The Eigenfunction of the Reed-Muller Transformation

T. Sasao

Department of Computer Science
and Electronics
Kyushu Institute of Technology
Iizuka, 820-8502 JAPAN
sasao@kyutech.ac.jp

J. T. Butler

Department of Electrical
and Computer Engineering
Naval Postgraduate School
Monterey, CA U.S.A. 93943-5212
Jon_Butler@msn.com

Abstract

We introduce eigenfunctions of the Reed-Muller transform. Eigenfunctions are functions whose canonical sum-of-products expression and PPRM (positive polarity Reed-Muller expression) are isomorphic. In the case of symmetric functions, the eigenfunction can be viewed as a function whose reduced truth vector is identical to the reduced Reed-Muller spectrum. We show that the number of symmetric (ordinary) eigenfunctions on n-variables is $2^{\lceil \frac{n+1}{2} \rceil}$ ($2^{2^{n-1}}$). We identify three special symmetric functions that correspond to the most complicated minimal fixed polarity Reed-Muller (FPRM) form. We show how the transeunt triangle can be used to convert between the reduced (ordinary) truth vector and the reduced (ordinary) Reed-Muller spectrum. We derive the number of products in the FPRM for these symmetric functions: this shows that they have the most complicated minimal FPRM among all n-variable functions.

1 AND-EXOR Expressions

In this part, we define some classes of AND-EXOR expressions.

Theorem 1.1 *An arbitrary logic function $f(x_1, x_2, \ldots, x_n)$ can be expanded as*

$$f(x_1, x_2, \ldots, x_n) = f_0 \oplus x_1 f_2 \quad (1.1)$$
$$f(x_1, x_2, \ldots, x_n) = \bar{x}_1 f_2 \oplus f_1 \quad (1.2)$$
$$f(x_1, x_2, \ldots, x_n) = \bar{x}_1 f_0 \oplus x_1 f_1, \quad (1.3)$$

where $f_0 = f(0, x_2, \ldots, x_n)$, $f_1 = f(1, x_2, \ldots, x_n)$, and $f_2 = f_0 \oplus f_1$.

(1.1)–(1.3) are the **positive Davio expansion**, the **negative Davio expansion**, and the **Shannon expansion**, respectively.

Definition 1.1 *By expanding the function f using (1.1) recursively, we have a logical expression with only uncomplemented literals:*

$$a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus \cdots$$
$$\oplus a_{n-1,n} x_{n-1} x_n \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n.$$

This is a **positive polarity Reed-Muller expression** *(***PPRM***).*

The **minimization problem** is the problem of finding an expression with the fewest products. For any logic function, the PPRM is unique and is, therefore, minimal. The average number of products in PPRMs for n-variable functions is 2^{n-1} [20].

Example 1.1 *Represent $f = \bar{x}_1 \bar{x}_2 \bar{x}_3$ by a PPRM. By substituting $\bar{x}_1 = x_1 \oplus 1$, $\bar{x}_2 = x_2 \oplus 1$, $\bar{x}_3 = x_3 \oplus 1$, we have*

$$f = (x_1 \oplus 1)(x_2 \oplus 1)(x_3 \oplus 1)$$
$$= 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_1 x_2 \oplus x_2 x_3 \oplus x_1 x_3 \oplus x_1 x_2 x_3.$$

Note that this expression uses uncomplemented literals only, and is therefore a PPRM. (End of Example)

In general, $\bar{x}_1 \bar{x}_2 \cdots \bar{x}_n$ requires 2^n products in a PPRM. Note that this is the **most complicated function to realize using a PPRM**.

Definition 1.2 *By expanding the function f using (1.2) recursively, we have a logical expression with only complemented literals:*

$$a_0 \oplus a_1 \bar{x}_1 \oplus \cdots \oplus a_n \bar{x}_n \oplus a_{12} \bar{x}_1 \bar{x}_2 \oplus a_{13} \bar{x}_1 \bar{x}_3 \oplus \cdots$$
$$\oplus a_{n-1,n} \bar{x}_{n-1} \bar{x}_n \oplus \cdots \oplus a_{12\cdots n} \bar{x}_1 \bar{x}_2 \cdots \bar{x}_n.$$

This is a **negative polarity Reed-Muller expression** *(***NPRM***).*

Definition 1.3 *By applying the positive Davio expansion or the negative Davio expansion to the given function f, we have a logical expression that has a form similar to a PPRM. In this case, assume that we can use either uncomplemented literals or complemented literals but not both for each variable. Such a logical expression is a* **fixed polarity Reed-Muller expression** *(***FPRM***).*

For an n-variable function, there are 2^n different FPRMs corresponding to 2^n ways to complement n variables. The minimization problem is to find one with the fewest products among all 2^n possible FPRMs.

