FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 31, N° 2, June 2018, pp. 303 - 311
https://doi.org/10.2298/FUEE1802303M

ON A PROPERTY OF THE REED-MULLER-FOURIER TRANSFORM

Claudio Moraga

Faculty of Computer Science, Technical University of Dortmund, Germany

Abstract. *The Reed-Muller-Fourier is reviewed and a new property is presented: The Reed-Muller-Fourier transform of an n-place p-valued function preserves any permutation of the arguments. This leads to the additional result that the Reed-Muller-Fourier spectrum of an n-place p-valued symmetric function is also symmetric. Furthermore, the Reed-Muller and the Vilenkin-Chrestenson spectra of an n-place p-valued symmetric function are also symmetric.*

Key words: *Multiple-valued Switching Theory, symmetric functions, Reed-Muller-Fourier transform.*

Dedicated to Prof. Radomir Stanković
on the occasion of his 65th birthday

1. INTRODUCTION

The fundamentals of the Reed-Muller transform may be found in the early work of I. Zhegalkin [1], [2]. However since his publications were in Russian, they remained practically unknown for scientists not proficient in that language. The transform was rediscovered with the works of I.S. Reed [3] and D.E. Muller [4] and since then, it carries their names. In the literature frequently this transform is mentioned as the RM transform. The transform was developed to be applied to Boolean functions. The later extension of the Reed-Muller transform to multiple-valued domains is due to D.H. Green and I.S. Taylor [5].

The Reed-Muller-Fourier transform (RMF) was introduced by Radomir. S. Stanković [6], [7] aiming to combine relevant properties of the Reed-Muller transform and the Discrete Fourier transform. In a way, this transform is another extension of the Reed-Muller transform to the multiple-valued domain. In the binary case, the RMF transform converges to the Reed-Muller transform.

Received August 3, 2017; received in revised form September 8, 2017
Corresponding author: Claudio Moraga
Faculty of Computer Science, Technical University of Dortmund, Germany
(E-mail: claudio.moraga@tu-dortmund.de)

An important common property of both the RM and RMF transforms is the fact that they represent bijections in the set of p–valued functions. This means that the RM spectrum or the RMF spectrum of an n–place p–valued functions is again an n–place p–valued function, not necessarily different from the original one. (It has been shown that both transforms have fixed points [8], [9]). Moreover, both the RM and the RMF transforms have a Kronecker product structure. (Kronecker product: see e.g. [10], [11]).

The RMF transform matrix is lower triangular [12] and exhibits special similarities with the Pascal matrix on finite fields [13].

2. FORMALISMS

Notation:

Vectors and Matrices will be written with upper case in bold. If $\mathbf{M}$ is a $p^m \times p^n$ matrix, it will be denoted simply as $\mathbf{M}_{m,n}$. Square matrices will be assigned just one index. If not clear from the context, the length of vectors will be explicitly given. An exception to this notation is "$\mathbf{X}_{p\mathrm{RMF}}$", which, for historical reasons [7] will be used to denote the basis of the RMF transform.

Spectral Techniques in a nut shell:

Let V = {0, 1, …, p–1} be the domain of p–valued functions and let f: $V^n \to V$, be an n-place p–valued function. To every function f, a value column vector $\mathbf{F}$ of length p^n is associated. The elements of $\mathbf{F}$ are the values of f for all the different value assignments to the arguments. The elements of $\mathbf{F}$ follow the lexicographic order of the value assignments to the arguments of f. Let $f \leftrightarrow \mathbf{F}$ denote the association. It is obvious that $f \leftrightarrow \mathbf{I}_n \cdot \mathbf{F}$, where $\mathbf{I}_n$ denotes the identity matrix, represents a valid association. If $\mathbf{M}_n$ is a non-singular matrix, its inverse is also non-singular and well defined. Moreover since $(\mathbf{M}_n)^{-1} \cdot \mathbf{M}_n = \mathbf{I}_n$, then $f \leftrightarrow (\mathbf{M}_n)^{-1} \cdot \mathbf{M}_n \cdot \mathbf{F}$ is also a valid association and represents the basic concept of spectral transformations. Since $(\mathbf{M}_n)^{-1}$ is non-singular, its columns form a linearly independent set. If the columns of $(\mathbf{M}_n)^{-1}$ are considered to represent value vectors of auxiliary functions, then $(\mathbf{M}_n)^{-1}$ constitutes a basis. $\mathbf{M}_n$, the inverse of $(\mathbf{M}_n)^{-1}$, is called a transform matrix and the product $\mathbf{M}_n \cdot \mathbf{F}$ is normally called the *spectrum* of f. The inner product of the basis and the spectrum leads to a polynomial expression of f. Depending on the choice of $(\mathbf{M}_n)^{-1}$, different polynomial expressions on elements of the basis will be obtained.

