Annales Univ. Sci. Budapest., Sect. Comp. 58 (2025) nn–nnn

HAAR SPECTRA OF GENERALIZED BOOLEAN BENT FUNCTIONS

Radomir S. Stanković and Milena Stanković (Niš, Serbia)
Claudio Moraga (Dortmund, Germany)
Jaakko Astola (Tampere, Finland)

Communicated by László Szili

(Received 29 April 2025; accepted 3 July 2025)

Abstract. This paper presents a discussion of Haar spectra for Generalized Boolean bent functions. The definition and multiresolution feature of Haar coefficients and their organization into packets provides a deeper insight into bent functions and their properties. It is shown that manipulation of packets of Haar coefficients for binary bent functions leads to the Generalized Boolean bent functions. The presentation is restricted to functions in $n = 4$ variables, since in this case a direct examination of examples is easily realisable. Possibilities for a straightforward extension to functions of a larger number of variables are illustrated by examples for $n = 6$.

1. Introduction

Bent functions are important mathematical, more concretely, combinatorial objects that are interesting not just because imposing various challenging theoretical tasks, such as methods of their construction, study of properties, enumeration, and related issues, but also due to their practical applications, notably in cryptography, but also in related areas [1], [6], [24].

Bent functions are a subset of Boolean functions with particular properties. They are defined as the most non-linear Boolean functions, since they are at

Key words and phrases: Bent functions, Generalized Boolean bent functions, Walsh transform, Haar transform.
2010 Mathematics Subject Classification: 42C40, 42C10, 94D10.
https://doi.org/10.71352/ac.58.030725
Published online: 9 July 2025

the farthest possible Hamming distance from all affine Boolean functions. Due to this feature, bent functions are resistant to linear and differential attacks, which makes them useful in cryptography [1], [6], [24]. For instance, bent functions are used in constructing low correlation sequences, then in the design of substitution boxes (S-boxes) in block ciphers like AES or DES. See, for instance [7]. They are also useful in constructing error-correcting codes with good distance properties.

Various generalizations of bent functions have been studied after the concept was published in [10] in connection with the notions as the generalized nonlinearity for functions that are relevant to generalized linear cryptanalysis. We refer to [23] for a review of various related concepts. They are useful for the same reasons as the binary bent functions, but in the context of non-binary systems, such as, for example, Quaternary DS-CDMA Systems, construction of quaternary sequences with low correlation, quantum error-correcting codes, etc. See, for instance [14], [15].

In this paper, we consider a particular generalization of binary bent functions called Generalized Boolean bent functions. The term Boolean refers to the domain of the functions, i.e., they are functions in binary variables. The term generalized refers to the range, meaning that functions take values in a set of q elements. As mentioned above, an example interesting for practical applications is when $q = 4$ with these four values conveniently interpreted as the first four non-negative integers allowing a simple binary encoding of quaternary values.

We consider the Haar spectra of the Generalized Boolean functions for $q = 4$ with the motivation that the multiresolution feature of the Haar transform will provide a further insight into properties of these functions. This idea comes from the property that the Haar coefficients are computed over subsets of function values and the sizes of these subsets correspond to the sizes of patterns of values appearing in function vectors of linear Boolean functions. Such patterns should be avoided in the function vectors of bent functions to provide maximal non-linearity which is the main feature of bent functions. Therefore, analysis of Haar spectra and packets of Haar coefficients in the definition of the Haar transform can be useful in dealing with bent functions. In the present considerations, we show that Generalized Boolean bent functions for $q = 4$ can be constructed by manipulating packets of coefficients in the Haar spectra of binary bent functions.

2. Binary bent functions

As is usually done, we assume that a function f defined at 2^n points is represented by its function vector $\mathbf{F} = [f_0, f_1, \ldots, f_{2^n-1}]^T$ specifying the value which f takes at each point. In the case of binary Boolean functions and Generalized Boolean functions these values are in $\{0, 1\}$ and $\{0, 1, 2, 3\}$, respectively. When convenient, Boolean functions are also expressed by the positive polarity Reed-Muller expressions.

Boolean functions are defined as mappings $Z_2^n \to Z_2$, where Z_2 is the ring of non-negative integers smaller than 2, and n denotes the number of variables. Binary bent functions are a particular subset of Boolean functions, and since they exists just for an even number of variables [1], in what follows we assume that n is an even number.

Binary bent functions are defined as the most nonlinear Boolean functions in the sense that they are at the farthest possible distance of $2^{(n-1)} - 2^{(n/2-1)}$ from all affine functions [10]. Recall that affine functions are defined as linear Boolean functions, i.e., Boolean variables and their EXOR sums, plus complements of linear functions which means adding to each linear function the constant 1. The distance of objects in the space of Boolean functions is measured in terms of the Hamming distance that is defined as the number of places, i.e., positions in the function vectors, where the compared functions have different values.

In the spectral domain, bent functions are defined as functions having flat Walsh spectrum, see definition of the Walsh transform below, which means that for a bent function all the Walsh coefficients have absolute value equal $2^{n/2}$, where n is the number of variables. Binary bent functions must have a strictly specified number of non-zero values, either $\rho_1(n) = 2^{(n-1)} - 2^{(n/2-1)}$ or $\rho_2(n) = 2^{(n-1)} + 2^{(n/2-1)}$, which is a necessary, but not sufficient condition for bentness. In this respect, the set of all bent functions can be split into two subsets of functions that are logic complements of each other [6], [24].