Definition 1.4 *A* **minimum FPRM** (**MFPRM**) *of a function f is an FPRM of f with the fewest products.*

Example 1.2 *Represent the function $f = x_1x_2x_3x_4 \vee \bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4$ by an FPRM. Since the two products are disjoint, f can be represented as $f = x_1x_2x_3x_4 \oplus \bar{x}_1\bar{x}_2\bar{x}_3\bar{x}_4$. By applying the positive Davio expansion to x_1 and x_2, and the negative Davio expansion to x_3 and x_4, we have an expression where x_1 and x_2 appear as uncomplemented literals, and x_3 and x_4 appear as complemented literals. Thus, by substituting $\bar{x}_1 = x_1 \oplus 1$, $\bar{x}_2 = x_2 \oplus 1$, $x_3 = \bar{x}_3 \oplus 1$, and $x_4 = \bar{x}_4 \oplus 1$ into f, we have*

$$\begin{aligned} f &= x_1x_2(\bar{x}_3 \oplus 1)(\bar{x}_4 \oplus 1) \oplus (x_1 \oplus 1)(x_2 \oplus 1)\bar{x}_3\bar{x}_4 \\ &= x_1x_2(1 \oplus \bar{x}_3 \oplus \bar{x}_4 \oplus \bar{x}_3\bar{x}_4) \\ &\qquad \oplus (1 \oplus x_1 \oplus x_2 \oplus x_1x_2)\bar{x}_3\bar{x}_4 \\ &= x_1x_2 \oplus x_1x_2\bar{x}_3 \oplus x_1x_2\bar{x}_4 \oplus \bar{x}_3\bar{x}_4 \oplus x_1\bar{x}_3\bar{x}_4 \\ &\qquad \oplus x_2\bar{x}_3\bar{x}_4. \end{aligned}$$

Note that the last expression is an FPRM. By deriving all FPRMs, it can be shown that this is an MFPRM. (End of Example)

In general, $x_1x_2\cdots x_n \vee \bar{x}_1\bar{x}_2\cdots\bar{x}_n$ $(n = 2r)$ requires $2^{r+1} - 2$ products in an MFPRM (See p.291 of [18]). This is a symmetric function. It is tempting to believe that this function has the largest MFPRM among all symmetric functions on n variables. However, as discussed later, this is not the case.

2 Reed-Muller Transformation

In this part, we define the Reed-Muller spectrum and the Reed-Muller transformation matrix [21].

Definition 2.1 *Let*

$$\mathbf{R}(1) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix},$$

and

$$\mathbf{R}(n) = \begin{bmatrix} \mathbf{R}(n-1) & 0 \\ \mathbf{R}(n-1) & \mathbf{R}(n-1) \end{bmatrix}.$$

$\mathbf{R}(n)$ is the **Reed-Muller transformation matrix of** *n* **variables***.*

Note that the calculations are done in GF(2). The **inverse** of a Reed-Muller transformation matrix $\mathbf{R}(n)$ is $\mathbf{R}(n)$, *i.e.*, $\mathbf{R}(n)$ is **self-inverse**.

Example 2.1 *The Reed-Muller transformation matrix of two variables* **R***(2) is*

$$\mathbf{R}(2) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

(End of Example)

Definition 2.2 *Let $\vec{F} = (f_0, f_1, \ldots, f_{2^n-1})$ be the* **truth vector** *of an n-variable logic function f, and let $\vec{S} = (s_0, s_1, \ldots, s_{2^n-1})$ be the* **Reed-Muller spectrum** *of f. Then, two relations $\vec{S} = \mathbf{R}(n)\vec{F}^t$ and $\vec{F} = \mathbf{R}(n)\vec{S}^t$ hold, where t denotes transpose of the vector. In this case, s_i is a* **Reed-Muller coefficient** *of f, where $i \in \{0, 1, \ldots, 2^n-1\}$.*

Example 2.2 *Consider the function $f = \bar{x}_1x_2 \vee x_1\bar{x}_2$. Note that $\vec{F} = (f_0, f_1, f_2, f_3) = (0, 1, 1, 0)$. The Reed-Muller spectrum is computed as*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}.$$

Thus, we have the spectrum $\vec{S} = (s_0, s_1, s_2, s_3) = (0, 1, 1, 0)$. Note that the first element corresponds to the constant function 1; the second element corresponds to the function x_2; the third element corresponds to the function x_1; and the last element corresponds to the function x_1x_2. This means that the function is represented by $f = x_1 \oplus x_2$. (End of Example)

3 Eigenfunction of the Reed-Muller Transform

In linear algebra, $\vec{x}$ is an **eigenvector** of a matrix A if there exists a constant λ such that $A\vec{x} = \lambda\vec{x}$. In the Reed-Muller transform, the computations are done in GF(2), and 1 is the only non-zero value of λ. Thus, we have

Definition 3.1 *Let $\vec{F}$ be a binary vector of 2^n elements, and $\mathbf{R}(n)$ be the Reed-Muller transformation matrix of n variables. Then, a vector $\vec{F}$ satisfying $\mathbf{R}(n)\vec{F} = \vec{F}$ is an* **eigenvector** *of Reed-Muller transformation. The function corresponding to the eigenvector is an* **eigenfunction** *of the Reed-Muller transform.*

For an eigenfunction, the canonical sum-of-products expression and the PPRM are isomorphic, and have the same number of products.