Definition 1:
Let $f, g : Z_p \to Z_p$. The Gibbs convolution product ($\times$) of p-valued functions is calculated as follows [6]:
If $x = 0$, then $(f \times g)(0) = 0$.
If $x \neq 0$, then $(f \times g)(x) = \sum_{s=0}^{x-1} f(x-1-s) \cdot g(s) \bmod p$

Definition 2:
The fundamental basis for the RMF transform, called $\mathbf{X}_{p\mathrm{RMF}}$ is the following [6], [7]:

$$\mathbf{X}_{p\mathrm{RMF}} = [x*^0 \quad x*^1 \quad \dots \quad x*^{(p-1)}],$$

where $x*^0$ is defined to be the constant $p-1$ for all x, and for $1 \le j \le p-1$, the powers $x*^j$ are calculated as the j–fold Gibbs product of $x*^0$ with itself.

It is simple to show that $\mathbf{X}_{p\mathrm{RMF}}$ is its own inverse. Therefore the basic RMF transform matrix, called $\mathbf{R}_1$ equals $\mathbf{X}_{p\mathrm{RMF}}$, and for all $n > 1$ holds:

$$\mathbf{R}_n = (\mathbf{X}_{p\mathrm{RMF}})^{\otimes n},$$

where the exponent "$\otimes n$" denotes the n-fold Kronecker product of $\mathbf{X}_{p\mathrm{RMF}}$ with itself. Since $\mathbf{X}_{p\mathrm{RMF}}$ is its own inverse, it is easy to see that $\mathbf{R}_n$ will also be its own inverse.

Example 1:

Let $n = 2$ and $p = 3$. Calculating mod 3,

$$\mathbf{R}_2 = \begin{bmatrix} 2 & 0 & 0 \\ 2 & 1 & 0 \\ 2 & 2 & 2 \end{bmatrix}^{\otimes 2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 2 & 2 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Notice that the borders of $\mathbf{R}_2$ look different than those of $\mathbf{R}_1$. This will happen whenever n is even, since for all p, $(p-1)^n \equiv 1 \bmod p$. If this is inconvenient for some application, then a *normalized* transform may be used.

Definition 3:

The *normalized* RMF transform is given by

$$\mathbf{R}_n = (-1)^{n+1}\, \mathbf{X}_{p\mathrm{RMF}}(1)^{\otimes n} \bmod p.$$

The factor $(-1)^{n+1}$ is introduced to preserve the value $(p-1)$, in the leftmost column of the matrix when n is even, since $(-1)^{n+1}(p-1)^n \equiv (p-1)^{n+1}(p-1)^n \equiv (p-1)^{2n+1} \bmod p$. $2n + 1$ will be an odd number and an odd power of $(p-1)$ equals $(p-1) \bmod p$. It is simple to see that in this case $\mathbf{R}_n$ is also self-inverse.

If for particular applications a "homogeneous and DFT-like look" is desirable, then a *special* RMF transform may be used.

Definition 4:

The *special* RMF transform equals $(p\text{-}1)(\mathbf{X}_{p\mathrm{RMF}})^{\otimes n} \bmod p$. See Figure 1.

$$\begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix} ; \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 1 & 3 & 3 \end{bmatrix} ; \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 4 & 0 & 0 & 0 \\ 1 & 3 & 1 & 0 & 0 \\ 1 & 2 & 3 & 4 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Fig. 1 Special RMF transform matrices for $p = 3$, 4, and 5 when $n = 1$

If for any p $\mathbf{R}_1$ is expressed as $[r_{i,j}]$, $i, j \in \mathbb{Z}_p$, then $r_{i,j} = (-1)^j \binom{i}{j} \bmod p$ [12].

