# Universal XOR Canonical Forms of Boolean Functions and its Subset Family of AND/OR/XOR Canonical Forms

Marek A. Perkowski
Dept. of Electrical Engineering
Portland State University

Andisheh Sarabi
Viewlogic Systems, Inc.
Fremont, CA

F. Rudolf Beyl
Dept. of Mathematical Sciences
Portland State University

**Abstract**

*In this paper a new concept of Universal XOR Canonical Forms is presented. Such forms include all well-known families of AND/XOR canonical forms as special cases. A general mathematical treatment of these forms is presented. It is shown that utilizing linear group theory, many properties and classes of these canonical forms can be studied. By this approach, the number of possible XOR canonical forms is shown to be enormous. Several operators to create various AND/OR/XOR canonical forms are also introduced. Such operators, which generalize the Kronecker tensor product, limit these canonical forms to the ones finding applications in most technologies.*

## 1 Introduction

The XOR logic is finding more interest due to its inherent characteristics, availability of new synthesis tools, and the new technologies which make efficient realization of this logic possible. In terms of inherent efficiency of XOR logic, it has been shown that AND/XOR PLAs on average are more compact than AND/OR PLAs [17]. Other studies have shown this compactness in practical circuits [18, 20, 11]. The circuit realizations in this logic can also be easily testable [15].

The large size of XOR gates in CMOS and their delays have historically been a major reason for underutilization of XORs in design. This is despite the fact that realization of arithmetic, encoding, telecommunication, and linear circuits with XOR logic has been well known to be more compact than other realizations. The recent advances in PLD and FPGA technologies have had a big impact on utilization of XORs in circuit design. Many PLDs include XOR gates as one of their main components which make the utilization of XOR logic much more practical. Furthermore, many FPGA architectures remove any distinction in realization among different logics. While this is true for LUT-type FPGAs, many fine grain FPGAs have XOR as one of their main blocks. With new advances in VLSI and deep submicron technologies, the delays due to XORs would be not a main issue as the routing will be the main source of area and delay. An advantage that XOR logic can provide in this aspect is the regularity that it provides which can contribute to layout driven synthesis [16].

A major other characteristic of the XOR logic is the numerous possible canonical representations of switching functions it provides. Various decision diagrams are basically multi-level representations of the functions based on this logic [6]. The canonicity provided in this logic has found applications not only in the representation of the functions but as an example in Boolean matching techniques [23]. While many AND/XOR canonical representations have been know in literature, it is the purpose of this paper to provide a systematic way of studying all possible canonical representations in XOR logic. It further provides an insight to the multitude of these representations compared to other forms such as AND/OR.

The AND/XOR canonical forms have been the subject of many studies [5, 8, 10, 19]. The first AND/XOR canonical form introduced in the literature is known as *Reed-Muller Canonical (RMC)* form [13, 9]. In this form, which was introduced earlier by Zhegalkin [24], all literals occur in positive polarity only. A larger class of AND/XOR canonical forms, known as *Consistent Generalized Reed-Muller (CGRM)* Canonical forms [5, 14] was introduced by Akers [1]. These forms have been also known as *fixed polarity Reed-Muller (FPRM)* Canonical forms [19]. *CGRM*s are members of several other larger classes of AND/XOR canonical forms. *Generalized Reed-Muller (GRM)* Canonical forms [5], also termed as *Canonical Restricted Mixed Polarity (CRMP)* [11, 4] are one such class. A different superclass of *CGRM*s are the *Kronecker Reed-Muller (KRM)* canonical forms [5, 7]. *KRM*s are members of a larger class of *Pseudo-Kronecker Reed-Muller (PKRM)* canonical forms which themselves are included in the class of *Quasi-Kronecker Reed-Muller (QKRM)* canonical forms. Other extensions to these forms can be found in [8]. The extensions to the multi-valued cases can be found in [10]. The largest class of AND/XOR expressions is called the *Exclusive Sum of Products (ESOP)* expressions.

This paper attempts to provide a tool to generate and investigate all XOR canonical forms. These forms in general are Exclusive Sum of general terms which include any possible operations on literals rather than just their products. This, obviously will include the

[1]This research was partially supported by the NSF grant MIP-9110772.

AND/XOR canonical forms as a particular case and encompasses a much larger set of canonical forms. The concept of basis functions allows for extending these studies and provides a formal method of investigation for all the forms in a systematic way. Central to this presentation is the concept of representation of the Boolean functions as vectors in the vector space of all Boolean functions.