Example 3.1 *Consider the EXOR function* $f = \bar{x}_1 x_2 \vee x_1 \bar{x}_2$. *As shown in Example 2.2,* $\vec{F} = (f_0, f_1, f_2, f_3) = (0,1,1,0)$, *and* $\vec{S} = (s_0, s_1, s_2, s_3) = (0,1,1,0)$. *Thus,* $(0,1,1,0)$ *is an eigenvector of* $\mathbf{R}(2)$. *In fact,* $f = \bar{x}_1 x_2 \vee x_1 \bar{x}_2$ *and* $f = 1 \cdot x_2 \oplus x_1 \cdot 1$ *are isomorphic: the complemented literals in the first expression correspond to constant 1's in the second expression. In a similar way, we can show that* $(0,1,1,1)$ *is also an eigenvector.* *(End of Example)*

One can solve for an eigenvector as follows. Since eigenvector $\vec{F}$ satisfies $\mathbf{R}(n)\vec{F} = \vec{F}$, it follows that $\mathbf{R}(n)\vec{F} - \mathbf{I}\vec{F} = (\mathbf{R}(n) - \mathbf{I})\vec{F} = (\mathbf{R}(n) \oplus \mathbf{I})\vec{F} = \vec{0}$. This yields 2^n simultaneous equations that can be solved for the components of $\vec{F}$.

Example 3.2 *Solve for the eigenvectors of* $\mathbf{R}(2)$. *From the observation above, we have*

$$\left[\begin{bmatrix} 1&0&0&0\\ 1&1&0&0\\ 1&0&1&0\\ 1&1&1&1 \end{bmatrix} \oplus \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix}\right] \begin{bmatrix} f_0\\ f_1\\ f_2\\ f_3 \end{bmatrix} = \begin{bmatrix} 0\\0\\0\\0 \end{bmatrix}.$$

$$\begin{bmatrix} 0&0&0&0\\ 1&0&0&0\\ 1&0&0&0\\ 1&1&1&0 \end{bmatrix} \begin{bmatrix} f_0\\ f_1\\ f_2\\ f_3 \end{bmatrix} = \begin{bmatrix} 0\\0\\0\\0 \end{bmatrix}.$$

From this, we obtain four simultaneous equations

$$\begin{aligned} 0 &= 0 \\ f_0 &= 0 \\ f_0 &= 0 \\ f_0 \oplus f_1 \oplus f_2 &= 0 \end{aligned}$$

From these equations, it follows that there are four eigenvectors $\vec{F}_0 = (0,0,0,0)$, $\vec{F}_1 = (0,0,0,1)$, $\vec{F}_2 = (0,1,1,0)$, *and* $\vec{F}_3 = (0,1,1,1)$. *Thus, for two-variable cases, the constant 0, the AND, the EXOR, and the OR functions are eigenfunctions.* *(End of Example)*

Note that, the truth vector of an eigenfunction is identical to the Reed-Muller spectrum of that function. Thus, from the canonical SOP, the PPRM is obtained by removing all the complemented literals from all product terms and by replacing the OR by the Exclusive OR. Eigenfunctions are interesting because among them, we can find the **functions with the largest MFPRMs**.

4 Symmetric Functions

Functions used in arithmetic circuits often have symmetries. Symmetric functions are interesting because **they contain the functions with the largest MFPRMs**.

Definition 4.1 *A function* f *is a* **(totally) symmetric function** *if any permutation of the variables in* f *leaves the function unchanged.*

Definition 4.2 *The* **elementary symmetric functions** *of* n *variables are*

$$\begin{aligned} S_0^n &= \bar{x}_1 \bar{x}_2 \cdots \bar{x}_n, \\ S_1^n &= x_1 \bar{x}_2 \cdots \bar{x}_n \vee \bar{x}_1 x_2 \bar{x}_3 \cdots \bar{x}_n \vee \cdots \\ &\quad \vee \bar{x}_1 \bar{x}_2 \cdots \bar{x}_{n-1} x_n, \\ &\cdots \\ S_n^n &= x_1 x_2 \cdots x_n. \end{aligned}$$

S_i^n *=1 iff exactly* i *of* n *variables are 1.*

Theorem 4.1 *An arbitrary symmetric function* $f(X)$ *is uniquely represented as follows:*

$$f(X) = \bigvee_{i=0}^{n} a_i S_i^n.$$

Definition 4.3 $\vec{a} = (a_0, a_1, \ldots, a_n)$ *is the* **reduced truth vector of the symmetric function**.

Note that any symmetric function on n variables can be uniquely represented by a reduced truth vector of $n+1$ bits.

Example 4.1 $f(x_1, x_2, x_3) = x_1 x_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 \bar{x}_3 \vee \bar{x}_1 \bar{x}_2 x_3$ *is a totally symmetric function.* $f = 1$ *when all the variables are 1, or when only one variable is 1. Thus,* f *can be represented by the reduced truth vector* $\vec{a} = (0,1,0,1)$. *(End of Example)*

Since each of the $n+1$ elements of the reduced truth table can be chosen in two ways, there are 2^{n+1} symmetric functions on n variables.

Definition 4.4 *An* **elementary symmetric EXOR function** *of* n *variables is an* n*-variable function represented by the EXOR sum of all the products consisting of* k *positive literals:*

$$\begin{aligned} R_0^n &= 1, \\ R_1^n &= \sum\nolimits^{\oplus} x_i, \\ R_2^n &= \sum_{(i<j)}\nolimits^{\oplus} x_i x_j, \\ R_3^n &= \sum_{(i<j<k)}\nolimits^{\oplus} x_i x_j x_k, \\ &\cdots \\ R_n^n &= x_1 x_2 \cdots x_n. \end{aligned}$$

Theorem 4.2 *An arbitrary symmetric function $f(X)$ is uniquely represented as follows:*

$$f(X) = \sum_{i=0}^{n} \oplus\, b_i R_i^n .$$

Definition 4.5 $\vec{b} = (b_0, b_1, \ldots, b_n)$ *is the* **reduced Reed-Muller spectrum of the symmetric function**.

