FACTA UNIVERSITATIS (NIŠ)
SER.: ELEC. ENERG. vol. 20, no. 3, December 2007, 281-294

Properties of the Reed-Muller Spectrum of Symmetric Functions

Claudio Moraga and Radomir S. Stanković

Abstract: Different forms of symmetry based on cofactors of Boolean functions are characterized in the Reed Muller spectral domain. Furthermore it is shown, that if the arguments of the function are reordered, the permutation that is needed on the truth vector applies also on the spectrum of the function.

Keywords: Boolean functions, Symmetric Boolean functions, Reed-Muller transform.

1 Introduction and Motivation for Research

Symmetric Boolean functions are a relatively large class of Boolean functions (there are 2^{n+1} out of the total of 2^{2^n} functions) which are very important in engineering practice, since many computing, control, and communications circuits are described by symmetric functions [1]. In general, symmetric functions can be compactly represented irrespectively to the data structure selected, as for instance, different functional expressions, cubes, decision diagrams, etc. This feature reduces the memory required to store a function and is also useful in software realizations. In hardware realizations, symmetric functions require fewer gates than other functions [2]. For these reasons, symmetric Boolean functions have been a subject of study from the beginning of the development of switching theory and logic design (see, for instance, [3]) and are intensively investigated presently, the research providing for a theoretical background of a variety of applications.

For a brief illustration of present interest in symmetric Boolean functions, we will point out few related concepts and the corresponding research results in this

Manuscript received August 30, 2007.

The first author is with European Center for Soft Computing, 33600 Mieres, Asturaia, Spain, and University of Dortmund, 44221 Dortmund, Germany claudio.moraga@udo.edu. The second author is with Dept. of Computer Science, Faculty of Electronics, 18 000 Niš, Serbia rstankovic@bankerinter.net.

area. Besides classical applications, as circuit synthesis and formal verification, (for example, [4–7].), a high recent interest in study of symmetric Boolean functions is related to their cryptographic features [8].

In particular, symmetric Boolean functions have been recently used in preventing algebraic attacks, an important tool in cryptanalysis stream and block chipper systems, which recover the secrete key by solving overdefined systems of multivariate equations. Algebraic immunity of Boolean functions is defined as the feature of Boolean functions to resist algebraic attacks. The algebraic immunity of an n-variable Boolean function is upper bounded by $\lceil \frac{n}{2} \rceil$ [9, 10].

A symmetric Boolean function of an odd number of variables with maximum algebraic immunity has been constructed in [11]. The exhaustive search for all balanced symmetric functions up to 128 variables presented in [12] shows that, for odd n, all balanced symmetric functions are trivial balanced except for $n \in \{13, 29, 31, 33, 35, 41, 47, 61, 63, 73, 97, 103\}$. In [13] it is proven that for each odd n, there is exactly one trivial balanced n-variable symmetric Boolean function achieving the algebraic immunity $\lceil \frac{n}{2} \rceil$. It is also derived a necessary condition for the algebraic normal form of an n-variable symmetric Boolean function with maximum algebraic immunity for any positive integer n.

Computational learning theory is another area with interesting recent results in applications of symmetric Boolean functions [14, 15].

This continuous research interest in symmetric Boolean functions as well as interesting recent applications pointed out above, provide a motivation for the research work presented in this paper.

2 Symmetries in Boolean Functions

Besides totally symmetric and partially symmetric Boolean functions, (defined as the invariance of function values to all possible permutations of variables, and pairs of variables, respectively), there have been defined symmetries with respect to pairs or in general subsets of variables by imposing invariance of co-factors of Boolean functions in terms of these variables [16]. The notion of co-symmetries is introduced in the similar way by requiring equivalence of certain co-factors and logic complements of other cofactors [17, 18].

In this paper, we consider symmetries in Boolean functions defined in terms of truth-vectors for functions and their co-factors as follows.

For a function of n variables $f(x_{n-1}, x_{n-2}, x_{n-3}, \ldots, x_0)$ given by the truth-vector $F = [f(0), \ldots, f(2^n - 1)]^T$, the cofactors with respect to the most significant argu-

ments x_{n-1} and x_{n-2} are defined as

$$\begin{aligned} f_{00} &= f(0,0,x_{n-3},\ldots,x_0), \\ f_{01} &= f(0,1,x_{n-3},\ldots,x_0), \\ f_{10} &= f(1,0,x_{n-3},\ldots,x_0), \\ f_{11} &= f(1,1,x_{n-3},\ldots,x_0), \end{aligned}$$

and in matrix notation written as the corresponding vectors F_{00}, F_{01}, F_{10}, F_{11}.

