FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 31, N° 2, June 2018, pp. 189 - 205
https://doi.org/10.2298/FUEE1802189S

AN IMPROVED SPECTRAL CLASSIFICATION OF BOOLEAN FUNCTIONS BASED ON EXTENDED SET OF INVARIANT OPERATIONS*

Milena Stanković[1], Claudio Moraga[2], Radomir S. Stanković[1]

[1]Faculty of Electronic Engineering, University of Niš, Niš, Serbia
[2]TU Dortmund University, Dortmund, Germany

Abstract.*Boolean functions expressing some particular properties often appear in engineering practice. Therefore, a lot of research efforts are put into exploring different approaches towards classification of Boolean functions with respect to various criteria that are typically selected to serve some specific needs of the intended applications. A classification is considered to be strong if there is a reasonably small number of different classes for a given number of variables n and it it desirable that classification rules are simple. A classification with respect to Walsh spectral coefficients, introduced formerly for digital system design purposes, appears to be useful in the context of Boolean functions used in cryptography, since it is in a way compatible with characterization of cryptographically interesting functions through Walsh spectral coefficients. This classification is performed in terms of certain spectral invariant operations. We show by introducing a new spectral invariant operation in the Walsh domain, that by starting from n≤5, some classes of Boolean functions can be merged which makes the classification stronger, and from the theoretical point of view resolves a problem raised already in seventies of the last century. Further, this new spectral invariant operation can be used in constructing bent functions from bent functions represented by quadratic forms.*

Key words: *Boolean functions, classication, Walsh spectrum, invarant operations.*

1 Introduction

Classification of Boolean functions is a classical and well explored problem in Switching theory [1]. Boolean functions can be classified for different purposes. Two of them that are most usually reported, NPN and LP classifications, are related to technology mapping in logic synthesis with standard gate libraries or in FPGA synthesis and unification and simplification of testing procedures [2], [3]. Classification can be performed with respect to various criteria usually appropriately defined to serve certain application

Received October 21, 2017; received in revised form February 6, 2018

Corresponding author: Milena Stanković
Faculty of Electronic Engineering, University of Niš, Medevedeva 14, 18000 Niš, Serbia
(E-mail: milena.stankovic@elfak.ni.ac.rs)

*An earlier version of this paper was presented as an invited address at the Reed-Muller 2017 Workshop, Novi Sad, Serbia, May 24-25, 2017 purposes. The present interest of some researchers in classification with respect to Walsh spectral coefficients, which we will shortly denote as the Walsh classification, is due to the spectral characterization of some classes of Boolean functions used in cryptography [4], [5], [6], [7], [8], [9]. In particular, bent functions [10] which are defined as Boolean functions that have maximal minimum distance to the set of affine functions, are alternatively defined as Boolean functions with flat Walsh spectra, meaning that all the Walsh coefficients have the same absolute value equal to $2^{n/2}$, where n is the number of variables. This requirement implies that all bent functions for a given n belong to the same class in the Walsh classification of Boolean functions. This classification has been discussed in a series of papers by different authors with the earliest of them published in the 1970's, [11], [12], [13]. In this classification, Boolean functions are split into classes satisfying certain conditions imposed on elements of appropriately defined canonic vectors specified in terms of their Walsh spectra as it will be discussed bellow. Functions belonging to the same class are converted to each other by certain operations that we will call affine spectral invariant operations. In the Boolean domain, these are affine operations over Boolean variables and function values, which in the spectral domain result in permutation and sign changes of Walsh coefficients but preserving their absolute values.

It was observed already in the early publications, when the analysis was restricted to functions up to 5 variables, that there is some inconsistency when the considerations are restricted to the realms of affine spectral invariant operations. Starting from functions of five variables, two different classes of functions with flat spectra have to be considered [12], since functions although satisfying the required conditions over canonic vectors for being members of the class with flat spectra, cannot be converted to each other with affine spectral invariant operations. Also, the functions having solely quadratic product terms in their Reed-Muller expressions are bent functions meaning that they have the flat Walsh spectra. Bent functions may have product terms with up to $n/2$ variables, and it means they cannot be derived from functions with quadratic terms by the application of affine spectral invariant operations since these operations cannot be used to increase the number of variables in product terms. It is clear that there are some other operations beyond the affine spectral invariant operations preserving the absolute values of Walsh coefficients and in this paper we present a possible answer to this problem by introducing a new spectral invariant operation the effect of which becomes apparent for functions of $n \geq 5$ variables.

2 Walsh Classification of Boolean Functions

Classification of Boolean functions in terms of Walsh spectral coefficients has been discussed in a series of papers with the first of them published in the sixties and seventies of the last century [11], [12], [13], [14], [15]. The Walsh transform in the Hadamard ordering is used, since in this ordering the structure of the transform matrix corresponds to the recursive structure of the domain for Boolean functions viewed as a decomposable Abelian group [3]. Links to the Hadamard matrices are used [2], [3], [12], [16].