Note that any symmetric function can be uniquely represented by its reduced Reed-Muller spectrum.

Example 4.2 $f(x_1, x_2, x_3) = x_1 x_2 x_3 \vee x_1 \bar{x}_2 \bar{x}_3 \vee \bar{x}_1 x_2 \bar{x}_3 \vee \bar{x}_1 \bar{x}_2 x_3 = x_1 \oplus x_2 \oplus x_3 = R_1^3$. *Thus, f can be represented by the reduced Reed-Muller spectrum $\vec{b} = (0,1,0,0)$. (End of Example)*

The following theorems show the relation between the reduced truth vector and the reduced Reed-Muller spectrum for each of three symmetric functions.

Theorem 4.3

$$\bigvee_{i=0\ \&\ i \neq 0 (mod\ 3)}^{n} S_i^n = \sum_{i=0\ \&\ i \neq 0 (mod\ 3)}^{n} \oplus\, R_i^n .$$

Example 4.3 $S_1^3 \vee S_2^3 = R_1^3 \oplus R_2^3$. *The reduced truth table is $\vec{a} = (0,1,1,0)$, and the reduced Reed-Muller spectrum is $\vec{b} = (0,1,1,0)$. This class of functions is quite interesting, since the expressions are isomorphic in both representations. In other words, the truth vector is invariant with the Reed-Muller transformation. In other words, they are eigenfunctions. (End of Example)*

Theorem 4.4

$$\bigvee_{i=0\ \&\ i \neq 1 (mod\ 3)}^{n} S_i^n = \sum_{i=0\ \&\ i \neq 2 (mod\ 3)}^{n} \oplus\, R_i^n .$$

Example 4.4 $S_0^3 \vee S_2^3 \vee S_3^3 = R_0^3 \oplus R_1^3 \oplus R_3^3$. *The reduced truth table is $\vec{a} = (1,0,1,1)$, and the reduced Reed-Muller spectrum is $\vec{b} = (1,1,0,1)$. (End of Example)*

Theorem 4.5

$$\bigvee_{i=0\ \&\ i \neq 2 (mod\ 3)}^{n} S_i^n = \sum_{i=0\ \&\ i \neq 1 (mod\ 3)}^{n} \oplus\, R_i^n .$$

Example 4.5 $S_0^3 \vee S_1^3 \vee S_3^3 = R_0^3 \oplus R_2^3 \oplus R_3^3$. *The reduced truth table is $\vec{a} = (1,1,0,1)$, and the reduced Reed-Muller spectrum is $\vec{b} = (1,0,1,1)$. (End of Example)*

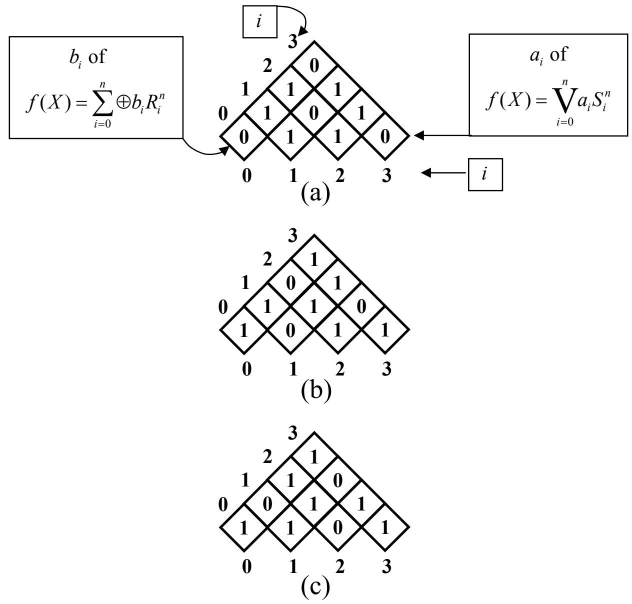

Figure 5.1. Transeunt triangle for each of three 3-variable symmetric functions.

5 Transeunt Triangle

Up to this point, we have discussed relations between the canonical sum-of-products expressions (canonical SOPs) and the positive polarity Reed-Muller expressions (PPRMs) of some symmetric functions. For these symmetric functions, the number of products in the canonical SOP and the number of products in the PPRM are the same and they are approximately $2^{n+1}/3$, when n is large, since about one-third of the truth table entries are 0's. Peryazev [12] has shown that these functions have the most products in their MFPRM. Pogossova and Egiazarian [13] also discuss symmetric functions realized as Reed-Muller expressions.

We consider the transeunt triangle discussed in Butler et al [1, 2] and Dueck et al [5], which had its origin in Suprun [24]. The transeunt triangle is related to a method to convert a truth table to a Reed-Muller spectrum by Green [8]. The **transeunt triangle** is a triangle of 0's and 1's representing the coefficients in the reduced truth table and the reduced Reed-Muller spectrum. For example, the function whose reduced truth table is $\vec{a} = (0,1,1,0)$, and whose reduced Reed-Muller spectrum is $\vec{b} = (0,1,1,0)$ is shown in Fig. 5.1 (a).

