

# Generalized Reed-Muller Canonical Form for a Multiple-Valued Algebra

E.V. Dubrova    J.C. Muzio

Department of Computer Science  
University of Victoria,  
P.O.Box 3055  
Victoria, B.C.,  
Canada, V8W 3P6

## Abstract

A multiple-valued algebra which is functionally complete with constants is considered. It is based on the operations of addition modulo  $m$ , minimum, and the set of all literal operators, where  $m$  is a positive integer. A decomposition, allowing a function of  $n$  variables to be expressed through  $n$  functions of  $n - 1$  variables, is developed. Using this decomposition, a generalization of fixed polarity Reed-Muller canonical form for the multiple-valued algebra under consideration is derived. An algorithm for computing the coefficients of such a canonical form, based on matrix multiplication, is given. Advantages of the introduced canonical form over other generalizations of the Reed-Muller canonical form previously proposed, are discussed.

Key words: multiple-valued algebra, canonical form, fixed polarity, Reed-Muller form

## 1 Introduction

In 1954 Reed [7] and Muller [4] observed that any Boolean function can be expressed as an expansion using AND and XOR operations. Their work leads to more economic implementations of some practical logic functions using AND-XOR arrays rather than the conventional AND-OR arrays [8].

In two-valued system, an  $n$ -variable Boolean function has  $2^n$  fixed polarity AND-XOR expansions, usually called Reed-Muller canonical forms of a Boolean function.

A fixed polarity Reed-Muller canonical form of an  $n$ -variable Boolean function has a form [4]:

$$f(x_1, \dots, x_n) = c_0 \oplus c_1 \dot{x}_1 \oplus \dots \oplus c_n \dot{x}_n \oplus \dots \oplus c_{2^n-1} \dot{x}_1 \dots \dot{x}_n$$

where  $\dot{x}_i$ ,  $i \in \{1, \dots, n\}$ , is either  $x_i$  or the complement of  $x_i$ , according to the polarity vector, and  $c_j \in \{0, 1\}$ ,  $j \in \{0, \dots, 2^n - 1\}$ , are constants.

The concept of Reed-Muller canonical form can be extended to  $m$ -valued logic in several ways, depending on how the AND and XOR operations are generalized. The first generalization, based on the operations of addition and multiplication modulo  $m$ , where  $m$  is a prime number, was proposed by Cohn in 1960 [1]. Modulo  $m$  addition and multiplication form a Galois field of order  $m$ . Later this generalization was further extended by Pradhan [6] for the case when  $m$  is a power of a prime, i.e.  $m = p^k$  ( $p$  - a prime number,  $k$  - a positive integer). Kodandapani and Setlur [2] proposed a canonical form, based on the operations of addition and multiplication modulo  $m$  ( $m$  - a prime number) and the set of all literal operators. All of these generalizations are only applicable for the algebras with  $m$  being a prime or a power of a prime number.

In this paper we introduce a generalization of the fixed polarity Reed-Muller canonical form, based on the operations of addition modulo  $m$ , minimum and the set of all literal operators, with  $m$  being any positive integer. An  $n$ -variable  $m$ -valued function has  $m^n$  such expansions, each characterized by a polarity vector and a corresponding vector of coefficients  $[c_0 \ c_1 \ \dots \ c_{m^n-1}]$ ,  $c_j \in \{0, 1, \dots, m - 1\}$ . We present a procedure for computing these coefficients, based on matrix multiplication. The vectors of coefficients for different polarities are obtained simultaneously, which makes it possible to choose the expansion with the minimal number of non-zero coefficients.

The paper is organized as follows. In Section 2 the description of the algebra, based on the operations of addition modulo  $m$ , minimum, and the set of all literal operators, where  $m$  is a positive integer, is given. In Section 3, a decomposition,

allowing a function of  $n$  variables to be expressed through  $n$  functions of  $n - 1$  variables, is developed. In Section 4, the canonical expansion for multiple-valued functions, which is a generalization of fixed polarity Reed-Muller canonical form, is derived. In the final Section, some conclusions are drawn and a topic for further research is proposed. The proofs of the main results are given in the Appendix.

## 2 The Algebra

The work in this paper is based on a multiple-valued algebra defined as follows:

**Definition 1** *A multiple-valued algebra is an algebra  $\mathcal{A} = \langle M; \oplus, \cdot, J; 0, m - 1 \rangle$ , where*

- (i)  $M := \{0, 1, \dots, m - 1\}$  is the totally ordered carrier of  $\mathcal{A}$ ;
- (ii) " $\oplus$ " is the binary operation addition modulo  $m$ ;
- (iii) " $\cdot$ " is the binary operation minimum (MIN);
- (iv)  $J := \{J_0, J_1, \dots, J_{m-1}\}$  is a set of literal operators such that

$$J_i x := \begin{cases} m - 1 & \text{if } x = i \\ 0 & \text{otherwise} \end{cases}$$

where  $x$  is a multiple-valued variable and  $i \in M$  is a constant. For convenience, we write  $J_i x$  as  $\overset{i}{x}$ ;

- (iv)  $0$  and  $(m - 1)$  are constants of the algebra.

The operations " $\oplus$ " and " $\cdot$ " are commutative and associative. They are not distributive over each other. " $\cdot$ " is idempotent. The constant  $0$  is a null element and the constant  $(m - 1)$  is an identity element with respect to " $\cdot$ ". The constant  $0$  is an identity element with respect to " $\oplus$ ".

Every element  $x$  of  $M$  has an *inverse*  $-x$  (with respect to  $\oplus$  operation), defined as

$$-x := \underbrace{x \oplus x \oplus \dots \oplus x}_{m-1 \text{ times}}$$

In order to simplify the derivations bellow, we define the operations of complement and subtraction modulo  $m$ . All operations are extended for functions as usual.

**Definition 2** *The complement of a multiple-valued variable  $x$  is defined by*

$$x' := (m - 1) \oplus (-x)$$

Obviously  $x \oplus x' = m - 1$  since for any  $x \in M$ ,  $x \oplus (-x) = 0$ .