The following concepts of symmetry have been earlier introduced [16–19]:

1. *Equivalence symmetry* based on x_{n-1}, x_{n-2} iff $F_{00} = F_{11}$
2. *Non-equivalence symmetry* based on x_{n-1}, x_{n-2} iff $F_{01} = F_{10}$
3. *Partial symmetry* of x_{n-1} with respect to x_{n-2}, iff $F_{01} = F_{11}$, and vice-versa iff $F_{10} = F_{11}$
4. Partial symmetry of x_{n-1} with respect to $\overline{x}_{n-2}$, iff $F_{00} = F_{10}$ and of x_{n-2} with respect to $\overline{x}_{n-1}$ iff $F_{00} = F_{01}$.

2.1 Characterization of symmetries

Symmetries of Boolean functions can be described (and detected) by decomposition charts [20] and related Boolean expressions, decision diagrams [21–23], logic differential operators, Gibbs derivatives on finite dyadic groups, various spectral transforms including Walsh transform [16], complex Hadamard transform [24], arithmetic transform and the Reed-Muller transform [7, 25]. In particular, efficient procedures for detection of symmetries defined above have been proposed in terms of Walsh spectral coefficients in [17, 26], see also [16, 18, 19].

In this paper, we discuss characterization of the above defined symmetries and co-symmetries in terms of Reed-Muller coefficients.

3 Analysis

Let $f(x_{n-1}, x_{n-2}, \ldots, x_1, x_0)$ be an n-place binary function and let $f_{value(x_{n-1})value(x_{n-2})}$ denote a cofactor of f with relation to its two most significant arguments. The notation for the corresponding truth vectors will be F and $F_{value(x_{n-1})value(x_{n-2})}$, respectively. Furthermore, let $R = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ denote the basic Reed Muller transform matrix. The Reed Muller spectrum of f consists of an ordered set of spectral coefficients denoted as $\{r_0, r_1, \ldots, r_N\}$, where $N = 2^n - 1$. The vector representation

of the spectrum will be denoted by **r** and, in analogy to the functions the spectral cofactors will be denoted as $r_{value(x_{n-1})value(x_{n-2})}$.

The well known equation to calculate the Reed Muller spectrum of a binary n-place function is

$$r = R^{\otimes n} \cdot F. \tag{1}$$

For the present paper, it will be considered that $F = [F_{00}, F_{01}, F_{10}, F_{11}]^T$. This is indeed formally not correct, since at the left hand side there is a vector with 2^n scalar elements, meanwhile at the right hand side there is a vector with 4 elements, which are vectors of length (actually, "height") 2^{n-2}. Since however for most following calculations block matrices and (sub)vectors of dimension 2^{n-2} will be used, the abuse of notation will not impair consistency. The following expression will be used to calculate the Reed Muller spectrum of a given function f:

$$\begin{aligned} R^{\otimes n} \cdot F &= (R^{\otimes 2} \otimes R^{\otimes (n-2)}) \cdot F \qquad (2) \\ &= \begin{bmatrix} R^{\otimes(n-2)} & [\mathbf{0}] & [\mathbf{0}] & [\mathbf{0}] \\ R^{\otimes(n-2)} & R^{\otimes(n-2)} & [\mathbf{0}] & [\mathbf{0}] \\ R^{\otimes(n-2)} & [\mathbf{0}] & R^{(n-2)} & [\mathbf{0}] \\ R^{\otimes(n-2)} & R^{\otimes(n-2)} & R^{\otimes(n-2)} & R^{\otimes(n-2)} \end{bmatrix} \cdot \begin{bmatrix} F_{00} \\ F_{01} \\ F_{10} \\ F_{11} \end{bmatrix} = \begin{bmatrix} r_{00} \\ r_{01} \\ r_{10} \\ r_{11} \end{bmatrix}, \end{aligned}$$

where $[\mathbf{0}]$ represents a 2^{n-2} by 2^{n-2} zero matrix. It is simple to see that

$$\begin{aligned} R^{\otimes n} \cdot F &= \begin{bmatrix} R^{\otimes(n-2)} \cdot F_{00} \\ R^{\otimes(n-2)} \cdot F_{00} \oplus R^{\otimes(n-2)} \cdot F_{01} \\ R^{\otimes(n-2)} \cdot F_{00} \oplus R^{\otimes(n-2)} \cdot F_{10} \\ R^{\oplus(n-2)} \cdot F_{00} \oplus R^{\oplus(n-2)} \cdot F_{01} \oplus R^{\oplus(n-2)} \cdot F_{10} \oplus R^{\oplus(n-2)} \cdot F_{11} \end{bmatrix} \qquad (3) \\ &= \begin{bmatrix} R^{\oplus(n-2)} \cdot F_{00} \\ R^{\oplus(n-2)} \cdot (F_{00} \oplus F_{01}) \\ R^{\oplus(n-2)} \cdot (F_{00} \oplus F_{10}) \\ R^{\oplus(n-2)} \cdot (F_{00} \oplus F_{01} \oplus F_{10} \oplus F_{11}) \end{bmatrix} = \begin{bmatrix} r_{00} \\ r_{01} \\ r_{10} \\ r_{11} \end{bmatrix}. \end{aligned}$$

After these considerations it is possible to formulate the following theorem.

