^m.$$

For the case of an even number of variables, say n, the function f in n variables is said to be *near-bent* if

$$W_f(y) \in \left\{0, \pm 2^{(n+2)/2}\right\}, \quad y \in \mathbb{F}_2^n.$$

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

$$\left|W_f(y)\right| = 2^{n/2}, \quad y \in \mathbb{F}_2^n.$$

The set of bent functions in n variables is denoted by $\mathcal{B}_n$. The Boolean function $\widetilde{f} \in \mathcal{F}_n$ such that $W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}$ for any $y \in \mathbb{F}_2^n$ is said to be *dual* of f. Note that the dual function is uniquely defined for every bent function, moreover the function $\widetilde{f}$ is bent as well. A bent function f is said to be *self-dual* if $f = \widetilde{f}$, and *anti-self-dual* if $f = \widetilde{f} \oplus 1$. The set of self-dual bent functions in n variables is denoted by $\mathcal{SB}_n^+$.

The *Rayleigh quotient* of a Boolean function in n variables is a number

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

This spectral characteristics of a Boolean function in a scope of bent functions were studied in [11]. It is interesting for bent functions since it completely characterizes the Hamming distance between the function and its dual. Indeed, for any bent function f it holds

$$S_f = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)} W_f(y) = 2^{n/2} \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y) \oplus \widetilde{f}(y)} = 2^{3n/2} - 2^{n/2+1} \mathrm{dist}\left(f, \widetilde{f}\right).$$

For a Boolean function f in n variables we call the number

$$\mathcal{S}_f = \frac{S_f}{2^{n/2}}$$

the *sub-normalized Rayleigh quotient*.

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

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

This matrix is known as the *Sylvester–Hadamard matrix*. It is known the Hadamard property of this matrix

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

where H_n^{T} is transpose of H_n (it holds $H_n^{\mathrm{T}} = H_n$ by symmetricity of H_n). Denote by $\mathcal{H}_n = 2^{-n/2} H_n$ its normalized version.

The matrix H_n describes the Walsh–Hadamard transform in matrix form. More precisely, it is known that the rows (columns) of this matrix are sign vectors of all linear Boolean functions in n variables $\langle a, x\rangle$, $a \in \mathbb{F}_2^n$, given in lexicographical order of vectors a, see [10]. Then the Walsh–Hadamard transform at the point $y \in \mathbb{F}_2^n$ is just the inner product of sign vector of the linear function $\langle y, x\rangle$, $x \in \mathbb{F}_2^n$, and sign vector F of the function f. Thus, the vector whose coordinates are Walsh–Hadamard coefficients is simply $H_n F$. So in terms of sign vectors the Rayleigh quotient of the function f has the expression

$$S_f = \langle F, H_n F\rangle,$$

where F is its sign vector.

For a real $d \times d$ matrix A a nonzero vector $v \in \mathbb{R}^d$ is called an *eigenvector* of A if $Av = \lambda v$ for some $\lambda \in \mathbb{C}$. This number is called the *eigenvalue* of A, associated with v.

It is clear that sign vectors if self-dual bent functions are eigenvectors of the normalized Sylvester–Hadamard matrix that correspond to the eigenvalue 1. At the same time sign vectors of anti-self-dual bent functions are eigenvectors of the normalized Sylvester–Hadamard matrix that correspond to the eigenvalue (-1).

3 Decomposition of the form (f_0, f_1)

In this section we study the decomposition for the case $k = 1$, that is consider the subfunctions of self-dual bent functions that are obtained by fixing the first variable. It is known that for any bent function in n variables such subfunctions are near-bent functions in $n-1$ variables with disjoint Walsh–Hadamard spectrum (see [42], for example).

In [8] and [14] the subfunctions in $n-1$ variables were used in the algorithms for the enumeration of all self-dual bent functions of prescribed algebraic degree. These algorithms explicitly exploit the fact that the vector (Y, Z), where $Y, Z \in \{\pm 1\}^{2^{n-1}}$, is the sign vector of some self-dual bent function in n variables if and only if

$$Y = Z + \frac{2H_{n-1}}{2^{n/2}} Z. \tag{1}$$

Regarding spectral characterization it is known [8] that for any Boolean function, say f, in even number n of variables it holds

$$\left|S_f\right| \le 2^{3n/2}$$

with equality if and only if f is either self-dual $\left(+2^{3n/2}\right)$ or anti-self-dual $\left(-2^{3n/2}\right)$ bent. It follows that extremal values are achieved if and only if

$$(-1)^{f(y)} W_f(y) = 2^{n/2} \text{ for any } y \in \mathbb{F}_2^n$$

or

$$(-1)^{f(y)} W_f(y) = -2^{n/2} \text{ for any } y \in \mathbb{F}_2^n.$$

Table 1 Multiplicities of Walsh–Hadamard coefficients of a near-bent function g

Value	Size
0	2^{m-1}
$2^{(m+1)/2}$	$2^{m-2} + (-1)^{g(\mathbf{0})} 2^{(m-3)/2}$
$-2^{(m+1)/2}$	$2^{m-2} - (-1)^{g(\mathbf{0})} 2^{(m-3)/2}$

Accordingly, only self-dual and anti-self-dual bent functions possess these conditions for the case of an even number of variables.

3.1 Self-duality for near-bent functions

Let $m \geq 3$ be an odd integer. In current paper we introduce the notions of self-duality and anti-self-duality for near-bent functions in odd number of variables that are based on the spectral characterization. We are to call a near-bent function g in m variables *self-dual* if

$$(-1)^{g(y)} W_g(y) \geq 0 \text{ for any } y \in \mathbb{F}_2^m.$$

In order, g is called an *anti-self-dual* near-bent if

$$(-1)^{g(y)} W_g(y) \leq 0 \text{ for any } y \in \mathbb{F}_2^m.$$

Finding the exact maximal (minimal) value of the Rayleigh quotient of a Boolean function in an odd number m of variables is an open problem. It is caused by the fact that for odd m there are no eigenvectors of the Sylvester Hadamard matrix H_m, with coordinates having the same absolute value. It is known that, as was shown in [8], it holds

$$\max_{f \in \mathcal{F}_m} \left| S_f \right| \geq 2^{(3m-1)/2}.$$

For this bound the authors used the concatenation of two self-dual bent functions in $m-1$ variables, so the obtained value was called the *bent-concatenation bound*. Nevertheless the experiments have shown that this bound is not tight, at least for small values of m.

Self-dual near-bent functions, proposed in current paper, are extremal objects within the set of near-bent functions in odd number of variables in a spectral sense, as we show in the following statement

Proposition 1 *Let g be a near-bent function in m variables, then*

$$|S_g| \leq 2^{(3m-1)/2}$$

with equality if and only if f is either self-dual or anti-self-dual near-bent.

Proof By definition of the Rayleigh quotient we have

$$S_g = \sum_{y \in \mathbb{F}_2^m} (-1)^{g(y)} W_g(y). \tag{2}$$

The multiplicities of Walsh coefficients of any near-bent function in m variables are well known (see [30], for example), we list them in Table 1.

Consider two nonnegative integers a_1, a_2, describing the signs of nonzero terms in the sum (2):

$$a_1 = \left|\left\{y \in \mathbb{F}_2^m : (-1)^{g(y)} W_g(y) > 0\right\}\right|,$$
$$a_2 = \left|\left\{y \in \mathbb{F}_2^m : (-1)^{g(y)} W_g(y) < 0\right\}\right|.$$

Then we have a following system

$$\begin{cases} 2^{(m+1)/2} a_1 - 2^{(m+1)/2} a_2 = S_g, \\ a_1 + a_2 = 2^{m-1}. \end{cases}$$

It is clear that the maximal value of S_g corresponds to the case $a_2 = 0$. Then $a_1 = 2^{m-1}$ and

$$S_g = 2^{(m+1)/2} \cdot 2^{m-1} = 2^{(3m-1)/2}.$$

By the same arguments the minimal value of S_g corresponds to the case $a_1 = 0$, that is $a_2 = 2^{m-1}$, and

$$S_g = \left(-2^{(m+1)/2}\right) \cdot 2^{m-1} = -2^{(3m-1)/2}.$$

Thus, it holds $|S_g| \leq 2^{(3m-1)/2}$ with the equality only when either

$$(-1)^{g(y)} W_g(y) \geq 0 \text{ for any } y \in \mathbb{F}_2^m,$$

or

$$(-1)^{g(y)} W_g(y) \leq 0 \text{ for any } y \in \mathbb{F}_2^m,$$

that is g is either self-dual or anti-self-dual near-bent. □

Thus, the value of the Rayleigh quotient of a self-dual near-bent function coincides with the bound for its maximal value, which is the best known one for today. Moreover, on self-dual near-bent functions and only on them the value of the Rayleigh quoutient is maximal within the set of near-bent functions. Just the same holds for the minimal value and anti-self-dual near-bent functions.

3.2 Connection between self-duality for even and odd cases

Further we show that there exists a bijection between two types of self-duality with a descent step from even to odd number of variables.

Theorem 1 *There exists a one-to-one correspondence between the set of self-dual bent functions in $n \geq 4$ variables and the set of (anti-)self-dual near-bent functions in $n-1$ variables.*

Proof Put $\mathcal{H} = \mathcal{H}_{n-1}$. Let f be a self-dual bent functions in n variables and (f_0, f_1) be its truth table, where $f_i \in \mathcal{F}_{n-1}$, $i = 1, 2$. Denote by F_i the sign vector of f_i, $i = 1, 2$. Then it holds

$$\frac{1}{\sqrt{2}} \begin{pmatrix} \mathcal{H} & \mathcal{H} \\ \mathcal{H} & -\mathcal{H} \end{pmatrix} \begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = \begin{pmatrix} F_0 \\ F_1 \end{pmatrix},$$

that is equal to the system

$$\begin{cases} \mathcal{H}F_0 + \mathcal{H}F_1 = \sqrt{2}F_0, \\ \mathcal{H}F_0 - \mathcal{H}F_1 = \sqrt{2}F_1. \end{cases} \tag{3}$$

Firstly one can notice that

$$\begin{aligned} \left\langle \sqrt{2}F_0, \sqrt{2}F_0 \right\rangle &= \langle \mathcal{H}F_0 + \mathcal{H}F_1, \mathcal{H}F_0 + \mathcal{H}F_1 \rangle \\ &= \langle \mathcal{H}F_0, \mathcal{H}F_0 \rangle + 2\langle \mathcal{H}F_0, \mathcal{H}F_1 \rangle + \langle \mathcal{H}F_1, \mathcal{H}F_1 \rangle \\ &= \langle F_0, F_0 \rangle + 2\langle F_0, F_1 \rangle + \langle F_1, F_1 \rangle \\ &= 2^{n-1} + 2\langle F_0, F_1 \rangle + 2^{n-1} \\ &= 2 \cdot 2^{n-1}, \end{aligned}$$

therefore it holds $\langle F_0, F_1 \rangle = 0$ (It also follows from the orthogonality of $\mathcal{H}F_0$ and $\mathcal{H}F_1$ and symmetricity of $\mathcal{H}$). Now consider the first equation from the system above:

$$\mathcal{H}F_0 = -\mathcal{H}F_1 + \sqrt{2}F_0.$$

Since $\mathcal{H}^2 = I_{n-1}$, it is the same as

$$F_0 = -F_1 + \sqrt{2}\mathcal{H}F_0.$$

Consider the inner product

$$\langle F_0, F_0 \rangle = -\langle F_0, F_1 \rangle + \sqrt{2}\langle F_0, \mathcal{H}F_0 \rangle.$$

The orthogonality of F_0 and F_1 implies the condition

$$\sqrt{2}\langle F_0, \mathcal{H}F_0 \rangle = 2^{n-1}.$$

Under the used notation we have

$$S_{f_0} = \langle F_0, H_{n-1}F_0 \rangle = 2^{\frac{3(n-1)-1}{2}}.$$

Since from (1) it immediately follows that function f_1 can be characterized by f_0, there exists an injective mapping from the set of all self-dual bent functions in n variables to the set of self-dual near-bent functions in $n-1$ variables. This mapping essentially maps every self-dual bent function to its subfunction obtained by fixing the first coordinate with 0.