2.1 Walsh spectrum

Definition 1 *Walsh spectrum.*
In the so-called Hadamard ordering, the Walsh spectrum $\mathbf{S}_f(n)$ *of a Boolean function* $f(x_1, \cdots, x_n)$ *is defined as*

$$\mathbf{S}_f(n) \quad = \quad \mathbf{W}(n)\mathbf{F}(n) = \mathbf{W}(1)^{\otimes n}\mathbf{F}(n), \tag{1}$$

where $\otimes$ *denotes the Kronecker product,* $\mathbf{W}(1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$*, and* $\mathbf{F}(n)$ *is the value vector of the function* f *in the* $(0,1) \to (1,-1)$ *encoding, i.e.,*

$$\mathbf{F}(n) = [(-1)^{f(0)}, (-1)^{f(1)}, \cdots, (-1)^{f(2^n-1)}].$$

The Walsh spectrum $\mathbf{S}_f(n)$ of a function of n binary variables is a vector of 2^n coefficients. Here we will use a notation for spectral coefficients with binary subscripts $S_{b_1,b_2,\cdots,b_n}$ where $b_i \in \{0,1\}$, $i = 1, 2, \cdots, n$

$$\mathbf{S}_f(n) = [S_{00\ldots0}, S_{00\ldots1}, \cdots, S_{11\ldots1}].$$

The first coefficient with the index $i = (00\ldots0)$ is called the zero order coefficient, and the coefficients with the single 1 in the binary representation of the indices are the coefficients of the first order.

Walsh spectral coefficients are seen to be a form of correlation between function inputs and the output.

2.2 Spectral invariant operations

In Walsh classification, classification rules are derived from the so-called spectral invariant operations defined as operations that preserve the absolute values of Walsh spectral coefficients of Boolean functions. In other words, spectral invariant operations perform permutation and change the sign of Walsh coefficients. In order to ensure that Walsh spectra with permuted coefficients will remain the spectra of Boolean and not some other integer valued functions, these permutations are not arbitrary. A permutation of some Walsh coefficients requires a simultaneous permutation of certain precisely specified subsets of Walsh coefficients (Definition 2).

Definition 2 *Spectral invariant operations are defined as*

1. *Negation (complement) of the $f(x_1, \cdots, x_n)$. This results in the change of sign of all spectral coefficients without the change of their absolute values.*

2. *Negation (complement) of any input variable $x_i, i \in (1, \cdots, n)$. This results in the change of the sign of all coefficients with $b_i = 1$ in the subscripts.*

$$S_{b_0, \cdots, b_i=1, \cdots, b_n} = -S_{b_0, \cdots, b_i=1, \cdots, b_n}.$$

3. *Interchange of any input variable x_i with $x_j, i \neq j$. In the spectral domain this corresponds to the permutation of the binary values at the positions i and j in the subscripts:*

$$S_{b_0, \cdots, b_i, \cdots, b_j \cdots, b_n} \leftrightarrow S_{b_0, \cdots, b_j, \cdots, b_i \cdots, b_n},$$

4. *Replacement of any input variable x_i, by the exclusive-OR sum $x_i \oplus x_j, i \neq j$. This operation results in the interchange of all coefficient values with $b_i = 1, b_j$ in the subscripts with the coefficients having $b_i = 1, \bar{b}_j$, while all the coefficients with $b_i = 0$ in the subscripts remain unchanged:*

$$S_{b_0, \cdots, b_i=1, \cdots, b_j, \cdots, b_n} \leftrightarrow S_{b_0, \cdots, b_i=1, \cdots, \bar{b}_j, \cdots, b_n}.$$

5. *Modifucation of the function $f(x_1, \cdots, x_n)$ into function*

$$f^*(x_1, \cdots, x_n) = f(x_1, \cdots, x_n) \oplus x_i,$$

where $x_i \in \{x_1, \cdots, x_n\}$ results in the interchange of all coefficient having $b_i = 1$ in the subscripts with the coefficients having $b_i = 0$, [12]:

$$S_{b_0,\cdots,b_i=1,\cdots,b_n} \leftrightarrow S_{b_0,\cdots,b_i=0,\cdots,b_n}.$$

It is important to note that referring to the Reed-Muller polynomial expressions for Boolean functions, the above defined spectral invariant operations do not increase the number of variables in the product terms.

2.3 Walsh classification of Boolean functions

By using spectral invariant operations, Hurst in [12] and Lechner in [13] proposed a procedure for reordering of spectral coefficients into the positive canonic order which represents the classification entry of the given Boolean function $f(x_1, \cdots, x_n)$. Positive canonic order is used for $S_{00\cdots0}$ and the first order coefficients, while other coefficients may take negative values.

In [12], it is shown a classification of all Boolean functions with $n \leq 5$ variables as a table with 48 canonic vectors. In this table, not all of the 32 coefficient values for each classified entry are shown. Instead, the values of first order coefficients are shown together with the number of coefficients having the same value in each entry. For example (6×10; 10×6; 16×2) indicates that the 6-th, 10-th, and 16-th coefficients have values 10, 6, and 2, respectively, in the entire spectrum of 32 coefficients. In Table 1, we show a part of this table from [12], starting from the class No. 30. We consider this part of the classification table, since there are some inconsistencies in this classification that can be summarized as follows:

- The $n + 1$ zero and first order coefficients are sufficient to identify unambiguously each classification entry for $n \leq 5$, except for functions with canonic vectors 35 and 36, as well as $45a$ and $46b$.
- There are 6 groups of classes with identical spectral summary and different canonical form of first order coefficients for functions 31 and 32, 33 and 35, 34 and 37, 38 and 39, 41, 42, and 43, as well as 45a, 45b and 47.