**Definition 3** *Subtraction modulo  $m$  " $\ominus$ " is defined by*

$$x \ominus y := x \oplus (-y)$$

where  $x$  and  $y$  denote multiple-valued variables.

Using  $\ominus$  operation, the complement of an  $x$  can be represented as  $x' = (m - 1) \ominus x$ .

It is well known, that a multiple-valued algebra, based on the operations MIN, MAX and the set of all literal operators is functionally complete [5]. Since MAX can be expressed through MIN and complement using de Morgan's law  $MAX(x, y) = (MIN(x', y'))'$ , and since complement is defined through addition modulo  $m$  and the constant  $(m-1)$  (Definition 2), we can conclude that the algebra  $\mathcal{A}$  is functionally complete with constants. Functional completeness of an algebra implies that every multiple-valued function can be expressed in it. In the following sections we derive a canonical expansion, uniquely representing any multiple-valued function in the algebra  $\mathcal{A}$ .

### 3 Decomposition Theorem

In this section a decomposition, allowing a function of  $n$  variables to be expressed through  $n$  functions of  $n - 1$  variables, is presented. This decomposition can be considered as a generalization of positive and negative decompositions in Boolean algebra [3] to multiple-valued algebra. We show later that a canonical form for

an  $m$ -valued  $n$ -variable function can be derived by expanding the function in all  $n$  variables using this decomposition.

We use the following notation. The subfunction  $f_u(x_1, \dots, x_p)$  of the function  $f(x_1, \dots, x_n)$  is defined by

$$f_u(x_1, \dots, x_p) := f(x_1, \dots, x_p, u_1, \dots, u_{n-p}),$$

where  $(u_1, \dots, u_{n-p})$  is the  $m$ -ary expansion of  $u$ ,  $u \in \{0, \dots, m^{n-p} - 1\}$ , with  $u_1$  being the least significant digit, i.e.  $u = \sum_{q=1}^{n-p} m^{q-1} u_q$ , and  $p \in \{1, 2, \dots, n-1\}$ . We denote as  $f_j$ ,  $j \in \{0, \dots, m^n - 1\}$ , the coefficients from the truth table for  $f(x_1, \dots, x_n)$ , with  $x_1$  the lowest order variable.

Theorem 1 is the general decomposition theorem for a function  $f(x_1, \dots, x_n)$  about some variable  $x_i$ . However, for notational convenience, the theorem is stated, and proved, for a decomposition about the variable  $x_n$ . The sign  $\sum$ , when used below, denotes addition modulo  $m$ .

**Theorem 1 (Decomposition Theorem)** *Every  $m$ -valued function  $f(x_1, \dots, x_n)$  can be decomposed with respect to a variable  $x_n$  and a given  $i \in M$  in the following way:*

$$f(x_1, \dots, x_n) = f_i(x_1, \dots, x_{n-1}) \oplus \sum_{j=1}^{m-1} (f_{i \oplus j}(x_1, \dots, x_{n-1}) \ominus f_i(x_1, \dots, x_{n-1})) \overset{i \oplus j}{x_n}$$

**Proof:** given in the Appendix.

For example, a 3-valued 2-variable function  $f(x_1, x_2)$  can be decomposed with respect to the variable  $x_2$  and a given  $i \in \{0, 1, 2\}$  in the following way:

$$f(x_1, x_2) = f_i(x_1) \oplus [(f_{i \oplus 1}(x_1) \ominus f_i(x_1)) \overset{i \oplus 1}{x_2}] \oplus [(f_{i \oplus 2}(x_1) \ominus f_i(x_1)) \overset{i \oplus 2}{x_2}].$$

The decompositions for all three possible values of  $i$  are:

For  $i = 0$ :  $f(x_1, x_2) = f_0(x_1) \oplus [(f_1(x_1) \ominus f_0(x_1)) \overset{1}{x}_2] \oplus [(f_2(x_1) \ominus f_0(x_1)) \overset{2}{x}_2]$ .

For  $i = 1$ :  $f(x_1, x_2) = f_1(x_1) \oplus [(f_2(x_1) \ominus f_1(x_1)) \overset{2}{x}_2] \oplus [(f_0(x_1) \ominus f_1(x_1)) \overset{0}{x}_2]$ .

For  $i = 2$ :  $f(x_1, x_2) = f_2(x_1) \oplus [(f_0(x_1) \ominus f_2(x_1)) \overset{0}{x}_2] \oplus [(f_1(x_1) \ominus f_2(x_1)) \overset{1}{x}_2]$ .

For example, suppose  $f(x_1, x_2)$  is defined by the table below:

		$x_2$		
		0	1	2
	0	0	1	2
$x_1$	1	1	1	2
	2	2	0	0

Then we have

$x_1$	$f_0(x_1)$	$f_1(x_1)$	$f_2(x_1)$
0	0	1	2
1	1	1	2
2	2	0	0

and, for the decomposition with respect to  $x_2$  with  $i = 0$

$$\begin{aligned} f(x_1, x_2) &= f_0(x_1) \oplus [(f_1(x_1) \ominus f_0(x_1)) \overset{1}{x}_2] \oplus [(f_2(x_1) \ominus f_0(x_1)) \overset{2}{x}_2] \\ &= f_0(x_1) \oplus g_1(x_1) \overset{1}{x}_2 \oplus g_2(x_1) \overset{2}{x}_2 \end{aligned}$$

where

$x_1$	$g_1(x)$	$g_2(x)$
0	1	2
1	0	1
2	1	1

Obviously, if each of the subfunctions  $f_j(x_1, \dots, x_{n-1})$ ,  $j \in M$ , in the decomposition of  $f(x_1, \dots, x_n)$  is further decomposed into its subfunctions  $f_k(x_1, \dots, x_{n-2})$ ,  $k \in M$ , and successively further decomposed about the remaining variables, we finally get an expression in which  $f(x_1, \dots, x_n)$  is expanded in all  $n$  variables. Since for each subfunction the decomposition can be made with respect to some constant

$i \in M$ , there are  $m^n$  different ways to expand the function  $f(x_1, \dots, x_n)$  in all  $n$  variables. In the next section we prove that these  $m^n$  expansions are canonical forms, uniquely representing a multiple-valued function, and show how to find these forms directly, without applying step-by-step decomposition.