Now let f_0 be a self-dual near-bent function in $n-1$ variables. From Proposition 1 it follows that the value of $(-1)^{f_0(y)}$ and the sign of the Walsh–Hadamard coefficient $W_{f_0}(y)$ of f_0 are agreed in a sense that their product is nonnegative for every $y \in \mathbb{F}_2^{n-1}$. Let F_0 be a sign vector of f_0. Define

$$F_1 = \frac{2H_{n-1}}{2^{n/2}}F_0 - F_0. \tag{4}$$

From (1) it follows that if $F_1 \in \{\pm 1\}^{2^{n-1}}$, then the vector (F_0, F_1) is the sign vector of a self-dual bent function in n variables. Indeed, the relation (1) for (F_0, F_1) is

$$F_0 = \left(I_{2^{n-1}} + \frac{2H_{n-1}}{2^{n/2}} \right) F_1,$$

and its multiplication by $\left(I_{2^{n-1}} - \frac{2H_{n-1}}{2^{n/2}} \right)$ from the left yields (4) since

$$\left(I_{2^{n-1}} + \frac{2H_{n-1}}{2^{n/2}} \right) \left(I_{2^{n-1}} - \frac{2H_{n-1}}{2^{n/2}} \right) = -I_{2^{n-1}}.$$

It is clear that the fact that $W_{f_0}(y)$ and $(-1)^{f_0(y)}$ are being agreed implies that

$$\left(\frac{2}{2^{n/2}}W_{f_0}(y) - (-1)^{f_0(y)}\right) \in \{\pm 1\}, \quad y \in \mathbb{F}_2^{n-1},$$

then we can define a Boolean function in $n-1$ variables, say f_1, which has a sign vector F_1 and consider the relation (4) in componentwise form

$$(-1)^{f_1(y)} = \frac{2}{2^{n/2}}W_{f_0}(y) - (-1)^{f_0(y)}, \quad y \in \mathbb{F}_2^{n-1}.$$

So the vector (F_0, F_1) is the sign vector of a self-dual bent function in n variables. Note that this self-dual bent function is unique since the pair of subfunctions of any self-dual bent function is defined uniquely.

Thus, it follows that for any self-dual near-bent Boolean function in $n-1$ variables there exists a self-dual bent function in n variables, moreover this function is an unique one.

Finally, we have that the mapping that maps every self-dual bent function to its subfunction obtained by fixing the first coordinate with 0, is an injective and surjective one from the set of all self-dual bent functions in n variables to the set of self-dual near-bent functions in $n-1$ variables. Therefore there exists a bijection between these sets of Boolean functions.

By the same arguments one can show that there exists a one-to-one correspondence between the set of all self-dual bent functions in $n \geq 4$ variables and the set of anti-self-dual near-bent functions in $n-1$ variables. In more details, it can be done by considering the second equation from (3) and showing that

$$S_{f_1} = \langle F_1, H_{n-1}F_1 \rangle = -2^{\frac{3(n-1)-1}{2}}.$$

So it follows that subfunction f_1 is anti-self-dual near-bent function in $n-1$ variables.

Again, from (1) it immediately follows that function f_0 can be characterized by f_1, hence there exists an injective mapping from the set of all self-dual bent functions in n variables to the set of anti-self-dual near-bent functions in $n-1$ variables. It maps every self-dual bent function to its subfunction obtained by fixing the first coordinate with 1.

Given an anti-self-dual near-bent function f_1 in $n-1$ variables with sign vector F_1, for surjectivity of the mentioned mapping it is enough to consider the vector

$$F_0 = \frac{2H_{n-1}}{2^{n/2}}F_1 + F_1.$$

From Proposition 1 it follows that the value of $(-1)^{f_1(y)}$ and the sign of the Walsh–Hadamard coefficient $W_{f_1}(y)$ of f_1 are disagreed in a sense that their product is nonpositive for every $y \in \mathbb{F}_2^{n-1}$. Therefore the vector (F_0, F_1) consists of ±1 only, that is it is the sign vector of a self-dual bent function in n variables. This self-dual bent function is unique since the pair of subfunctions of any self-dual bent function is defined uniquely.

Thus, it follows that for any anti-self-dual near-bent Boolean function in $n-1$ variables there exists a self-dual bent function in n variables, moreover this function is an unique one. □

We have shown that for self-dual bent function f with vector of values $\left(f_0, f_1\right)$ the subfunction f_0 is always self-dual near-bent and f_1 is always anti-self-dual near-bent. From the other side for every self-dual near-bent function g in $n-1$ variables there exists a unique self-dual bent function in n variables such that g is its subfunctions obtained by fixing the first variable with 0. At the same time for every every anti-self-dual near-bent function h

in $n-1$ variables there also exists a unique self-dual bent function in n variables such that h is its subfunctions obtained by fixing the first variable with 1.

Thus, the mentioned bijection is defined via the mapping $f \leftrightarrow f_0$ for self-dual near-bent case and $f \leftrightarrow f_1$ for anti-self-dual near-bent one.

We also have a bijection between self-dual and anti-self-dual near-bent functions, it is provided by the considerations above and the relation (1).

There is an interesting consequence that if we want to obtain Boolean function in even number n of variables that has the maximal value of the Rayleigh quotient, by using the concatenation of two Boolean functions in $n-1$ variables, we likely should not take functions that have extremal values of the Rayleigh quotient. The same holds if we are to construct a Boolean function in odd number m of variables that also has the maximal value of the Rayleigh quotient. Since in the first case self-dual or anti-self-dual near-bent functions are not chosen, therefore the obtained Boolean functions will not be self-dual bent. In the second case we obtain a bent-concatenation bound that is likely to be not tight for infinitely many n.

The reason of that can be explained by the following considerations. Assume we have the Boolean function f in k variables (even or odd) with sign vector F, which is a concatenation of functions f_0 and f_1 in $k-1$ variables with sign vectors F_0 and F_1. Then it holds

$$\begin{aligned}
S_f &= \langle F, H_n F\rangle = \left\langle (F_0, F_1), \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix} \begin{pmatrix} F_0 \\ F_1 \end{pmatrix} \right\rangle \\
&= \left\langle (F_0, F_1), \begin{pmatrix} H_{n-1}(F_0 + F_1) \\ H_{n-1}(F_0 - F_1) \end{pmatrix} \right\rangle \\
&= \langle F_0, H_{n-1}F_0\rangle - \langle F_1, H_{n-1}F_1\rangle + \langle F_0, H_{n-1}F_1\rangle + \langle F_1, H_{n-1}F_0\rangle \\
&= S_{f_0} - S_{f_1} + \langle F_0, H_{n-1}F_1\rangle + \langle F_1, H_{n-1}F_0\rangle \\
&= S_{f_0} - S_{f_1} + 2\langle F_0, H_{n-1}F_1\rangle ,
\end{aligned}$$

where we have different signs for the Rayleigh quotients of the subfunctions and also the term comprising both subfunctions, one of which is given in its Walsh–Hadamard transfrom form.

Thus, the maximization of the Rayleigh quotient of subfunctions may lead to the “instability” and decrease of the Rayleigh quotient of the whole function. The maximization of the Rayleigh quotient for the case of an odd number of variables is a problem of a complex optimization, in particular, of the values of the Rayleigh quotient of its subfunctions.

4 Decomposition of the form (f_0, f_1, f_2, f_3) for self-dual case

In this section we study the subfunctions of self-dual bent functions that are obtained by fixing the first and the second coordinates of the argument. Metrical properties of subfunctions and interconnections between them are considered.

Subfunctions of a bent function, in more general form, comprising the restriction of a bent function on all subspaces of codimension 2, were extensively studied in works [3, 4]. The considered sets of subfunctions were referred to as 4-*decompositions* of a bent function. In particular, it was shown that such subfunctions of a bent function in n variables have the same Walsh–Hadamard spectrum: either all of them are bent, all are the three valued almost optimal (these are precisely near-bent functions with the spectrum having three values $0, \pm 2^{n/2}$), or they have the same Walsh–Hadamard spectrum with five values $0, \pm 2^{(n-2)/2}, \pm 2^{n/2}$. In [17] the family of so-called totally (non-overlap) disjoint spectra plateaued functions was studied. These functions are interesting since they are constituent functions in the 4-decompositions.

Throughout this section given a function f in n variables we will refer to four Boolean functions f_i, $i = 0, 1, 2, 3$, in $n-2$ variables as to its subfunctions obtained by fixing the first and the second coordinates of the argument with the values $\{(00), (01), (10), (11)\}$, correspondingly. In turn, vector of values of f will have the form (f_0, f_1, f_2, f_3). The sign vector of f_i will be denoted by F_i, $i = 0, 1, 2, 3$. Let the notation $\mathcal{H}$ states for $\mathcal{H}_{n-2}$.

Further we will use the following observation. Let f be a bent function in n variables, then

$$\frac{1}{2}\begin{pmatrix} \mathcal{H} & \mathcal{H} & \mathcal{H} & \mathcal{H} \\ \mathcal{H} & -\mathcal{H} & \mathcal{H} & -\mathcal{H} \\ \mathcal{H} & \mathcal{H} & -\mathcal{H} & -\mathcal{H} \\ \mathcal{H} & -\mathcal{H} & -\mathcal{H} & \mathcal{H} \end{pmatrix}\begin{pmatrix} F_0 \\ F_1 \\ F_2 \\ F_3 \end{pmatrix} = \begin{pmatrix} R_0 \\ R_1 \\ R_2 \\ R_3 \end{pmatrix}$$

or, equivalently,

$$\begin{cases} F_0 + F_1 + F_2 + F_3 = 2\mathcal{H}R_0, \\ F_0 - F_1 + F_2 - F_3 = 2\mathcal{H}R_1, \\ F_0 + F_1 - F_2 - F_3 = 2\mathcal{H}R_2, \\ F_0 - F_1 - F_2 + F_3 = 2\mathcal{H}R_3, \end{cases} \tag{5}$$

where R_i, $i = 0, 1, 2, 3$, are sign vectors of subfunctions of $\widetilde{f}$. Obviously, the function f is self-dual if and only if $R_i = F_i$, $i = 0, 1, 2, 3$.

4.1 Concatenation of four bent functions

The case when all four subfunctions are bent essentially leads to the idea of an iterative construction of a bent function in $n+2$ variables through four bent functions in n variables. In [33] Preneel et al. proved that given four bent functions f_i, $i = 0, 1, 2, 3$, in n variables, the concatenation of vectors of values of f_i yields a bent function in $n+2$ variables if and only if

$$W_{f_0}(y)W_{f_1}(y)W_{f_2}(y)W_{f_3}(y) = -2^{2n} \text{ for any } y \in \mathbb{F}_2^n.$$

In terms of duals this condition is equivalent to the following

$$\widetilde{f_0}(y) \oplus \widetilde{f_1}(y) \oplus \widetilde{f_2}(y) \oplus \widetilde{f_3}(y) = 1 \text{ for any } y \in \mathbb{F}_2^n.$$

Note that the idea of concatenation also appears in a scope of so-called “bent based” bent sequences, see [1]. The approach allows to obtain a bent sequence of length $4l$ through the concatenation of four bent sequences of length l provided the similar conditions on these sequences are satisfied.