Theorem 1 *(Characterization of symmetries)*

1. $F_{00} = F_{01}$ *iff* $r_{01} \oplus r_{10} = r_{11}$,
2. $F_{10} = F_{01}$ *iff* $r_{10} = r_{01}$,
3. $F_{01} = F_{11}$ *iff* $r_{10} = r_{11}$,

4. $F_{10} = F_{11}$ *iff* $r_{01} = r_{11}$,
5. $F_{00} = F_{10}$ *iff* $r_{10} = 0$,
6. $F_{00} = F_{01}$ *iff* $r_{01} = 0$.

Proof of (1)

$\Longrightarrow$

Recall (3) that $r_{11} = R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{10} \oplus F_{01} \oplus F_{11})$ and that in $GF(2)^{(n-2)}$, $F_{00} = F_{11}$ implies that $F_{00} \oplus F_{11} = [\mathbf{0}] = [00\ldots0]^T$ of length 2^{n-2}.

Therefore r_{11} in this case reduces to $R^{\oplus(n-2)} \cdot (F_{10} \oplus F_{01})$. This can however be written as:

$$\begin{aligned} r_{11} &= R^{\oplus(n-2)} \cdot (F_{10} \oplus F_{01} \oplus F_{00} \oplus F_{00}) \\ &= R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{10} \oplus F_{00} \oplus F_{01}) \\ &= R^{\oplus(n-2)} \cdot (F_{00} \oplus F_{10}) \oplus R^{\oplus(n-2)} \cdot (F_{00} \oplus F_{01}) = r_{10} \oplus r_{01}. \end{aligned}$$

$\Longleftarrow$

$$\begin{aligned} r_{10} \oplus r_{01} &= R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{10}) \oplus R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{01}) \\ &= R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01}) \end{aligned}$$

$r_{10} \oplus r_{01} = r_{11}$ implies that

$$R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01}) = R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{10} \oplus F_{01} \oplus F_{11}),$$

but this equality holds only if $F_{00} \oplus F_{11} = [\mathbf{0}]$, from where $F_{00} = F_{11}$.

Corollary 1 *(From Theorem 1)*

1. *If both (1) and (2) of Theorem* 1 *apply, then* $r_{11} = 0$.
2. *If both (3) and (5) of Theorem* 1 *apply, then* $r_{11} = 0$.
3. *If both (4) and (6) of Theorem* 1 *apply, then* $r_{11} = 0$.

Theorem 2 *Up to equivalence:*

1. $F_{00} = \overline{F}_{11}$ *iff* $r_{11} = r_{01} \oplus r_{10} \oplus R^{\otimes(n-2)} \cdot [111\cdots11]^T = r_{01} \oplus r_{10} \oplus [100\cdots00]^T$
2. $F_{10} = \overline{F}_{01}$ *iff* $r_{10} = r_{01} \oplus [100\ldots00]^T$
3. $F_{01} = \overline{F}_{11}$ *iff* $r_{10} = r_{11} \oplus R^{\otimes(n-2)} \cdot [111\ldots11]^T = r_{11} \oplus [100\ldots00]^T$
4. $F_{10} = \overline{F}_{11}$ *iff* $r_{01} = r_{11} \oplus R^{\otimes(n-2)} \cdot [111\cdots11]^T = r_{11} \oplus [100\cdots00]^T$.
5. $F_{00} = \overline{F}_{10}$ *iff* $r_{10} = R^{\otimes(n-2)} \cdot [111\cdots11]^T = [100\cdots00]^T$.
6. $F_{00} = \overline{F}_{01}$ *iff* $r_{01} = R^{\otimes(n-2)} \cdot [111\cdots11]^T = [100\cdots00]^T$.

Proof of (1) $\Longrightarrow$

$\overline{F}_{11}$ represents the complement of the truth vector F_{11}, i.e., it is the vector containing all elements of F_{11} respectively complemented. Formally, $\overline{F}_{11} = F_{11} \oplus [\mathbf{1}]$, where $[\mathbf{1}] = [11\ldots11]^T$, of length 2^{n-2}.