This transeunt triangle is created as follows. Make the bottom row the reduced truth table. Specifically, the bottom row should be $\vec{a} = (a_0, a_1, \ldots, a_n)$, where a_i is the i-th coefficient in the reduced truth table of the given function $f(X) = \bigvee_{i=0}^{n} a_i S_i^n$. Form the second row above the row associated with the reduced truth table, as the exclusive OR of adjacent elements in the first row. That is, the second row is $(a_0 \oplus a_1, a_1 \oplus a_2, \ldots, a_{n-1} \oplus a_n)$. Form the third row above the second row as the exclusive OR of adjacent elements in the second row. Continue in this way and stop after forming the apex of the triangle consisting of one 0 or one 1.

It is known [1, 24] that the left edge is $\vec{b}$, the reduced Reed-Muller spectrum of a symmetric function. Thus, the reduced Reed-Muller spectrum can be derived from the reduced truth table. Note that the transeunt triangle can be produced starting from the reduced Reed-Muller spectrum. This is because the Reed-Muller transform is self-inverse. Thus, the reduced truth table can be derived from the reduced Reed-Muller spectrum.

Fig. 5.1 (b) and (c) show the transeunt triangles for the other two functions discussed above, namely the functions whose reduced truth table is $(1,0,1,1)$ and $(1,1,0,1)$, respectively. From the three transeunt triangles, it can be seen that the three functions are related. Note that, for all three triangles, a $120°$ rotation leaves the triangle unchanged.

In preparation for the discussion on counting the number of eigenvectors, we state the following

Lemma 5.1 [23] *In the transeunt triangle of a symmetric function f, where the base is the reduced truth vector of f, the left side is the PPRM or the spectrum of f, while the right side is the NPRM of f.*

This was proven by Suprun [23]. As far as we know, no English version has been published.

First, consider symmetric functions. An eigenvector in a transeunt triangle has the property that two sides are identical. For example, Fig. 5.2 shows a transeunt triangle of a 7-variable symmetric function whose reduced truth table, represented by the base of the triangle, is identical to its reduced spectrum, represented by the left side. It follows that the function represented is an eigenvector.

1

0 **1**

1 **1** 0

1 0 **1** **1**

0 **1** **1** 0 **1**

1 **1** 0 **1** **1** 0

1 0 **1** **1** 0 **1** **1**

0 **1** **1** 0 **1** **1** 0 **1**

Figure 5.2. Example transeunt triangle of an eigenvector.

Definition 5.1 *The* **NPRM side** *of the transeunt triangle corresponds to the negative polarity Reed-Muller vector[1]. By convention, we choose it to be the right side. The* **PPRM side** *corresponds to the positive polarity Reed-Muller vector, and, by convention, is the left side. The* **truth table side** *corresponds to the truth table, and, by convention, is the base.*

Note that the right side vector is a palindrome. This example is a specific instance of the following general statement.

Lemma 5.2 *In the transeunt triangle of a symmetric function f, the NPRM side is a palindrome iff f is an eigenfunction.*

(Proof) (only if) Let the NPRM side be a palindrome. Assume, on the contrary, that the function is not an eigenfunction. Therefore, the PPRM side and the truth table side are different. As observed in [1], the entire transeunt triangle can be uniquely generated by the NPRM side by forming the exclusive OR of adjacent elements in the same way the entire triangle is generated from the truth table. Since the palindrome is the same rotated about its center point and the generated triangles is unique, the PPRM side and the truth table side must be identical, contradicting the assumption there are different. Therefore, the function is an eigenfunction.

(if) Let the function f associated with the transeunt triangle be an eigenfunction. It follows that the PPRM side and the truth table side are identical vectors. The transeunt triangle is uniquely generated from each side. The triangles must be the same and they must be invariant to a flip about a line bisecting the angle between the PPRM side and the truth table side. From this, it follows that the triangle's base (*i.e.* the NPRM side) must be invariant to the flip. It must be a palindrome. $(Q.E.D.)$

From this, we can count the eigenvectors.

Theorem 5.1 *The number $N_{\mathrm{sym\_eigen}}(n)$ of symmetric eigenfunctions on n-variable is*

$$N_{\mathrm{sym\_eigen}}(n) = 2^{\lceil \frac{n+1}{2} \rceil}. \tag{5.1}$$

(Proof) From Lemma 5.2, to count symmetric eigenfunctions, we can enumerate palindromes. Each side of the transeunt triangle of an n-variable symmetric function is a binary $n+1$-tuple. If that tuple is a palindrome, then there are $\lceil \frac{n+1}{2} \rceil$ pairs of elements except for one middle element in the case of even n, each of which can be chosen in two ways, 0 or 1, for a total of $2^{\lceil \frac{n+1}{2} \rceil}$ ways. $(Q.E.D.)$

Note that the transeunt triangle in Fig. 5.2 corresponds to a PPRM whose minimal FPRM is the most complicated among all n-variable functions. The 1's in the triangle form an interconnected hexagonal pattern.

Next, consider general functions. Fig. 5.2 shows how the transeunt triangle can be used in the case of general functions. That is, if the bottom vector is viewed as the truth vector of a function, then the left side is the PPRM of that function. In this example, the bottom vector is $f(x,y,z) = \bar{x}\bar{y}z \vee \bar{x}y\bar{z} \vee x\bar{y}\bar{z} \vee x\bar{y}z \vee xyz$. The left side is the PPRM of this function, $f(x,y,z) = x \oplus y \oplus z \oplus xz \oplus xyz$. The right side is the NPRM side, since it represents the negative Reed-Muller vector. In general, we can state

Lemma 5.3 *In the transeunt triangle of a general function f, the NPRM side is a palindrome iff f is an eigenfunction.*

From this, we can count the number of eigenvectors.