3. Generalized Boolean bent functions

The Generalized Boolean bent functions are a particular extension of the concept of binary bent functions [16], [17]. They are defined as mappings $Z_2^n \to Z_q$, having flat Walsh spectra, where the symbol Z_q stands for the ring of integers smaller than q. Particularly interesting are Generalized Boolean functions for $q = 4$. A reason for that is the easy encoding of four values by two binary bits, i.e., $(0, 1, 2, 3) \to (00, 01, 10, 11)$. A Generalized Boolean function is conveniently represented as $f(x) = a(x) + 2b(x)$, $x = (x_1, x_2, \ldots, x_n)$, where a and b are Boolean functions defined by function vectors whose elements are determined respectively by the first and second bits in the binary encoding of quaternary values for the Generalized Boolean functions [16], [17].

For clarity and simplicity of presentation, in the present considerations, we discuss bent functions and Generalized Boolean bent functions just for the cases $n = 4, 6$ for $q = 2$, and $q = 4$, respectively. Extension to larger even values of n is rather straightforward since in the present considerations, we do not exploit directly the restriction on the number of variables, except to make the experiments feasible and their analysis manageable for all possible bent functions which in the case $n = 4$ is 896 functions. Examples of functions for $n = 6$ are provided to illustrate the ways of extensions.

4. Walsh and Haar transforms

The Walsh transform serves to define bent functions, while in this paper, the Haar transform is used to explore their properties. These transforms are defined in terms of the Walsh functions [25], and Haar functions [2], respectively. For processing discrete functions, we use discrete versions of these transforms, see, for instance, [3], [4], [5], [13], [18], [22].

In matrix notation, the discrete Walsh transform is defined by the $(2^n \times 2^n)$ transform matrix

$$\mathbf{W}(n) = \bigotimes_{i=1}^{n} \mathbf{W}(1), \quad \mathbf{W}(1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

where $\otimes$ denotes the Kronecker product of matrices.

We use the non-normalized Haar transform defined in matrix notation as the $(2^n \times 2^n)$ matrix

$$\mathbf{H}(n) = \begin{bmatrix} \mathbf{H}(n-1) & \otimes & \begin{bmatrix} 1 & 1 \end{bmatrix} \\ \mathbf{I}(n-1) & \otimes & \begin{bmatrix} 1 & -1 \end{bmatrix} \end{bmatrix},$$

where $\mathbf{H}(0) = [1]$, and $\mathbf{I}(n)$ is the $(2^n \times 2^n)$ identity matrix with $\mathbf{I}(0) = [1]$.

The Walsh functions take two values ± 1, while the Haar functions take three values, $-1, 0, 1$. By following the original approach introduced by A. Haar [2], the Haar functions are ordered by the number of non-zero values and the set of 2^n Haar functions is split into packets of functions having identical number of non-zero values. It means that the Haar coefficients in the spectrum are also arranged in packets, which is a feature that will be used later.

A function in n variables is specified by the vector $\mathbf{F} = [f_0, f_1, \ldots, f_{2^n-1}]^T$ of function values. The Haar spectrum is represented by a vector of Haar coefficients $\mathbf{S}_{f,h} = [s_0, s_1, \ldots, s_{2^n-1}]^T$ which is determined as

$$\mathbf{S}_{f,h} = \mathbf{H}(n)\mathbf{F}.$$

The Walsh spectrum represented by a vector $\mathbf{W}_{f,w} = [w_0, w_1, \ldots, w_{2^n-1}]^T$ is defined in the same way by using the Walsh transform matrix $\mathbf{W}(n)$ instead of the Haar transform matrix $\mathbf{H}(n)$.

When processing Boolean functions, it is a customary practice to use the encoding $(0,1) \to (1,-1)$ for Boolean values making in this way the functions to be processed more compatible with the Walsh and Haar functions that are the kernels of the Walsh and Haar transforms, respectively. For more details about the Walsh and Haar transforms and their applications we refer to [3], [4], [5], [11], [12], [13], [18], [22].

When defining Generalized Boolean bent function, we require that their Walsh spectrum is flat, but computation is done over the function vectors whose four function values are encoded as $(0,1,2,3) \to (1,i,-1,-i)$ [16], [17]. Notice that this encoding maps the elements of Z_4 to equidistant points on the unit circle of the complex plane.

Regarding bentness, it is shown in [16] that the following two statements are equivalent

1. The Generalized Boolean function f is bent in $2n$ variables.
2. Recall that $f(x) = a(x) + 2b(x)$. The Boolean functions of $2n$ variables b and $c = a \oplus b$ are both bent.

5. Haar spectra of bent functions

The Haar transform is a multiresolution transform in the sense that Haar coefficients are computed over subsets of function values where the number of elements in these subsets is different for coefficients in different packets of Haar functions. This feature allows a deeper insight into possible relationships between function values. Since the Haar functions, rows in the Haar transform matrix, are arranged into packets with respect to the number of non-zero values a Haar function takes, it is the same ordering with the Haar coefficients. They are also arranged per packets in the same way as the Haar functions in the Haar matrix. The number of packets is $(n+1)$.