## 4 Canonical form of a multiple-valued function

In a Boolean algebra with carrier set  $B = \{0, 1\}$  there are  $2^n$  fixed polarity Reed-Muller canonical forms for any  $n$ -variable Boolean function [4], [7]. In a fixed polarity form, each variable  $x_i$  is either in a complemented, or in an uncomplemented form, according to some polarity vector  $k = (k_n \dots k_2 k_1)$ . If  $k_i = 1$  the variable  $x_i$  appears in complemented form, otherwise  $x_i$  appears in uncomplemented form. For example, the polarity vector  $k = (011)$  implies that  $x_1$  and  $x_2$  appear complemented in the Reed-Muller canonical form, and  $x_3$  appears uncomplemented ( $x_1$  is the lowest order variable). A polarity can be given not only as a binary vector  $(k_n \dots k_2 k_1)$ , but also as a decimal number  $k \in \{0, 1, \dots, 2^n - 1\}$ , whose binary expansion is this binary vector. For example, for  $k = (011)$  the polarity can be given as  $k = 3$ .

We generalize the notion of fixed polarity for multiple-valued logic, assuming that in a fixed polarity form each variable  $x_i$ ,  $i \in \{1, \dots, n\}$ , is represented by all literals except  $\overset{k_i}{x}_i$ , where  $(k_n \dots k_2 k_1)$  is the  $m$ -ary expansion of a polarity  $k \in \{0, 1, \dots, m^n - 1\}$ , given as a decimal number. For example, if  $m = 3$ , polarity vector  $k = (021)$  implies that  $x_1$  is represented by literals  $\overset{0}{x}_1$  and  $\overset{2}{x}_1$  in the canonical form,  $x_2$  by literals  $\overset{0}{x}_2$  and  $\overset{1}{x}_2$ , and  $x_3$  by literals  $\overset{1}{x}_3$  and  $\overset{2}{x}_3$ .

The following theorem shows that there exist  $m^n$  canonical forms of a  $m$ -valued  $n$ -variable function, each characterized by a polarity  $k \in \{0, 1, \dots, m^n - 1\}$  and a corresponding vector of coefficients  $[c_0 c_1 \dots c_{m^n-1}]$ ,  $c_j \in M$ . The notation  $\overset{i}{x}^j$  used in the theorem is defined as follows:

$$\overset{i}{x}^j := \begin{cases} m-1 & \text{if } i = 0 \\ \overset{i \oplus j}{x} & \text{otherwise} \end{cases}$$

where  $x$  is a multiple-valued variable and  $i, j \in M$  are constants.

**Theorem 2** Any  $m$ -valued  $n$ -variable function can be expressed in a canonical form with a fixed polarity  $k \in \{0, 1, \dots, m^n - 1\}$  as:

$$f(x_1, x_2, \dots, x_n) = \sum_{j=0}^{m^n-1} c_j \overset{j_1}{x_1}{}^{k_1} \overset{j_2}{x_2}{}^{k_2} \dots \overset{j_n}{x_n}{}^{k_n}$$

where  $c_j \in M$  are constants, and  $(j_n \dots j_2 j_1)$  and  $(k_n \dots k_2 k_1)$  are the  $m$ -ary expansions of  $j$  and  $k$ , respectively, with  $j_1$  and  $k_1$  being the least significant digits.

**Proof:** given in the Appendix.

For example, the canonical form of a 3-valued 2-variable function  $f(x_1, x_2)$  for every given fixed polarity  $k$ ,  $k \in \{0, 1, \dots, 8\}$  is given by:

$$\begin{aligned} f(x_1, x_2) = & \sum_{j=0}^8 c_j \overset{j_1}{x_1}{}^{k_1} \overset{j_2}{x_2}{}^{k_2} = c_0 \oplus c_1 \overset{1 \oplus k_1}{x_1} \oplus c_2 \overset{2 \oplus k_1}{x_1} \oplus c_3 \overset{1 \oplus k_2}{x_2} \oplus \\ & \oplus c_4 \overset{1 \oplus k_1}{x_1} \overset{1 \oplus k_2}{x_2} \oplus c_5 \overset{2 \oplus k_1}{x_1} \overset{1 \oplus k_2}{x_2} \oplus c_6 \overset{2 \oplus k_2}{x_2} \oplus c_7 \overset{1 \oplus k_1}{x_1} \overset{2 \oplus k_2}{x_2} \oplus c_8 \overset{2 \oplus k_1}{x_1} \overset{2 \oplus k_2}{x_2} \end{aligned}$$

where  $(k_2 k_1)$  is the ternary expansion of  $k$ . For example, for  $k = 1$  the ternary expansion is  $(k_2 k_1) = (01)$  and the function has the following form:

$$f(x_1, x_2) = c_0 \oplus c_1 \overset{2}{x_1} \oplus c_2 \overset{0}{x_1} \oplus c_3 \overset{1}{x_2} \oplus c_4 \overset{2}{x_1} \overset{1}{x_2} \oplus c_5 \overset{0}{x_1} \overset{1}{x_2} \oplus c_6 \overset{2}{x_2} \oplus c_7 \overset{2}{x_1} \overset{2}{x_2} \oplus c_8 \overset{0}{x_1} \overset{2}{x_2} .$$

In order to compute the coefficients of the canonical form, we first define a matrix  $B^n$  whose rows correspond to certain permutations of the values of the truth vector of the function  $f(x_1, \dots, x_n)$ . With  $B_u^p$  we denote a matrix whose rows correspond to certain permutations of the values of the truth vector of the subfunction  $f_u(x_1, \dots, x_p)$  of  $f(x_1, \dots, x_n)$ . Clearly  $B^n$  can be defined through  $B_u^p$ . Formally, we define  $B^n$  as  $B_0^n$  in order to start the induction in the definition below. The notation  $[X]_{ij}$  used in the definition refers to the submatrix in the  $i$ th row and  $j$ th column of the matrix  $X$ .