Table 1: A part of the classification table in the Walsh classification of Boolean functions for $n \leq 5$.

Class	Primary coefficients						Complete spectral summary
30	14	10	10	10	10	6	$1 \times 14, 5 \times 10, 7 \times 6, 19 \times 2$
31	14	10	10	10	6	6	$1 \times 14, 3 \times 10, 13 \times 6, 15 \times 2$
32	14	10	10	6	6	6	$1 \times 14, 3 \times 10, 13 \times 6, 15 \times 2$
33	12	12	12	12	8	4	$4 \times 12, 4 \times 8, 12 \times 4, 12 \times 0$
34	12	12	12	12	4	4	$4 \times 12, 28 \times 4$
35	12	12	12	8	8	8	$4 \times 12, 4 \times 8, 12 \times 4, 12 \times 0$
36	12	12	12	8	8	8	$3 \times 12, 6 \times 8, 13 \times 4, 10 \times 0$
37	12	12	12	4	4	4	$4 \times 12, 28 \times 4$
38	12	12	8	8	8	8	$2 \times 12, 8 \times 8, 14 \times 4, 8 \times 0$
39	12	12	8	8	8	4	$2 \times 12, 8 \times 8, 14 \times 4, 8 \times 0$
40	12	8	8	8	8	8	$1 \times 12, 10 \times 8, 15 \times 4, 6 \times 0$
41	10	10	10	10	10	10	$6 \times 10, 10 \times 6, 16 \times 2$
42	10	10	10	10	10	6	$6 \times 10, 10 \times 6, 16 \times 2$
43	10	10	10	10	10	2	$6 \times 10, 10 \times 6, 16 \times 2$
44	10	10	10	10	6	6	$4 \times 10, 16 \times 6, 12 \times 2$
45a	8	8	8	8	8	8	$16 \times 8, 16 \times 0$
45b	8	8	8	8	8	8	$16 \times 8, 16 \times 0$
46	8	8	8	8	8	4	$12 \times 8, 16 \times 4, 4 \times 0$
47	8	8	8	8	8	0	$16 \times 8, 16 \times 0$

- The two entries 45a and 45b are the only entries for $n \leq 5$ with equal first order coefficients up to the ordering under spectral invariant operations. Further, these functions have the same spectral summaries. However, it is proved to be impossible to map a function in the class $45a$ into a function in the class $45b$ and vice versa by using the affine spectral invariant operations used in this classification [12]. These two classes are illustrated by functions shown in the Karnaugh maps in Table 2 and Table 3 [12].

Similar problems in the Walsh classification using affine invariant operations are mentioned by Lechner in [13] by using a different notation as shown in Table 4.

In what follows, we show that certain appropriately defined spectral invariant operations defined for functions with disjoint products of pairs variables [17] permit a refinement of this classification in the sense that these

Table 2: A function from the class 45a.

	x_2x_3							
x_4x_5	00	01	11	10	00	01	11	10
00	0	0	0	0	0	0	1	0
01	0	0	1	1	0	0	1	0
11	0	0	1	1	1	1	1	0
10	0	0	0	0	1	1	1	0
	$x_1 = 0$				$x_1 = 1$			

Table 3: A function from the class 45b.

	x_2x_3							
x_4x_5	00	01	11	10	00	01	11	10
00	0	0	0	0	0	0	1	0
01	0	0	0	0	0	1	1	1
11	0	0	1	1	0	1	1	1
10	0	1	0	1	0	1	1	0
	$x_1 = 0$				$x_1 = 1$			

classes, which are considered as related but different, can be unified. We introduce a new spectral invariant operation that permits to convert functions from these two classes to each other, meaning that they belong to the same class under this new operation being added to the classification rules.

Table 4: Correspondence between notations of Walsh classes used by Hurst and Lechner.

Hurst's classes				Lechner's classes		
Functions	31,	32		Classes	30A,	30B
Functions	33,	35		Classes	32A,	32B
Functions	34,	37		Classes	33A,	33B
Functions	38,	39		Classes	35A,	35B
Functions	41,	43		Classes	37A,	37B
Functions	45a,	45b	47	Classes	39A,	39B
Functions	42			Not illustrated by Lechner		

3 New Spectral Invariant Operations

The fifth spectral invariant operation in Definition 2, which is called disjoint spectral translation [11], [12], concerns with the adding of a linear term x_i to a function f without changing the absolute values of Walsh coefficients of f. The spectral invariant operation introduced in the present section concerns with conditions under which adding of a non-linear term to a function f satisfies requirements of the Walsh spectrum invariance.

We show that when the Reed-Muller polynomial of a Boolean function contains two disjoint products of pairs of variables it is possible to add a certain products with three variables such that some spectral coefficients will be permuted or will change the sign but their absolute values remain unchanged. Therefore, this operation can be viewed as a spectral invariant operation in the sense discussed above.