It may be observed that in the case when p is a prime, the matrices are skew-symmetric, i.e., symmetric with respect to the diagonal with positive slope. Furthermore besides being skew-symmetric and self inverse, starting at the lower left corner and moving along the diagonal with positive slope, a Pascal triangle mod p is found.

An important property of the RMF transform is the following: The RMF transform of a non-zero constant vector is an "impulse" vector, i.e. a vector with only one non-zero entry, at the 0-th position [12]. This is a well known property of the DFT, which is preserved by the RMF transform.

3. THEOREMS

Theorem 1.

Preliminaries:

Let V = {0, 1, …, p–1} be the domain of p–valued functions and let $f : V^2 \to V$, with value vector **F** of length p^2. Moreover let $g : V^2 \to V$, such that $g(x_1, x_2) = f(x_2, x_1)$. Let the value vector of g be **G**. Furthermore, let $\mathbf{P}_2$ be a permutation matrix such that when applied upon **F** induces a permutation of its components according to the reordering of the arguments of the function. Hence $\mathbf{G} = \mathbf{P}_2 \cdot \mathbf{F}$.

Claim: The RMF transform of a p-valued function of two variables preserves the order of the arguments.

$$\mathbf{R}_2 \cdot \mathbf{G} = \mathbf{R}_2 \cdot \mathbf{P}_2 \cdot \mathbf{F} = \mathbf{P}_2 \cdot \mathbf{R}_2 \cdot \mathbf{F} \quad \bmod p.$$

Proof:

Let $i, j \in \left(\mathbb{Z}_p\right)^2$, with $i = i_1 i_0$ and $j = j_1 j_0$.

Since **R** has a Kronecker product structure, then $\mathbf{R}_2 = \mathbf{R}_1 \otimes \mathbf{R}_1 \bmod p$.

If $\mathbf{R}_2$ is expressed as $[r_{i,j}]$ then

$$r_{i,j} = \left((-1)^{j_1}\binom{i_1}{j_1}\right) \cdot \left((-1)^{j_0}\binom{i_0}{j_0}\right) = (-1)^{j_1+j_0}\frac{i_1!\cdot i_0!}{j_1!(i_1-j_1)!\, j_0!(i_0-j_0)!} \bmod p.$$

If i_1 and i_0 are exchanged, then

$$\text{modified } r_{i,j} = (-1)^{j_1+j_0}\frac{i_0!\cdot i_1!}{j_1!(i_0-j_1)!\, j_0!(i_1-j_0)!} \bmod p.$$

and if j_1 and j_0 are exchanged, then

$$\text{modified } r_{i,j} = (-1)^{j_0+j_1}\frac{i_1!\cdot i_0!}{j_0!(i_1-j_0)!\, j_1!(i_0-j_1)!} \quad \bmod p.$$

It is simple to see that in both cases the modified $r_{i,j}$ takes the same value. Moreover, exchanging i_1 and i_0 has the effect of exchanging (the corresponding) two rows of $\mathbf{R}_2$ and, similarly, exchanging j_1 and j_0 has the effect of exchanging (the corresponding) two columns of $\mathbf{R}_2$. Exchanging i_1 and i_0 corresponds to $\mathbf{P}_2 \cdot \mathbf{R}_2$, while exchanging j_1 and j_0 corresponds to $\mathbf{R}_2 \cdot \mathbf{P}_2$.

The assertion follows.

□

Although not explicitly needed for Theorem 1, it is not difficult to construct the $\mathbf{P}_2$ matrices for different values of p, because of the strong regularity of their structure. They are symmetric, skew-symmetric and self inverse. See Figure 2.

$$\begin{bmatrix} \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} \end{bmatrix} \quad \begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{bmatrix} \quad \begin{bmatrix} \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & \mathbf{0} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{bmatrix}$$

Fig. 2 $\mathbf{P}_2$ matrices for $p = 2$, $p = 3$, and $p = 4$

Corollary 1.1:

From $\mathbf{P}_2 \cdot \mathbf{R}_2 = \mathbf{R}_2 \cdot \mathbf{P}_2$ and recalling that $\mathbf{R}_2$ is self inverse follows that $\mathbf{P}_2 = \mathbf{R}_2 \cdot \mathbf{P}_2 \cdot \mathbf{R}_2$.