It has long been known that the set of $n$-variable Boolean functions under addition mod-2 forms a $2^n$-dimensional vector space over the Galois field of two elements, GF(2) [12, 22]. Utilizing this concept, it will be possible to investigate all the above canonical forms as well as all other possible XOR canonical forms which have not been studied yet.

An example of utilization of these representations in physical driven synthesis will also be provided as a possible application.

In section 2, certain linear algebra concepts are reviewed which provide the general framework of this presentation. In section 3, the concept of a Universal XOR canonical form will be presented and the number of such forms will be calculated. In section 4, the utilization of UXFs in a generalized PLA realization of functions will be presented. In section 5, a subset of these forms will be given that have a suitable realization in these generalized PLA configurations.

## 2 Background

We use the following basic concepts of linear algebra:

**Definition 1** *Let $V$ be a vector space over $F$. A subset $B = \{\alpha_i | i \in I\}$ of $V$ is a* basis *for $V$ over $F$ if each vector $\beta \in V$ can be expressed as $\beta = a_1\alpha_{i_1} + a_2\alpha_{i_2} + ... + a_n\alpha_{i_n}$ with unique coefficients $a_j \in F$ where $\alpha_{i_1}, ..., \alpha_{i_n} \in B$. A vector of the form $\sum_{j=1}^{n} a_j\alpha_{i_j}$ is called a* linear combination *of the $\alpha_{i_j}$.*

The vectors and linear transformations, which are functions of vectors that preserve all linear combinations, have meaning independent of any particular basis, but their representations are entirely dependent on the bases chosen. Indeed, many such representations may be simplified by choosing a new basis.

To this end, we describe how bases can be represented in terms of each other. Specifically, let $\alpha_1, \alpha_2, ..., \alpha_m$ be one basis of the vector space $V$ and $\beta_1, \beta_2, ..., \beta_m$ be another. Then each basis vector $\beta$ can be expressed as a linear combination of the $\alpha$'s, $\beta_i = \sum_{j=1}^{n} P_{ij}\alpha_j$ with unique $P_{ij} \in F$. The matrix thus defined, $P = [P_{ij}]$, is called the *transition matrix* from the basis $A$ to the basis $B$.

**Definition 2** *A square matrix $A$ of field elements is called* nonsingular *if $\det A$ is nonzero.*

It is the nonsingular matrices that are of interest here, because a matrix is the transition matrix of suitable basis change precisely when it is nonsingular [2].

## 3 Universal XOR Canonical Forms and their Number

Each basis in the vector space $\boldsymbol{\Psi}$ over GF(2) formed by the set of $n$-variable Boolean functions under addition mod-2, has $2^n$ vectors in it. The addition mod-2 is obviously the XOR operation. Once a basis has been chosen, its vectors are called *basis functions.* Thus every Boolean function can be represented uniquely as a linear combination of the basis functions, or in other words, their Exclusive Sum. The task of the identification of all canonical forms of the Boolean functions in this field thus entails the identification of all possible bases of the $2^n$-dimensional vector space $\boldsymbol{\Psi}$. In the following, a systematic method of identifying these bases will be presented.

A well known canonical form of the Boolean functions is the sum of minterms form. In the notion of the vector spaces, the $2^n$ minterms of the function provide a basis for the vector space and each minterm is a basis function. Any Boolean function then can be uniquely represented as a linear combination of the minterms.

Two of the most well-known AND/XOR canonical forms are the *Reed-Muller* and the *Consistent Generalized Reed-Muller* Canonical forms. The *RMC* representation consists of only positive product terms and is given as:

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{i=0}^{2^n-1} a_i\mu_i \tag{1}$$

where $a_i \in \{0, 1\}$ and $\mu_i = {x_n}^{e_n}{x_{n-1}}^{e_{n-1}} \ldots {x_2}^{e_2}{x_1}^{e_1}$ $= \prod_{j=1}^{n} {x_j}^{e_j}$ where $e_j \in \{0, 1\}$ such that $e_n e_{n-1} ... e_2 e_1$ is the binary representation of the number $i$. Moreover ${x_i}^0 = 1$ and ${x_i}^1 = x_i$. The symbol $\oplus$ denotes the summation over GF(2).

If the restriction that all the variables should take positive polarity is removed and they are also allowed to take negative polarities, one has a *Generalized Reed-Muller (GRM)* canonical form. If the variables are, however, restricted to retain the same polarity, either positive or negative, in all product terms, the canonical form will be that of the *Consistent Generalized Reed-Muller (CGRM)* form.