Example 5.1. For $n = 4$, the Haar spectrum is arranged into packets as

$$\begin{aligned} \mathbf{S}_{h,f} &= [P_1|P_2|P_3|P_4|P_5]^T, \\ &= [s_0|s_1|s_2, s_3|s_4, s_5, s_6, s_7|s_8, s_9, s_{10}, s_{11}, s_{12}, s_{13}, s_{14}, s_{15}]^T, \end{aligned} \tag{5.1}$$

where s_i, $i \in \{0, 1, \ldots, 15\}$, are the Haar coefficients.

It is shown in [9] that the sum of Haar coefficients in a packet must be equal to the Walsh coefficients for bent functions, i.e., $2^{n/2}$. As explained in [19], this immediately follows from the property that the sum of Haar functions in a packet is the Rademacher function [8], which is a particular Walsh function and for bent functions the corresponding Walsh coefficient must have the value $2^{n/2}$.

Table 1 shows function vectors, Walsh, and Haar spectra for all 8 bent functions for $n = 2$. These spectra will be used in the following considerations. It can be observed that due to the requirement that bent functions cannot be balanced, the non-zero and zero values appear in the ratio $\rho_2 = 3$ to $\rho_1 = 1$, and it is the same for the signs of the Walsh coefficients.

i	Function	$\mathbf{F}$	$\mathbf{S}_{w,f}$	$\mathbf{S}_{h,f}$
1.	x_1x_2	$[0,0,0,1]$	$[2,2,2,-2]$	$[2,\|2,\|0,2]$
2.	$x_1x_2 \oplus x_2$	$[0,1,0,0]$	$[2,2,-2,2]$	$[2,\|-2,\|2,0]$
3.	$x_1x_2 \oplus x_1$	$[0,0,1,0]$	$[2,-2,2,2]$	$[2,\|2,\|0,-2]$
4.	$x_1x_2 \oplus x_1 \oplus x_2$	$[0,1,1,1]$	$[-2,2,2,2]$	$[-2,\|2,\|2,0]$
5.	$1 \oplus x_1x_2$	$[1,1,1,0]$	$[-2,-2,-2,2]$	$[-2,\|-2,\|0,-2]$
6.	$1 \oplus x_1x_2 \oplus x_2$	$[1,0,1,1]$	$[-2,-2,2,-2]$	$[-2,\|2,\|-2,0]$
7.	$1 \oplus x_1x_2 \oplus x_1$	$[1,1,0,1]$	$[-2,2,-2,-2]$	$[-2,\|-2,\|0,2]$
8.	$1 \oplus x_1x_2 \oplus x_1 \oplus x_2$	$[1,0,0,0]$	$[2,-2,-2,-2]$	$[2,\|-2,\|-2,0]$

Table 1. Function vectors, Walsh, and Haar spectra of bent functions for $n = 2$.

Recall that the functions in the bottom half of this table are logic complements of functions in the upper half. For both Walsh and Haar transforms, the spectral coefficients of these subsets of functions mutually differ just in the signs of the coefficients. We denote the Walsh spectra of all bent functions for $n = 2$ as $\mathbf{W}_i$, $i = 1, 2, \ldots, 8$, where the index i corresponds to the position of the vector in the table by starting from the top. In the case of Haar spectra, a value 0 appears. Inserting zero values in the last packet of Haar coefficients for larger n has an important role in the present considerations.

An exhaustive search over all 896 binary bent function in four variables permits the following conclusions.

The packets P_1 and P_2 consist of a single coefficient each and its value should be 4 or -4 since the corresponding Haar functions are identical to the two particular Walsh functions, and this is the value a Walsh coefficient can take for bent functions when $n = 4$. The Haar coefficient in P_1 is the sum of all function values in encoding $(0, 1) \to (1, -1)$, since the corresponding Haar function is the constant 1.

The coefficient must have the value ± 4, since the sum of Haar coefficients in each packet is ± 4, and at the same time this is the value of the Walsh coefficients for bent functions. The sign of this coefficient determines if the bent function has 10 or 6 non-zero values, for -4 and 4, respectively.

The Haar coefficient in P_2 is the sum of values obtained as the componentwise subtraction of the second half of the function vector from the first half of it. The value of this coefficient can also be ± 4. The sign of this coefficient shows in which half of the function vector non-zero values are concentrated.

The packet P_3 consists of two coefficients, whose value can be either 0 or ± 4. This also follows from the same requirement for the sum of Haar coefficients. The non-zero value can be at any of two positions in this packet. If a non-zero value is at the first position, it means that the first half of the function vector is non-balanced. Non-zero coefficient at the second position corresponds to the functions for which the second half of the function vector is non-balanced. The value of this coefficient equal 4 means that in the non-balanced half of the function vector there are 6 zero values and two values 1. It is the opposite if the value of this coefficient is -4. Then, the non-balanced half of the function vector contains more values 1 than 0, or when encoded -1 and 1. Notice that in the present context, the term half does not mean literary the half of a function vector, i.e., a subvector consisting of adjacent function values. Thus, elements of balanced and non-balanced subvectors can be mutually mixed, but not in an arbitrary way. This is further discussed below for the Haar coefficients in certain packets, see Table 2 and Table 3.