Bent functions in $n+2$ variables obtained by the concatenation of four bent functions in n variables were also studied in [40] from the point of view of obtaining lower bounds on the cardinality of the set of bent functions. Such functions were referred to as *bent iterative* functions. Concatenation construction was also considered in [16] in a scope of generic concatenation methods. New constructions of bent functions, based on the concatenation, were recently proposed in [2, 32]. In [9] one can find another iterative approaches.

There are known two constructions of self-dual bent functions in $n+2$ variables, based on the concatenation of four bent functions in n variables. They are

- the construction **C1**:

$$\left(f, \widetilde{f}, \widetilde{f}, f \oplus 1\right),$$

  where f is a bent function in n variables [8];
- the construction **C2**:

$$\left(f, g \oplus 1, g, f\right),$$

  where f is a self-dual bent function, g is an anti-self-dual bent function both in n variables [21].

It is worth noting that the best known for today lower bound on the cardinality of the set of self-dual bent functions is the sum of cardinalities of **C1** and **C2**.

In [21] the criteria of self-duality of a bent function in $n + 2$ variables obtained via concatenation of four bent functions in n variables was presented.

4.2 Gram matrix for sign vectors of subfunctions

In this subsection we will study the Gram matrix of vectors F_i, $i = 0, 1, 2, 3$ which are sign vectors of subfunctions of a Boolean function f. Recall that elements g_{ij} of the Gram matrix of vectors $\{v_k\}_{k\in M} \subset \mathbb{R}^d$ are inner products between v_i and v_j, $i, j \in M$. The determinant of the Gram matrix is called the Gramian of the corresponding system of vectors. The basic properties of real Gram matrices are:

- symmetricity;
- positive semi-definiteness;
- the Gramian is zero if and only if the vectors are linearly dependent.

Denote the inner products by $g_{ij} = \langle F_i, F_j \rangle$, $i, j = 0, 1, 2, 3$.

The form of the Gram matrix of self-dual bent functions is characterized in the following statement

Theorem 2 *The Gram matrix of any self-dual bent function in n variables has form*

$$\begin{pmatrix} 2^{n-2} & b & b & -a \\ b & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -b \\ -a & -b & -b & 2^{n-2} \end{pmatrix},$$

for some even integers a, b such that

$$-2^{n-2} + 2|b| \leq a \leq 2^{n-2}.$$

Proof For self-dual case the system (5) has form

$$\begin{cases} F_0 + F_1 + F_2 + F_3 = 2\mathcal{H}F_0, \\ F_0 - F_1 + F_2 - F_3 = 2\mathcal{H}F_1, \\ F_0 + F_1 - F_2 - F_3 = 2\mathcal{H}F_2, \\ F_0 - F_1 - F_2 + F_3 = 2\mathcal{H}F_3. \end{cases} \tag{6}$$

Consider pairwise inner products of right parts of all equations in the system (6). The symmetricity of $\mathrm{Gram}(f)$ implies that we have at most six different coefficients outside the main diagonal in fact. For example, the 1st equation's expression inner product with itself is

$$\begin{aligned}\langle 2\mathcal{H}F_0, 2\mathcal{H}F_0\rangle &= \langle F_0 + F_1 + F_2 + F_3, F_0 + F_1 + F_2 + F_3\rangle \\ &= \sum_{i,j=0}^{3} g_{ij} = 4\cdot 2^{n-2} + \sum_{\substack{i,j=0,\\ i\neq j}}^{3} g_{ij} = 2^n.\end{aligned}$$

It yields the following equation on the coefficients:

$$g_{01} + g_{02} + g_{03} + g_{12} + g_{13} + g_{23} = 0.$$

Finally, after considering the rest ones, we have the following system of equations that describe necessary relations between the entries of the Gram matrix:

$$\begin{cases} g_{01} + g_{02} + g_{03} + g_{12} + g_{13} + g_{23} = 0, \\ g_{01} - g_{02} + g_{03} + g_{12} - g_{13} + g_{23} = 0, \\ g_{01} - g_{02} - g_{03} - g_{12} - g_{13} + g_{23} = 0, \\ g_{01} + g_{02} - g_{03} - g_{12} + g_{13} + g_{23} = 0, \\ 2g_{01} = g_{02} - g_{13}, \\ 2g_{02} = g_{01} - g_{23}, \\ g_{03} = -g_{12}, \\ 2g_{13} = g_{23} - g_{01}, \\ 2g_{23} = g_{13} - g_{02}. \end{cases}$$

The system has rank 4, its general solution is

$$\begin{aligned} &g_{01} = -g_{23}, && g_{02} = -g_{23}, && g_{03} = -g_{12}, \\ & && g_{12} = g_{12}, && g_{13} = g_{23}, \\ & && && g_{23} = g_{23} \end{aligned}$$

for g_{12} and g_{23} being free variables. Denote $b = -g_{23}$ and $a = g_{12}$, then we obtain the desired form of the Gram matrix:

$$\mathrm{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & b & -a \\ b & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -b \\ -a & -b & -b & 2^{n-2} \end{pmatrix}.$$

Now we are to point essential bounds on values of a and b and deduce some relations between them. In order to do it recall that any Gram matrix is positive semi-definite, hence all its eigenvalues must be nonnegative. The matrix $\mathrm{Gram}(f)$ has four eigenvalues, they are

$$\begin{aligned} \lambda_{1,2} &= 2^{n-2} - a, \\ \lambda_3 &= 2^{n-2} + a - 2b, \\ \lambda_4 &= 2^{n-2} + a + 2b. \end{aligned}$$

Note that the eigenvalue $2^{n-2} - a$ has algebraic multiplicity 2, also its nonnegativity is obvious. The rest imply that

$$\begin{aligned} a &\geq -2^{n-2} + 2b, \\ a &\geq -2^{n-2} - 2b, \end{aligned}$$

that is

$$a \geq -2^{n-2} + \max\{2b, -2b\},$$

and, consequently,

$$a \geq -2^{n-2} + 2|b|,$$

where $|b|$ is essentially bounded by 2^{n-2} from above. □

For example, the constructions **C1** and **C2** provide the following matrices:

$$\mathrm{Gram}(\mathbf{C1}) = \begin{pmatrix} 2^{n-2} & \mathcal{S}_f & \mathcal{S}_f & -2^{n-2} \\ \mathcal{S}_f & 2^{n-2} & 2^{n-2} & -\mathcal{S}_f \\ \mathcal{S}_f & 2^{n-2} & 2^{n-2} & -\mathcal{S}_f \\ -2^{n-2} & -\mathcal{S}_f & -\mathcal{S}_f & 2^{n-2} \end{pmatrix},$$

which has rank 1 in the case when $\mathcal{S}_f = 2^{n-2}$ that is f is self-dual bent, and 2 otherwise, and

$$\mathrm{Gram}(\mathbf{C2}) = \begin{pmatrix} 2^{n-2} & 0 & 0 & 2^{n-2} \\ 0 & 2^{n-2} & -2^{n-2} & 0 \\ 0 & -2^{n-2} & 2^{n-2} & 0 \\ 2^{n-2} & 0 & 0 & 2^{n-2} \end{pmatrix}$$

with rank equal to 2. It is obvious that for both constructions the sets $\{F_i\}$ are linearly dependent.

Inner products between sign functions are interesting since it is easy to deduce the Hamming distance between two Boolean functions provided the inner product between their sign functions is known. Indeed,

$$\mathrm{dist}\left(f_i, f_j\right) = 2^{n-3} - \frac{1}{2}\left\langle F_i, F_j\right\rangle = 2^{n-3} - \frac{1}{2}g_{ij}, \quad i, j = 0, 1, 2, 3.$$

Thus, Theorem 6 can be reformulated in terms of Hamming distances between subfunctions:

Corollary 1 *Let f be a self-dual bent function in n variables. The Hamming distances between $\{f_i\}_{i=0}^{3}$ are characterized by the matrix*

$$\mathrm{Dist}(f) = \begin{pmatrix} 0 & 0 & 0 & 2^{n-2} \\ 0 & 0 & 0 & 2^{n-2} \\ 0 & 0 & 0 & 2^{n-2} \\ 2^{n-2} & 2^{n-2} & 2^{n-2} & 0 \end{pmatrix} + \begin{pmatrix} 0 & d_1 & d_1 & -d_2 \\ d_1 & 0 & d_2 & -d_1 \\ d_1 & d_2 & 0 & -d_1 \\ -d_2 & -d_1 & -d_1 & 0 \end{pmatrix}$$

for some positive even integers d_1, d_2 such that

$$|2^{n-2} - 2d_1| \leq 2^{n-2} - d_2.$$

Proof The relation between the inner product and the Hamming distance yields the matrix whereas the inequality

$$|2^{n-2} - 2d_1| \leq 2^{n-2} - d_2$$

is obtained from

$$-2^{n-2} + 2|b| \leq a \leq 2^{n-2}$$

with

$$b = 2^{n-2} - 2d_1,$$
$$a = 2^{n-2} - 2d_2.$$

□

4.3 Rayleigh quotients of subfunctions

Another application of the Gram matrix deals with the relations between Rayleigh quotients of subfunctions. Let f be a self-dual bent function in n variables. Recall that by (5) we have

$$\begin{cases} F_0 + F_1 + F_2 + F_3 = 2\mathcal{H}F_0, \\ F_0 - F_1 + F_2 - F_3 = 2\mathcal{H}F_1, \\ F_0 + F_1 - F_2 - F_3 = 2\mathcal{H}F_2, \\ F_0 - F_1 - F_2 + F_3 = 2\mathcal{H}F_3. \end{cases}$$

The Gram matrix provides the expression of the Rayleigh quotients of the subfunctions in terms of the coefficients a ans b.

$$\begin{cases} 2^{n-2} + 2b - a = \langle F_0, 2\mathcal{H}F_0 \rangle, \\ -2^{n-2} + a + 2b = \langle F_1, 2\mathcal{H}F_1 \rangle, \\ -2^{n-2} + 2b + a = \langle F_2, 2\mathcal{H}F_2 \rangle, \\ 2^{n-2} - a + 2b = \langle F_3, 2\mathcal{H}F_3 \rangle. \end{cases}$$

Finally we have expressions

$$S_{f_0} = 2^{n/2-2}\left(2^{n-2} - a + 2b\right), \qquad S_{f_1} = 2^{n/2-2}\left(-2^{n-2} + a + 2b\right),$$
$$S_{f_2} = 2^{n/2-2}\left(-2^{n-2} + a + 2b\right), \qquad S_{f_3} = 2^{n/2-2}\left(2^{n-2} - a + 2b\right),$$

and

$$S_{f_0} + S_{f_1} = S_{f_2} + S_{f_3} = 2^{n/2}b.$$

It follows that the Rayleigh quotients of f_0 and f_3 coincide, as well as of f_1 and f_2. The sum of all Rayleigh quotients is equal to

$$S_{f_0} + S_{f_1} + S_{f_2} + S_{f_3} = 2^{n/2+1}b.$$

We collect all this to the following statement

Proposition 2 *Let f be a self-dual bent function in n variables with Gram matrix*

$$\mathrm{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & b & -a \\ b & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -b \\ -a & -b & -b & 2^{n-2} \end{pmatrix},$$

then

$$S_{f_0} = S_{f_3} = 2^{n/2-2}\left(2^{n-2} - a + 2b\right),$$
$$S_{f_1} = S_{f_2} = 2^{n/2-2}\left(-2^{n-2} + a + 2b\right).$$

4.4 Sufficient condition for the subfunctions of self-dual bent function to be bent

In this subsection we study the special cases of parameters a, b for which the Gram matrix is singular.