Each term in the above canonical forms is a basis function. These basis functions can be expressed in terms of the minterm basis using a transition matrix. These transitions will be shown for two bases in Examples 1 and 2 for the case of functions of two variables.

**Example 1** *In the vector space of two-variable Boolean functions, the Reed-Muller basis functions are 1, a, b, and ab, while the minterms are $\bar{a}\bar{b}$, $a\bar{b}$, $\bar{a}b$, and $ab$. The transition from the minterm basis to the Reed-Muller basis is given by:*

$$\begin{bmatrix} ab \\ b \\ a \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} ab \\ \bar{a}b \\ a\bar{b} \\ \bar{a}\bar{b} \end{bmatrix} \tag{2}$$

*The operations are in GF(2).*

**Example 2** *A CGRM form of a two-variable Boolean function is represented by basis functions* $1, \bar{a}, b, \bar{a}b$. *Similarly, the transition is given by:*

$$\begin{bmatrix} \bar{a}b \\ b \\ \bar{a} \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} ab \\ \bar{a}b \\ a\bar{b} \\ \bar{a}\bar{b} \end{bmatrix} \tag{3}$$

*The operations are again in GF(2).*

As it can be observed, the rows of the transition matrices are linearly independent. In general, in the space $\boldsymbol{\Psi}$ of Boolean functions, all nonsingular matrices of dimension $2^n$ provide the transition matrices for all possible bases. These are the bases of *Universal XOR forms (UXF)*. Among the UXFs, there exist all AND/XOR canonical forms, XOR of products of literals which include all the previously mentioned canonical forms. There exist also other XOR forms which their basis functions can not be realized by product of the literals alone.

**Definition 3** *Let* $\boldsymbol{\Psi}$ *be a vector space of n-variable Boolean functions over* $GF(2)$. *A* Universal XOR form (UXF) *is a basis in this vector space. If a basis function in a UXF can be realized as a product of literals, it is called a* monoterm. *In general, a term in a UXF is called a* uxf-term *of f.*

The Exclusive Sum of the uxf-terms is the UXF canonical representation of the Boolean function $f$. The monoterms are only a subset of all possible basis functions. Hence the number of all UXFs is much more than the number of all possible AND/XOR canonical forms. The number of all possible XOR canonical forms can be given in terms of the number of all nonsingular matrices of a given dimension. This is related to the notion of *general linear group.*

**Definition 4** *The group of all nonsingular m-by-m matrices with entries in the field k is called the* general linear group *and denoted by* $GL_m(k)$ *[2].*

The number of such matrices is given in the following Lemma:

**Lemma 1** *Let* $k = GF(q)$ *be the Galois field with q elements. The order of* $GL_m(k)$ *is*

$$q^{m(m-1)/2} \prod_{i=1}^{m} (q^i - 1). \tag{4}$$

*Proof:* See Theorem 4.11 in [2].

**Theorem 1** *Let* $f(x_1, x_2, ..., x_n)$ *be a Boolean function of n variables. The number of all possible XOR canonical representations of the function is given by:*

$$\frac{2^{(2^{n-1})(2^n-1)}}{2^n!} \prod_{i=1}^{2^n} (2^i - 1). \tag{5}$$

*Proof:* Substituting $q = 2$ and $m = 2^n$ in Lemma 1, the number of such matrices can be seen to be

$$2^{(2^{n-1})(2^n-1)} \prod_{i=1}^{2^n} (2^i - 1)$$

for this special case. This is the number of all ordered bases. As the order of basis functions is not relevant to the canonicity of the expansion, it is the number of unordered bases that is of interest here. Hence, the number of canonical forms is given by the number of unordered bases which is the above quantity divided by $m! = 2^n!$. *QED*

By Theorem 1, there exist $20160/4! = 840$ different XOR canonical forms for a 2-variable function alone. This number for a 3-variable function is around $1.326 \times 10^{14}$. As it is evident, the number of canonical forms grows astronomically with the number of variables in this field. Up until now, only AND/XOR canonical forms have been studied in the literature. Here, the most general XOR canonical forms are introduced which utilize gates other than AND and NOT for their realization and could provide more compact realizations than *ESOP*s. Since there are many more of these than AND/XOR forms, the probability of finding the minimal circuit among them is much higher.