The packet P_4 contains four Haar coefficients. There are two possibilities for values of four Haar coefficients in this packet and with respect to them we distinguish two classes of functions

1. *Class 1* - A coefficient has the value ± 4 at any of four positions within the packet P_4, while the other three coefficients in this packet are equal 0.
2. *Class 2* - The values of the four coefficients in the packet P_4 are a Walsh spectrum for bent functions in two variables.

Computation of Haar coefficients in P_4 is performed over a quadruple of function values. From the positions of non-zero values in the corresponding Haar functions, the position of the non-zero value corresponds to the balanced quadruple of the form $0, 0, 1, 1$ or $1, 1, 0, 0$ in the function vector. The sign of the non-zero coefficient in this package determines which of these quadruples appears in the function vector. The following example illustrates this statement.

Example 5.2. Consider the bent function $f = x_2x_3 \oplus x_1x_4$ with the function vector $\mathbf{F} = [1, 1, 1, 1, |1, 1, -1, -1, |1, -1, 1, -1, |1, -1, -1, 1]^T$. The Haar coefficients are computed as the scalar product of Haar functions, rows of the Haar matrix, with the function vector. The Haar spectrum of this function is

$$\mathbf{S}_{h,f} = [4, |4, |4, 0, |0, 4, 0, 0, |0, 0, 0, 0, 2, 2, 2, -2]^T.$$

The packet $P_4 = (0, 4, 0, 0)$. The Haar coefficients in the packet P_4 are computed with respect the following four Haar functions $har_4(x)$, $har_5(x)$, $har_6(x)$, $har_7(x)$ specified by their function vectors as

$$\begin{aligned}
\mathbf{har}_4 &= [1, 1, -1, -1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]^T, \\
\mathbf{har}_5 &= [0, 0, 0, 0, 1, 1, -1, -1, 0, 0, 0, 0, 0, 0, 0, 0]^T, \\
\mathbf{har}_6 &= [0, 0, 0, 0, 0, 0, 0, 0, 1, 1, -1, -1, 0, 0, 0, 0]^T, \\
\mathbf{har}_7 &= [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, -1, -1]^T.
\end{aligned}$$

	P_5		P_5
1.	$P_{5,1} = [0,0,0,0,2,2,2,-2]^T$	4.	$P_{5,4} = [2,2,0,0,0,0,2,-2]^T$
2.	$P_{5,2} = [0,0,2,2,0,0,2,-2]^T$	5.	$P_{5,5} = [0,0,2,2,2,-2,0,0]^T$
3.	$P_{5,3} = [2,2,0,0,2,-2,0,0]^T$	6.	$P_{5,6} = [2,2,2,-2,0,0,0,0]^T$

Table 2. Allowed combinations of Haar coefficients in P_5 with zero values inserted in pairs.

	P_5		P_5
1.	$P_{5,1} = [0,2,0,2,0,2,0,-2]^T$	5.	$P_{5,5} = [2,0,0,2,2,0,0,-2]^T$
2.	$P_{5,2} = [2,0,2,0,2,0,-2,0]^T$	6.	$P_{5,6} = [2,0,0,2,0,2,-2,0]^T$
3.	$P_{5,3} = [2,0,2,0,0,2,0,-2]^T$	7.	$P_{5,7} = [0,2,2,0,0,2,-2,0]^T$
4.	$P_{5,4} = [0,2,0,2,2,0,-2,0]^T$	8.	$P_{5,8} = [0,2,2,0,2,0,0,-2]^T$

Table 3. Allowed combinations of Haar coefficients in P_5 with single zero values inserted.

The second quadruple in $\mathbf{F}$ matches the pattern in $\mathbf{har}_5$, and the resulting coefficients in this packet are $\mathbf{P}_4 = (0,4,0,0)$. It can be observed that Haar coefficients offer a possibility to get an information about the positions of non-zero values in the function vectors of bent functions.

The fifth packet P_5 contains 8 Haar coefficients. By the definition of the Haar functions in this packet, their values are computed as the difference between two adjacent function values. There are four possible combinations for these function values. In the used encoding, these are $(1,1)$, $(1,-1)$, $(-1,1)$, and $(-1,-1)$ and the Haar coefficients compare them. When equal, the Haar coefficient has the value 0, otherwise it has absolute value 2. It follows that each Haar coefficient specifies a pair of function values. Knowing the position of non-zero values of the Haar functions in the packet P_5, we know the position of the related pair of function values in the function vector.

For bent functions, four of the Haar coefficients in P_5 are zero-valued, while the other four are Walsh coefficients for bent functions in two variables. This follows from the computation of Haar coefficients as the difference of two adjacent function values and the requirement that the sum of the coefficients in the packet is ± 4. An exhaustive search over all 896 bent functions for $n = 4$ permits the conclusions which can be formulated as follows.

