Efficient Computation of Fixed and Mixed Polarity Reed-Muller Function Vector over GF(p)

YoungGun Kim* and Jong O Kim** and Heung-Soo Kim***

*Dept. of I.I.P, Ansan College, Ansan, Korea E-mail: ygkim@ansan.ac.kr

**Dept. of Electrical Eng., Dongyang Tech. College, Seoul, Korea E-mail: jokim@dongyang.ac.kr

***Dept. of Electronic Eng., Inha University, Inchon, Korea

Abstract : This paper proposes an efficient computation method for fixed and mixed polarity Reed-Muller function vector over Galois field $GF(p)$. Function vectors of fixed polarity Reed-Muller function with single variable can be generated by proposed method. The n-variable function vectors can be calculated by means of the Kronecker product of a single variable function vector corresponding to each variable. Thus, all fixed and mixed polarity Reed-Muller function vectors are calculated directly without using a polarity function vector table or polarity coefficient matrix.

Fixed and Mixed polarity, Reed-Muller function, Galois field, Kronecker product

1. INTRODUCTION

It is well known that any binary and multiple valued functions can be expressed by a Reed-Muller expansion and by more general exclusive-OR sum of products. This representation has various advantages over the conventional description[1-4]. The Reed-Muller transform is a method by which finite fields may play a more significant role in logic design. The transform involves representation of logic functions as polynomials over finite fields. The concepts of fixed and mixed polarity Reed-Muller expansions have recently been extended to a finite field $GF(p)$[5-11], this is known as the Galois field of order $p=q^k$ where q is a prime number and k is a positive integer.

A lot of work has been done on optimizing fixed or mixed polarity Reed-Muller expansion[1-11], however, little research has been done on how to find out the function vector from a given Reed-Muller expansion[6,12]. Fei[12] introduced a calculation method of function vector for ternary mixed polarity Reed-Muller expansions using a function vector table. This approach has the value of all element of a vector are not zero and not same value. In this case, they are represented in a two term even mixed polarity, this representation is not unique. Also, in the p valued logic system, the table vector size is p^p. Thus, for $p>3$, this approach is very difficult to use to generate a function vector table because vector table size becomes very large. In order to overcome these limitations, this paper proposes an equation for calculation of fixed and mixed polarity Reed-Muller function vector. A computationally efficient alternative for calculating multiple valued fixed or mixed polarity Reed-Muller function vector is presented.

2. BASIC DEFINITIONS

Binary Reed-Muller expansion can be easily extended to the general case. p-valued switching circuits, provided p is a prime number. The prime fields $GF(p)$ can be represented by the intergers modulo-p, and $GF(p)$ the operations of modulo-p addition and multiplication. The nonprime fields $GF(q)$, $q=p^k$, cannot be represented in this way. One possible form of representation employs the p^k polynomials of degree $k-1$ or less with coefficients from $GF(p)$ as basic elements. The operations of polynomial addition and multiplication are performed modulo a primitive polynomial of degree k with coefficients from $GF(p)$[6,11].

Definition 1 : In a q-valued logic system, the Reed-Muller expansion for a one variable function in polarity $\langle k\rangle$ is

$$f(\tilde{x}) = a_0^{\langle k\rangle} + a_1^{\langle k\rangle}\tilde{x} + a_2^{\langle k\rangle}\tilde{x}^2 + a_3^{\langle k\rangle}\tilde{x}^3 + \cdots + a_{q-1}^{\langle k\rangle}\tilde{x}^{q-1} \quad (1)$$

where $\tilde{x}$ is the literal of a variable x, and all operations are in $GF(q)$.

Definition 2 : The generalized Reed-Muller expansion for an n-variable q-valued function in polarity $\langle k\rangle$ takes the form

$$f(\tilde{x}_n, \tilde{x}_{n-1}, \cdots, \tilde{x}_1) = \sum_{i=0}^{q^n-1} a_i^{\langle k\rangle} \prod_{j=1}^{n} \tilde{x}_j^{i_j} \quad (2)$$

where

$\tilde{x}_j^0 = 1,\ \tilde{x}_j^1 = \tilde{x}_j,\ \tilde{x}_j^2 = \tilde{x}_j \times \tilde{x}_j, \cdots,$

$\tilde{x}_j^n = \tilde{x}_j \times \tilde{x}_j \times \cdots \times \tilde{x}_j$ n times, i_j, $\tilde{x}_j$,

$a_i \in \{0,1,2,\cdots,q-1\}$ and $\langle i_n, i_{n-1}, \cdots, i_1\rangle$ denotes the respective q-ray expression of the decimal number i, i.e.,

$\langle i\rangle_{10} = \langle i_n, i_{n-1}, \cdots, i_1\rangle_q$, and the term $\tilde{x}_j^{i_j}$ denotes the i_jth power of the variable x_j.