Theorem 1 *(Adding to f a product of three variables)*
Let f be a Boolean function of n variables, which has two disjoint products of two variables in its polynomial form

$$f(x_1, \cdots, x_n) = x_{i_1}x_{i_2} \oplus x_{i_3}x_{i_4} \oplus h(x_1, \cdots, x_k),$$

where $\{i_1, i_2\} \cap \{i_3, i_4\} = \emptyset$, and $h(x_1, \cdots, x_k)$ is an arbitrary function of $\{x_1, \cdots, x_k\} \subset \{x_1, \cdots, x_n\}$ variables.

Furthermore, let

$$g(x_1, \cdots, x_n) = f(x_1, \cdots, x_n) \oplus x_{j_1}x_{j_2}x_{j_3},$$

where $j_1 \in \{i_1, i_2\}$, $j_2 \in \{i_3, i_4\}$ and $j_3 \notin \{i_1, i_2, i_3, i_4\}$.

The Walsh spectral coefficients of f and g are related as

$$S_{g_{b_1, \cdots, b_{j_4}=1, b_{j_5}=1, b_{j_3}=0, \cdots, b_n}} \leftrightarrow S_{f_{b_1, \cdots, b_{j_4}=1, b_{j_5}=1, b_{j_3}=1, \cdots, b_n}},$$

$$S_{g_{b_1, \cdots, b_{j_4}=1, b_{j_5}=1, b_{j_3}=1, \cdots, b_n}} \leftrightarrow S_{f_{b_1, \cdots, b_{j_4}=1, b_{j_5}=1, b_{j_3}=0, \cdots, b_n}},$$

where $j_4 = \{i_1, i_2\} \setminus j_1$ and $j_5 = \{i_3, i_4\} \setminus j_2$. Coefficients with $b_{j_4} = b_{j_5} = 1$, and $b_{j_3} = 0$ in the subscripts are permuted with the coefficients with $b_{j_4} = b_{j_5} = 1$, and $b_{j_3} = 1$ in the subscripts.

Proof: For simplicity assume that h does not appear in f, $h(x_1, \cdots, x_k) = 0$. Therefore, consider a function $f(x_1, \cdots, x_n)$ in n variables defined by the polynomial form consisting of two disjoint product terms of pairs of variable

$$f(x_1, \cdots, x_n) = x_{i_1}x_{i_2} \oplus x_{i_3}x_{i_4}.$$

Table 5: Variables, functions, and spectral coefficients in the proof of Theorem 1.

x_{i_1}	x_{i_2}	x_{i_3}	x_{i_4}	x_{i_5}	f	g	F	G	$W_{2,4}$	$W_{2,4,5}$	$S_{f_{1,1,0}}$	$S_{g_{1,1,1}}$
1	0	1	0	1	0	1	1	-1	1	-1	1	1
1	0	1	1	1	1	0	-1	1	-1	1	1	1
1	1	1	0	1	1	0	-1	1	-1	1	1	1
1	1	1	1	1	0	1	1	-1	1	-1	1	1

By adding the product of variables $x_{j_1}x_{j_2}x_{j_3}$ where $j_1 \in \{i_1, i_2\}$, $j_2 \in \{(i_3, i_4\}$ and $j_3 \notin \{i_1, i_2, i_3, i_4\}$, we get the function

$$g(x_1, \cdots, x_n) = x_{i_1}x_{i_2} \oplus x_{i_3}x_{i_4} \cdots \oplus x_{j_1}x_{j_2}x_{j_3}.$$

To simplify the notation in the proof, consider the case when $j_1 = i_1, j_2 = i_3$, and $j_3 = i_5$. By adding the product $x_{i_1}x_{i_3}x_{i_5}$ only the values of the function f for $x_{i_1} = 1, x_{i_3} = 1$, and $x_{i_5} = 1$ will be complemented. Since $f(x_1, \cdots, x_n) = x_{i_1}x_{i_2} \oplus x_{i_3}x_{i_4}$, the values of the function in these points are $f(x_1, \cdots, x_n) = 1 \cdot x_{i_2} \oplus 1 \cdot x_{i_4} = x_{i_2} \oplus x_{i_4}$, and the values of the function $g(x_1, \cdots, x_n) = x_{i_1}x_{i_2} \oplus x_{i_3}x_{i_4} \oplus x_{i_1}x_{i_3}x_{i_5} =$
$1 \cdot x_{i_2} \oplus 1 \cdot x_{i_4} \oplus 1 = x_{i_2} \oplus x_{i_4} \oplus 1$, as it is shown in Table 5.

In this table the first five columns show the values of the input variables x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}, and x_{i_5}. In columns f, g, F, and G, the values of functions f and g in $(0, 1)$ and F and G in the $(1, -1)$ encoding are shown. In the next two columns the values of the rows in the Walsh matrix $W_{2,4}$ and $W_{2,4,5}$ through which the coefficients $S_{b_{i_2}=1, b_{i_4}=1}$ and $S_{b_{i_2}=1, b_{i_4}=1, b_{i_5}=1}$ are calculated. In the last two columns, denoted as $S_{f_{1,1,0}}$ and $S_{g_{1,1,1}}$, the values of the coefficients $S_{b_{i_2}=1, b_{i_4}=1, b_{i_5}=0}$ for the function f and the values of the coefficients $S_{b_{i_2}=1, b_{i_4}=1, b_{i_5}=1}$ for the function g are shown.