$r_{11} = R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{10} \oplus F_{01} \oplus F_{11})$ which under the conditions of (1) of the Theorem 2 becomes

$$\begin{aligned} r_{11} &= R^{\otimes(n-2)} \cdot (\overline{F}_{11} \oplus F_{10} \oplus F_{01} \oplus F_{11}) \\ &= R^{\otimes(n-2)} \cdot (F_{11} \oplus [\mathbf{1}] \oplus F_{10} \oplus F_{01} \oplus F_{11}) \\ &= R^{\otimes(n-2)} \cdot ([\mathbf{1}] \oplus F_{10} \oplus F_{01}) \\ &= R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01}) \oplus R^{\otimes(n-2)} \cdot [\mathbf{1}] \\ &= (R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01}) \oplus [10\cdots00]^T). \end{aligned}$$

Since from the proof of the former Theorem it is known that $R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01}) = r_{10} \oplus r_{01}$ the assertion follows.

$\Longleftarrow$

$$\begin{aligned} r_{10} \oplus r_{01} &= R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{10}) \oplus R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{01}) \\ &= R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01}). \end{aligned}$$

$$\begin{aligned} r_{10} \oplus r_{01} \oplus [10\ldots00]^T &= r_{10} \oplus r_{01} \oplus R^{\otimes(n-2)} \cdot [\mathbf{1}] \\ &= R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01}) \oplus R^{\otimes(n-2)} \cdot [\mathbf{1}] \\ &= (R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01} \oplus [\mathbf{1}])). \end{aligned}$$

From the condition $r_{11} = r_{01} \oplus r_{10} \oplus [100\ldots00]^T$ follows

$$\begin{aligned} r_{11} &= R^{\otimes(n-2)} \cdot (F_{00} \oplus F_{10} \oplus F_{01} \oplus F_{11}) \\ &= R^{\otimes(n-2)} \cdot (F_{10} \oplus F_{01} \oplus [\mathbf{1}]), \end{aligned}$$

i.e., $(F_{00} \oplus F_{10} \oplus F_{01} \oplus F_{11}) = (F_{10} \oplus F_{01} \oplus [\mathbf{1}])$ from where $(F_{00} \oplus F_{11}) = [\mathbf{1}]$ or, equivalently,

$$F_{00} = \overline{F}_{11}, \quad \overline{F}_{00} = F_{11}, \quad F_{00} \oplus F_{11} \oplus [\mathbf{1}] = [\mathbf{0}].$$

Corollary 2 *(From Theorem 2)*

1. *If both (1) and (2) of Theorem 2 apply, then* $r_{11} = 0$.
2. *If both (3) and (5) of Theorem 2 apply, then* $r_{11} = 0$.
3. *If both (4) and (6) of Theorem 2 apply, then* $r_{11} = 0$.

If another "context" instead of "x_{n-1}, x_{n-2}" would be needed, then a permutation matrix may be used to reorder the elements of the truth vector of the function corresponding to the exchange of the components of the target context with those of the above context. Then, the two theorems may be directly applied to the modified truth vector and its spectrum. It is however possible to do the whole transformation in the spectral domain.

Let P be a 2^n by 2^n permutation matrix which reorders the elements of a truth vector F of a given function, to "move" the arguments x_i and x_j to the positions of x_{n-1} and x_{n-2}, (and vice versa) respectively. Let $\mathbf{R}$ denote $R^{\otimes(n-2)}$ and let $F' = P \cdot F$. Then:

$$r' = \mathbf{R} \cdot F' = \mathbf{R} \cdot (P \cdot F) = (\mathbf{R} \cdot P) \cdot F.$$

The product of matrices $(\mathbf{R} \cdot P)$ introduces a permutation of the columns of $\mathbf{R}$. However, notice that the matrix equation $\mathbf{R} \cdot P = Q \cdot \mathbf{R}$ has the solution $Q = \mathbf{R} \cdot P \cdot \mathbf{R}^{-1}$ and it is known that $\mathbf{R}$ is its own inverse in $GF(2)$, therefore $Q = \mathbf{R} \cdot P \cdot \mathbf{R}$. Then:

$$r' = \mathbf{R} \cdot F' = \mathbf{R} \cdot (P \cdot F) = (\mathbf{R} \cdot P) \cdot F = (Q \cdot \mathbf{R})F = Q \cdot (\mathbf{R} \cdot F) = Q \cdot r.$$

Notice that this "Q-transformation" of the Reed Muller spectrum of a function applies for any permutation of the elements of a truth vector and not only to that induced by pairwise permutation of arguments of the function. Furthermore, this transformation applies to any type of spectrum, as long as the transform matrix is not singular (which is a basic requirement in spectral techniques).

The next important question is: could it be that $Q = P$? If yes, under which conditions?

If $Q = P$ then:

$$P = \mathbf{R} \cdot P \cdot \mathbf{R}, \quad (4)$$

$$P \cdot \mathbf{R} = \mathbf{R} \cdot P, \quad (5)$$

i.e., the permutation of the rows of $\mathbf{R}$ has to have the same effect as the permutation of the columns of $\mathbf{R}$.