Recall that the Gramian is equal to the product of the eigenvalues of the matrix so for a self-dual bent function f with the Gram matrix $\mathrm{Gram}(f)$ it has the following expression

$$\mathrm{Gramian}(f) = \left(2^{n-2} - a\right)^2 \left(2^{n-2} + a - 2b\right) \left(2^{n-2} + a + 2b\right). \tag{7}$$

Further the values such that the Gramian is zero will be considered for a self-dual case.

But before, we can characterize all self-dual bent functions that possess $a = 2^{n-2}$, that is $f_1 = f_2$. In order to do it consider the general system

$$\begin{cases} F_0 + F_1 + F_2 + F_3 = 2\mathcal{H}F_0, \\ F_0 - F_1 + F_2 - F_3 = 2\mathcal{H}F_1, \\ F_0 + F_1 - F_2 - F_3 = 2\mathcal{H}F_2, \\ F_0 - F_1 - F_2 + F_3 = 2\mathcal{H}F_3, \end{cases}$$

which is transformed to

$$\begin{cases} F_0 + 2F_1 + F_3 = 2\mathcal{H}F_0, \\ F_0 - F_3 = 2\mathcal{H}F_1, \\ F_0 - F_3 = 2\mathcal{H}F_1, \\ F_0 - 2F_1 + F_3 = 2\mathcal{H}F_3. \end{cases}$$

By the triangle inequality we obtain

$$\|F_0 - F_3\| \le \|F_0\| + \|F_3\| = 2 \cdot 2^{(n-2)/2} = 2^{n/2}.$$

From the other side by orthogonality of the matrix $\mathcal{H}$ we obtain that $\|2\mathcal{H}F_1\| = 2 \cdot 2^{(n-2)/2} = 2^{n/2}$. So we have an equality

$$\|F_0 - F_3\| = \|F_0\| + \|F_3\|,$$

hence F_0 and F_3 are linearly dependent vectors, that is either $F_0 = F_3$ or $F_0 = -F_3$. But from the second and third equalities it follows that F_0 and F_3 can not coincide, therefore $F_3 = -F_0$. Finally we obtain $F_0 = \mathcal{H}F_1$, that is all subfunctions are bent and f_0 and f_1 are dual of each other. This situation is exactly the construction **C1**.

Proposition 3 *If for a self-dual bent function f it holds $f_1 = f_2$, then it is constructed via* ***C1****.*

In Sect. 4.2 it was mentioned that sign vectors of subfunctions mentioned in constructions **C1** and **C2** are linearly dependent. Also all those subfunctions are bent. The next results covers all combinations for which the Gramian is zero.

Theorem 3 *If the Gram matrix of a self-dual bent function f is singular then subfunctions $\{f_i\}_{i=0}^3$ are bent.*

Proof At first notice that the condition (1) for the case of subfunctions in $n - 2$ variables has the following form

$$\begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = \begin{pmatrix} F_2 \\ F_3 \end{pmatrix} + \begin{pmatrix} \mathcal{H} & \mathcal{H} \\ \mathcal{H} & -\mathcal{H} \end{pmatrix} \begin{pmatrix} F_2 \\ F_3 \end{pmatrix}. \tag{8}$$

Table 2 All possible relations between values of subfunctions and their Walsh–Hadamard transform

i	$F_0(y)$	$F_1(y)$	$F_2(y)$	$F_3(y)$	$\mathcal{H}F_0(y)$	$\mathcal{H}F_1(y)$	$\mathcal{H}F_2(y)$	$\mathcal{H}F_3(y)$
1	$+1$	$+1$	$+1$	$+1$	$+2$	0	0	0
2	$+1$	-1	$+1$	-1	0	$+2$	0	0
3	-1	$+1$	-1	$+1$	0	-2	0	0
4	-1	-1	-1	-1	-2	0	0	0
5	-1	$+1$	$+1$	-1	0	0	0	-2
6	$+1$	-1	-1	$+1$	0	0	0	$+2$
7	$+1$	$+1$	-1	-1	0	0	$+2$	0
8	-1	-1	$+1$	$+1$	0	0	-2	0
9	$+1$	$+1$	-1	$+1$	$+1$	-1	$+1$	$+1$
10	$+1$	-1	-1	-1	-1	$+1$	$+1$	$+1$
11	-1	$+1$	$+1$	$+1$	$+1$	-1	-1	-1
12	-1	-1	$+1$	-1	-1	$+1$	-1	-1
13	$+1$	$+1$	$+1$	-1	$+1$	$+1$	$+1$	-1
14	-1	$+1$	-1	-1	-1	-1	$+1$	-1
15	$+1$	-1	$+1$	$+1$	$+1$	$+1$	-1	$+1$
16	-1	-1	-1	$+1$	-1	-1	-1	$+1$

Also by the condition $\mathcal{H}^2 = I_{2^{n-2}}$ we obtain

$$\begin{pmatrix}\mathcal{H}F_0\\ \mathcal{H}F_1\end{pmatrix} = \begin{pmatrix}\mathcal{H}F_2\\ \mathcal{H}F_3\end{pmatrix} + \begin{pmatrix}F_2 + F_3\\ F_2 - F_3\end{pmatrix}. \tag{9}$$

Both of conditions (8) and (9) allow to characterize all possible combinations of signs of F_i and $\mathcal{H}F_i$, $i = 0, 1, 2, 3$. As it was mentioned in Sect. 4.1, either all of subfunctions are bent, all are near-bent, or they have the same Walsh–Hadamard spectrum with five values $0, \pm 2^{(n-2)/2}, 2^{n/2}$ [3, 4]. It means that in general case $\mathcal{H}F_i \in \{0, \pm 1, \pm 2\}$, $i = 0, 1, 2, 3$.

For every row of Table 2 by c_i we denote the number of vectors $y \in \mathbb{F}_2^{n-2}$ for which the corresponding sequence of values and signs stands. The Gram matrix from Theorem 6 for the function f gives six equations:

$$\begin{aligned}\langle F_0, F_1\rangle &= c_1 - c_2 - c_3 + c_4 - c_5 - c_6 + c_7 + c_8 + c_9 - c_{10} - c_{11} + c_{12}\\ &\quad + c_{13} - c_{14} - c_{15} + c_{16} = b,\end{aligned}$$

$$\begin{aligned}\langle F_0, F_2\rangle &= c_1 + c_2 + c_3 + c_4 - c_5 - c_6 - c_7 - c_8 - c_9 - c_{10} - c_{11} - c_{12}\\ &\quad + c_{13} + c_{14} + c_{15} + c_{16} = b,\end{aligned}$$

$$\begin{aligned}\langle F_0, F_3\rangle &= c_1 - c_2 - c_3 + c_4 + c_5 + c_6 - c_7 - c_8 + c_9 - c_{10} - c_{11} + c_{12}\\ &\quad - c_{13} + c_{14} + c_{15} - c_{16} = -a,\end{aligned}$$

$$\begin{aligned}\langle F_1, F_2\rangle &= c_1 - c_2 - c_3 + c_4 + c_5 + c_6 - c_7 - c_8 - c_9 + c_{10} + c_{11} - c_{12}\\ &\quad + c_{13} - c_{14} - c_{15} + c_{16} = a,\end{aligned}$$

$$\begin{aligned}\langle F_1, F_3\rangle &= c_1 + c_2 + c_3 + c_4 - c_5 - c_6 - c_7 - c_8 + c_9 + c_{10} + c_{11} + c_{12}\\ &\quad - c_{13} - c_{14} - c_{15} - c_{16} = -b,\end{aligned}$$

$$\begin{aligned}\langle F_2, F_3\rangle &= c_1 - c_2 - c_3 + c_4 - c_5 - c_6 + c_7 + c_8 - c_9 + c_{10} + c_{11} - c_{12}\\ &\quad - c_{13} + c_{14} + c_{15} - c_{16} = -b.\end{aligned}$$

Finally, taking into account the cardinality of the space $\mathbb{F}_2^{n-2}$, we obtain the system of 7 linear equations

$$\begin{cases} c_1 - c_2 - c_3 + c_4 - c_5 - c_6 + c_7 + c_8 + c_9 - c_{10} - c_{11} + c_{12} + c_{13} - c_{14} - c_{15} + c_{16} = b\\ c_1 + c_2 + c_3 + c_4 - c_5 - c_6 - c_7 - c_8 - c_9 - c_{10} - c_{11} - c_{12} + c_{13} + c_{14} + c_{15} + c_{16} = b\\ c_1 - c_2 - c_3 + c_4 + c_5 + c_6 - c_7 - c_8 + c_9 - c_{10} - c_{11} + c_{12} - c_{13} + c_{14} + c_{15} - c_{16} = -a\\ c_1 - c_2 - c_3 + c_4 + c_5 + c_6 - c_7 - c_8 - c_9 + c_{10} + c_{11} - c_{12} + c_{13} - c_{14} - c_{15} + c_{16} = a\\ c_1 + c_2 + c_3 + c_4 - c_5 - c_6 - c_7 - c_8 + c_9 + c_{10} + c_{11} + c_{12} - c_{13} - c_{14} - c_{15} - c_{16} = -b\\ c_1 - c_2 - c_3 + c_4 - c_5 - c_6 + c_7 + c_8 - c_9 + c_{10} + c_{11} - c_{12} - c_{13} + c_{14} + c_{15} - c_{16} = -b\\ c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 + c_8 + c_9 + c_{10} + c_{11} + c_{12} + c_{13} + c_{14} + c_{15} + c_{16} = 2^{n-2} \end{cases}$$

The system has rank 7, its equations in a row echelon form yield the relations

$$\begin{aligned} c_1 + c_4 + c_{14} + c_{15} &= \frac{2^{n-2} - a}{4},\\ c_2 + c_3 + c_{14} + c_{15} &= \frac{2^{n-2} - a}{4},\\ c_5 + c_6 + c_{14} + c_{15} &= \frac{2^{n-2} - a}{4},\\ c_7 + c_8 + c_{14} + c_{15} &= \frac{2^{n-2} - a}{4},\\ c_9 + c_{12} - c_{14} - c_{15} &= 0,\\ c_{10} + c_{11} - c_{14} - c_{15} &= \frac{a - b}{2},\\ c_{13} - c_{14} - c_{15} + c_{16} &= \frac{a + b}{2}. \end{aligned}$$

Now we are to consider all combinations of a, b such that the Gramian (7) is zero. In order to do it we take c_i, $i = 1, 2, \ldots, 16$, as nonnegative integer variables. Before one can note that one of subfunctions is bent (consequently all of them are bent) if and only if $c_i = 0$ for $i = 1, 2, \ldots, 8$. So we introduce an auxiliary equation

$$c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 + c_8 = k,$$

where k is nonnegative integer and put it to the system. The rank of the resulting system of equations is 8. From the nonnegativity of variables it follows that if for a fixed pair a, b provided by some self-dual bent function, the system has no solutions with positive k, all subfunctions of this function are bent.

At first, note that for every eigenvalue of the Gram matrix given in the general form there exists a self-dual bent function with a, b such that the eigenvalue is zero. Indeed, for $\lambda_{1,2} = 2^{n-2} - a = 0$ the construction **C1** is suitable, since it provides $a = 2^{n-2}$, $b = \mathcal{S}_f$. For $\lambda_3 = 2^{n-2} + a - 2b = 0$ and $\lambda_4 = 2^{n-2} + a + 2b = 0$ the contruction **C2** meets the desired condition because it is clear that it admits $a = -2^{n-2}$, $b = 0$.

Now consider all pairs of a, b, vanising the corresponding eigenvalue, and analyze the obtained system:

- $2^{n-2} - a = 0$: in this case

$$c_1 = c_2 = c_3 = c_4 = c_5 = c_6 = c_7 = c_8 = 0,$$

that holds if only if $k = 0$.