Since $\mathbf{P}_2$ is also self inverse, then $\mathbf{P}_2 \cdot \mathbf{P}_2 = \mathbf{R}_2 \cdot \mathbf{P}_2 \cdot \mathbf{R}_2 \cdot \mathbf{P}_2 = \mathbf{I}_2$, meaning that $\mathbf{R}_2 \cdot \mathbf{P}_2$ is also its own inverse.

Theorem 2.

Let $n \geq 2$ and $k < n$. Define f and g to be p-valued functions of n variables (i.e. n-place functions) with value vectors $\mathbf{F}$ and $\mathbf{G}$, respectively, such that for all value assignments to the arguments, g equals f, but with transposed arguments x_k and x_{k+1}. Let $\mathbf{P}_n$ be a permutation which when applied to $\mathbf{F}$ has the effect of transposing only the two selected arguments, i.e., $\mathbf{P}_n = (\mathbf{I}_{k\text{-}1} \otimes \mathbf{P}_2 \otimes \mathbf{I}_{n\text{-}k\text{-}1})$.

Then

$$\mathbf{R}_n \cdot \mathbf{P}_n \cdot \mathbf{F} = \mathbf{P}_n \cdot \mathbf{R}_n \cdot \mathbf{F} \bmod p.$$

Proof:

Decompose $\mathbf{R}_n$ to match the structure of $\mathbf{P}_n$. I.e. $\mathbf{R}_n = \mathbf{R}_{k\text{-}1} \otimes \mathbf{R}_2 \otimes \mathbf{R}_{n\text{-}k\text{-}1}$, and apply it to both sides of the claim, taking advantage of the compatibility between Kronecker and matrix products [11]:

$$\begin{aligned} \mathbf{R}_n \cdot \mathbf{P}_n \cdot \mathbf{F} &= (\mathbf{R}_{k\text{-}1} \otimes \mathbf{R}_2 \otimes \mathbf{R}_{n\text{-}k\text{-}1}) \cdot (\mathbf{I}_{k\text{-}1} \otimes \mathbf{P}_2 \otimes \mathbf{I}_{n\text{-}k\text{-}1}) \cdot \mathbf{F} \\ &= (\mathbf{R}_{k\text{-}1} \otimes \mathbf{R}_2 \mathbf{P}_2 \otimes \mathbf{R}_{n\text{-}k\text{-}1}) \cdot \mathbf{F} \bmod p. \end{aligned}$$

$$\begin{aligned} \mathbf{P}_n \cdot \mathbf{R}_n \cdot \mathbf{F} &= (\mathbf{I}_{k\text{-}1} \otimes \mathbf{P}_2 \otimes \mathbf{I}_{n\text{-}k\text{-}1}) \cdot (\mathbf{R}_{k\text{-}1} \otimes \mathbf{R}_2 \otimes \mathbf{R}_{n\text{-}k\text{-}1}) \cdot \mathbf{F} \\ &= (\mathbf{R}_{k\text{-}1} \otimes \mathbf{P}_2 \mathbf{R}_2 \otimes \mathbf{R}_{n\text{-}k\text{-}1}) \cdot \mathbf{F} \bmod p. \end{aligned}$$

It is easy to see that the claim will be satisfied if and only if $\mathbf{P}_2 \mathbf{R}_2 = \mathbf{R}_2 \mathbf{P}_2$. This was proven in Theorem 1.

The assertion follows. □

Example 2.

Let $p = 4$ and $n = 2$. Calculate $\mathbf{P}_2 \cdot \mathbf{R}_2$ operating mod 4.

$$\mathbf{P}_2 \cdot \mathbf{R}_2 = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1
\end{bmatrix} \cdot \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&2&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&3&3&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0\\
1&3&0&0&3&1&0&0&0&0&0&0&0&0&0&0\\
1&2&1&0&3&2&3&0&0&0&0&0&0&0&0&0\\
1&1&3&3&3&3&1&1&0&0&0&0&0&0&0&0\\
1&0&0&0&2&0&0&0&1&0&0&0&0&0&0&0\\
1&3&0&0&2&2&0&0&1&3&0&0&0&0&0&0\\
1&2&1&0&2&0&2&0&1&2&1&0&0&0&0&0\\
1&1&3&3&2&2&2&2&1&1&3&3&0&0&0&0\\
1&0&0&0&1&0&0&0&3&0&0&0&3&0&0&0\\
1&3&0&0&1&3&0&0&3&1&0&0&3&1&0&0\\
1&2&1&0&1&2&1&0&3&2&3&0&3&2&3&0\\
1&1&3&3&1&1&3&3&3&3&1&1&3&3&1&1
\end{bmatrix} =$$