Consider first the case of $f(x_1, x_0)$ and let $P_{0,1}$ be the permutation to obtain the truth vector of $f(x_0, x_1)$ from the truth vector of $f(x_1, x_0)$. Then,

$$P_{01} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Then,

$$P_{01}\cdot\mathbf{R}=\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}\cdot\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&1&1&1\end{bmatrix}=\begin{bmatrix}1&0&0&0\\1&0&1&0\\1&1&0&0\\1&1&1&1\end{bmatrix},$$

and

$$\mathbf{R}\cdot P_{01}=\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&0&1&0\\1&1&1&1\end{bmatrix}\cdot\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}=\begin{bmatrix}1&0&0&0\\1&0&1&0\\1&1&0&0\\1&1&1&1\end{bmatrix},$$

The above condition (4) is satisfied then for $n=2$. Consider now the case of $n>2$ and the exchange of two *neighbour* arguments. Let $p_{j,j+1}$ denote a "local" permutation matrix, (with the same structure as $P_{0,1}$ above), which modifies the corresponding 2^2-"sub-truthvectors" when x_j and x_{j+1} are exchanged. Then,

$$\begin{aligned}P_{j,j+1} &= I_{(0)}\otimes I_{(1)}\otimes\cdots\otimes I_{(j-1)}\otimes p_{j,j+1}\otimes I_{(j+2)}\otimes\cdots\otimes I_{(n-1)}\\ &= I^{\otimes j}\otimes p_{j,j+1}\otimes I^{\otimes(n-j-2)},\end{aligned}$$

where $I_{(i)}$ denotes a 2 by 2 identity associated to the i-th (non exchanged) argument. Then:

$$\begin{aligned}P_{j,j+1}\cdot R^{\otimes n} &= (I^{\otimes j}\otimes p_{j,j+1}\otimes I^{\otimes(n-j-2)})\cdot(R^{\otimes j}\otimes R^{\otimes 2}\otimes R^{\otimes(n-j-2)})\\ &= (I^{\otimes j}\cdot R^{\otimes j})\otimes(p_{j,j+1}\cdot R^{\otimes 2})\otimes(I^{\otimes(n-j-2)}\cdot R^{\otimes(n-j-2)})\\ &= R^{\otimes j}\otimes(p_{j,j+1}\cdot R^{\otimes 2})\otimes R^{\otimes(n-j-2)}\end{aligned}$$

and similarly

$$R^{\otimes n}\cdot P_{j,j+1}=R^{\otimes j}\otimes(R^{\otimes 2}\cdot p_{j,j+1})\otimes R^{\otimes(n-j-2)}$$

but according to the case of a 2-place function analyzed above,

$$R^{\otimes 2}\cdot p_{j,j+1}=p_{j,j+1}\cdot R^{\otimes 2}.$$

Therefore,

$$R^{\otimes n}\cdot P_{j,j+1}=P_{j,j+1}\cdot R^{\otimes n}$$

and the condition (4) is satisfied.

Finally recall that the exchange of any two symbols of a string may be obtained as a chain of permutations of pairs of neighbour symbols. This concludes the proof of the following

Theorem 3 *Let* $f(x_{n-1},\ldots,x_i,\ldots,x_k,\ldots,x_0) = f'(x_{n-1},\ldots,x_k,\ldots,x_i,\ldots,x_0)$ *and let* F *and* F' *denote their respective truth vectors. Furthermore let* r *and* r' *denote their respective Reed Muller spectra. Then*

$$P_{i,k} \cdot F = F' \Longleftrightarrow P_{i,k} \cdot r = r'.$$

4 Examples

In this section, we will present some examples that illustrate the concepts discussed above.

$f_1(x)$

x_1x_0 \ x_3x_2	00	01	10	11
00	1	0	1	0
01	0	1	1	1
10	1	1	1	1
11	1	0	0	0

$\leftrightarrow$

$R^{\otimes 2} f_1$

x_1x_0 \ x_3x_2	00	01	10	11
00	1	1	0	0
01	1	0	1	1
10	0	1	0	0
11	1	1	0	0

$F_{01} = F_{11} \quad \leftrightarrow \quad r_{10} = r_{11}$ (Theorem 1, iii)

$f_2(x)$

x_1x_0 \ x_3x_2	00	01	10	11
00	1	0	1	1
01	0	1	0	1
10	1	1	1	0
11	1	0	1	0

$\leftrightarrow$

$R^{\otimes 2} f_2$

x_1x_0 \ x_3x_2	00	01	10	11
00	1	1	0	1
01	1	0	0	1
10	0	1	0	0
11	1	1	0	0

$F_{00} = F_{10} \quad \leftrightarrow \quad r_{10} = [0]$ (Theorem 1, v)