- $2^{n-2} + a - 2b = 0$: the relations between variables must satisfy

$$c_1 + c_4 = \frac{k}{4}, \quad c_2 + c_3 = \frac{k}{4}, \quad c_5 + c_6 = \frac{k}{4}, \quad c_7 + c_8 = \frac{k}{4}, \quad c_{10} + c_{11} = -\frac{k}{4},$$

so the solution does not exist if $k > 0$, therefore $k = 0$.

- $2^{n-2} + a + 2b = 0$: we have relations

$$c_1 + c_4 = \frac{k}{4}, \quad c_2 + c_3 = \frac{k}{4}, \quad c_5 + c_6 = \frac{k}{4}, \quad c_7 + c_8 = \frac{k}{4}, \quad c_{13} + c_{16} = -\frac{k}{4},$$

so again the solution does not exist if $k > 0$, therefore $k = 0$.

□

From Theorem 3 and properties of the Gram matrix we conclude that

Corollary 2 *If sign vectors of subfunctions of a self-dual bent function f are linearly dependent then subfunctions $\{f_i\}_{i=0}^3$ are bent.*

Thus, we obtain a sufficient condition for bentness of the subfunctions. The interesting question arises: is it **necessary** to have linear dependence for sign vectors of subfunctions in order to obtain a self-dual bent function with bent subfunctions? In particular, the experiments show that

Remark 1 For $n = 4$ all self-dual bent functions with bent subfunctions have singular Gram matrices.

We consider this question further in Sect. 5. Note that according to experiments conducted for small n, most of self-dual bent functions are not bent concatenations hence their Gram matrices are necessarily non-singular. In particular, from 42896 self-dual bent functions in 6 variables only 3408 are bent concatenations and 192 of them have singular Gram matrices.

From Table 2 we can also deduce an interesting property that can be useful.

Proposition 4 *Let f be an (anti-)self-dual bent function in n variables, then $\{f_i\}_{i=0}^3$ are bent if and only if*

$$f_0(y) \oplus f_1(y) \oplus f_2(y) \oplus f_3(y) = 1 \textit{ for any } y \in \mathbb{F}_2^{n-2}.$$

This condition is not well seen from the results of [21] but can be deduced from [3]. Anti-self-dual case follows from the existence of a certain bijection between self-dual and anti-self-dual bent functions (see [8, 18, 22]). By using the condition we can clarify the decomposition of a self-dual bent function with bent subfunctions:

$$\begin{aligned} f(y_1, y_2, x) &= (y_1 \oplus 1)(y_2 \oplus 1) f_0(x) \oplus (y_1 \oplus 1) y_2 f_1(x) \\ &\oplus y_1 (y_2 \oplus 1) f_2(x) \oplus y_1 y_2 f_3(x) \\ &= y_1 y_2 (f_0(x) \oplus f_1(x) \oplus f_2(x) \oplus f_3(x)) \\ &\oplus y_1 (f_0(x) \oplus f_2(x)) \oplus y_2 (f_0(x) \oplus f_1(x)) \oplus f_0(x) \\ &= f_0 \oplus y_1 (f_0 \oplus f_2) \oplus y_2 (f_0 \oplus f_1) \oplus y_1 y_2, \quad y_1, y_2 \in \mathbb{F}_2, x \in \mathbb{F}_2^{n-2}. \end{aligned}$$

From Corollary 1 it follows that Hamming weights of functions $f_0 \oplus f_1$ and $f_0 \oplus f_2$ coincide.

5 Linear independence of sign vectors and bentness of the subfunctions of self-dual bent function

As it was mentioned in the previous section, the singularity of the Gram matrix is also necessary for the case $n = 4$. It is known that all (self-dual) bent functions in 4 variables are quadratic. So further we are to check if this property holds for *any* quadratic self-dual bent function.

Any quadratic function in n variables, say f, can be written as

$$f(z) = \langle z, Az\rangle \oplus d, \quad z \in \mathbb{F}_2^n, \tag{10}$$

where A is an upper triangular matrix of order $n \times n$ over $\mathbb{F}_2$ and d is constant. The quadratic part of f, as well as its Hamming weight, is completely characterized by the so-called *associate alternating matrix* $Q = A \oplus A^{\mathrm{T}}$, see MacWilliams and Sloane [28]. Recall that a square matrix over $\mathbb{F}_2$ is called alternating if it is symmetric with zero diagonal.

In [18] self-dual quadratic bent functions were completely characterized through a classification of all $n \times n$ involutory alternating matrices over $\mathbb{F}_2$ under the action of the orthogonal group. In particular, it was proved that the function (10) is self-dual or anti-self-dual bent if and only if $Q^2 = I_n$, that is Q is an involution (initially was proved in [8]), and the matrix $QAQ \oplus A^{\mathrm{T}}$ is an alternating matrix. We will use this result in following.

Denote $m = n - 2$ and consider arbitrary (anti-)self-dual quadratic bent function in n variables:

$$f\,(y_1, y_2, x) = \lambda_1 y_1 \oplus \lambda_2 y_2 \oplus \lambda_{12} y_1 y_2 \oplus y_1\,\langle u, x\rangle \oplus y_2\,\langle v, x\rangle \oplus g(x),$$
$$y_1, y_2 \in \mathbb{F}_2, x \in \mathbb{F}_2^m,$$

where $\lambda_1, \lambda_2, \lambda_{12} \in \mathbb{F}_2,\ u, v \in \mathbb{F}_2^m$ and g is a function in m variables with degree at most 2. Without loss of generality we assume that $d = 0$. The subfunctions $\{f_i\}_{i=0}^3$ have form

$$\begin{aligned}
f(00, x) &= f_0(x) = g(x),\\
f(01, x) &= f_1(x) = g(x) \oplus \langle v, x\rangle \oplus \lambda_2,\\
f(10, x) &= f_2(x) = g(x) \oplus \langle u, x\rangle \oplus \lambda_1,\\
f(11, x) &= f_3(x) = g(x) \oplus \langle u \oplus v, x\rangle \oplus \lambda_1 \oplus \lambda_2 \oplus \lambda_{12}, \quad x \in \mathbb{F}_2^m.
\end{aligned}$$

Assume these subfunctions are bent, then g is bent and by Proposition 4 we have $\lambda_{12} = 1$. It is clear that f has invertible Gram matrix if and only if the vectors u, v are linearly independent.

The upper triangular matrix A and associate alternating matrix Q are

$$A = \begin{pmatrix} \lambda_1 & 1 & u^{\mathrm{T}} \\ 0 & \lambda_2 & v^{\mathrm{T}} \\ \mathbf{0} & \mathbf{0} & B \end{pmatrix}, \qquad Q = A \oplus A^{\mathrm{T}} = \begin{pmatrix} 0 & 1 & u^{\mathrm{T}} \\ 1 & 0 & v^{\mathrm{T}} \\ u & v & B \oplus B^{\mathrm{T}} \end{pmatrix},$$

where the $m \times m$ submatrix $B = \left(b_{ij}\right)$ characterizes quadratic function g. Note that the matrix $B \oplus B^{\mathrm{T}}$ must have full rank since g is bent. Associate alternating matrix Q must be an involutory matrix, therefore we have

$$Q^2 = \begin{pmatrix} 1 \oplus \langle u, u\rangle & \langle u, v\rangle & v^{\mathrm{T}} \oplus u^{\mathrm{T}}\left(B \oplus B^{\mathrm{T}}\right) \\ \langle u, v\rangle & 1 \oplus \langle v, v\rangle & u^{\mathrm{T}} \oplus v^{\mathrm{T}}\left(B \oplus B^{\mathrm{T}}\right) \\ v \oplus \left(B \oplus B^{\mathrm{T}}\right) u & u \oplus \left(B \oplus B^{\mathrm{T}}\right) v & M \oplus \left(B \oplus B^{\mathrm{T}}\right)^2 \end{pmatrix} = I_n,$$

where $M = \left(m_{ij}\right)$ is a square matrix with elements $m_{ij} = u_i u_j \oplus v_i v_j$, $i, j = 1, 2, \dots, m$. The relation $Q^2 = I_n$ holds if and only if

$$\langle u, u\rangle = \langle u, v\rangle = \langle v, v\rangle = 0, \qquad \left(B \oplus B^{\mathrm{T}}\right) u = v, \qquad \left(B \oplus B^{\mathrm{T}}\right) v = u,$$

$$M \oplus \left(B \oplus B^{\mathrm{T}}\right)^2 = I_m.$$

Also, one can easily show that M^2 is all-zero matrix, hence $\left(B \oplus B^{\mathrm{T}}\right)^4 = I_m$.

The next condition for (anti-)self-duality of quadratic bent functions is that the matrix $QAQ \oplus A^{\mathrm{T}}$ is alternating. In [18] it was noted that under condition $Q^2 = I_n$ the matrix $QAQ \oplus A^{\mathrm{T}}$ is symmetric, hence it is alternating if and only if its diagonal elements are equal to zero. Consider them in details:

$$\operatorname{diag}\left(QAQ \oplus A^{\mathrm{T}}\right) = \begin{pmatrix} \langle u, Bu\rangle \oplus \lambda_1 \oplus \lambda_2 \\ \langle v, Bv\rangle \oplus \lambda_1 \oplus \lambda_2 \\ \lambda_1 u_1 \oplus u_1 v_1 \oplus \lambda_2 v_1 \oplus c_1 \oplus b_{11} \\ \lambda_2 u_2 \oplus u_2 v_2 \oplus \lambda_2 v_2 \oplus c_2 \oplus b_{22} \\ \vdots \\ \lambda_1 u_m \oplus u_m v_m \oplus \lambda_2 v_m \oplus c_m \oplus b_{mm} \end{pmatrix},$$

where $c_i = \left(B \oplus B^{\mathrm{T}}\right)_i B \left(B \oplus B^{\mathrm{T}}\right)^{(i)}$, $i = 1, 2, \dots, m$.

Let us gather all the conditions for (anti-)self-duality of quadratic bent function, given in the form of decomposition with a respect to the first and the second variables:

$$\begin{cases} \langle u, u\rangle = \langle u, v\rangle = \langle v, v\rangle = 0, \\ \left(B \oplus B^{\mathrm{T}}\right) u = v, \\ \left(B \oplus B^{\mathrm{T}}\right) v = u, \\ u_i u_j \oplus v_i v_j \oplus \left\langle \left(B \oplus B^{\mathrm{T}}\right)^{(i)}, \left(B \oplus B^{\mathrm{T}}\right)^{(j)} \right\rangle = \delta_{ij}, \\ \langle u, Bu\rangle = \lambda_1 \oplus \lambda_2, \\ \langle v, Bv\rangle = \lambda_1 \oplus \lambda_2, \\ \lambda_1 u_i \oplus u_i v_i \oplus \lambda_2 v_i \oplus \left(B \oplus B^{\mathrm{T}}\right)_i B \left(B \oplus B^{\mathrm{T}}\right)^{(i)} \oplus b_{ii} = 0, \\ i, j = 1, 2, \dots, m. \end{cases} \tag{$\star$}$$

These relations form the criteria of (anti-)self-duality of a bent function and we implicitly join here the requirement that the matrix $B \oplus B^{\mathrm{T}}$ has full rank and also take into account linear independence of u and v.