When a function is in *Class 1*, i.e., P_4 consists of a single non-zero value ± 4 and three other coefficients are 0, the positions of non-zero Haar coefficients in P_5 are restricted to the following 6 combinations as in Table 2 explained on the example of the Walsh spectrum W_1 in Table 1, although any other spectrum out of 8 spectra in this table can be equally used. When using other spectra, the difference is in the signs of the Haar coefficients. When discussing these combinations, we should take into account that bent functions cannot be

balanced, and must have an exactly specified number of non-zero values. From that follows the restriction on the number of possible combinations, 6 in the case of functions in $n = 4$ variables. It can be observed that in these allowed combinations for Haar coefficients in P_5 for functions in *Class 1*, the zero values and absolute values 2 appear in pairs. Since in this packet, Haar coefficients are computed as differences of adjacent function values, the adjacent function values also appear in pairs, as in Table 2. In this table, the pairs of Haar coefficients consist of two elements with the same absolute values. The *Class 1* for $n = 4$ consists of 384 bent functions.

It can be observed that for functions in Class 1 with $n = 4$, zero values in P_5 are inserted between the non-zero coefficients in pairs. For functions in Class 2, there are 8 possible arrangements of Haar coefficients in P_5, and single 0's are inserted between non-zero Haar coefficients. Table 3 shows the possible subspectra in P_5 for $n = 4$ with W_1. Again, any other Walsh spectrum from Table 1 can be used. In this table, the pairs of values consist of elements with different absolute values 0 and 2. This class consists of 512 bent functions.

The requirements that a bent function must be non-balanced and takes an exactly specified number of non-zero values impose some further restrictions on the distribution of non-zero values in the function vectors of bent functions. Conversely, the same requirements result in specific patterns of values per packets of Haar spectral coefficients. It is shown in [21] that due to this, it is possible to construct the sets of bent functions from Haar coefficients in the packet P_{n+1}, which is one half of the total of Haar coefficients. For $n = 4$, and the given packet P_5, this is the set of 8 bent functions. Clearly, to determine a unique function, we should know other Haar coefficients, i.e., the entire spectrum, since the Haar functions are a complete basis in the space of functions defined at 2^n points.

6. Haar spectra of Generalized Boolean bent functions

In what follows, we show that manipulation of packets of Haar coefficients leads to the Generalized Boolean bent functions. For $n = 4$, the Generalized Boolean bent functions are constructed by manipulating packets P_2, P_3, and P_4. We consider the following manipulations

1. In a Haar spectrum with P_5 as in Table 2, the packet P_4 is replaced by the packet P_4 for functions with P_5 in Table 3, and vice versa,

2. Permutation of values in P_3,

3. Change of signs in P_2.

The following examples illustrate these possibilities to construct Generalized Boolean bent functions from Haar spectra of binary bent functions.

6.1. Manipulation of the packet P_4

The Generalized Boolean bent functions are constructed by exchanging packets P_4 for functions with P_5 in Table 2 and Table 3. It means, in the given Haar spectrum of a function with the packet P_5 in Table 2, the packet P_4 is replaced by the packet P_4 for functions with the packet P_5 in Table 3, while other packets remain unchanged. The opposite replacement is equally possible.

Recall that in Table 3, the values in P_4 are Walsh spectra for binary bent functions for $n = 2$, while in Table 2 these are quadruples with a single non-zero value ± 4.

Example 6.1. Consider the Haar spectrum with P_5 from Table 2

$$\mathbf{S}_{h,f} = [4|4|4, 0, |0, -4, 0, 0, |0, 0, 0, 0, 2, 2, 2, -2]^T,$$

where the packet $P_4 = [0, -4, 0, 0]$. We replace this packet by the packet $P_4 = [2, 2, 2, -2]$ for functions with P_5 in Table 3. Therefore, we get the Haar spectrum

$$\mathbf{S}_{h,f} = [4, |4, |4, 0, |2, 2, 2, -2, |0, 0, 0, 0, 2, 2, 2, -2]^T.$$

The inverse Haar transform produces the function

$$\begin{aligned}\mathbf{F} \quad = \quad & [1.5, 1.5, 0.5, 0.5, 0.5, 0.5, -0.5, -0.5, \\ & 1.5, -0.5, 0.5, -1.5, 0.5, -1.5, -0.5, 1.5]^T.\end{aligned}$$

After multiplication by 2, we get the integer-valued function as

$$\mathbf{F} = [3, 3, 1, 1, 1, 1, -1, -1, 3, -1, 1, -3, 1, -3, -1, 3]^T.$$

We perform non-negative integer encoding of function values from the minimum to the maximum value by $(0, 1, 2, 3)$, i.e., in this example this encoding is $(-3, -1, 1, 3) \to (0, 1, 2, 3)$, and get

$$\mathbf{F} = [3, 3, 2, 2, 2, 2, 1, 1, 3, 1, 2, 0, 2, 0, 1, 3]^T.$$

Binary encoded this function vector is

$$\mathbf{F} = [11, 11, 10, 10, 10, 10, 01, 01, 11, 01, 10, 00, 10, 00, 01, 11]^T.$$

From there, the functions a and b determined by the first and the second bit in the binary encoded $\mathbf{F}$, as well as the function $c = a \oplus b$, are

$$\begin{aligned}\mathbf{a} &= [1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 1, 1]^T, \\ \mathbf{b} &= [1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1]^T, \\ \mathbf{c} &= [0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0]^T.\end{aligned}$$