**Definition 4** The  $m^n \times m^n$  matrix  $B^n$  is defined inductively by:

1.  $B^n := B_0^n$
2.  $B_u^0 := [f_u]$
3.  $[B_u^p]_{ij} := B_{um+(i\oplus j)}^{p-1}$

where  $i, j \in M$ ,  $p \in \{1, \dots, n\}$ ,  $u \in \{0, \dots, m^{n-p} - 1\}$ .

The scheme is obvious from an example. For instance, for  $m = 3$ ,  $n = 2$  the matrix  $B^2$  is constructed as follows:

$$B^2 = B_0^2 = \begin{bmatrix} B_0^1 & B_1^1 & B_2^1 \\ B_1^1 & B_2^1 & B_0^1 \\ B_2^1 & B_0^1 & B_1^1 \end{bmatrix}$$

$$\text{where } B_0^1 = \begin{bmatrix} f_0 & f_1 & f_2 \\ f_1 & f_2 & f_0 \\ f_2 & f_0 & f_1 \end{bmatrix}, \quad B_1^1 = \begin{bmatrix} f_3 & f_4 & f_5 \\ f_4 & f_5 & f_3 \\ f_5 & f_3 & f_4 \end{bmatrix}, \quad B_2^1 = \begin{bmatrix} f_6 & f_7 & f_8 \\ f_7 & f_8 & f_6 \\ f_8 & f_6 & f_7 \end{bmatrix}.$$

So:

$$B^2 = \begin{bmatrix} f_0 & f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 & f_8 \\ f_1 & f_2 & f_0 & f_4 & f_5 & f_3 & f_7 & f_8 & f_6 \\ f_2 & f_0 & f_1 & f_5 & f_3 & f_4 & f_8 & f_6 & f_7 \\ f_3 & f_4 & f_5 & f_6 & f_7 & f_8 & f_0 & f_1 & f_2 \\ f_4 & f_5 & f_3 & f_7 & f_8 & f_6 & f_1 & f_2 & f_0 \\ f_5 & f_3 & f_4 & f_8 & f_6 & f_7 & f_2 & f_0 & f_1 \\ f_6 & f_7 & f_8 & f_0 & f_1 & f_2 & f_3 & f_4 & f_5 \\ f_7 & f_8 & f_6 & f_1 & f_2 & f_0 & f_4 & f_5 & f_3 \\ f_8 & f_6 & f_7 & f_2 & f_0 & f_1 & f_5 & f_3 & f_4 \end{bmatrix}.$$

The definition below presents a transformation matrix  $T^n$ , needed to obtain the coefficients of the canonical form from the matrix  $B^n$ .

**Definition 5** The  $m^n \times m^n$  matrix  $T^n$  is defined inductively by:

1.  $T^0 = [1]$
2.  $T^n := \begin{bmatrix} T^{n-1} & (m-1)*T^{n-1} & (m-1)*T^{n-1} & \dots & (m-1)*T^{n-1} \\ 0 & T^{n-1} & 0 & \dots & 0 \\ 0 & 0 & T^{n-1} & \dots & 0 \\ & & & \dots & \\ 0 & 0 & 0 & \dots & T^{n-1} \end{bmatrix}$

where  $*$  denotes multiplication modulo  $m$ .

For example, for  $m = 3$  the corresponding matrices  $T^0$ ,  $T^1$  and  $T^2$  are as follows:

$$T^0 = [1], \quad T^1 = \begin{bmatrix} 122 \\ 010 \\ 001 \end{bmatrix}, \quad T^2 = \begin{bmatrix} 122 & 211 & 211 \\ 010 & 020 & 020 \\ 001 & 002 & 002 \\ 000 & 122 & 000 \\ 000 & 010 & 000 \\ 000 & 001 & 000 \\ 000 & 000 & 122 \\ 000 & 000 & 010 \\ 000 & 000 & 001 \end{bmatrix}.$$

To find the coefficients of a fixed polarity canonical form of a multiple-valued function  $f(x_1, \dots, x_n)$ , the matrix  $B^n$  is multiplied by the transformation matrix  $T^n$ :

$$\mathbf{C} = B^n * T^n$$

Every row  $k$  of the resulting  $m^n \times m^n$  matrix  $\mathbf{C}$  corresponds to the vector of coefficients  $[c_0 c_1 \dots c_{m^n-1}]$  with polarity  $k$ . It is clear from the detailed inspection that coefficients that result from this process are these defined by the Theorem 2.

The step-by-step execution of the operation  $B^n * T^n$  involves the summation of a total  $m^n \times m^n \times m^n$  individual product terms. However, due to the regular structure of the matrix  $T^n$  a "fast" procedure for performing  $B^n * T^n$  is possible, with the total number of summations reduced to  $n \frac{m-1}{m} \times m^n \times m^n$ , which makes the complexity of the procedure  $O(N^2 \lg N)$ , where  $N = m^n$ . A fragment of the graphical representation of the fast procedure for  $n = 2, m = 3$  is shown on Fig. 1. The butterfly diagram illustrates the multiplication of  $i$ th row of  $B^2$  by  $T^2$ . The result is a vector of coefficients  $[c_0 c_1 \dots c_8]$  with polarity  $i$ . The total number of summations required is  $n \frac{m-1}{m} \times m^n = 12$ . The complete butterfly diagram for multiplication of  $B^2$  by  $T^2$  consists of  $m^n = 9$  such fragments.

The following example illustrates the calculation of the matrix of coefficients  $\mathbf{C}$ .

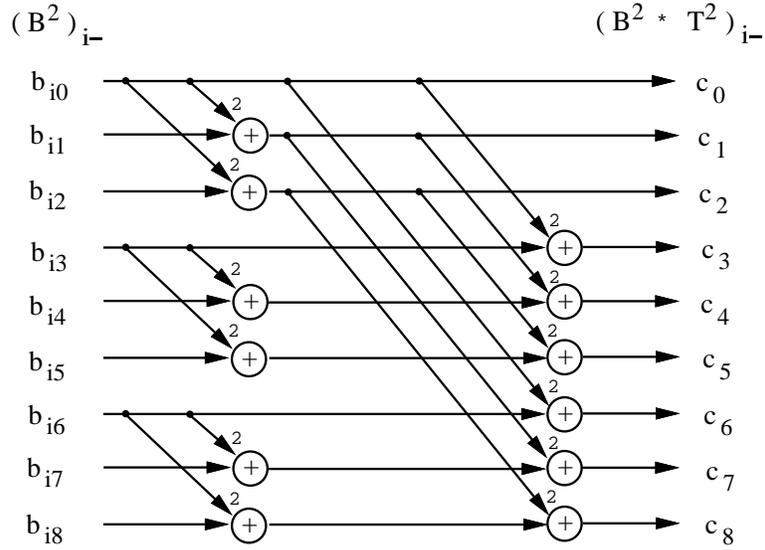


Figure 1: Butterfly diagram illustrating the multiplication of  $i$ th row of the matrix  $B^2$  by the matrix  $T^2$ .