We are to provide the construction that satisfies criteria $\star$. Let the matrix B and vectors u, v be equal to

$$B = \begin{pmatrix} b_{11} & 1 & 1 & \cdots\cdots\cdots & & 1 & 1 \\ 0 & b_{22} & 0 & \cdots\cdots & 0 & 1 & 0 \\ 0 & 0 & b_{33} & 0 & \cdot^{\cdot^{\cdot}} & 0 & 0 \\ \vdots & & & \ddots\ 1 & & & \vdots \\ \vdots & & & & \ddots & & \vdots \\ \vdots & & & & & \ddots & \vdots \\ \vdots & & & & & \ddots & 0 \\ 0 & \cdots & \cdots & \cdots\cdots\cdots & & 0 & b_{mm} \end{pmatrix} \quad u = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \quad v = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$$

for some $b_{11}, b_{22}, \dots, b_{mm} \in \mathbb{F}_2$. These numbers must satisfy the following consistent system of m linear equations:

$$\begin{cases} \bigoplus_{i=1}^{m} b_{ii} \oplus (m/2) = \lambda_1 \oplus \lambda_2, \\ b_{11} \oplus b_{kk} \oplus b_{m-k+1,m-k+1} = \lambda_2 \oplus 1, \quad \text{for all } k \in \{2, 3, \dots, m-1\}, \\ b_{11} \oplus b_{mm} = \lambda_1 \oplus \lambda_2 \oplus 1, \end{cases}$$

which has rank $m/2$ or $m/2+1$, depending the parity of m. So any solution yields either self-dual or anti-self-dual quadratic bent function with bent subfunctions and nonzero Gramian.

If we obtain an anti-self-dual bent function, say f, then just apply the following transformation:

$$\begin{pmatrix} G_0 \\ G_1 \\ G_3 \\ G_4 \end{pmatrix} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & I_{2^{n-2}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & I_{2^{n-2}} \\ -I_{2^{n-2}} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & -I_{2^{n-2}} & \mathbf{0} & \mathbf{0} \end{pmatrix} \begin{pmatrix} F_0 \\ F_1 \\ F_3 \\ F_4 \end{pmatrix},$$

that maps it to the self-dual quadratic bent function g. It follows from the fact that the affine mapping

$$f(y_1, y_2, x) \to f(y_1 \oplus 1, y_2, x) \oplus y_1, \quad y_1, y_2 \in \mathbb{F}_2, x \in \mathbb{F}_2^m,$$

is a bijection between the sets of self-dual and anti-self-dual bent functions, see [8, 18, 22]. However the function g has Gram matrix

$$\text{Gram}(g) = \begin{pmatrix} 2^{n-2} & -b & -b & -a \\ -b & 2^{n-2} & a & b \\ -b & a & 2^{n-2} & b \\ -a & b & b & 2^{n-2} \end{pmatrix},$$

for which it holds $\text{Gramian}(g) = \text{Gramian}(f)$.

For now we can give an answer to the question about necessity of singularity of the Gram matrix for the subfunctions to be bent that is to resolve the converse of Theorem 3.

Theorem 4 *For every even $n \geq 6$ there exists a (quadratic) self-dual bent function f in n variables with invertible Gram matrix, such that subfunctions $\{f_i\}_{i=0}^3$ are bent.*

One can show that this assertion holds also for anti-self-dual bent functions. For proof it is enough to consider aforementioned one-to-one correspondence between the sets of self-dual and anti-self-dual bent functions.

From Theorem 4 and properties of the Gram matrix we again conclude that

Corollary 3 *For every even $n \geq 6$ there exists a self-dual bent function f in n variables whose subfunctions $\{f_i\}_{i=0}^3$ are bent functions with linearly independent sign vectors.*

Thus, the converse of Theorem 3 does not hold for $n \geq 6$, that is the linear dependence of sign vectors provides only **sufficient** condition for subfunctions in $n-2$ variables to be bent. It is also clear why this does not hold for $n = 4$ since there are only two distinct vectors in $\mathbb{F}_2^2$ that could satisfy the criteria $(\star)$: (00) and (11), but these vectors are linearly dependent.

6 New iterative constructions and lower bound for the cardinality of the set of self-dual bent functions

In current section we propose three new constructions **C3**, **C4** and **C5** of self-dual bent functions. The constructions use a 4-variables step. Let h be a bent function in $n-4$ variables, r be a self-dual bent function in $n-4$ variables and g be an anti-self-dual bent function in $n-4$ variables.

- the construction **C3**:

$$\left(h, g, g\oplus 1, h, \widetilde{h}, r, r\oplus 1, \widetilde{h}, \widetilde{h}, r\oplus 1, r, \widetilde{h}, h\oplus 1, g, g\oplus 1, h\oplus 1\right)$$

  It is clear that the subfunctions f_0, f_1, f_2, f_3 are bent;
- the construction **C4**:

$$\left(h, g, \widetilde{h}, r, g\oplus 1, h, r\oplus 1, \widetilde{h}, \widetilde{h}, r\oplus 1, h\oplus 1, g, r, \widetilde{h}, g\oplus 1, h\oplus 1\right)$$

  The subfunctions f_0, f_1, f_2, f_3 are bent if and only if $h\oplus\widetilde{h}\oplus r\oplus g=0$, so in some cases we do not obtain bent decompositions. Thus, this construction also yields a class of bent functions which cannot be decomposed into the concatenation of four bent functions;
- the construction **C5**:

$$\left(h, h\oplus 1, \widetilde{h}, \widetilde{h}, h, h, \widetilde{h}\oplus 1, \widetilde{h}, \widetilde{h}, \widetilde{h}, h\oplus 1, h, \widetilde{h}\oplus 1, \widetilde{h}, h\oplus 1, h\oplus 1\right)$$

  It is clear that the subfunctions f_0, f_1, f_2, f_3 are bent.

It is possible to estimate the **C4** case related with the (im)possibility of a bent decomposition:

Proposition 5 *The number of self-dual bent functions in $n\geq 8$ variables constructed via **C4**, which cannot be (can be) decomposed into the concatenation of four bent functions, is at least $2\left|\mathcal{SB}^+_{n-6}\right|^2$.*

Proof Let r_1 and r_2 be two bent functions in $n-6$ variables $x_7, x_8, \ldots, x_n$, such that the first one is either self-dual or anti-self-dual while the second is a self-dual one. Define

$$\begin{aligned} f\left(x_5, x_6, x_7, \ldots, x_n\right) &= x_5x_6\oplus r_1\left(x_7, x_8, \ldots, x_n\right), \\ g\left(x_5, x_6, x_7, \ldots, x_n\right) &= x_5x_6\oplus x_5\oplus x_6\oplus r_1\left(x_7, x_8, \ldots, x_n\right), \\ h\left(x_5, x_6, x_7, \ldots, x_n\right) &= x_5x_6\oplus x_5\oplus r_2\left(x_7, x_8, \ldots, x_n\right), \end{aligned}$$

one can check that

$$\widetilde{h}\left(x_5, x_6, x_7, \ldots, x_n\right) = x_5x_6\oplus x_6\oplus r_2\left(x_7, x_8, \ldots, x_n\right).$$

Thus, the self-dual bent function constructed via **C4**, is the concatenation of four bent functions.

Finally, note that in order to obtain the function which is not the concatenation of four bent functions, it is enough to take a negation of the two-variables part of either f or g, for instance

$$f\left(x_5, x_6, x_7, \ldots, x_n\right) = x_5x_6\oplus 1\oplus r_1\left(x_7, x_8, \ldots, x_n\right).$$

□

Table 3 Iterative lower bounds and lower bounds provided by some primary constructions

Class	$n = 2$	$n = 4$	$n = 6$	$n = 8$
Dillon's class $\mathcal{PS}_{ap}$ [8]	2	2	6	70
Maiorana–McFarland class [8]	2	8	48	768
Quadratic functions [18]	2	20	752	$\cong 2^{16.68}$
Direct sum [8]	—	8	80	$\cong 2^{17.39}$
Construction **C1** [8]	—	8	896	$\cong 2^{32.34}$
Constructions **C1**, **C2** [21]	—	12	1296	$\cong 2^{32.7606}$
Constructions **C1**, **C2**, **C3**, **C4**, **C5**	—	—	1332	$\cong 2^{32.7607}$
Exact number [8, 14]	2	20	42896	$\geq 2^{50.56}$

The constructions **C3**, **C4** and **C5** have the following Gram matrices:

$$\mathrm{Gram}(\mathbf{C3}) = \begin{pmatrix} 2^{n-2} & 2\mathcal{S}_h & 2\mathcal{S}_h & 0 \\ 2\mathcal{S}_h & 2^{n-2} & 0 & -2\mathcal{S}_h \\ 2\mathcal{S}_h & 0 & 2^{n-2} & -2\mathcal{S}_h \\ 0 & -2\mathcal{S}_h & -2\mathcal{S}_h & 2^{n-2} \end{pmatrix},$$

$$\mathrm{Gram}(\mathbf{C4}) = \begin{pmatrix} 2^{n-2} & 0 & 0 & 0 \\ 0 & 2^{n-2} & 0 & 0 \\ 0 & 0 & 2^{n-2} & 0 \\ 0 & 0 & 0 & 2^{n-2} \end{pmatrix},$$

$$\mathrm{Gram}(\mathbf{C5}) = \begin{pmatrix} 2^{n-2} & 0 & 0 & -4\mathcal{S}_h \\ 0 & 2^{n-2} & 4\mathcal{S}_h & 0 \\ 0 & 4\mathcal{S}_h & 2^{n-2} & 0 \\ -4\mathcal{S}_h & 0 & 0 & 2^{n-2} \end{pmatrix}$$

with parameters $a = 0$, $b = 2\mathcal{S}_h$, $a = b = 0$ and $a = 4\mathcal{S}_h, b = 0$, correspondingly. The Gramian of **C3** is equal to $2^{4n-8} - 2^{2n}\mathcal{S}_h^2$ hence it is nonzero besides the case $|\mathcal{S}_h| = 2^{n-4}$, that is when h is either self-dual or anti-self-dual bent. The Gramian of **C4** is equal to 2^{4n-8}. The Gramian of **C5** is equal to $\left(2^{2n-4} - 16\mathcal{S}_h^2\right)^2$, hence it is nonzero besides the case $|\mathcal{S}_h| = 2^{n-4}$, that is again when h is either self-dual or anti-self-dual bent.

Note that the constructions **C1**, **C2**, **C3** and **C4** provide disjoint sets of self-dual bent functions whereas **C5** has clear intersection with **C1** and **C2**. So we conclude that the sum of the cardinalities of the first four constructions and the disjoint part of **C5** is a lower bound for the cardinality of the set of self-dual bent functions in n variables.

Theorem 5 *The number of self-dual bent functions in $n \geq 6$ variables is at least*

$$|\mathcal{B}_{n-2}| + \left|\mathcal{SB}^+_{n-2}\right|^2 + |\mathcal{B}_{n-4}|\left(2\left|\mathcal{SB}^+_{n-4}\right|^2 + 1\right) - 2\left|\mathcal{SB}^+_{n-4}\right|.$$

Thus, it increases the previous iterative bound $|\mathbf{C1}| + |\mathbf{C2}|$ by the summand that corresponds to the constructions that exploit functions in $n - 4$ variables. The comparison with other iterative bounds and lower bounds provided by some primary constructions is given in Table 3. Note that constructions **C1**, **C2** can be build via the so-called indirect sum construction [8] of self-dual bent functions but it is difficult to estimate its cardinality for large n.

7 Decomposition of the form (f_0, f_1, f_2, f_3) for the general case

In this section the form and properties of the Gram matrix of an *arbitrary* bent function are considered.

It is interesting to study the conditions when the subfunctions f_0, f_1, f_2, f_3 of the function itself and its dual are bent simultaneously. In current section we give an example of the property of the initial bent function that provides such double bentness.