The function a is balanced, and therefore non-bent. Functions b and c are both bent and their Walsh spectra are flat

$$\begin{aligned}\mathbf{S}_b &= [-4,-4,-4,-4,-4,-4,4,4,-4,4,-4,4,-4,4,4,-4]^T,\\ \mathbf{S}_c &= [-4,-4,4,4,4,4,4,4,-4,4,4,-4,4,-4,4,-4]^T.\end{aligned}$$

Therefore, the constructed function is a Generalized Boolean bent function since b and c are binary bent functions. To verify this, by following the approach in definition of the Generalized Boolean bent functions [16], [17], we encode the elements of the function vector $\mathbf{F}$ as $(0,1,2,3) \to (1,i,-1,-i)$, obtained as i^z for all $z \in \{0,1,2,3\}$,

$$\mathbf{F}_e = [-i,-i,-1,-1,-1,-1,i,i,-i,i,-1,1,-1,1,i,-i]^T,$$

and compute the Walsh spectrum as

$$\mathbf{S}_{F_e} = [-4,-4,-4i,-4i,-4i,-4i,4,4,-4,4,-4i,4i,-4i,4i,4,-4]^T,$$

which is flat as required for bent functions.

Any other packet P_4 in Table 3 can be used as a replacement for the packet P_4. Further, the Generalized Boolean bent functions can be constructed by the converse replacement of packets for functions in Table 3 by the corresponding packets for functions in Table 2.

6.2. Manipulation of the packet P_3

In the next example, we consider manipulation of packet P_3 in order to construct a Generalized Boolean bent function from the Haar spectrum of a bent function in four variables.

Example 6.2. Consider the Haar spectrum of a bent function with the packet P_5 as $P_{5,4}$ in Table 2 for the Walsh spectrum W_6 in Table 1

$$\mathbf{S}_{h,f} = [4,|-4|0,4,|0,4,0,0,|-2,-2,0,0,0,0,2,-2]^T.$$

The packet $P_3 = [0,4]$. After reordering the coefficients in this packet, we get the Haar spectrum

$$\mathbf{S}_{h,f} = [4,|-4|4,0,|0,4,0,0,|-2,-2,0,0,0,0,2,-2]^T.$$

The inverse Haar transform produces the function vector

$$\begin{aligned}\mathbf{F} = [&-0.5,1.5,-0.5,1.5,0.5,0.5,-1.5,-1.5,\\ &0.5,0.5,0.5,0.5,1.5,-0.5,-0.5,1.5]^T.\end{aligned}$$

After multiplication by 2, the non-negative integer encoding, and binary encoding as in Example 6.1, we get

$$\begin{aligned}\mathbf{a} &= [1,1,1,1,0,0,0,0,0,0,0,0,1,1,1,1]^T,\\ \mathbf{b} &= [0,1,0,1,1,1,0,0,1,1,1,1,1,0,0,1]^T,\\ \mathbf{c} &= [1,0,1,0,1,1,0,0,1,1,1,1,0,1,1,0]^T.\end{aligned}$$

The function a is balanced and, therefore, non-bent, while functions b and c are bent. We verify that also by complex encoding of $\mathbf{F}$ and computing its Walsh spectrum to see that this spectrum is flat.

We can construct in the same way Generalized Boolean bent functions by manipulation of packet P_3 in a function with the packet P_4 equal to any of 8 Walsh spectra for bent functions for $n = 2$ in Table 1 and the packet P_5 is any of the packets in Table 3.

6.3. Manipulation of the packet P_2

The next example illustrates manipulation of the packet P_2, in which case the single option is to change the sign of the coefficient in this packet.

Example 6.3. Consider the Haar spectrum of a bent function as

$$\mathbf{S}_{h,f} = [-4, |4, | - 4, 0, |2, -2, -2, -2, | - 2, 0, 2, 0, 0, -2, 0, -2]^T.$$

The single coefficient in P_2 is 4, and we change its value into -4, so that the Haar spectrum is converted into

$$\mathbf{S}_{h,f} = [-4, | - 4, | - 4, 0, |2, -2, -2, -2, | - 2, 0, 2, 0, 0, -2, 0, -2]^T.$$

The inverse Haar transform constructs the function with the function vector

$$\begin{aligned}\mathbf{F} \quad = \quad & [-1.5, 0.5, -1.5, -1.5, 0.5, -1.5, 0.5, 0.5, \\ & -0.5, -0.5, -0.5, 1.5, -0.5, -0.5, -0.5, 1.5]^T.\end{aligned}$$

After multiplication by 2, the non-negative integer encoding, and binary encoding as in Example 6.1, we get

$$\begin{aligned}\mathbf{a} &= [0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1]^T, \\ \mathbf{b} &= [0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1]^T, \\ \mathbf{c} &= [0, 1, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0]^T.\end{aligned}$$

The function a is balanced and therefore non-bent, while b and c are bent functions with the flat Walsh spectra. Therefore, the function constructed by changing the sign of the coefficient in P_2 is a Generalized Boolean bent function, as we can also verify by complex encoding of $\mathbf{F}$ and computing its Walsh spectrum that appears to be flat.