### Example

Consider the following 3-valued 2-variable function:

$$f(x_1, x_2) = 1 \begin{smallmatrix} 0 & 0 \\ x_1 & x_2 \end{smallmatrix} + 1 \begin{smallmatrix} 1 & 0 \\ x_1 & x_2 \end{smallmatrix} + \begin{smallmatrix} 2 & 0 \\ x_1 & x_2 \end{smallmatrix} + 1 \begin{smallmatrix} 1 & 1 \\ x_1 & x_2 \end{smallmatrix} + \begin{smallmatrix} 1 & 2 \\ x_1 & x_2 \end{smallmatrix} + 1 \begin{smallmatrix} 2 & 2 \\ x_1 & x_2 \end{smallmatrix}.$$

The defining table for the function  $f(x_1, x_2)$  is shown below:

		$x_2$		
		0	1	2
$x_1$	0	1	0	0
	1	1	1	2
	2	2	0	1

In order to obtain the coefficients of the fixed polarity canonical form we construct the matrix  $B^2$ , and then multiply it by  $T^2$ .

$$\mathbf{C} = B^2 * T^2 = \begin{bmatrix} 112 & 010 & 021 \\ 121 & 100 & 210 \\ 211 & 001 & 102 \\ 010 & 021 & 112 \\ 100 & 210 & 121 \\ 001 & 102 & 211 \\ 021 & 112 & 010 \\ 210 & 121 & 100 \\ 102 & 211 & 001 \end{bmatrix} * \begin{bmatrix} 122 & 211 & 211 \\ 010 & 020 & 020 \\ 001 & 002 & 002 \\ 000 & 122 & 000 \\ 000 & 010 & 000 \\ 000 & 001 & 000 \\ 000 & 000 & 122 \\ 000 & 000 & 010 \\ 000 & 000 & 001 \end{bmatrix} = \begin{bmatrix} 101 & 212 & 220 \\ 110 & 012 & 111 \\ 222 & 112 & 202 \\ 010 & 011 & 121 \\ 122 & 102 & 021 \\ 001 & 120 & 221 \\ 021 & 110 & 022 \\ 221 & 222 & 201 \\ 121 & 101 & 210 \end{bmatrix}$$

The fourth, sixth and seventh rows of  $\mathbf{C}$  have the largest number of zero-valued coefficients (three). Hence, polarities  $k = 3, 5$  and  $6$  are the polarities for which the canonical form of the function  $f(x_1, x_2)$  has a minimal number of non-zero valued coefficients. For example, for  $k = 6$ , i.e.  $(k_2 k_1) = (20)$ , the function  $f(x_1, x_2)$  has the following canonical form:

$$\begin{aligned} f(x_1, x_2) &= c_1 \overset{1 \oplus k_1}{x_1} \oplus c_2 \overset{2 \oplus k_1}{x_1} \oplus c_3 \overset{1 \oplus k_2}{x_2} \oplus c_4 \overset{1 \oplus k_1 1 \oplus k_2}{x_1 x_2} \oplus c_5 \overset{2 \oplus k_1 1 \oplus k_2}{x_1 x_2} \oplus c_6 \overset{2 \oplus k_2}{x_2} \oplus \\ &\quad \oplus c_7 \overset{1 \oplus k_1 2 \oplus k_2}{x_1 x_2} \oplus c_8 \overset{2 \oplus k_1 2 \oplus k_2}{x_1 x_2} \\ &= 0 \oplus 2 \overset{1 \oplus 0}{x_1} \oplus 1 \overset{2 \oplus 0}{x_1} \oplus 1 \overset{1 \oplus 2}{x_2} \oplus 1 \overset{1 \oplus 0}{x_1} \overset{1 \oplus 2}{x_2} \oplus 0 \overset{2 \oplus 0}{x_1} \overset{1 \oplus 2}{x_2} \oplus 0 \overset{2 \oplus 2}{x_2} \oplus \\ &\quad \oplus 2 \overset{1 \oplus 0}{x_1} \overset{2 \oplus 2}{x_2} \oplus 2 \overset{2 \oplus 0}{x_1} \overset{2 \oplus 2}{x_2} \\ &= \overset{1}{x_1} \oplus 1 \overset{2}{x_1} \oplus 1 \overset{0}{x_2} \oplus 1 \overset{1}{x_1} \overset{0}{x_2} \oplus \overset{1}{x_1} \overset{1}{x_2} \oplus \overset{2}{x_1} \overset{1}{x_2}. \end{aligned}$$

## 5 Conclusion

This paper introduces a canonical form for multiple-valued functions, based on the operations of addition modulo  $m$ , minimum and the set of all literal operators. In the two-valued case this form reduces to fixed polarity Reed-Muller canonical form.

One advantage of the new generalization over other generalizations of the Reed-Muller canonical form previously proposed [1] [6] [2] is that it is defined for  $m$  being any positive integer, whereas other representations are applicable only for the case of  $m$  being a prime or a power of a prime number.

Another advantage is that, from the implementation point of view, the MIN operation is much easier to implement than the multiplication modulo  $m$  operation. For example, MIN can be implemented as a current-mode CMOS MVL circuit using only 5 transistors [10]. Moreover, this implementation is independent of  $m$ , i.e. the number of transistors does not increase with increasing values of  $m$ . On the other hand, the implementation of multiplication modulo  $m$  is much more complex and always depends on  $m$ . For example, for  $m = 3$ , a current-mode CMOS MVL circuit, realizing a multiplication modulo  $m$ , consists of 16 transistors [9].