7.1 General form of the Gram matrix

The form of the Gram matrix of a bent function and its dual one is characterized by the following

Theorem 6 *The Gram matrices of any bent function, say f, in n variables and its dual bent function $\widetilde{f}$ have form*

$$\mathrm{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & c & -a \\ b & 2^{n-2} & a & -c \\ c & a & 2^{n-2} & -b \\ -a & -c & -b & 2^{n-2} \end{pmatrix}, \qquad \mathrm{Gram}\big(\widetilde{f}\big) = \begin{pmatrix} 2^{n-2} & c & b & -a \\ c & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -c \\ -a & -b & -c & 2^{n-2} \end{pmatrix},$$

where a, b, c are even integers such that

$$-2^{n-2} + |b+c| \le a \le 2^{n-2} - |b-c|.$$

Proof Recall the subsystem from the proof of Theorem 2, obtained via the inner products $\langle 2\mathcal{H}R_i, 2\mathcal{H}R_i\rangle$, $i = 0, 1, 2, 3$:

$$\begin{cases} g_{01} + g_{02} + g_{03} + g_{12} + g_{13} + g_{23} = 0, \\ g_{01} - g_{02} + g_{03} + g_{12} - g_{13} + g_{23} = 0, \\ g_{01} - g_{02} - g_{03} - g_{12} - g_{13} + g_{23} = 0, \\ g_{01} + g_{02} - g_{03} - g_{12} + g_{13} + g_{23} = 0. \end{cases} \tag{11}$$

This system has rank 3, its general solution is

$$\begin{array}{lll} g_{01} = -g_{23}, & g_{02} = -g_{13}, & g_{03} = -g_{12}, \\ & g_{12} = g_{12}, & g_{13} = g_{13}, \\ & & g_{23} = g_{23} \end{array}$$

for g_{12}, g_{13} and g_{23} being free variables. Denote $a = g_{12}$, $b = -g_{23}$ and $c = -g_{13}$, then we obtain the desired form of the Gram matrix:

$$\begin{pmatrix} 2^{n-2} & b & c & -a \\ b & 2^{n-2} & a & -c \\ c & a & 2^{n-2} & -b \\ -a & -c & -b & 2^{n-2} \end{pmatrix}.$$

We can also deduce that the Gram matrix of the dual function is strictly connected with the matrix of the function itself. Since the dual function $\widetilde{f}$ is bent as well, it is enough to investigate the first row of its Gram matrix. We have

$$\begin{aligned}\langle 2\mathcal{H}R_0, 2\mathcal{H}R_1\rangle &= \langle F_0+F_1+F_2+F_3, F_0-F_1+F_2-F_3\rangle\\ &= 2g_{02}-2g_{13} = 2c-2(-c) = 4c,\\ \langle 2\mathcal{H}R_0, 2\mathcal{H}R_2\rangle &= \langle F_0+F_1+F_2+F_3, F_0+F_1-F_2-F_3\rangle\\ &= 2g_{01}-2g_{23} = 2b-2(-b) = 4b,\\ \langle 2\mathcal{H}R_0, 2\mathcal{H}R_3\rangle &= \langle F_0+F_1+F_2+F_3, F_0-F_1-F_2+F_3\rangle\\ &= 2g_{03}-2g_{12} = 2(-a)-2a = -4a,\end{aligned}$$

hence $\langle R_0, R_1\rangle = c$, $\langle R_0, R_2\rangle = b$ and $\langle R_0, R_3\rangle = -a$.

Now we are to point essential bounds on values of a, b and c and deduce some relations between them. In order to do it recall that any Gram matrix is positive semi-definite, hence all its eigenvalues must be nonnegative. The matrix $\mathrm{Gram}(f)$ has four eigenvalues, they are

$$\begin{aligned}\lambda_1 &= 2^{n-2}-a+b-c,\\ \lambda_2 &= 2^{n-2}-a-b+c,\\ \lambda_3 &= 2^{n-2}+a-b-c,\\ \lambda_4 &= 2^{n-2}+a+b+c.\end{aligned}$$

One can note that these numbers are nonnegative if and only if

$$\begin{aligned}a &\le 2^{n-2} \pm (b-c),\\ a &\ge -2^{n-2} \pm (b+c),\end{aligned}$$

that is

$$\begin{aligned}a &\le 2^{n-2} + \min\{b-c, c-b\},\\ a &\ge -2^{n-2} + \max\{b+c, -b-c\},\end{aligned}$$

and, consequently,

$$\begin{aligned}a &\le 2^{n-2} - |b-c|,\\ a &\ge -2^{n-2} + |b+c|,\end{aligned}$$

where $|b|$ and $|c|$ are essentially bounded by 2^{n-2} from above. Parity of the numbers a, b, c comes from the fact that they are are inner products of integer vectors of an even dimension having odd coordinates. □

Thus, the duality mapping acts on the Gram matrix by switching values of the coefficients b and c. One can show that these matrices are singular simultaneously and, moreover,

Corollary 4 *The matrices* $\mathrm{Gram}(f)$ *and* $\mathrm{Gram}\big(\widetilde{f}\big)$ *have the same spectrum.*

Theorem 6 can be reformulated in terms of Hamming distances between subfunctions:

Corollary 5 *Let f be a bent function in n variables. The Hamming distances between $\{f_i\}_{i=0}^3$ are characterized by the matrix*

$$\mathrm{Dist}(f) = \begin{pmatrix} 0 & 0 & 0 & 2^{n-2}\\ 0 & 0 & 0 & 2^{n-2}\\ 0 & 0 & 0 & 2^{n-2}\\ 2^{n-2} & 2^{n-2} & 2^{n-2} & 0 \end{pmatrix} + 2\begin{pmatrix} 0 & d_2 & d_3 & -d_1\\ d_2 & 0 & d_1 & -d_3\\ d_3 & d_1 & 0 & -d_2\\ -d_1 & -d_3 & -d_2 & 0 \end{pmatrix}$$

for some positive integers d_1, d_2, d_3 such that

$$|d_2 - d_3| \le d_1 \le 2^{n-2} - \left|2^{n-2} - d_2 - d_3\right|,$$
$$\left|2^{n-2} - 2 \cdot \min(d_2, d_3)\right| \le d_1 + \left|2^{n-2} - d_2 - d_3\right|.$$

Proof The relation between the inner product and the Hamming distance yields the matrix whereas the inequalities are obtained from

$$-2^{n-2} + |b + c| \le a \le 2^{n-2} - |b - c|$$

with

$$a = 2^{n-2} - 2d_1, \qquad b = 2^{n-2} - 2d_2, \qquad c = 2^{n-2} - 2d_3.$$

□

7.2 Linear dependence and bentness

In this subsection we are to consider the connection between singularity of the Gram matrix of an arbitrary bent function and bentness of its subfunctions.

We will need the following

Lemma 1 *Let f and g be Boolean functions in even number k of variables, such that $W_f(y), W_g(y) \in \left\{0, \pm 2^{k/2}, \pm 2^{(k+2)/2}\right\}$ for any $y \in \mathbb{F}_2^k$ and*

$$\sum_{x,y \in \mathbb{F}_2^k} (-1)^{f(x) \oplus g(y) \oplus \langle x,y \rangle} = 2^{3k/2}. \tag{12}$$

Then f and g are bent functions, moreover, it holds $g = \widetilde{f}$.

Proof Consider five nonnegative integers

$$t_0 = \left|\left\{y \in \mathbb{F}_2^k : W_f(y) = 0\right\}\right|,$$
$$t_1 = \left|\left\{y \in \mathbb{F}_2^k : (-1)^{g(y)} W_f(y) = 2^{k/2}\right\}\right|,$$
$$t_2 = \left|\left\{y \in \mathbb{F}_2^k : (-1)^{g(y)} W_f(y) = -2^{k/2}\right\}\right|,$$
$$t_3 = \left|\left\{y \in \mathbb{F}_2^k : (-1)^{g(y)} W_f(y) = 2^{(k+2)/2}\right\}\right|,$$
$$t_4 = \left|\left\{y \in \mathbb{F}_2^k : (-1)^{g(y)} W_f(y) = -2^{(k+2)/2}\right\}\right|.$$

Then we have the following system

$$\begin{cases} t_0 + t_1 + t_2 + t_3 + t_4 = 2^k, \\ (t_1 + t_2)\, 2^k + (t_3 + t_4)\, 2^{k+2} = 2^{2k}, \\ (t_1 - t_2)\, 2^{k/2} + (t_3 - t_4)\, 2^{(k+2)/2} = 2^{3k/2}, \end{cases}$$

where the second equation follows from the Parseval's identity applied for the function g, and the third one is the product (12). The only nonnegative solution is

$$t_0 = 0, \qquad t_1 = 2^k, \qquad t_2 = 0, \qquad t_3 = 0, \qquad t_4 = 0.$$

Hence, we have $\left|W_f(y)\right| = 2^{k/2}$ for any $y \in \mathbb{F}_2^k$.

By the same arguments one can show that $\left|W_g(y)\right| = 2^{k/2}$ for any $y \in \mathbb{F}_2^k$, therefore both of f and g are bent functions. Finally, it is enough to note that in this case the product (12) is exactly

$$\sum_{x,y\in\mathbb{F}_2^k} (-1)^{f(x)\oplus g(y)\oplus\langle x,y\rangle} = 2^{k/2}\sum_{y\in\mathbb{F}_2^k}(-1)^{\widetilde{f}(y)\oplus g(y)} = 2^{3k/2},$$

that is $\widetilde{f} = g$. □

For a bent function f with the Gram matrix $\mathrm{Gram}(f)$ the Gramian has the following expression

$$\begin{aligned}\mathrm{Gramian}(f) = &\left(2^{n-2} - a + b - c\right)\left(2^{n-2} - a - b + c\right)\left(2^{n-2} + a - b - c\right)\\ &\times\left(2^{n-2} + a + b + c\right).\end{aligned} \tag{13}$$

In Sect. 4.4 it was proved that the singularity of the Gram matrix of a self-dual bent function implies bentness of its subfunctions. It appears that this fact holds for *any* bent function as well.

Theorem 7 *If the Gram matrix of a bent function f is singular, then subfunctions $\{f_i\}_{i=0}^3$ are bent. Moreover, the subfunctions of $\widetilde{f}$ are also bent.*

Proof It is enough to consider all such combinations of a, b, c that the Gramian (13) is zero. We will consider all the cases separately.

$2^{n-2} - a + b - c = 0$: in terms of sign vectors it is equivalent to the following

$$2^{n-2} + \langle F_0, F_1 - F_2 + F_3\rangle = 0.$$

From system (5) it follows that

$$\begin{cases} F_0 + (-F_1 + F_2 - F_3) = 2\mathcal{H}R_1,\\ \langle F_0, -F_1 + F_2 - F_3\rangle = 2^{n-2},\end{cases}$$

that after simple transformations becomes

$$\begin{cases} -F_1 + F_2 - F_3 = 2\mathcal{H}R_1 - F_0,\\ \langle F_0, \mathcal{H}R_1\rangle = 2^{n-2}.\end{cases}$$

By Lemma 1 from the second equation we obtain that F_0 and R_1 are sign vectors of bent functions.

For other cases it is sufficient to list the systems, the rest of considerations are the same.