The values in the column f are in correlation with the values of the Walsh function $W_{2,4}$ which is used for calculation of the coefficients with $b_{i_2} = 1, b_{i_4} = 1$, and $b_{i_5} = 0$ in the subscript, while the values of the column g are in correlation with the values of the Walsh function $W_{2,4,5}$ used for calculation of the coefficient with $b_{i_2} = 1, b_{i_4} = 1$, and $b_{i_5} = 1$ in the subscript. From that it follows that the changes in the function f have influence only on the coefficients having $b_{i_2} = 1, b_{i_4} = 1$, and $b_{i_5} = 0$ in the subscripts, and for function g they will have the same values as the coefficients of the function f having $b_{i_2} = 1, b_{i_4} = 1$, and $b_{i_5} = 1$. Also, the coefficients of the function g having $b_{i_2} = 1, b_{i_4} = 1$, and $b_{i_5} = 1$ in the subscripts have the same values as the coefficients of the function f having $b_{i_2} = 1, b_{i_4} = 1$, and $b_{i_5} = 0$ in the subscripts.

Theorem 2 *(Adding two products of three variables)*
Let f be a Boolean function of n variables, which has two disjoint products of two variables in its polynomial form

$$f(x_1,\cdots,x_n)=x_{i_1}x_{i_2}\oplus x_{i_3}x_{i_4}\oplus h(x_1,\cdots,x_k),$$

where $\{i_1,i_2\}\cap\{i_3,i_4\}=\emptyset$, and $\{x_1,\cdots,x_k\}\subset\{x_1,\cdots,x_n\}$. Define

$$g(x_1,\cdots,x_n)=f(x_1,\cdots,x_n)\oplus x_{j_1}x_{j_2}x_{j_3}\oplus x_{j_4}x_{j_5}\bar{x}_{j_3}$$

where $j_1\in\{i_1,i_2\}$, $j_2\in\{i_3,i_4\}$, $j_3\notin\{i_1,i_2,i_3,i_4\}$, $j_4=\{i_1,i_2\}\setminus j_1$, and $j_5=\{i_3,i_4\}\setminus j_2$.

The following relations between pairs of spectral coefficients of f and g exist

$$\begin{array}{lll}
S_{g_{b_1,b_2=1,b_3,b_4=1,b_5=0}} & \leftrightarrow & S_{f_{b_1,b_2=1,b_3,b_4=1,b_5=1}}, \\
S_{g_{b_1,b_2=1,b_3,b_4=1,b_5=1}} & \leftrightarrow & S_{f_{b_1,b_2=1,b_3,b_4=1,b_5=0}}, \quad \textit{for } b_1,b_3\in(0,1), \\
S_{g_{b_1=1,b_2,b_3=1,b_4,b_5=0}} & \leftrightarrow & -S_{f_{b_1=1,b_2,b_3=1,b_4,b_5=1}}, \\
S_{g_{b_1=1,b_2,b_3=1,b_4,b_5=1}} & \leftrightarrow & -S_{f_{b_1=1,b_2,b_3=1,b_4,b_5=0}}, \quad \textit{for } b_2,b_4\in(0,1).
\end{array}$$

It is possible to prove the Theorem 2 by using the same approach as in Theorem 1.

Example 1 *Consider the function*

$$f(x_1,\cdots,x_5)=x_1x_2\oplus x_3x_4\oplus x_5$$

with the spectrum

$$\begin{aligned}\mathbf{S}_f &= [0,8,0,8,0,8,0,-8,0,8,0,8,0,8,0,-8,\\ &\quad 0,8,0,8,0,8,0,-8,0,-8,0,-8,0,-8,0,8]^T.\end{aligned}$$

By adding to f the product of three variables (one variable from the first product, the second from the second product and as the third the variable x_5, not included in the products), a new function

$$\begin{aligned}g_1(x_1,\cdots,x_5) &= f(x_1,\cdots,x_5)\oplus x_1x_3x_5\\ &= x_1x_2\oplus x_3x_4\oplus x_5\oplus x_1x_3x_5,\end{aligned}$$

is generated. The spectrum of g_1 is

$$\begin{aligned}\mathbf{S}_{g_1} &= [0,8,0,8,0,8,0,-8,0,8,8,0,0,8,-8,0,\\ &\quad 0,8,0,8,0,8,0,-8,0,-8,-8,0,0,-8,8,0]^T,\end{aligned}$$

and it is related to the spectrum of f as follows

$$\begin{array}{ll}
S_{g_1 01010} = S_{f\,01011} & S_{g_1 01011} = S_{f\,01010} \\
S_{g_1 01110} = S_{f\,01111} & S_{g_1 01111} = S_{f\,01110} \\
S_{g_1 11010} = S_{f\,11011} & S_{g_1 11011} = S_{f\,11010} \\
S_{g_1 11110} = S_{f\,11111} & S_{g_1 11111} = S_{f\,11110}.
\end{array}$$

Also, it is possible to generate from f a new function by adding two products with three variables, one product with x_5 and the second with $\bar{x}_5$ as in the following example.