$f_3(x)$

x_1x_0 \ x_3x_2	00	01	10	11
00	1	0	1	1
01	0	1	1	0
10	1	0	1	1
11	1	1	0	0

$\leftrightarrow$

$R^{\otimes 2} f_3$

x_1x_0 \ x_3x_2	00	01	10	11
00	1	1	0	1
01	1	0	1	1
10	0	0	0	0
11	1	1	0	0

$P_{01} = P_{11} \quad \leftrightarrow \quad r_{10} = r_{11} \oplus [1000]^T$ (Theorem 2. iii)

Remark 1 *Notice that* $f_1(x_3,x_2,x_1,x_0) = f_2(x_3,x_0,x_1,x_2)$.

$$P_{02} = I_3 \otimes p_{0,2} = I_3 \otimes$$

1	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	1	0
0	1	0	0	0	0	0	0
0	0	0	0	0	1	0	0
0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	1

Now:

$$\begin{aligned} R^{\otimes 4} \cdot P_{0,2} \cdot R^{\otimes 4} &= (R \otimes R^{\otimes 3}) \cdot (I_{(3)} \otimes p_{0,2}) \cdot (R \otimes R^{\otimes 3}) \\ &= (R \cdot I_{(1)} \cdot R) \otimes (R^{\otimes 3} \cdot p_{0,2} \cdot R^{\otimes 3}) \\ &= I_{(1)} \otimes (R^{\otimes 3} \cdot p_{0,2} \cdot R^{\otimes 3}). \end{aligned}$$

It becomes apparent that it is enough to check whether $(R^{\otimes 3} \cdot p_{0,2} \cdot R^{\otimes 3}) = p_{0,2}$ to illustrate the validity of Theorem 3.

$R^{\otimes 3} \cdot p_{0,2} \cdot R^{\otimes 3} =$

$=$

1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	1	1	0	0	0	0
1	0	0	0	1	0	0	0
1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1

$\cdot$

1	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	1	0
0	1	0	0	0	0	0	0
0	0	0	0	0	1	0	0
0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	1

$\cdot$

1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	1	1	0	0	0	0
1	0	0	0	1	0	0	0
1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1

$=$

1	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0
1	0	1	0	0	0	0	0
1	0	1	0	1	0	1	0
1	1	0	0	0	0	0	0
1	1	0	0	1	1	0	0
1	1	1	1	0	0	0	0
1	1	1	1	1	1	1	1

$\cdot$

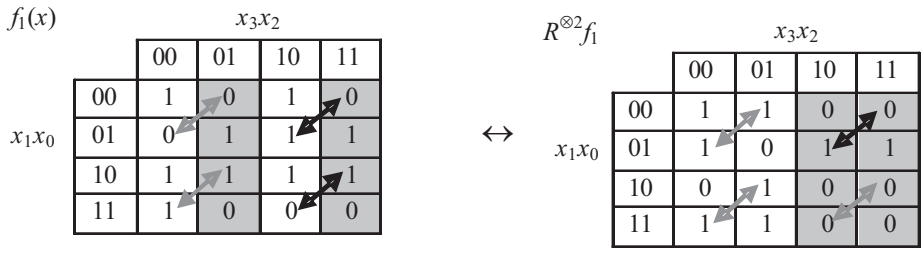
1	0	0	0	0	0	0	0
1	1	0	0	0	0	0	0
1	0	1	0	0	0	0	0
1	1	1	1	0	0	0	0
1	0	0	0	1	0	0	0
1	1	0	0	1	1	0	0
1	0	1	0	1	0	1	0
1	1	1	1	1	1	1	1

$=$

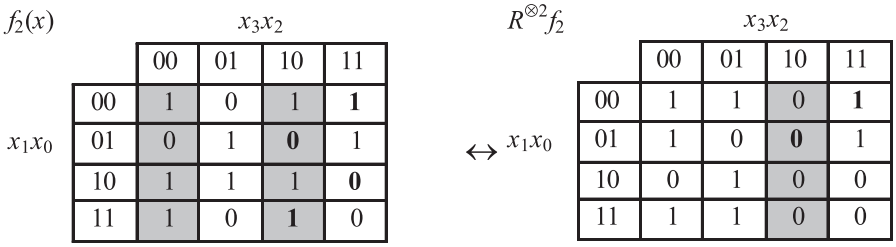
1	0	0	0	0	0	0	0
0	0	0	0	1	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	1	0
0	1	0	0	0	0	0	0
0	0	0	0	0	1	0	0
0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	1

i.e., $(R^{\otimes 3} \cdot p_{0,2} \cdot R^{\otimes 3}) = p_{0,2}$.