$2^{n-2} - a - b + c = 0$:

$$\begin{cases} F_1 - F_2 - F_3 = 2\mathcal{H}R_2 - F_0,\\ \langle F_0, \mathcal{H}R_2\rangle = 2^{n-2};\end{cases}$$

$2^{n-2} + a - b - c = 0$:

$$\begin{cases} F_1 + F_2 + F_3 = 2\mathcal{H}R_0 - F_0,\\ \langle F_0, \mathcal{H}R_0\rangle = 2^{n-2};\end{cases}$$

$2^{n-2}+a+b+c=0$:

$$\begin{cases} -F_1-F_2+F_3=2\mathcal{H}R_3-F_0, \\ \langle F_0,\mathcal{H}R_3\rangle=2^{n-2}. \end{cases}$$

□

Again, from Theorem 7 and properties of the Gram matrix we conclude that

Corollary 6 *If sign vectors of subfunctions $\{f_i\}_{i=0}^3$ of a bent function f are linearly dependent, then these subfunctions are bent. Moreover, the subfunctions of $\widetilde{f}$ are bent as well.*

We can also consider 4×4 integer matrix, say M, with elements

$$m_{ij}=\left\langle F_i,\mathcal{H}R_j\right\rangle=\left\langle \mathcal{H}F_i,R_j\right\rangle.$$

In order to calculate its elements one can refer to the system (5) and consider inner products of equations with sign vectors of the subfunctions of f. The matrix $\frac{1}{2}M$ is the following

$$\begin{pmatrix} 2^{n-2}-a+b+c & 2^{n-2}+a-b+c & 2^{n-2}+a+b-c & 2^{n-2}-a-b-c \\ 2^{n-2}+a+b-c & -2^{n-2}+a+b+c & 2^{n-2}-a+b+c & -2^{n-2}-a+b-c \\ 2^{n-2}+a-b+c & 2^{n-2}-a+b+c & -2^{n-2}+a+b+c & -2^{n-2}-a-b+c \\ 2^{n-2}-a-b-c & -2^{n-2}-a-b+c & -2^{n-2}-a+b-c & 2^{n-2}-a+b+c \end{pmatrix}$$

It is clear that it is symmetric if and only if $b=c$. This matrix provides one more condition for bentness of subfunctions.

Proposition 6 *If matrix M of a bent function f is singular, then the subfunctions $\{f_i\}_{i=0}^3$ are bent. Moreover, the subfunctions of $\widetilde{f}$ are bent as well.*

Proof It is enough to straightly calculate the eigenvalues of the matrix M and consider cases when at least one of them is zero. The eigenvalues are

$$\begin{aligned} \mu_1&=\sqrt{\left(2^{n-2}-a\right)^2-(b-c)^2}, \\ \mu_2&=-\sqrt{\left(2^{n-2}-a\right)^2-(b-c)^2}, \\ \mu_3&=-2^{n-2}-a+b+c, \\ \mu_4&=2^{n-2}+a+b+c. \end{aligned}$$

Note that $\mu_3=-\lambda_3$ and $\mu_4=\lambda_4$. The eigenvalues $\mu_{1,2}$ are zero if and only if $2^{n-2}-a=|b-c|$, but it implies that either $\lambda_1=0$ or $\lambda_2=0$. So, in all cases we have that at least one of the eigenvalues of the matrix $\mathrm{Gram}(f)$ is zero, hence from Theorem 7 the result follows. □

Thus, we obtain the properties of a matrix that consists of the inner products between sign vectors of subfunctions of a bent function and its dual. Whereas one of vectors is given in its Walsh–Hadamard transform.

8 Conclusion

In this work we studied the decompositions of the vector of values of a self-dual bent function and introduced the notation of the Gram matrix of a bent function. It is interesting to continue the study of this matrix and obtain new metrical relations between subfunctions of an arbitrary (self-dual) bent function. The search of the constructions of bent functions with particular Gram matrix is also a goal worth pursuing.

Subfunctions, considered in this work, were obtained by fixation of one or two first variables. We can also consider another way of choosing them, for instance by fixing some planes of dimension $n - 1$ and $n - 2$.

Considering the Gram matrices for the constructions **C1** and **C3** we can conclude that the problem of the classification of Gram matrices of self-dual bent functions (even in the case when all subfunctions are bent) comprises the problem of finding all values of the Rayleigh quotient that can be achieved by some of their subfunctions. The last problem has intersection with the investigation of the Hamming distances spectrum between bent functions and their duals.

Here we list main notation and results on the Gram matrix of a bent function, presented in current work:

$f = (f_0, f_1, f_2, f_3)$ — decomposition of the vector of values of a (self-dual) bent function f in n variables

$$g_{ij} = \sum_{x \in \mathbb{F}_2^{n-2}} (-1)^{f_i(x) \oplus f_j(x)}$$

$\mathrm{Gram}(f) = \left(g_{ij}\right)$ — the Gram matrix of the function f

General form of the Gram matrix of bent function and its dual one:

$$\mathrm{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & c & -a \\ b & 2^{n-2} & a & -c \\ c & a & 2^{n-2} & -b \\ -a & -c & -b & 2^{n-2} \end{pmatrix}$$

$$\mathrm{Gram}\left(\widetilde{f}\right) = \begin{pmatrix} 2^{n-2} & c & b & -a \\ c & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -c \\ -a & -b & -c & 2^{n-2} \end{pmatrix}$$

The determinant of the Gram matrix:

$$\mathrm{Gramian}(f) = \left(2^{n-2} - a + b - c\right)\left(2^{n-2} - a - b + c\right)\left(2^{n-2} + a - b - c\right) \times \left(2^{n-2} + a + b + c\right)$$

If the Gramian is equal to zero, all subfunctions $\{f_i\}_{i=0}^3$ are bent. The converse holds for $n = 4$ if the considered function is self-dual and does not hold for $n \geq 6$.

Acknowledgements The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. FWNF-2022-0018).

References

1. Adams C.M., Tavares S.E.: Generating bent sequences. Discret. Appl. Math. **39**, 155–159 (1992).

2. Bapić A., Pasalic E., Zhang F., Hodžić S.: Constructing new superclasses of bent functions from known ones. Cryptogr. Commun. **14**(6), 1229–1256 (2022).
3. Canteaut A., Charpin P.: Decomposing bent functions. IEEE Trans. Inform. Theory **49**(8), 2004–2019 (2003).
4. Canteaut A., Carlet C., Charpin P., Fontaine C.: On cryptographic properties of the cosets of $R(1, m)$. IEEE Trans. Inform. Theory **47**(4), 1494–1513 (2001).
5. Carlet C.: Two new classes of bent functions. In: Advances in Cryptology—EUROCRYPT '93, pp. 77–101 Part of the Lecture Notes in Computer Science book series (LNCS, volume 765) (1994).
6. Carlet C.: Boolean Functions for Cryptography and Coding Theory (2020).
7. Carlet C., Mesnager S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016).
8. Carlet C., Danielsen L.E., Parker M.G., Solé P.: Self-dual bent functions. Int. J. Inf. Coding Theory **1**, 384–399 (2010).
9. 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 **2014** (2014). Article ID 701298.
10. Cusick T.W., Stănică P.: Cryptographic Boolean Functions and Applications, 2nd edn. (2017).
11. Danielsen L.E., Parker M.G., Solé P.: The Rayleigh quotient of bent functions. In: Cryptography and Coding, pp. 418–432 Part of the Lecture Notes in Computer Science book series (LNCS, volume 5921) (2009).
12. Dillon J.: A survey of bent functions, pp. 191–215 (1972).
13. Dillon J.F.: Elementary Hadamard difference sets. PhD thesis, Univ. of Maryland (1974).
14. 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).
15. Givens C.R.: Some observations on eigenvectors of Hadamard matrices of order 2^n. Linear Algebra Appl. **56**, 245–250 (1984).
16. Hodžić S., Pasalic E., Wei Y.: A general framework for secondary constructions of bent and plateaued functions. Des. Codes Cryptogr. **88**(10), 2007–2035 (2020).
17. Hodžić S., Pasalic E., Zhang W.: Generic constructions of five-valued spectra Boolean functions. IEEE Trans. Inform. Theory **65**(11), 7554–7565 (2019).
18. Hou X.-D.: Classification of self dual quadratic bent functions. Des. Codes Cryptogr. **63**(2), 183–198 (2012).
19. 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).
20. Kutsenko A.V.: The Hamming distance spectrum between self-dual Maiorana-McFarland bent functions. J. Appl. Ind. Math. **12**(1), 112–125 (2018).
21. Kutsenko A.: Metrical properties of self-dual bent functions. Des. Codes Cryptogr. **88**(1), 201–222 (2020).
22. Kutsenko A.: The group of automorphisms of the set of self-dual bent functions. Cryptogr. Commun. **12**(5), 881–898 (2020).
23. Kutsenko A., Tokareva N.: Metrical properties of the set of bent functions in view of duality. Appl. Discret. Math. **49**, 18–34 (2020).
24. Kuz'min A.S., Markov V.T., Nechaev A.A., Shishkin V.A., Shishkov A.B.: Bent and hyper-bent functions over a field of 2^l elements. Probl. Inf. Transm. **44**(1), 12–33 (2008).
25. Li Y., Kan H., Mesnager S., Peng J., Tan C.H., Zheng L.: Generic constructions of (Boolean and vectorial) bent functions and their consequences. IEEE Trans. Inform. Theory **68**(4), 2735–2751 (2022).
26. Logachev O.A., Sal'nikov A.A., Yashchenko V.V.: Bent functions on a finite abelian group. Discret. Math. Appl. **7**(6), 547–564 (1997).
27. Luo G., Cao X., Mesnager S.: Several new classes of self-dual bent functions derived from involutions. Cryptogr. Commun. **11**(6), 1261–1273 (2019).
28. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes (1977).
29. Mesnager S.: Bent Functions: Fundamentals and Results (2016).
30. Mesnager S.: On semi-bent functions and related plateaued functions over the Galois field $\mathbb{F}_{2^n}$, pp. 243–273 (2014).
31. Mesnager S.: Several new infinite families of bent functions and their duals. IEEE Trans. Inform. Theory **60**(7), 4397–4407 (2014).
32. Pasalic E., Bapić A., Zhang F., Wei Y.: Explicit infinite families of bent functions outside the completed Maiorana-McFarland class. Des. Codes Cryptogr. **91**(7), 2365–2393 (2023).
33. Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandewalle J.: Propagation characteristics of Boolean functions. In: Advances in Cryptology—EUROCRYPT '90, pp. 161–173 (LNCS, volume 473) (1991).
34. Rifá J., Zinoviev V.A.: On binary quadratic symmetric bent and almost bent functions. arXiv:1211.5257v3.

35. Rothaus O.S.: On "bent" functions. J. Comb. Theory Ser. A. **20**(3), 300–305 (1976).
36. Shi M., Li Y., Cheng W., Crnković D., Krotov D., Solé P.: Self-dual bent sequences for complex Hadamard matrices. Des. Codes Cryptogr. **91**(4), 1453–1474 (2023).
37. Shi M., Li Y., Cheng W., Crnković D., Krotov D., Solé P.: Self-dual Hadamard bent sequences. J. Syst. Sci. Complex **36**(2), 894–908 (2023).
38. Su S., Guo X.: A further study on the construction methods of bent functions and self-dual bent functions based on Rothaus's bent function. Des. Codes Cryptogr. **91**(4), 1559–1580 (2023).
39. Tang C., Zhou Z., Qi Y., Zhang X., Fan C., Helleseth T.: Generic construction of bent functions and bent idempotents with any possible algebraic degrees. J. Pure Appl. Algebra **63**(10), 6149–6157 (2017).
40. Tokareva N.: On the number of bent functions from iterative constructions: lower bounds. Adv. Math. Commun. **5**(4), 609–621 (2011).
41. Tokareva N.: Bent Functions: Results and Applications to Cryptography (2015).
42. Wolfmann J.: Special bent and near-bent functions. Adv. Math. Commun. **8**(1), 21–33 (2014).
43. Yarlagadda R., Hershey J.: A note on the eigenvectors of Hadamard matrices of order 2^n. Linear Algebra Appl. **45**, 43–53 (1982).