Example 2 *Consider again the function f in Example 1 and a new function*

$$\begin{array}{rcl}
g_2(x_1, \cdots, x_5) & = & f(x_1, \cdots, x_5) \oplus x_1 x_3 \bar{x}_5 \oplus x_2 x_4 x_5 \\
& = & x_1 x_2 \oplus x_3 x_4 \oplus x_5 \oplus x_1 x_3 x_5 \oplus x_1 x_3 \oplus x_2 x_4 x_5.
\end{array}$$

The function g_2 has the spectrum

$$\begin{array}{rcl}
\mathbf{S}_{g_2} & = & [0, 8, 0, 8, 0, 8, 0, -8, 0, 8, -8, 0, 0, 8, 8, 0, \\
& & 0, 8, 0, 8, 8, 0, -8, 0, 0, -8, 8, 0, -8, 0, 0, -8]^T,
\end{array}$$

related to the spectrum of f by the permutation of the following coefficients

$$\begin{array}{ll}
S_{g_2 01010} = -S_{f\,01011} & S_{g_2 01011} = -S_{f\,01010} \\
S_{g_2 01110} = -S_{f\,01111} & S_{g_2 01111} = -S_{f\,01110} \\
S_{g_2 11010} = -S_{f\,11011} & S_{g_2 11011} = -S_{f\,11010} \\
S_{g_2 11110} = -S_{f\,11111} & S_{g_2 11111} = -S_{f\,11110} \\
S_{g_2 10100} = S_{f\,10101} & S_{g_2 10101} = S_{f\,10100} \\
S_{g_2 10110} = S_{f\,10111} & S_{g_2 10111} = S_{f\,10110} \\
S_{g_2 11100} = S_{f\,11101} & S_{g_2 11101} = S_{f\,11100} \\
S_{g_2 11110} = S_{f\,11111} & S_{g_2 11111} = S_{f\,11110}.
\end{array}$$

Note that it is possible to generalize the operations defined in Theorem 1 and Theorem 2. When the function f has more than two disjoint product in the polynomial form it is possible to add products with more than three variables by selecting the variables by following the described rules.

4 Classes 45a, 45b and 47

In this section, we consider relationships between functions in the classes 45*a*, 45*b*, and 47.

Table 6: Functions in 5 variables with solely products of two and three variables in the polynomial form.

	Number of cubes										
Pairs	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	5	0	0
1	0	0	0	0	0	60	120	180	150	0	0
2	115	60	180	360	615	1320	1170	900	300	120	0
3	90	360	990	1860	3990	4980	4470	2520	1110	120	60
4	190	840	2250	4740	8490	11700	9630	4800	2340	480	0
5	222	1020	3270	7980	11310	15012	10290	6900	2730	480	72
6	200	720	3390	7080	11130	10320	9270	5760	2460	360	0
7	110	300	2010	3600	5610	6120	5250	2580	1410	360	60
8	30	60	630	1440	1470	3000	1290	780	285	0	0
9	10	0	210	240	570	180	270	60	0	0	0
10	1	0	30	60	15	12	0	0	0	0	0

From a direct evaluation, the function $f(x_1, \cdots, x_5)$ has the canonic representation

$$(8 \quad 8 \quad 8 \quad 8 \quad 8 \quad 0 \quad 16 \times 8; 16 \times 0) \ ,$$

which means that this function is from the class 47.

The function g_1 has the canonic representation

$$(8 \quad 8 \quad 8 \quad 8 \quad 8 \quad 8 \quad 16 \times 8; 16 \times 0) \ ,$$

and, therefore, it is from the class $45a$, while the function g_2 with the identical canonic representation is from the class $45b$.

It is impossible to transform the function f into any of functions g_1 or g_2 by using the affine spectral invariant operations. The function f has only quadratic product terms in the polynomial form and with these operations it is impossible to generate a product with a higher number of variables, while in the polynomial form of the functions g_1 and g_2 there are products with three variables.

All these functions f, g_1, and g_2, are connected with the new invariant operation, from which it follows that classes $45a$, $45b$, and 47 are subclasses of a single class. Table 5 shows the number of functions from this class having exclusively products of two variables or three variables in their polynomial forms and no other terms. The total number of such functions is 219604, and the total number of all functions in that class, including linear terms in the polynomial forms, is $219604 \times 32 = 7027328$. In the column denoted by 0, the number of functions with quadratic polynomial forms is shown. For example, there are 115 functions in this class with two products in the polynomial forms, while the number of functions with five products of

Table 7: Parallels in notation of the classes by Hurst and Lechner.

Hurst classes				Lechner classes			New class
Functions	31,	32		Classes	30A,	30B	30
Functions	33,	35		Classes	32A,	32B	32
Functions	34,	37		Classes	33A,	33B	33
Functions	38,	39		Classes	35A,	35B	35
Functions	41,	42,	43	Classes	37A,	37B	37
Functions	45a,	45b,	47	Classes	39A,	39B	39

Table 8: Basic functions for the new classes.

New class	Basic function
30	$x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_3x_4x_5$
32	$x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_3x_4$
33	$x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_5$
35	$x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_3x_5$
37	$x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_3x_4x_5$
39	$x_1x_2 \oplus x_3x_4$

two variables in the polynomial form is 222. All other functions from this class have some products with three variables in the polynomial form. For example, there are 15012 functions with five products of two variables and five products of three variables. It is possible to generate all these functions by the spectral invariant operations including the new operations.