Obviously, this implementation advantage would lead to decreasing the overall complexity of the realization of an  $m$ -valued function only if the number of terms and number of literals per term in the new canonical form is smaller than the corresponding numbers in other representations for the same function. So, further research needs to be done to estimate the complexity of the new canonical form in terms of the evaluation of the number of terms and number of literals per term in the expression for a given function as compared to corresponding numbers in other representations.

## References

- [1] M. Cohn, Switching function canonical form over integer fields, Ph.D thesis, Harvard University, Cambridge, Mass., Dec. 1960.
- [2] K.L. Kodandapani, R.V. Setur, Multi-valued algebraic generalization of Reed-Muller Canonical forms, *Proc. 1974 Int. Symp. on MVL*, 505-544.
- [3] P.K. Lui, J.C. Muzio, Simplified Theory of Boolean Functions, *Int. J. Electronics* **68** (1992), 329-341.
- [4] D.E. Muller, Application of Boolean algebra to switching circuit design and to error detection, *IRE Trans. Electron. Comput.* **EC-3** (1954), 6-12.
- [5] J.C. Muzio, T.C. Wesselkamper, Multiple-Valued Switching Theory, Adam Hilger Ltd Bristol and Boston, 1986.
- [6] D.K. Pradhan, A multi-valued algebra based on finite fields, *Proc. 1974 Int. Symp. on MVL*, 95-112.
- [7] I.S. Reed, A class of multiple-error-correcting codes and their decoding scheme, *IRE Trans. on Inform. Theory* **4** (1954), 38-42.
- [8] T. Sasao, P. Besslich, On the complexity of Mod-2 Sum PLA's, *IEEE Trans. on Computers* **39** No. 2 (1990), 262-266.
- [9] Z. Zilic, Z. Vranesic, Current-mode CMOS Galois Field Circuits, *Proc. 23rd Int. SYMP. on MVL* (1993), 245-250.
- [10] L. Zhijian, J. Hong, A CMOS Current-Mode High Speed Fuzzy Logic Microprocessor for a Real-Time Expert System, *Proc. 20th Int. Symp. on MVL* (1990), 394-400.

## APPENDIX

The proofs of the Theorem 1 and Theorem 2 are based on the following six properties. Let  $f, h$  denote multiple-valued functions and  $i, j$  denote constants over  $M$ .

### Property 1

$$(\overset{i}{x})' = \sum_{j \in M - \{i\}} \overset{j}{x}$$

**Proof:** 1) Let  $x = i$ . Then clearly  $\sum_{j \in M - \{i\}} \overset{j}{x} = 0$ . On the other hand  $(\overset{i}{x})' = (m - 1)' = 0$ .

2) Let  $x \neq i$ . Then there exists exactly one  $k$  in  $M$  such that  $x = k$  and so  $\overset{k}{x} = m - 1$ . Consequently  $\sum_{j \in M - \{i\}} \overset{j}{x} = m - 1$ . On the other hand  $(\overset{i}{x})' = 0' = m - 1$ .

Hence for both cases  $(\overset{i}{x})' = \sum_{j \in M - \{i\}} \overset{j}{x}$ .

□

### Property 2

$$f \cdot \overset{i}{x} = f \oplus [(-f) \cdot (\overset{i}{x})']$$

**Proof:** 1) Let  $x = i$ . Then  $f \cdot \overset{i}{x} = f$ . On the other hand:

$$\begin{aligned} f \oplus [(-f) \cdot (\overset{i}{x})'] &= f \oplus [(-f) \cdot (m - 1)'] \\ &= f \oplus [(-f) \cdot 0] \\ &= f \oplus 0 \\ &= f \end{aligned}$$

2) Let  $x \neq i$ . Then  $f \cdot \overset{i}{x} = 0$ . On the other hand:

$$\begin{aligned}
f \oplus [(-f) \cdot (\overset{i}{x})'] &= f \oplus [(-f) \cdot \mathbf{0}'] \\
&= f \oplus [(-f) \cdot (m-1)] \\
&= f \ominus f \\
&= \mathbf{0}
\end{aligned}$$

Hence for both cases  $f \cdot \overset{i}{x} = f \oplus [(-f) \cdot (\overset{i}{x})']$

□

### Property 3

$$f \cdot \overset{i}{x} + h \cdot \overset{j}{x} = f \cdot \overset{i}{x} \oplus h \cdot \overset{j}{x}$$

where  $i \neq j$  and " + " denotes MAX.

**Proof:** Since  $i \neq j$ ,  $x$  cannot be equal to both  $i$  and  $j$  at once. So, it is always the case that either  $x \neq i$  or  $x \neq j$  or both. Let  $x \neq i$ . Then the left hand side is  $f \cdot \overset{i}{x} + h \cdot \overset{j}{x} = f \cdot \mathbf{0} + h \cdot \overset{j}{x} = \mathbf{0} + h \cdot \overset{j}{x} = h \cdot \overset{j}{x}$ . And the right hand side is  $f \cdot \overset{i}{x} \oplus h \cdot \overset{j}{x} = f \cdot \mathbf{0} \oplus h \cdot \overset{j}{x} = \mathbf{0} \oplus h \cdot \overset{j}{x} = h \cdot \overset{j}{x}$ .

Hence for  $x \neq i$ ,  $f \cdot \overset{i}{x} + h \cdot \overset{j}{x} = f \cdot \overset{i}{x} \oplus h \cdot \overset{j}{x}$ . For the other cases the proof is similar.

□

### Property 4

$$f \cdot (\overset{i}{x} \oplus \overset{j}{x}) = f \cdot \overset{i}{x} \oplus f \cdot \overset{j}{x}$$

where  $i \neq j$ .

**Proof:** Since  $i \neq j$ ,  $x$  cannot be equal to both  $i$  and  $j$  at once. So, it is always the case that either  $x \neq i$  or  $x \neq j$  or both. Let  $x \neq i$ . Then the left hand side is  $f \cdot (\overset{i}{x} \oplus \overset{j}{x}) = f \cdot (\mathbf{0} \oplus \overset{j}{x}) = f \cdot \overset{j}{x}$ . And the right hand side is  $f \cdot \overset{i}{x} \oplus f \cdot \overset{j}{x} = f \cdot \mathbf{0} \oplus f \cdot \overset{j}{x} = f \cdot \overset{j}{x}$ .