The effect of $P_{0,2}$ on f_1 and its RM-spectrum may be illustrated as:



leading to:



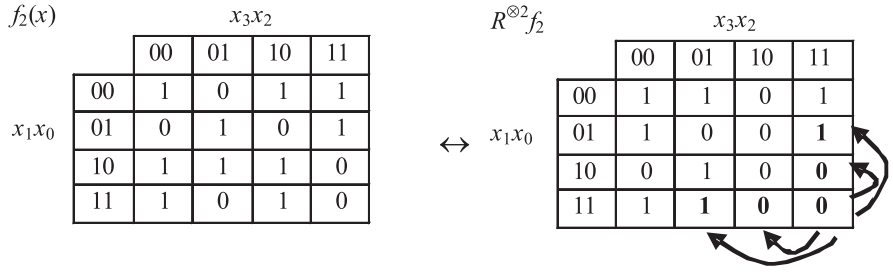
Remark 2 *Notice that* $f_3(x_3,x_2,x_1,x_0) = f_2(x_1,x_0,x_3,x_2)$ *and that this has as effect "transposing the Karnaugh map" (considered as a matrix). The same effect may be observed in the RM spectrum of* f_3.

Remark 3 *Recall Theorem 1, (3):*

$$F_{01} = F_{11} \quad \textit{iff} \quad r_{10} = r_{11}.$$

Notice that whichever the arguments may be that will occupy the positions $n-1$ and $n-2$ and will therefore determine the cofactors, the RM-spectral element r_N will always be an element of the prevailing r_{11}. It is easy to see that if r_N is compared with the RM spectral elements in positions with a Hamming distance of 1, a rejecting criterion is obtained to identify which F_{01} will not possibly be equal to F_{11}. Moreover, since the comparison is based on r_N, then the same applies with respect to Theorem 2, (3). This means that several candidates for partial symmetry may be rejected *with just one scalar comparison*.

Consider, for instance,



Since for the first time the explicit identification of which arguments are considered to be at the positions $(n-1, n-2)$ is needed, the notation will be extended to include this information as superindex. Therefore if the arguments are considered as reordered into (x_2, x_0, x_3, x_1), then $r(x)$ with $x_2 = 1$, $x_0 = 0$, $x_3 = x_1 = 1$, will be written as $r_{1011}^{(0,2)}$, meanwhile $r_{10}^{(2,0)}$ will denote the cofactor when $x_2 = 1$ and $x_0 = 0$. Similarly for $F_{10}^{(2,0)}$.

The comparisons give the following results and implications:

1. $r_{1011}^{(3,2)} = r_{1111}^{(3,2)}$,
2. $r_{0111}^{(3,2)} = r_{1011}^{(2,3)} \neq r_{1111}^{(2,3)} \Longleftrightarrow F_{01}^{(2,3)} \neq F_{11}^{(2,3)}; F_{01}^{(2,3)} \neq \overline{F}_{11}^{(2,3)}$,
3. $r_{1011}^{(1,0)} = r_{1111}^{(1,0)}$,
4. $r_{0111}^{(1,0)} = r_{1011}^{(0,1)} \neq r_{1111}^{(0,1)} \Longleftrightarrow F_{01}^{(0,1)} = (F_{10}^{(1,0)}) \neq F_{11}^{(0,1)}; F_{01}^{(0,1)} \neq \overline{F}_{11}^{(0,1)}$.

Notice that the first equality is satisfied, but $F_{01}^{(3,2)} \neq F_{11}^{(3,2)}$; meanwhile the third is satisfied and this is consistent with $F_{01}^{(1,0)} = \overline{F}_{11}^{(1,0)}$. This shows that the conditions are necessary and sufficient for a rejection, but only necessary for accomplishing the properties presented in Theorems 1 and 2 (3).

5 Conclusions

It has been shown that some classes of partial symmetry of Boolean functions may be characterized in the Reed Muller spectral domain, as earlier was done in the Walsh domain. Particularly interesting is the preservation of permutations of type $P_{i,k}$: when applied to a truth vector, they also apply to the corresponding Reed Muller spectrum.

References

[1] M. Davio, P. Deschamps, and A. Thayse, *Discrete and Switching Functions*. New York NY: McGraw Hill, 1978.

[2] I. Wegener, *The Complexity of Boolean Functions*. NY: Wiley, 1987.

[3] Y. Komamiya, "Theory of computing networks," in *Proc. of the First National Congress for Applied Mathematics*, May 1952, pp. 527–532.

[4] M. Perkowski, P. Kerntopf, A. Buller, M. Chrzanowska-Jeske, A. Mishchenko, X. Song, A. Al-Rabadi, L. Jezwiak, A. Coppola, and B. Massey, "Regular realization of symmetric functions using reversible logic," in *Proc. Euromicro Symp. on Digital Systems Design*, Warsaw, Poland, Sept. 4–6, 2001, pp. 245–252.