Theorem 5.2 *The number $N_{\text{gen\_eigen}}(n)$ of eigenfunctions on n-variable is*

$$N_{\text{gen\_eigen}}(n) = 2^{2^{n-1}}. \tag{5.2}$$

(Proof). From Lemma 5.3, to count symmetric functions that are eigenvectors, we can enumerate palindromes. Each side of the transeunt triangle of an n-variable symmetric function is a binary 2^n-tuple. If that tuple is a palindrome, then there are 2^{n-1} pairs of elements, each of which can be chosen in two ways, 0 or 1, for a total of $2^{2^{n-1}}$ ways. $(Q.E.D.)$

6 Number of Products in a PPRM

In Section 4, we identified three symmetric function having special properties. We now consider the number of products needed to represent such symmetric functions using positive polarity Reed-Muller expressions (PPRMs). Note that a function f that has the largest number of products in its MFPRM among all n-variable functions, can be converted to another function g whose PPRM is f's MFPRM with all complemented variables converted to uncomplemented variables. Therefore, it is possible to view an MPPRM as a PPRM with the largest number of products, such that all FPRM's of this function have the same or fewer products. We consider MPPRM's in this section.

We define two types of n-variable symmetric functions, whose Reed-Muller spectrum has a special characteristic. In the case of the first type, every third element is 1 and the other two elements are 0. Conversely, in the case of the second type, every third element is 0 and the other two elements are 1.

Specifically, let $\vec{s}_\alpha(n)$ ($\vec{d}_\alpha(n)$), for $\alpha \in \{0,1,2\}$, be the reduced Reed-Muller spectrum, $\vec{b} = (b_0, b_1, \ldots, b_n)$, of a symmetric function that has the property $b_j = 1$ ($b_j = 0$) if $j = \alpha \pmod 3$ and $b_j = 0$ ($b_j = 1$), otherwise. For example, if $n = 3$, then

$$\begin{aligned}
\vec{s}_0(3) &= (1,0,0,1)\ (f = 1 \oplus x_1x_2x_3), \\
\vec{s}_1(3) &= (0,1,0,0)\ (f = x_1 \oplus x_2 \oplus x_3), \\
\vec{s}_2(3) &= (0,0,1,0)\ (f = x_1x_2 \oplus x_1x_3 \oplus x_2x_3). \\
\vec{d}_0(3) &= (0,1,1,0)\ (f = x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \\
&\qquad \oplus x_1x_3 \oplus x_2x_3), \\
\vec{d}_1(3) &= (1,0,1,1)\ (f = 1 \oplus\ x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \\
&\qquad \oplus\ x_1x_2x_3), \\
\vec{d}_2(3) &= (1,1,0,1)\ (f = 1 \oplus\ x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2x_3).
\end{aligned}$$

When n is large, approximately one-third of the elements in the spectrum of $\vec{s}_\alpha$ are 1 and approximately one-third of the elements in the spectrum of $\vec{d}_\alpha$ are 0, for $\alpha \in \{0,1,2\}$. Let $\sigma_\alpha(n)$ be the number of products in $\vec{s}_\alpha(n)$, and let $\delta_\alpha(n)$ be the number of products in $\vec{d}_\alpha(n)$, for $\alpha \in \{0,1,2\}$. For example,

$$\begin{aligned}
\sigma_0(3) &= \binom{3}{0} + \binom{3}{3} = 2, \text{and} \\
\sigma_1(3) &= \binom{3}{1} = 3, \text{and} \\
\sigma_2(3) &= \binom{3}{2} = 3. \\
\delta_0(3) &= \binom{3}{1} + \binom{3}{2} = 6,\ \text{and} \\
\delta_1(3) &= \binom{3}{0} + \binom{3}{2} + \binom{3}{3} = 5, \text{and} \\
\delta_2(3) &= \binom{3}{0} + \binom{3}{1} + \binom{3}{3} = 5.
\end{aligned}$$

From Pascal's rule

$$\binom{n}{i} = \binom{n-1}{i-1} + \binom{n-1}{i},$$

we can write

$$\begin{aligned}
\sigma_0(n) &= \delta_1(n-1),\ \text{where } \delta_0(1) = 1,\ \text{and} \quad (6.1)\\
\sigma_1(n) &= \delta_2(n-1),\ \text{where } \delta_1(1) = 1,\ \text{and} \quad (6.2)\\
\sigma_2(n) &= \delta_0(n-1),\ \text{where } \delta_2(1) = 2. \quad (6.3)
\end{aligned}$$

By direct observation, we can write

$$\begin{aligned}
\delta_0(n) = \sigma_1(n) + \sigma_2(n) = \delta_0(n-1) + \delta_2(n-1), \quad (6.4)\\
\delta_1(n) = \sigma_0(n) + \sigma_2(n) = \delta_0(n-1) + \delta_1(n-1), \quad (6.5)\\
\delta_2(n) = \sigma_0(n) + \sigma_1(n) = \delta_1(n-1) + \delta_2(n-1). \quad (6.6)
\end{aligned}$$