If $\tilde{x}_i$ takes the value of $x_i + \delta_i (\delta_i \in \{0,1,2,\cdots,q-1\})$, eqn.(2) can be rewritten as

$$f(\tilde{x}_n, \tilde{x}_{n-1}, \cdots, \tilde{x}_1) = \sum_{i=0}^{q^n-1} a_i^{\langle k\rangle} \prod_{j=1}^{n} (x_j + \delta_j)^{i_j} \quad (3)$$

where $\langle k\rangle_{10} = \langle \delta_1 \delta_2 \cdots \delta_n\rangle_q$. According to the different values of $\delta_1\delta_2\cdots\delta_n$, $f(\tilde{x}_n, \tilde{x}_{n-1}, \cdots, \tilde{x}_1)$ has the q^n kinds of polarity.

Definition 3 : The coefficient vector of the function $f(\tilde{x}_n, \tilde{x}_{n-1}, \cdots, \tilde{x}_1)$ in polarity $\langle k\rangle$ is denoted as $\boldsymbol{a}^{\langle k\rangle}$, where

$\boldsymbol{a}^{\langle k\rangle} = [a_0^{\langle k\rangle}, a_1^{\langle k\rangle}, \cdots, a_{q^n-1}^{\langle k\rangle}]$,

$k = 0, 1, 2, \cdots, q^n - 1$.

The individual product terms in the n-variable expansion can also be generated by using a Kronecker product on n basis vectors of the form [6],

$$f(\tilde{x}_n, \tilde{x}_{n-1}, \cdots, \tilde{x}_1) = ([1 \ \ \tilde{x}_n \ \ \tilde{x}_n^2 \cdots \tilde{x}_n^{q-1}] * [1 \ \ \tilde{x}_{n-1} \ \ \tilde{x}_{n-1}^2 \cdots \tilde{x}_{n-1}^{q-1}] * \cdots * [1 \ \ \tilde{x}_1 \ \ \tilde{x}_1^2 \cdots \tilde{x}_1^{q-}]) \ \boldsymbol{a}^{\langle k \rangle} \quad (4)$$

3. COMPUTATION OF FUNCTION VECTOR

A switching function of n-variables is completely defined by a set of q^n coefficients $d_i (0 \le i \le q^n - 1)$ which represents the values in the output column of the truth table of the function. When represented in vector form $\boldsymbol{d}$, this will be termed the truth vector. The Reed-Muller canonical form also has q^n coefficients $d_i (0 \le i \le q^n - 1)$ represented in vector form as $\boldsymbol{a}$, the function vector.

Definition 4 : Let

$\boldsymbol{d} = [f_0, f_1, \cdots, f_{q^n-1}] = [d_0, d_1, \cdots, d_{q^n-1}]$ be a n variable function vector with q^n elements, where

$f_0 = f(0, \cdots, 0)$, $f_1 = f(0, \cdots, 1)$, $\cdots$,
$f_{q^n-1} = f(q-1, \cdots, q-1)$.

Definition 5 : For an one variable function $f(\tilde{x})$, let the $\boldsymbol{e}_i$ be the function vector corresponding to x^i , and let a e_j be elements of function vector $\boldsymbol{e}_i$, where $i, j \in \{0, 1, 2, \cdots, q-1\}$.

Theorem 1 : For a single variable function $f(\tilde{x}) = \tilde{x}^n$ in polarity $\langle k \rangle$, the value of elements e_j of function vector is directly given by

$$e_j = (j+k)^n \quad (5)$$

,where $j, k, n \in (0, 1, 2, \cdots, q-1)$

Proof : When $f(x) = l, l \in \{0, 1, 2, \cdots, q-1\}$, the value of elements of function vector is $e_j = l$. In the case of Zero polarity, the function vectors are, by Definition 2, given by

$\boldsymbol{e}_1 = [e_0, e_1, e_2, \cdots, e_{q-1}]$ where $e_j = j$

$\boldsymbol{e}_2 = \boldsymbol{e}_1 \times \boldsymbol{e}_1 = [e_0^2 \ e_1^2 \ e_2^2 \cdots e_{(q-1)}^2]$