[5] T. Sasao, "A new expansion of symmetric functions and their application to non-disjoint functional decompositions for LUT type FPGAs," in *IEEE Int. Workshop on Logic Synthesis, IWLS-2000*, Dana Point, CA, USA, May31-June2, 2000.

[6] J. Shi, G. Fey, and R. Drechsler, "BDD based synthesis of symmetric functions with full path-delay fault testability," in *12th Asian Test Symposium ATS 2003*, Xian, China, Nov. 16–19, November 16-19, 2003, pp. 290–293.

[7] J. Zhang, A. Mishchenko, R. Brayton, and M. Chrzanowska-Jeske, "Symmetry detections for large Boolean functions using circuit representation, simulation and satisfiability," in *Proc. 43rd Design Automation Conf.*, San Francisco, CA, USA, 2006, pp. 510–515.

[8] M. Canteaut, A.and Videau, "Symmetric Boolean functions," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2791–2811, Aug. 2005.

[9] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *Advances in Cryptology - EUROCRYPT 2003 (Lecture Notes in Computer Science)*, Berlin, Germany: Springer-Verlag, 2003, pp. 345–359.

[10] W. Meier, E. Pasalić, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *Advances in Cryptology - EUROCRYPT 2004 (Lecture Notes in Computer Science)*, Berlin, Germany: Springer Verlag, 2004, pp. 474–491.

[11] A. Braeken and B. Preneel, "On the algebraic immunity of symmetric Boolean functions," in *INDOCRYPT 2005 - Lecture Notes in Computer Science*, Berlin, Germany: Springer-Verlag, 2005, pp. 35–48.

[12] J. von zur Gathen and J. Roche, "Polynomials with two values," *Combinatorica*, vol. 17, no. 3, pp. 345–362, 1997.

[13] N. Li and W.-F. Qi, "Symmetric Boolean function depending on odd number of variables with maximum algebraic immunity," *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2271–2273, 2006.

[14] R. Lipton, E. Markakis, A. Mehta, and N. Vishnoi, "On the Fourier spectrum of symmetric Boolean functions," *Combinatorica*, vol. 17, no. 3, pp. 345–362, 1997.

[15] N. Linial, Y. Mansour, and N. N., "Constant depth circuits, Fourier transform and learnability," *Journal of the ACM*, vol. 40, no. 3, pp. 607–620, 1993.

[16] S. Hurst, "Detection of symmetries in combinational functions by spectral means," *IEE Jr. Electronic Circuits and Systems*, vol. 1, pp. 321–342, 1977.

[17] C. Moraga, "Spectral analysis of co-symmetries," in *Proceedings 3rd. International Workshop on Spectral Techniques*, 1988, pp. 127–139, ISSN 0933-6192.

[18] J. Rice and J. Muzio, "Antisymmetries in the realization of Boolean functions," in *Proc. Int. Symp. on Circuits and Systems, ISCAS 2002*, Scottsdale Princess Resort, Scottsdale, Arizona, USA, May 26–29, 2002, paper 2666.

[19] S. Hurst, D. Miller, and J. Muzio, *Spectral Techniques in Digital Logic*. NY: Academic Press, 1985.

[20] D. Dietmeyer and P. Schneider, "Identification of symmetry, redundancy, and equivalence of Boolean functions," *IEEE Trans. Electron. Comput.*, vol. EC-16, pp. 804–817, 1967.

[21] A. Mishchenko, "Fast computation of symmetries in Boolean functions," *IEEE Trans. CAD*, vol. 22, no. 11, pp. 1588–1593, 2003.

[22] D. Moller, J. Mohnke, and M. Weber, "Detection of symmetry of Boolean functions represented by ROBDDs," in *Proc. ICCAD*, Santa Clara, California, USA, 1993, pp. 680–684.

[23] S. Panda, F. Somenzi, and B. Plessier, "Symmetry detection and dynamic variable ordering of decision diagrams," in *Proc. Int. Conf on CAD, ICCAD-94*, San Jose, California, USA, Nov. 6–10, 1994, pp. 628–631.

[24] S. Rahardja and B. Falkowski, "Symmetry conditions of Boolean functions in complex Hadamard transform," *Electronic Letters*, vol. 34, pp. 1634–1635, Aug. 1998.

[25] E. Pogossova and K. Egiazarian, "Reed-Müller representations of symmetric functions," *Multiple Valued Logic and Soft Computing, special issue on* Spectral Techniques, vol. 10, no. 1, pp. 51–72, 2004.

[26] C. Moraga and R. Heider, "A tutorial review on applications of the Walsh transform in switching theory," in *Proc. 1st. International Workshop on Transforms and Filter Banks*, Tampere University of Technology, Finland, 1998, pp. 494–512, ISBN 952-15-0069-7, ISSN 1456-2774.