Here, the rightmost expressions of (6.4, 6.5, 6.6) were obtained from (6.1, 6.2, 6.3). Each expressions of $\delta_\alpha(n)$ represents an infinite series of numbers that can be represented by generating functions $D_\alpha(x) = \delta_\alpha(0) + \delta_\alpha(1)x + \delta_\alpha(2)x^2 \ldots + \delta_\alpha(i)x^i + \ldots$, related as follows.

$$\begin{aligned}
D_0(x) &= xD_0(x) + xD_2(x) + x,\ \text{and} \\
D_1(x) &= xD_0(x) + xD_1(x) + x,\ \text{and} \\
D_2(x) &= xD_1(x) + xD_2(x) + 2x.
\end{aligned}$$

Solving for $D_\alpha(x)$ yields

$$D_0(x) = \frac{xD_2(x)+x}{1-x}, \text{ and}$$
$$D_1(x) = \frac{xD_0(x)+x}{1-x}, \text{ and}$$
$$D_2(x) = \frac{xD_1(x)+2x}{1-x}.$$

Note, for example, that $D_0(x)$ is expressed as a function of $D_2(x)$, which, in turn, is expressed as a function of $D_1(x)$, which, in turn, is expressed as a function of $D_0(x)$. Therefore, by a process of repeated substitutions, we can express $D_0(x)$ as a function of $D_0(x)$ only. Then, we can solve explicitly for $D_0(x)$. Similarly, we can solve explicitly for $D_1(x)$ and $D_2(x)$. This process proves the following.

Theorem 6.1 *The generating functions for the number of products in the functions $\vec{d_0}(n)$, $\vec{d_1}(n)$, and $\vec{d_2}(n)$ are*

$$D_0(x) = \frac{x}{(1-2x)(1-x+x^2)}, \text{ and}$$
$$D_1(x) = \frac{x(1-x+2x^2)}{(1-2x)(1-x+x^2)}, \text{ and}$$
$$D_2(x) = \frac{x(2-3x+2x^2)}{(1-2x)(1-x+x^2)}.$$

The result is shown in the first row of Table 6.1. Rows below the first show the number of products in the three symmetric functions as a function of n, the number of variables. That is, these are coefficients of various powers of x for the three generating functions, $D_0(x)$, $D_1(x)$, and $D_2(x)$. For example, the third column shows that $D_0(x) = \frac{x}{(1-2x)(1-x+x^2)} = x+3x^2+6x^3+11x^4+21x^5+42x^6+85x^6+171x^7+342x^9+\ldots$, where the coefficient of x^n is the number of products in the symmetric function $\vec{d_0}(n)$. We seek the minimum, $e(n)$ of the number of products in $\sigma_0(n)$, $\sigma_1(n)$, and $\sigma_2(n)$. This is $e(n) = \left\lfloor \frac{2^{n+1}}{3} \right\rfloor$.

It is interesting that the number of products in the function with the most products in its MFPRM, expressed as a binary number, is uniquely the binary numbers with no adjacent pair of bits the same. For example, $1_{10} = 1_2$, $2_{10} = 10_2$, $5_{10} = 101_2$, $10_{10} = 1010_2$, $21_{10} = 10101_2$, $42_{10} = 101010_2$, $85_{10} = 1010101_2$, $170_{10} = 10101010_2$, and $341_{10} = 101010101_2$.

7 Conclusions

In this paper, we

- introduced eigenfunctions of Reed-Muller transformation, where the canonical sum-of-products expression and the PPRM are isomorphic.
- identified three symmetric functions having special properties.
- showed that among eigenfunctions, we can find the above symmetric functions.
- showed that the number of eigenfunctions on n variables is $2^{2^{n-1}}$.
- showed that the number of symmetric eigenfunction on n variables is $2^{\lceil \frac{n+1}{2} \rceil}$.
- showed that the number of products in PPRMs for such symmetric functions is $\lfloor 2^{n+1}/3 \rfloor$ and this corresponds to the MPPRM.

Acknowledgments

This research is supported in part by the Grants in Aid for Scientific Research of JSPS, and by a contract from the National Security Agency.

References

[1] J. T. Butler, G. W. Dueck, V. P. Schmerko, and S. N. Yanushkevich, "Comments on Sympathy: Fast, exact minimization of fixed polarity Reed-Muller expansion of symmetric functions," *IEEE Trans. Comput. Aided Design*, vol. 19, No. 11,pp. 1386-1388, Nov. 2000.

[2] J. T. Butler, G. W. Dueck, S. N. Yanushkevich, and V. P. Schmerko, "On the number of generators for transeunt triangles," *Discrete Applied Mathematics*, vol. 108, Issue 3,pp. 309-316, March 2001.

[3] C. Damm, "The complexity of symmetric functions in parity normal form," *Proc. of Mathematical Foundations of Computer Science '90*, Bansk'a Bystrica, Czechoslovakia, pp.232-238, Aug. 1990.

[4] M. Davio, J-P. Deschamps and A. Thayse, *Discrete and switching functions*, McGraw-Hill International,1978.

[5] G. W. Dueck, D. Maslov, J. T. Butler, V. P. Schmerko, and S. N. Yanushkevich, "A method to find the best mixed polarity Reed-Muller using transeunt triangle," *Proc. of the 5th Int. Reed-Muller Workshop* (*RM*'2001), Starkville, MA, USA, pp. 82-92, August 2001.