Hence for  $x \neq i$ ,  $f \cdot (\overset{i}{x} \oplus \overset{j}{x}) = f \cdot \overset{i}{x} \oplus f \cdot \overset{j}{x}$ . For the other cases, the proof is similar.

□

### Property 5

$$\overset{i}{x} \cdot (f \oplus h) = \overset{i}{x} \cdot f \oplus \overset{i}{x} \cdot h$$

**Proof:** 1) Let  $x = i$ . Then the left hand side is  $\overset{i}{x} \cdot (f \oplus h) = (m-1) \cdot (f \oplus h) = f \oplus h$ .  
And the right hand side is  $\overset{i}{x} \cdot f \oplus \overset{i}{x} \cdot h = (m-1) \cdot f \oplus (m-1) \cdot h = f \oplus h$ .

2) Let  $x \neq i$ . Then the left hand side is  $\overset{i}{x} \cdot (f \oplus h) = 0 \cdot (f \oplus h) = 0$ . And the right hand side is  $\overset{i}{x} \cdot f \oplus \overset{i}{x} \cdot h = 0 \cdot f \oplus 0 \cdot h = 0$ .

Hence for both cases  $\overset{i}{x} \cdot (f \oplus h) = \overset{i}{x} \cdot f \oplus \overset{i}{x} \cdot h$ .

□

### Property 6

$$\overset{i}{x} \cdot (f \ominus h) = \overset{i}{x} \cdot f \ominus \overset{i}{x} \cdot h$$

**Proof:** 1) Let  $x = i$ . Then the left hand side is  $\overset{i}{x} \cdot (f \ominus h) = (m-1) \cdot (f \ominus h) = f \ominus h$ .  
And the right hand side is  $\overset{i}{x} \cdot f \ominus \overset{i}{x} \cdot h = (m-1) \cdot f \ominus (m-1) \cdot h = f \ominus h$ .

2) Let  $x \neq i$ . Then the left hand side is  $\overset{i}{x} \cdot (f \ominus h) = 0 \cdot (f \ominus h) = 0$ . And the right hand side is  $\overset{i}{x} \cdot f \ominus \overset{i}{x} \cdot h = 0 \cdot f \ominus 0 \cdot h = 0$ .

Hence for both cases  $\overset{i}{x} \cdot (f \ominus h) = \overset{i}{x} \cdot f \ominus \overset{i}{x} \cdot h$ .

□

## 1. Proof of the Theorem 1

Using the generalized Shannon decomposition (see [5]) we can express the function  $f(x_1, \dots, x_n)$  as follows:

$$f(x_1, \dots, x_n) = \overset{0}{x_n} f_0(x_1, \dots, x_{n-1}) + \overset{1}{x_n} f_1(x_1, \dots, x_{n-1}) + \dots + \overset{m-1}{x_n} f_{m-1}(x_1, \dots, x_{n-1})$$

To simplify the exposition, we use  $X$  to stand for the term  $x_1, \dots, x_{n-1}$ . Then the above expression becomes:

$$\begin{aligned}
f(x_1, \dots, x_n) &= \overset{0}{x_n} f_0(X) + \overset{1}{x_n} f_1(X) + \dots + \overset{m-1}{x_n} f_{m-1}(X) \\
&= \overset{0}{x_n} f_0(X) \oplus \overset{1}{x_n} f_1(X) \oplus \dots \oplus \overset{m-1}{x_n} f_{m-1}(X) && \{\text{property 3}\} \\
&= (f_0(X) \oplus [-f_0(X) \cdot (\overset{0}{x_n})']) \oplus \sum_{j=1}^{m-1} \overset{j}{x_n} f_j(X) && \{\text{property 2}\} \\
&= (f_0(X) \oplus [-f_0(X) \cdot \sum_{i=1}^{m-1} \overset{i}{x_n}]) \oplus \sum_{j=1}^{m-1} \overset{j}{x_n} f_j(X) && \{\text{property 1}\} \\
&= f_0(X) \oplus \sum_{j=1}^{m-1} (-f_0(X)) \overset{j}{x_n} \oplus \sum_{j=1}^{m-1} \overset{j}{x_n} f_j(X) && \{\text{property 4}\} \\
&= f_0(X) \oplus \sum_{j=1}^{m-1} f_j(X) \overset{j}{x_n} \oplus (-f_0(X)) \overset{j}{x_n} && \{\text{commutativity of } \oplus\} \\
&= f_0(X) \oplus \sum_{j=1}^{m-1} (f_j(X) \oplus (-f_0(X))) \overset{j}{x_n} && \{\text{property 5}\} \\
&= f_0(X) \oplus \sum_{j=1}^{m-1} (f_j(X) \ominus f_0(X)) \overset{j}{x_n} && \{\text{definition 3}\}
\end{aligned}$$

In the above derivation we expanded  $\overset{0}{x_n} \cdot f_0(X)$  using Property 2. If alternatively we expanded  $\overset{i}{x_n} \cdot f_i(X)$  for some  $i \neq 0$ , then the derivation gives the proof for the corresponding value of  $i$ .

□

## 2. Proof of the Theorem 2

By induction on  $n$ .

1) Let  $n = 1$ . According to Theorem 1, any function of one variable can be decomposed with respect to this variable and a given  $i \in M$  as:

$$\begin{aligned}
 f(x) &= f_i \oplus \sum_{j=1}^{m-1} (f_{i \oplus j} \ominus f_i) x^{i \oplus j} && \{\text{theorem 1}\} \\
 &= c_0 \oplus \sum_{j=1}^{m-1} c_j x^{i \oplus j} && \{\text{where } c_0 = f_i \text{ and } c_j = f_{i \oplus j} \ominus f_i\} \\
 &= c_0 x^i \oplus \sum_{j=1}^{m-1} c_j x^{i \oplus j} && \{0 x^i = m - 1, \text{ and } x^{i \oplus j} = x^j, \text{ for } j \neq 0\} \\
 &= \sum_{j=0}^{m-1} c_j x^j
 \end{aligned}$$

Which is the canonical form for  $n = 1$  and polarity  $i \in \{0, 1, \dots, m - 1\}$ .