$\vdots$

$\boldsymbol{e}_n = \boldsymbol{e}_1 \times \boldsymbol{e}_1 \times \cdots \times \boldsymbol{e}_1$ n times

$= [e_0^n \ e_1^n \ e_2^n \cdots e_{(q-1)}^n]$

In the case of polarity $\langle k \rangle$, performing the additive transform of replacing e_i by $e_i + k, k \in GF(q)$

$\boldsymbol{e}_1 = [(e_0 + k) \ (e_1 + k) \ (e_2 + k) \ \cdots \ (e_{q-1} + k)]$

$\boldsymbol{e}_2 = [(e_0 + k)^2 \ (e_1 + k)^2 \ (e_2 + k)^2 \cdots (e_{q-1} + k)^2]$

$\vdots$

$\boldsymbol{e}_n = [(e_0 + k)^n \ (e_1 + k)^n \ (e_2 + k)^n \cdots (e_{q-1} + k)^n]$

The value of element of function vector is defined as follows,

$$e_j = (j+k)^n \qquad \text{QED}$$

[Example 1] The function vectors of fixed polarity Reed-Muller expansion with single variable over GF(3) are as follows;

polarity $\langle k \rangle = 0$

$e_1 = [0, 1, 2]$

$e_2 = [0^2, 1^2, 2^2] = [0, 1, 1]$

polarity $\langle k \rangle = 1$

$e_1 = [(0+1), (1+1), (2+1)] = [1, 2, 0]$

$e_2 = [(0+1)^2, (1+1)^2, (2+1)^2] = [1, 1, 0]$

polarity $\langle k \rangle = 2$

$e_1 = [(0+2), (1+2), (2+2)] = [2, 0, 1]$

$e_2 = [(0+2)^2, (1+2)^2, (2+2)^2] = [1, 0, 1]$ ■

Theorem 2 : For n variables, the function vector of $f(\tilde{x}_n, \tilde{x}_{n-1}, \cdots, \tilde{x}_1)$ is

$$d = [d_0, d_1, \cdots, d_{q^n-1}]$$

$$= \sum_{i=0}^{q^n-1} a_i^{\langle k \rangle}\left[e_{j_n} * e_{j_{n-1}} * \cdots * e_{j_1} \right] \qquad (6)$$

, where $\langle i \rangle_{10} = \langle j_n j_{n-1} \cdots j_1 \rangle_q$

Proof : By using induction, the function vector of $f(\tilde{x})$ is, by eqn.(1), given by

$$d = [d_0, d_1, \cdots, d_{q-1}]$$

$$= a_0^{\langle k \rangle} e_0 + a_1^{\langle k \rangle} e_1 + \cdots + a_{q-1}^{\langle k \rangle} e_{q-1} \qquad (7)$$

For two variable function, the function vector is $q \times q$ dimensional. This function vector can be calculated by the Kronecker product of function vector corresponding to $x_2^{j_2}, x_1^{j_1}$[12]. Thus eqn.(7) can be rewritten as

$$d = [d_0, d_1, \cdots, d_{q^2-1}]$$

$$= a_0(e_0 * e_0) + a_1(e_0 * e_1) + a_2(e_0 * e_2) + a_3(e_0 * e_3) + \cdots + a_{q-1}(e_0 * e_{q-1}) + a_q(e_1 * e_0) + a_{q+1}(e_1 * e_1) + a_{q+2}(e_1 * e_2) + \cdots + a_{q^2-1}(e_{q-1} * e_{q-1})$$

For n variable function, the function vector is

$$d = [d_0, d_1, \cdots, d_{q^n-1}]$$

$$= a_0(e_0 * e_0 * \cdots * e_0) + a_1(e_0 * e_0 * \cdots * e_1) + a_2(e_0 * e_0 * \cdots * e_2) + \cdots + a_{q-1}(e_0 * e_0 * \cdots * e_{q-1}) + a_q(e_0 * e_0 * \cdots * e_1 * e_0) + a_{q+1}(e_0 * e_0 * \cdots * e_1 * e_1) + \cdots + a_{q^n-1}(e_{q-1} * e_{q-1} * \cdots * e_{q-1})$$

$$= \sum_{i=0}^{q^n-1} a_i\left[e_{j_n} * e_{j_{n-1}} * \cdots * e_{j_1} \right] \quad \text{QED.}$$

[Example 2] Consider an n variable single product term function vector over GF(4).