7. Extensions to larger n

The following examples for $n = 6$ illustrate that the extension of the previous considerations to functions in a larger number of variables is straightforward.

Example 7.1. Consider the function

$f = 1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_1x_4x_6$.

It is a bent function of degree 3, since its Positive polarity Reed-Muller expression has the largest product with three variables [1]. Its Haar spectrum is

$$\begin{aligned}\mathbf{S}_{h,F} \quad = \quad & [-8, |8, | -8, 0, | -4, 4, -4, -4, |0, 4, 0, -4, 0, 4, 0, 4, | \\ & -2, -2, 2, -2, 2, 2, -2, 2, -2, 2, 2, 2, -2, 2, 2, 2, | \\ & 0, -2, 0, -2, 0, 2, 0, -2, 0, 2, 0, 2, 0, -2, 0, 2, \\ & 0, -2, -2, 0, 0, 2, -2, 0, 0, -2, -2, 0, 0, 2, -2, 0]^T.\end{aligned}$$

The packet P_4 is $P_4 = [-4, 4, -4, -4]$, which is the Walsh spectrum W_7 in Table 1 multiplied by 2. When disregarding zero values, the packet P_5 is the Walsh spectrum W_3 in Table 1.

The packet $P_6 = [-2, -2, 2, -2, 2, 2, -2, 2, -2, 2, 2, 2, -2, 2, 2, 2]$ is a concatenation of $W_6 = [-2, -2, 2, -2]$, $W_2 = [2, 2, -2, 2]$, $W_4 = [-2, 2, 2, 2]$, and $W_4 = [-2, 2, 2, 2]$.

When disregarding zero values, the packet

$P_7 = [-2, -2, 2, -2, |2, 2, -2, 2, | -2, -2, 2, -2, | -2, -2, 2, -2]$

which is a concatenation of W_6, W_2, W_6, and W_6. When multiplied by 2, the packets P_6 and P_7 are the Walsh spectra of bent functions

$f_6 = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_3x_4 \oplus x_2x_3 \oplus x_1x_2$, and

$f_7 = 1 \oplus x_1 \oplus x_4 \oplus x_3x_4 \oplus x_1x_2$.

Function vectors are

$\mathbf{F}_6 = [0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1]^T$,

$\mathbf{F}_7 = [1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1]^T$.

In F_6, there can be observed non-balanced patterns $(0, 1, 1, 1)$, $(1, 0, 1, 1)$, $(1, 0, 0, 0)$, $(1, 0, 1, 1)$. The first and the third pattern are complements of each other, and the second and the fourth are identical patterns. In F_7, the non-balanced pattern, $(1, 0, 1, 1)$ appears three times, and the remaining pattern is the logic complement of it $(0, 1, 0, 0)$.

8. Closing remarks

The multiresolution feature of the Haar transform offers possibilities to observe relationships between elements of vectors representing Haar spectra and also of function vectors of bent functions. In the largest packet of Haar coefficients P_{n+1}, the Haar coefficients appear in pairs whose elements have either identical or different absolute values. In the same way, the elements of the function vectors appear in pairs corresponding to the pairs of Haar

coefficients, since in this packet, Haar coefficients are computed as differences of function values at adjacent positions in the function vectors. In the packet P_{n+1}, non-zero Haar coefficients constitute up to the multiplicative constant Walsh spectra of bent functions in $(n-2)$ variables. For a bent function, pairs of Haar coefficient in a packet can be reordered, but not arbitrarily, to get the other bent functions. The allowed reorderings correspond to the reorderings determined by the spectral invariance operations in the Walsh domain [3], [4], [5]. The same is true for the reordering of the corresponding function values. Destroying pairs in either packets of Haar coefficients or in function vectors by reordering of their elements does not preserve bentness. The restricted possibilities for reordering of either pairs of function values or pairs of Haar coefficients explain a small number of bent functions. We show that certain manipulation with packets of Haar coefficients convert Haar spectra of binary bent functions into Haar spectra of the Generalized Boolean functions that are defined in terms of binary valued variables, but functionally take four different values. Further work will be devoted to the formulation of formal procedures for construction of Generalized Boolean bent functions from the Haar spectra of binary bent functions. Also, the analysis of possible relationships between pairs of function values constituting the balanced and non-balanced parts of function vectors of binary bent functions by using the Haar coefficients could be an interesting task.

Acknowledgment. The authors thank the reviewer whose constructive remarks were very useful to improve the presentation in the paper.

References

[1] **Cusick, T.W. and P. Stănică,** *Cryptographic Boolean Functions and Applications*, Academic Press, 2009. https://doi.org/10.1016/B978-0-12-374890-4.00009-4

[2] **Haar, A.,** Zur Theorie der orthogonalen Funktionsysteme, *Math. Annal.*, **69** (1910), 331–371. https://doi.org/10.1007/BF01456326

[3] **Hurst, S.L.,** *Logical Processing of Digital Signals*, Crane Russak and Edward Arnold, London and Basel, 1978.