Here we will show how functions ϕ_1 and ϕ_2, defined by the the Karnaugh maps in Table 2 and Table 3 are mutually related and how it is possible to generate these two functions starting from the function $x_1x_2 \oplus x_3x_4$ by increasing the number of variables in the product terms by using the spectral invariant operation introduced above. The polynomial forms of these functions are

$$\begin{aligned} \phi_1 &= x_1x_4 \oplus x_2x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \\ \phi_2 &= x_1x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_3x_4x_5. \end{aligned}$$

Constructing ϕ_1

- Start from $\zeta_1(x_1, \cdots, x_5) = x_1x_2 \oplus x_3x_4$.
- Permutation of x_1 and x_5, produces the function $\zeta_2(x_1, \cdots, x_5) = x_2x_5 \oplus x_3x_4$.

- Permutation of x_1 and x_3, produces the function $\zeta_3(x_1,\cdots,x_5) = x_2x_5 \oplus x_1x_4$.
- Adding $x_1x_2x_3$ according to the new invariant operation, produces the function $\zeta_4(x_1,\cdots,x_5) = x_2x_5 \oplus x_1x_4 \oplus x_1x_2x_3$.
- Replacing x_3 with $x_3 \oplus x_4$ produces the function $\zeta_5(x_1,\cdots,x_5) = x_2x_5 \oplus x_1x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4$.
- Replacing x_3 with $x_3 \oplus x_5$ in ζ_5 produces the function $\phi_1 = x_2x_5 \oplus x_1x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5$.

Constructing ϕ_2

- Start from $\zeta_1(x_1,\cdots,x_5) = x_1x_2 \oplus x_3x_4$.
- Permutation of x_2 and x_3 in ζ_1 produces the function $\zeta_2(x_1,\cdots,x_5) = x_1x_3 \oplus x_2x_4$.
- Adding $x_1x_2x_5$ and $x_3x_4\bar{x}_5$ according to the new invariant operation produces the function $\zeta_3(x_1,\cdots,x_5) = x_1x_3 \oplus x_2x_4 \oplus x_1x_2x_5 \oplus x_3x_4x_5 \oplus x_3x_4$.
- Replacing x_5 with $x_5 \oplus x_4$ produces the function $\zeta_4(x_1,\cdots,x_5) = x_1x_3 \oplus x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_4 \oplus x_3x_4x_5$.
- Replacing x_5 with $x_5 \oplus x_3$ in ζ_4 produces the function $\phi_2 = x_1x_3 \oplus x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_3x_4x_5 \oplus x_3x_4$.

5 Consideration of Other Classes

It is possible to repeat the considerations for three classes 45a, 45b, and 47, to all other classes in Table 4. In all these cases it is possible to find a basic function from which all other functions from the class considered are generated by the usage of the five affine invariant operation together with the new invariant operations, as shown in Table 7. Note that all these basic functions have disjoint products of pairs of variables in the polynomial forms. In the following example it will be shown how classes 34 and 37 from Table 1 are mutually related.

Example 3 *Let us start from the function*

$$\eta_1 = x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_5.$$

The spectrum of this function is

$$\begin{aligned}\mathbf{S}\eta_1 &= [12,-4,12,-4,12,-4,-12,4,4,4,4,4,4,4,-4,-4,\\ &\quad 4,4,4,4,4,4,-4,-4,-4,-4,-4,-4,-4,-4,4,4]^T,\end{aligned}$$

The characteristic vector of the function η_1 *is* $(12,12,12,4,4,4)$ *which means that it belongs to the class* 37*.*

By adding $x_1x_3\bar{x}_5$ *and* $x_2x_4x_5$ *according to the new invariant operation, we have the function*

$$\eta_2 = x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_5 \oplus x_1x_3 \oplus x_2x_4x_5,$$

with the spectrum

$$\begin{aligned}\mathbf{S}_{\eta_2} &= [12,-4,12,-4,4,4,-4,-4,4,4,-4,-4,12,-4,-4,12,\\ &\quad 4,4,4,4,4,4,-4,-4,-4,-4,4,4,-4,-4,-4,-4]^T.\end{aligned}$$

By replacing x_2 *with* $x_2 \oplus x_3$*, the function* η_2 *is transformed into the function*

$$\eta_3 = x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5$$

with the spectrum

$$\begin{aligned}\mathbf{S}_{\eta_3} &= [12,-4,12,-4,4,4,-4,-4,12,-4,-4,12,4,4,-4,-4,\\ &\quad 4,4,4,4,4,4,-4,-4,-4,-4,-4,-4,-4,-4,4,4]^T.\end{aligned}$$

After the replacement of x_5 *with* $x_5 \oplus x_2 \oplus x_4$*, the function* η_3 *is transformed into the function*

$$\eta_4 = x_1x_2x_5 \oplus x_1x_2x_4 \oplus x_2x_4x_5 \oplus x_3x_4x_5 \oplus x_2x_3x_4$$

with the spectrum

$$\begin{aligned}\mathbf{S}_{\eta_4} &= [12,12,12,-4,4,-4,-4,4,12,-4,-4,-4,4,-4,-4,4,\\ &\quad 4,-4,4,-4,4,4,-4,-4,-4,4,-4,4,-4,-4,4,4]^T.\end{aligned}$$