$$f(x_3, x_2, x_1) = A^{\langle 27 \rangle}\, \tilde{x}_3^{\,2} \tilde{x}_2 \tilde{x}_1^{\,3}$$

$$d = A[(0+1)^2(1+1)^2(A+1)^2(B+1)^2] * [(0+A)(1+A)(A+A)(B+A)] * [(0+B)^3(1+B)^3(A+B)^3(B+B)^3]$$

$$= [A\,0\,B\,1] * [A\,B\,0\,1] * [1110]$$

$$= [BBB0111\,00000AAA00000000000001110\;AAA00000BBB0AAA0BBB000001110]$$ ■

[Example 3] Consider an n-variable multiple product term function vector over GF(3).

$$f(x_3, x_2, x_1) = 2^{\langle 4 \rangle}\, \tilde{x}_2^{\,2} \tilde{x}_1 + 2^{\langle 14 \rangle} \tilde{x}_3 \tilde{x}_2^{\,2} \tilde{x}_1^{\,2}$$

$$d = [222] * [(0+1)^2(1+1)^2(2+1)^2] * [(0+1)(1+1)(2+1)] + 2 * [(0+1)(1+1)(2+1)] * [(0+1)^2(1+1)^2(2+1)^2] *$$

$$[(0+2)^2(1+2)^2(2+2)^2]$$
$$=[222]*[110]*[120]+[210]*[110]*[101]$$
$$=[210210000210210000210210000]+$$
$$[202202000101101000000000000]$$
$$=[112112000011011000210210000]\ \blacksquare$$

4. CONCLUSION

A new method to calculate the function vectors of multiple valued fixed and mixed polarity Reed-Muller expansion has been presented. The function vectors of fixed polarity Reed-Muller expansion with single variable over $GF(q)$ can be generated by the proposed equation. By using the Kronecker product of a single variable function vector, an n variable function vector can be calculated. The new approach is especially advantageous in comparison to the existing approach[12] for $q>3$ in over $GF(q)$. Another advantage of the presented method is that it is more efficient for mixed polarity Reed Muller function and can be applied to multiple valued Reed-Muller function. Also, this method is very convenient because there is no need to make vector table or transform matrix for calculations.

References

[1] D.H. Green, "Reed-Muller canonical forms with mixed polarity and their manipulations", *IEE Proc. Vol. 137, Pt. E, No.1*, pp. 103-113, 1990

[2] B. Harking, "Efficient algorithm for canonical Reed-Muller expansion of Boolean functions", *IEE Proc. Vol. 137, Pt. E, No.5*, pp. 366-370, 1990

[3] D.H. Green, "Dual forms of Reed-Muller expansions", *IEE Proc. Comput. Digit. Tech., Vol. 141, No 35*, pp. 184-192, 1994

[4] T.G. Clarkson and N. Zhuang, "Vector algorithm for Reed-Muller expansion", *Electronics Letters, Vol. 30 No. 7*, pp. 549-550, 1994

[5] D.H. Green, "Ternary Reed-Muller switching function with fixed and mixed polarities", *Int. J. Electronics*, pp. 761-775, 1989

[6] D.H. Green, "Reed-Muller expansion with fixed and mixed polarities over GF(4)", *IEE Proc. Vol. 137, Pt. E, No.5*, pp. 380-388, 1990

[7] B. Harking and C. Moraga, "Efficient Derivation of Reed-Muller Expansions in Multiple Valued Logic Systems", *IEEE Proc. 22th ISMVL*, pp. 436-441, 1992

[8] B. Fei and Q. Hong, H. Wu, M.A. Perkowski, Zhuang, and N. Zhuang, "Efficient computation for ternary Reed-Muller expansion under fixed Polarities", *Int. J. Electronic*, pp. 685-688, 1993

[9] S. Rahardja and B.J. Falkowski, "A new algorithm to compute quaternary Reed-Muller expansion", *IEEE Proc. 30th ISMVL*, pp. 153-158, 2000

[10] Yanushkevich S. Popel D.,Shemrko V., Cheushev V. and Stankovic R., "Information theoretical approach to minimization of

polynomial expressions over GF(4)", *IEEE Proc. 30th ISMVL*, pp. 265-270, 2000

[11] S. Rahardja and B.J. Falkowski,"Efficient algorithm to calculate Reed-Muller expansion over GF(4)", *IEE Proc. Circuits Syst. Vol. 148, No. 6*, pp289-295, 2001

[12] B. Fei and Q. Hong, N. Zhuang,"Calculation of Ternary Mixed Polarity Function Vector", *IEEE Proc. 23th ISMVL*, pp. 236-238, 1993