$$= \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&3&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&2&0&0&0&1&0&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&3&0&0&0&3&0&0&0\\
1&3&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&3&0&0&3&1&0&0&0&0&0&0&0&0&0&0\\
1&3&0&0&2&2&0&0&1&3&0&0&0&0&0&0\\
1&3&0&0&1&3&0&0&3&1&0&0&3&1&0&0\\
1&2&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&2&1&0&3&2&3&0&0&0&0&0&0&0&0&0\\
1&2&1&0&2&0&2&0&1&2&1&0&0&0&0&0\\
1&2&1&0&1&2&1&0&3&2&3&0&3&2&3&0\\
1&1&3&3&0&0&0&0&0&0&0&0&0&0&0&0\\
1&1&3&3&3&3&1&1&0&0&0&0&0&0&0&0\\
1&1&3&3&2&2&2&2&1&1&3&3&0&0&0&0\\
1&1&3&3&1&1&3&3&3&3&1&1&3&3&1&1
\end{bmatrix}$$

From Corollary 1.1, $(\mathbf{P}_2 \cdot \mathbf{R}_2)^{-1} = \mathbf{P}_2 \cdot \mathbf{R}_2 = \mathbf{R}_2 \cdot \mathbf{P}_2$ therefore commuting the factor matrices will give the same result.

Theorem 3.

Let f and g be n-place p-valued functions with value vectors **F** and **G**, respectively, such that for all value assignments to the arguments, g equals f, but with transposed arguments x_k and x_{k+1} and transposed arguments x_h and x_{h+1}. $(n > k > h > 0)$. If applied independently, let the corresponding transposition matrices be $\mathbf{P}_n^{(k)}$ and $\mathbf{P}_n^{(h)}$, respectively, leading to $\mathbf{G} = \mathbf{P}_n^{(k)} \cdot \mathbf{P}_n^{(h)} \cdot \mathbf{F}$. The following holds:

$$\mathbf{R}_n \cdot \mathbf{G} = \mathbf{P}_n^{(k)} \cdot \mathbf{P}_n^{(h)} \cdot \mathbf{R}_n \cdot \mathbf{F} \bmod p.$$

Proof:

Consider first one of the transpositions.

Let $\mathbf{G'} = \mathbf{P}_n^{(h)} \cdot \mathbf{F} \bmod p$.

Then from Theorem 1 follows that

$\mathbf{R}_n \cdot \mathbf{G'} = \mathbf{R}_n \cdot \mathbf{P}_n^{(h)} \cdot \mathbf{F} = \mathbf{P}_n^{(h)} \cdot \mathbf{R}_n \cdot \mathbf{F} \bmod p$.

Now let the second transposition be executed.

$\mathbf{G} = \mathbf{P}_n^{(k)} \cdot \mathbf{G'}$.

Then from Theorem 1 follows that

$$\mathbf{R}_n \cdot \mathbf{G} = \mathbf{R}_n \cdot \mathbf{P}_n^{(k)} \cdot \mathbf{G'} = \mathbf{P}_n^{(k)} \cdot \mathbf{R}_n \cdot \mathbf{G'} =$$
$$= \mathbf{P}_n^{(k)} \cdot \mathbf{P}_n^{(h)} \cdot \mathbf{R}_n \cdot \mathbf{F} \bmod p.$$

□

Theorem 4.

Let f and g be n-place p-valued functions with value vectors **F** and **G**, respectively, such that for all value assignments to the arguments, g equals f, but with permuted arguments. Let $\mathbf{P}_n$ be a permutation matrix, which when applied to **F** has the same effect as permuting the corresponding arguments.