[6] S. Even, I. Kohavi and A. Paz, "On minimal modulo-2 sum of products for switching functions," *IEEE Trans. on Electron Computers*, Vol. EC-16,pp.671-674, Oct. 1967.

[7] D. Green, *Modern Logic Design*, Addison-Wesley Publishing Company, 1986.

[8] D. Green, "Families of Reed-Muller canonical forms", *Int. Journal of Electronics*, Vol. 63, No. 2m pp. 259-280, Jan. 1991.

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

Table 6.1. Generating Functions for the Number of Products in the Functions With the Most Complicated FPRM

n		$D_0(x) = \frac{x}{(1-2x)(1-x+x^2)}$	$D_1(x) = \frac{x(1-x+2x^2)}{(1-2x)(1-x+x^2)}$	$D_2(x) = \frac{x(2-3x+2x^2)}{(1-2x)(1-x+x^2)}$	$D_0(x) + D_1(x) + D_2(x) = \frac{4x}{1-2x}$	Minimum
1	x	1	1	2	4	$1 = \lfloor \frac{4}{3} \rfloor$
2	x^2	3	2	3	8	$2 = \lfloor \frac{8}{3} \rfloor$
3	x^3	6	5	5	16	$5 = \lfloor \frac{16}{3} \rfloor$
4	x^4	11	11	10	32	$10 = \lfloor \frac{32}{3} \rfloor$
5	x^5	21	22	21	64	$21 = \lfloor \frac{64}{3} \rfloor$
6	x^6	42	43	43	128	$42 = \lfloor \frac{128}{3} \rfloor$
7	x^7	85	85	86	256	$85 = \lfloor \frac{256}{3} \rfloor$
8	x^8	171	170	171	512	$170 = \lfloor \frac{512}{3} \rfloor$
9	x^9	342	341	341	1024	$341 = \lfloor \frac{1024}{3} \rfloor$
n	x^n				2^{n+1}	$\lfloor \frac{2^{n+1}}{3} \rfloor$

[10] J. Manstivoda and N. Peryazev "The complexity of symmetric functions in the polynomial forms," *Proc. Workshop Applications of the Reed-Muller Expansion in Circuit Design (Reed-Muller 1997)*, Sept. 19-20, 1997, Oxford, UK, pp.166-173.

[11] M. A. Perkowski, L. Csanky, A. Sarabi, and I. Schäfer, "Fast minimization of mixed-polarity AND-XOR canonical networks," *Proc. ICCD-92*, pp. 33-36, Oct. 1992.

[12] N. A. Peryazev, "Complexity of Boolean functions in the class of polarized polynomial forms," *Journal Algebra and Logic*, Springer New York ISSN 0002-5232, Volume 34, Number 3, May, 1995, pp. 177-179.

[13] E. Pogossova and K. Egiazarian, "Reed-Muller representation of symmetric functions," *Journal of Multiple-Valued Logic and Soft Computing*, Old City Publishing, Inc., Volume 10, Number 1, 2004, pp. 51-72.

[14] U. Rollwage, "The complexity of mod-2 sum PLA's for symmetric functions," *Proc. IFIP WG 10.5 Workshop Applications of the Reed-Muller Expansion in Circuit Design*, pp. 6-12, Hamburg, 1993.

[15] A. Sarabi and M. A. Perkowski, "Fast exact and quasi-minimal minimization of highly testable fixed polarity AND/XOR canonical networks," *Design Automation Conference 1992*, pp. 20-35, June 1992.

[16] T. Sasao and P. Besslich, "On the complexity of MOD-2 Sum PLA's," *IEEE Trans. on Comput.*, Vol. 32, No. 2, pp. 262-266, Feb. 1990.

[17] T. Sasao, "EXMIN2: A simplification algorithm for exclusive-OR-sum-of-products expressions for multiple-valued input two-valued output functions," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 12, No. 5, May 1993, pp. 621-632.

[18] T. Sasao (ed.), *Logic Synthesis and Optimization*, Kluwer Academic Publishers, 1993.

[19] T. Sasao and M. Fujita (ed.), *Representation of Discrete Functions*, Kluwer Academic Publishers, 1996.

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

[21] R. S. Stankovic, T. Sasao, and C. Moraga, "Spectral transform decision diagrams," *Representations of Discrete Functions*, T. Sasao and M. Fujita, eds., pp. 55-92, Kluwer Academic, 1996.

[22] R. Stankovic and J. Astola, *Spectral Interpretation of Decision Diagrams, Springer-Verlag*, May 16, 2003.

[23] V. P. Suprun, "Polynomial expression of symmetric Boolean functions," *Izvestija AN USSR. Techn. Kibernetika*, No. 4, pp. 123-127 1985 (in Russian).

[24] V. P. Suprun, "Fixed polarity Reed-Muller expression of symmetric Boolean functions," *Proc. IFIP WG10.5 Workshop on Applications of the Reed-Muller Expansions in Circuit Design*, pp. 246-249, 1995.

[25] C. C. Tsai and M. Marek-Sadowska, "Minimisation of fixed-polarity AND/XOR canonical networks," *IEE Proc.*, Vol. 141, pt. E, No. 6, pp. 369-374, Nov. 1994.

[26] M. A. Thornton, R. Drechsler, and D. M. Miller, *Spectral Techniques in VLSI CAD*, Kluwer Academic Publishers, July, 2001.