2) Hypothesis: Assume the result for the functions of  $n$  variables. According to Theorem 1, any function of  $n+1$  variables can be decomposed with respect the variable  $x_{n+1}$  and a given  $i \in M$  as:

$$f(x_1, \dots, x_{n+1}) = f_i(x_1, \dots, x_n) \oplus \sum_{p=1}^{m-1} (f_{i \oplus p}(x_1, \dots, x_n) \ominus f_i(x_1, \dots, x_n)) x_{n+1}^{i \oplus p}$$

By the induction hypothesis which assumes the result for the functions of  $n$  variables, we can express each of the subfunctions  $f_i(x_1, \dots, x_n)$ ,  $f_{i \oplus p}(x_1, \dots, x_n)$ ,  $p \in \{1, 2, \dots, m - 1\}$  in the canonical form for some polarity  $k = (k_n \dots k_2 k_1)$ . We use the notation  $c_j^r$  to denote  $j$ th coefficient of the canonical form of the subfunction  $f_r(x_1, \dots, x_n)$ . Then we have:

$$\begin{aligned}
 f(x_1, \dots, x_{n+1}) &= \sum_{j=0}^{m^n-1} c_j^i j_1 x_1^{k_1} \dots j_n x_n^{k_n} \oplus \sum_{p=1}^{m-1} \left( \sum_{j=0}^{m^n-1} c_j^{i \oplus p} j_1 x_1^{k_1} \dots j_n x_n^{k_n} \ominus \right. \\
 &\quad \left. \ominus \sum_{j=0}^{m^n-1} c_j^i j_1 x_1^{k_1} \dots j_n x_n^{k_n} \right) x_{n+1}^{i \oplus p}
 \end{aligned}$$

To simplify the exposition, we use the notation  ${}^j X^k$  to stand for the term  ${}^{j_1} x_1^{k_1} \dots {}^{j_n} x_n^{k_n}$ .

Then the above expression becomes:

$$\begin{aligned}
f(x_1, \dots, x_{n+1}) &= \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \oplus \sum_{p=1}^{m-1} \left( \sum_{j=0}^{m^n-1} c_j^{i \oplus p} {}^j X^k \ominus \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \right) {}^{i \oplus p} x_{n+1} \\
&= \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \oplus \sum_{p=1}^{m-1} \left( \sum_{j=0}^{m^n-1} c_j^{i \oplus p} {}^j X^k \oplus \left( - \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \right) \right) {}^{i \oplus p} x_{n+1} \\
&\hspace{20em} \{\text{definition 3}\} \\
&= \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \oplus \sum_{p=1}^{m-1} \left( \sum_{j=0}^{m^n-1} c_j^{i \oplus p} {}^j X^k \oplus \sum_{j=0}^{m^n-1} -c_j^i {}^j X^k \right) {}^{i \oplus p} x_{n+1} \\
&\hspace{10em} \{\text{distributivity of " - " over " } \oplus \text{ "}\} \\
&= \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \oplus \sum_{p=1}^{m-1} \left( \sum_{j=0}^{m^n-1} (c_j^{i \oplus p} {}^j X^k \oplus (-c_j^i {}^j X^k)) \right) {}^{i \oplus p} x_{n+1} \\
&\hspace{15em} \{\text{commutativity of " } \oplus \text{ "}\} \\
&= \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \oplus \sum_{p=1}^{m-1} \left( \sum_{j=0}^{m^n-1} (c_j^{i \oplus p} {}^j X^k \ominus c_j^i {}^j X^k) \right) {}^{i \oplus p} x_{n+1} \\
&\hspace{20em} \{\text{definition 3}\} \\
&= \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \oplus \sum_{p=1}^{m-1} \left( \sum_{j=0}^{m^n-1} (c_j^{i \oplus p} \ominus c_j^i) {}^j X^k \right) {}^{i \oplus p} x_{n+1} \\
&\hspace{20em} \{\text{property 6}\} \\
&= \sum_{j=0}^{m^n-1} c_j^i {}^j X^k \oplus \sum_{p=1}^{m-1} \sum_{j=0}^{m^n-1} (c_j^{i \oplus p} \ominus c_j^i) {}^j X^k {}^{i \oplus p} x_{n+1} \\
&\hspace{20em} \{\text{property 5}\} \\
&= \sum_{j=0}^{m^n-1} c_j^i {}^j X^k {}^0 x_{n+1}^i \oplus \sum_{p=1}^{m-1} \sum_{j=0}^{m^n-1} (c_j^{i \oplus p} \ominus c_j^i) {}^j X^k {}^p x_{n+1}^i \\
&\hspace{15em} \{ {}^0 x^i = m-1, \text{ and } {}^p x^i = {}^{i \oplus p} x^i, \text{ for } p \neq 0 \}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{j=0}^{m^n-1} c_j^i X^{k_0} x_{n+1}^i \oplus \sum_{j=0}^{m^n-1} (c_j^{i \oplus 1} \ominus c_j^i)^j X^{k_1} x_{n+1}^i \oplus \dots \oplus \sum_{j=0}^{m^n-1} (c_j^{i \oplus (m-1)} \ominus c_j^i)^j X^{k_{m-1}} x_{n+1}^i \\
&\hspace{25em} \{\text{reordering}\} \\
&= \sum_{j=0}^{m^{n+1}-1} c_j^i X^{k_{j_{n+1}}} x_{n+1}^i,
\end{aligned}$$

where  $c_j = c_j^i$ , for  $0 \leq j \leq m^n - 1$ , and  $c_{pm^n+j} = (c_j^{i \oplus p} \ominus c_j^i)$ , for  $1 \leq p \leq m - 1$ ,  $0 \leq j \leq m^n - 1$ .

Which is the canonical form for a function of  $n + 1$  variables for polarity vector  $k = (k_{n+1}k_n \dots k_2k_1)$ , where  $k_{n+1} = i$ . This proves the theorem.

□