Finally, after permutation of variables x_2 *and* x_3 *the function* η_4 *will be transformed into the function*

$$\eta_5 = x_1x_3x_5 \oplus x_1x_3x_4 \oplus x_3x_4x_5 \oplus x_2x_4x_5 \oplus x_2x_3x_4$$

with the spectrum

$$\begin{aligned}\mathbf{S}_{\eta_5} &= [12,12,12,-4,12,-4,-4,-4,4,-4,-4,4,4,-4,-4,4,\\ &\quad 4,-4,4,-4,-4,4,-4,4,4,4,-4,-4,-4,-4,4,4]^T.\end{aligned}$$

The characteristic vector of the function η_5 is $(12, 12, 12, 12, 4, 4)$ which means that this function belongs to the class 34, from which it is possible to conclude that classes 34 and 37 are subclasses of a single class. It is possible to generate all functions from these two subclasses from the function η_1 by using the spectral invariant operations including the new operation.

6 Conclusion

The classification of Boolean functions with respect to Walsh spectral coefficients is reconsidered. For this classification, besides the five known invariant operations, a new invariant operation is proposed. This operation is defined for functions with disjoint products of pairs of variables in their Reed-Muller polynomial form. By using this extended set of invariant operations, it is possible to merge some classes in the Walsh classification and to reduce the total number of classes from 48 to 40, for functions with $n \leq 5$ input variables.

Since the goal of the paper was reduction of the number of classes in the Walsh classification for functions with $n \leq 5$, examples of functions with $n = 5$ variables are considered. However, the introduced spectral invariant operations are valid for functions with more than 5 variables. When the Reed-Muller polynomial form of a given function has more than two disjoint products it is possible to add products with more of three variables. Due to that, the introduced operation can be used to construct bent functions starting from the bent functions represented by quadratic forms.

Acknowledgments

The work leading to this paper was partially supported by the Ministry of Education, Science and Technological Development, Republic of Serbia, project No OI 174026.

Authors are grateful to the Reviewers and the Editors of this special issue for their constructive comments that were very useful in improving the presentation in the paper.

References

[1] T. Sasao, *Switching Theory for Logic Synthesis*, Kluwer Academic Publishers, 1999.

[2] S. L. Hurst, D. M. Miller, J. C. Muzio, *Spectral Techniques for Digital Logic*, Academic Press, 1985.

[3] M. Karpovsky, R. S. Stanković, J. Astola, *Spectral Logic and Its Applications for the Design of Digital Devices*, Wiley, 2008.

[4] A. Braeken, Y. Borisov, S. Nikova, B. Preneel, ”Classification of Boolean functions of 6 variables or less with respect to cryptographic properties”, *Int. Colloquium on Automata, Languages and Programming ICALP 2005*, M. Yung, G.F. Italiano, C. Palamidessi (eds.), Lecture Notes in Computer Science, Vol. 3580, Springer-Verlag, 2005, 324-334.

[5] C. Carlet, P. Sarkar, ”Spectral domain analysis of correlation immune and resilient Boolean functions”, *Finite Fields Appl.*, Vol. 8, 2002, 120-130.

[6] K. Miranovich, ”Spectral analysis of Boolean functions under nonuniformity of arguments”, http://eprint.iacr.org/2002/021

[7] P. Sarkar, ”A note on the spectral characterization of Boolean functions”, *Inform Process Lett*, 74, Vol. 74, 2000, 195.

[8] Y. Tarannikov, ”Spectral analysis of high order correlation immune functions”, *Proc. IEEE Int. Symp. on Information Theory*, June 29, 2001, DOI 10.1109/ISIT.2001.935932.

[9] G. Z. Xiao, J. L. Massey, ”A spectral characterization of correlation-immune combining functions”, *IEEE Trans. on Inform. Theory*, Vol. 34, No. 3, 1988, 569-571.

[10] O. S. Rothaus, ”On bent functions”, *Journal Combinatorial Theory*, Vol. 20, No. A, 1976, 300-305.

[11] C. R. Edwards, ”The application of the Rademacher-Walsh transform to Boolean function classification and threshold logic synthesis”, *Trans. IEEE*, Vol. C-24, 1975, 48-62.

[12] S. L. Hurst, *The Logical Processing of Digital Signals*, Crane, Russak & Company, Inc., New York, Edward Arnold, London, 1978.

[13] R. J. Lechner, ”Harmonic analysis of swiching functions” in A. Mukhopadyay, (Ed.), *Recent Developments in Switching Theory*, New York, Academic, 1971.

[14] S. W. Golomb, ”On the classiffication of Boolean functions”, *IRE Trans. Circuit Theory*, Vol. CT-6, No. 5, May 1959, 176-186.

[15] S. W. Golomb, G. Gong, *Signal Design for Good Correlation for Wireless Communications, Cryptogtaphy and Radar*, Cambridge University Press, 2005.

[16] S.W. Golomb, L. D. Baumert, ”The search for Hadamard matrices”, *Amer. Math. Monthly*, Vol. 70, 1963, 12-17.

[17] M. Stanković, C. Moraga, R. S. Stanković, ”New spectral invariant operations for functions with disjoint products in the polynomial form”, in *Proc. EUROCAST 2017*, 19-23, February, 2017, Las Palmas, Spain.