[4] **Hurst, S.L., D.M. Miller and J.C. Muzio,** *Spectral Techniques in Digital Logic*, Academic Press, Bristol, 1985. https://doi.org/10.1016/0165-1684(85)90052-0

[5] **Karpovsky, M.G., R.S. Stanković and J.T. Astola,** *Spectral Logic and Its Application in the Design of Digital Devices*, Wiley, 2008. https://doi.org/10.1002/9780470289228

[6] **Mesnager, S.,** *Bent Functions – Fundamentals and Results*, Springer, 2016. https://doi.org/10.1007/978-3-319-32595-8

[7] **Nyberg, K.,** Perfect nonlinear S-boxes, in Davies, D.W. (eds) *Advances in Cryptology — EUROCRYPT '91*, Lecture Notes in Computer Science, Vol. 547, Springer, 1991, 378–386. https://doi.org/10.1007/3-540-46416-6_32

[8] **Rademacher, H.,** Einige Sätze von allgemeinen Orthogonalfunktionen, *Math. Annalen*, **87** (1922), 112–138. https://doi.org/10.1007/BF01458040

[9] **Rafiq, H.M. and M.U. Siddiqi,** Haar spectrum of bent Boolean functions, *Malaysian Journal of Mathematical Sciences*, Vol. 10(S), February 2016, 409–421.

[10] **Rothaus, O.S.,** On bent functions, *J. Combin. Theory. Ser. A*, **20(3)** (1976), 300–305. https://doi.org/10.1016/0097-3165(76)90024-8

[11] **Schipp, F.,** On a generalization of the Haar system, *Acta Math. Acad. Sci. Hung.*, **33(1-2)** (1979), 183–188. https://doi.org/10.1007/BF01903393

[12] **Schipp, F.,** Remarks on dyadic analysis, *Annales Univ. Sci. Budapest., Sect. Comp.*, **56** (2024), 319–330. https://doi.org/10.71352/ac.56.319

[13] **Schipp, F., W.R. Wade, P. Simon and J. Pál,** *Walsh Series – An Introduction to Dyadic Harmonic Analysis*, Akadémiai Kiadó, Budapest, and Adam Hilger, Bristol and New York, 1990.

[14] **Schmidt, K-U.,** Quaternary constant-amplitude codes for multicode CDMA, *IEEE Trans. Inf. Theory*, Vol. 55, No. 4, 2009, 1824–1832. https://doi.org/10.1109/TIT.2009.2013041

[15] **Singh, D., A. Chawla, P. Bhogta and A. Paul,** A characterization of generalized Boolean functions employed in CDMA communications, *International Journal of Mathematical, Engineering and Management Sciences*, **9(2)** (2024), 352–365. https://doi.org/10.33889/IJMEMS.2024.9.2.019

[16] **Solé, P. and N.N. Tokareva,** On quaternary and binary bent functions, *Prikl. Diskr. Mat. Supplement*, **1** (2009), 16–18.

[17] **Solé, P. and N.N. Tokareva,** Connections between quaternary and binary bent functions, in *2011 IEEE International Symposium on Information Theory Proceedings, ISIT 2011*, St. Petersburg, Russia, July 31–August 5, 2011.

[18] **Stanković, R.S. and B.J. Falkowski,** Haar functions and transforms and their generalizations, *Proc. of IEEE Int. Conf. on Information, Communications and Signal Processing (1st ICICS)*, Singapore, Vol. 4, September 1997, 1–5.

[19] **Stanković, R.S., M. Stanković, C. Moraga and J. Astola,** A note on the Haar spectra of bent functions, *Reed-Muller Workshop 2023*, Matsue City, Shimane, Japan, May 24, 2023.

[20] **Stanković, R.S., M. Stanković, C. Moraga and J. Astola,** *Bent Functions and Permutation Methods*, Springer, 2024. https://doi.org/10.1007/978-3-031-50650-5

[21] **Stanković, R.S., M. Stanković, C. Moraga and J. Astola,** Haar spectra of binary bent functions, *Reed-Muller Workshop 2025*, Montreal, Canada, June 3, 2025.

[22] **Thornton, M.A., R. Drechsler and D.M. Miller,** *Spectral Techniques in VLSI CAD*, Kulwer Academic Publishers, 2001. https://doi.org/10.1007/978-1-4615-1425-1

[23] **Tokareva, N.,** Generalizations of bent functions. A survey, translated from *Discrete Analysis and Operation Research* (Diskretn. Anal. Issled. Oper.), **17(1)** (2010), 34-64.

[24] **Tokareva, N.,** *Bent Functions – Results and Applications to Cryptography*, Elsevier, 2015. https://doi.org/10.1016/B978-0-12-802318-1.00002-9

[25] **Walsh, J.L.,** A closed set of orthogonal functions, *Amer. J. Math.*, **45** (1923), 5–24. https://doi.org/10.2307/2387224

Radomir S. Stanković and Milena Stanković
Faculty of Electronic Engineering
Niš
Serbia
Radomir.Stankovic@gmail.com and milstankovic@gmail.com

Claudio Moraga
TU Dortmund University
Dortmund
Germany
Claudio.Moraga@udo.edu

Jaakko Astola
Tampere
Finland
Jaakko.Astola@outlook.com