Then

$$\mathbf{R}_n \cdot \mathbf{G} = \mathbf{R}_n \cdot \mathbf{P}_n \cdot \mathbf{F} = \mathbf{P}_n \cdot \mathbf{R}_n \cdot \mathbf{F} \bmod p.$$

Proof:

Recall that any permutation of an ordered set of arguments may be obtained with an appropriate sequence of transpositions, and any transposition may be obtained with a cascade of transpositions of neighbor arguments. Apply accordingly Theorems 2 and 3 as many times as needed.

□

Theorem 5.

The RMF spectrum of an n-place p-valued symmetric function is symmetric.

Proof:

Recall that a p-valued function is symmetric iff it is invariant with respect to any permutation of its arguments. (See e.g. [14], [15], [16], [17])

Let **F** be the value vector of a symmetric function and let $\mathbf{P}_n$ be equivalent to a random permutation of its arguments.

Then

$$\mathbf{F} = \mathbf{P}_n \cdot \mathbf{F}.$$

From Theorem 4,

$$\mathbf{R}_n \cdot \mathbf{F} = \mathbf{R}_n \cdot \mathbf{P}_n \cdot \mathbf{F} = \mathbf{P}_n \cdot \mathbf{R}_n \cdot \mathbf{F} \bmod p.$$

Therefore $\mathbf{R}_n \cdot \mathbf{F} \bmod p$ is symmetric.

□

Example 3:

Let $p = 4$ and $f : \mathrm{V}^2 \to \mathrm{V}$ be symmetric, such that

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

Let $\mathbf{S} = \mathbf{R}_2 \cdot \mathbf{F}$

$$\mathbf{S} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 3 & 2 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 3 & 3 & 3 & 3 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 2 & 2 & 0 & 0 & 1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 2 & 0 & 2 & 0 & 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 3 & 3 & 2 & 2 & 2 & 2 & 1 & 1 & 3 & 3 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 1 & 3 & 0 & 0 & 3 & 1 & 0 & 0 & 3 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 & 1 & 2 & 1 & 0 & 3 & 2 & 3 & 0 & 3 & 2 & 3 & 0 \\ 1 & 1 & 3 & 3 & 1 & 1 & 3 & 3 & 3 & 3 & 1 & 1 & 3 & 3 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 3 \\ 1 \\ 2 \\ 3 \\ 1 \\ 0 \\ 3 \\ 3 \\ 2 \\ 3 \\ 1 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 3 \\ 3 \\ 0 \\ 1 \\ 3 \\ 0 \\ 3 \\ 3 \\ 0 \\ 3 \\ 3 \\ 0 \\ 3 \\ 2 \end{bmatrix}$$

Symmetry proof:

x_2	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
x_1	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3
$\mathbf{F}^T$	1	1	0	3	1	2	3	1	0	3	3	2	3	1	2	0
$\mathbf{S}^T$	1	0	3	3	0	1	3	0	3	3	0	3	3	0	3	2

It is easy to see that **S**, the spectrum of **F**, is also symmetric.

Remark:

It was shown in [18] that an analog to Theorem 3 holds for spectra obtained with the Reed-Muller or the Vilenkin-Chrestenson transforms. This also includes the circular Vilenkin-Chrestenson spectrum.

Corollary 5.1.

The Reed-Muller and the Vilenkin-Chrestenson spectra of p–valued symmetric functions are symmetric.

Corollary 5.2.

If f is a p–valued bent function [20], [19], then the function obtained after permuting the value assignment to the arguments is also bent, since the circular Vilenkin-Chrestenson spectrum will remain flat., i.e. all its components will have a constant absolute value equal to $p^{n/2}$.

4. CONCLUSIONS

It has been shown that the RMF transform shares with the Reed-Muller and the Vilenkin-Chrestenson transforms the property of preserving any permutation of the arguments, in spite of their different structural attributes. Recall that the Vilenkin-Chrestenson transform is complex-valued, symmetric, and unitary up to a normalizing coefficient; the Reed-Muller transform is integer-valued and neither symmetric nor orthogonal; and the Reed-Muller-Fourier transform is integer-valued, lower triangular, and self inverse.

REFERENCES

[1] I.I. Zhegalkin, “O tekhnyke vychyslenyi predlozhenyi v symbolytscheskoi logykye,” *Math. Sb.*, vol. 34, pp. 9-28, in Russian, 1927.

[2] I.I. Zhegalkin, “Aritmetizatiya symbolytscheskoi logyky,” *Math. Sb.*, vol. 35, pp. 311-377, in Russian, 1928.

[3] I.S. Reed, “A class of multiple-error-correcting codes and the decoding scheme.” *IRE Trans. on Information Theory* PGIT-4, pp. 38-49, 1954.

[4] D.E. Muller, “Application of Boolean algebra to switching circuit design and to error correction.” *IRE Trans. on Elec. Computers* EC-3, vol. 3, pp. 6-12, 1954.

[5] D.H. Green and I.S. Taylor, “Multiple-valued switching circuit design by means of generalized Reed-Muller expansions.” *Digital Processes* 2, pp. 63-81, 1976.

[6] R.S. Stanković, “Some remarks on Fourier transforms and differential operators for digital functions,” In Proceedings of the 22nd International Symposium on Multiple-valued Logic, Sendai, Japan, IEEE Press N.Y., 1992, pp. 365-370.

[7] R.S. Stanković, "The Reed-Muller-Fourier Transform – Computing Methods and Factorizations", *Claudio Moraga: A Passion for Multi-Valued Logic and Soft Computing.* (R. Seising, H. Allende-Cid, Eds.), Springer 2017, pp. 121-151.

[8] C. Moraga, S. Stojković and R.S. Stanković, "On fixed points and cycles in the Reed Muller domain." In Proceedings of the 38th International Symposium on Multiple-valued Logic, IEEE Press, 2008, pp. 82-88.

[9] C. Moraga, R.S. Stanković, M. Stanković and S. Stojković, "On fixed points of the Reed-Muller-Fourier Transform." In Proceedings of the 47th International Symposium on Multiple-valued Logic, IEEE Press, 2017, pp. 55-60.

[10] A. Graham, *Kronecker products and matrix calculus with applications.* Ellis Horwood Ltd., Chichester UK, 1981.

[11] R.A. Horn and Ch.R. Johnson, *Topics in matrix analysis.* Cambridge University Press, New York, 1991.

[12] C. Moraga, R.S. Stanković and M. Stanković, "A comparative study of the Reed-Muller-Fourier transform, the Pascal matrix, and the Discrete Pascal Transform." Research Report FSC-2015-02, European Centre for Soft Computing, Mieres, Asturias, Spain, 2015.

[13] R.S. Stanković, J.T. Astola and C. Moraga, "Pascal matrices, Reed-Muller expressions, and Reed-Muller error correcting codes." In *Logic in Computer Science II*, (S. Ghilezan, Ed.), Press Mathematical Institute of the Serbian Academy of Science, Belgrade, Serbia, 2015., Zbornik radova 18 (26), pp. 145-172.

[14] E. Pogossova and K. Egiazarian, "Reed-Muller representation of symmetric functions." *J. Multiple-valued Logic and Soft Computing*, vol. 10, no. 1, pp. 51-72, 2004.

[15] R.S. Stanković, J.T. Astola and K. Egiazarian, "Remarks on symmetric binary and multiple-valued functions." In Proceedings of the 6th International Workshop Boolean Problems, B. Steinbach (Ed.), 2004, pp. 83-87.

[16] J.T. Butler and K. A. Schueller, "Worst Case Number of Terms In Symmetric Multiple-valued Functions." In Proceedings of the 21st International Symposium on Multiple-valued Logic. IEEE Press, 1991.

[17] J.C. Muzio, "Concerning the maximum size of the terms in the realization of symmetric functions." In Proceedings of the 20th International Symposium on Multiple-valued Logic, 1990, pp. 292-299.

[18] C. Moraga, "Permutations under Spectral Transforms." In Proceedings of the 38th International Symposium on Multiple-valued Logic, IEEE Press, 2008, pp. 76-81.

[19] P.V. Kumar, R.A. Scholz and L.R. Welch, "Generalized bent functions and their properties." *Jr. Combinatorial Theory Series A*, vol. 40, no. 1, 90-107, 1985.

[20] C. Moraga, M. Stanković, R.S. Stanković and S. Stojković, "Contribution to the study of Multiple-valued Bent Functions." In Proceedings of the 33rd International Symposium on Multiple-Valued Logic, IEEE Press, 2013, pp. 340-345.