## 4 Utilization of UXFs in Generalized PLA Realizations

As there are huge number of possible UXFs, there will be two problems of practical interest. The first is to find such families of forms which have easy circuit realization. The second is to find the best form among all forms of each family; i.e. the one with the minimal number of uxf-terms. This paper addresses the first problem and the second will be the subject of another paper.

UXFs can be utilized as a Boolean approach to the logic optimization stage of the *Complex Maitra Logic Array, CMLA* [16] realizations. CMLA realization of Boolean functions is a combined logic synthesis and physical design approach which is comprised of realizing functions in two distinct planes: the complex (input) plane and the collecting (output) plane. The input variables of the input plane run in vertical buses. These inputs are AND, OR, or XORed together in the rows of the complex plane resulting in *Maitra terms.* In other words, the Maitra terms, which are the generalization of product terms, are realized in the rows of the complex plane.

The outputs of the Maitra terms are placed on the horizontal buses. The Maitra terms are then collected in the output plane composed of the two-dimensional array with OR or XOR gates. The CMLA concept, shown in Figure 1, is a powerful generalization of PLAs. An example of a complex plane of a CMLA is shown in Figure 2.

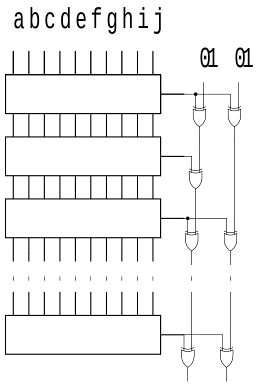


Figure 1: Example of a Complex Maitra Logic Array

The comprehensive approach to the logic and layout synthesis here includes two stages:

- **Logic optimization** which takes the geometry and layout constraints into account to create a CMLA in which every output function is an OR or XOR of Maitra terms.
- **Technology-folding** which maps the CMLA representation of the function to the target architecture, such that the area of the layout is minimized.

A distinct feature of this approach is minimization of routing resources as well as the logic. Furthermore, the placement is already figured out by the end of the two stages. Hence, it can prove useful not only in cellular array type FPGAs with limited routing resources but also in deep submicron technologies in general.

In the CMLA approach, the UXFs can be utilized in the logic optimization stage where the Boolean functions are realized as XOR of Maitra terms. In this case, the basis elements that are comprised of AND, negation, and OR of literals will be the most useful ones, as they exist in most technologies. Hence, developing methods for generation of such terms would be of most practical interest. In the next section, methods for systematic generation of such bases will be presented.

# 5 Generation of Different Families of Bases

In the following, certain operational transforms on matrices to generate different product and AND/OR terms will be described. The terms with positive polarities will be discussed first with more general terms, incorporating NOT gates, following. The significance of these operations is in that the huge number of UXFs will be reduced to fewer manageable numbers. Furthermore, the underlying structures bring in a simple methodology to handle the UXFs which find more applications in circuit design.

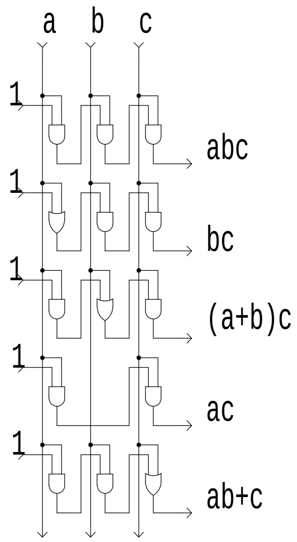


Figure 2: An Example of a Complex Plane of a CMLA

## 5.1 Positive Polarity $\alpha\rho$ Family of Bases

Different positive polarity AND/OR bases can be generated by application of two basic operations in various orders. These two operations are called the Reed-Muller and the AND/OR operators. From now on, the basis of reference consists of the minterms in reverse binary order with reversed bits, similar to the order presented in the previous examples.

**Definition 5** *Let $R$ be a nonsingular matrix. The* Reed-Muller Operator $\boldsymbol{\rho}$ *on $R$ is:*

$$\boldsymbol{\rho}(R) = \begin{bmatrix} R & \mathbf{0} \\ R & R \end{bmatrix} \tag{6}$$

*where $\mathbf{0}$ stands for a square matrix of the size of $R$ with all entries 0 .*

**Definition 6** *Let $R$ be a nonsingular matrix. The* AND-OR Operator $\boldsymbol{\alpha}$ *on $R$ is:*

$$\boldsymbol{\alpha}(R) = \begin{bmatrix} R & \mathbf{0} \\ \mathbf{1} & R \end{bmatrix} \tag{7}$$

*where $\mathbf{1}$ stands for a square matrix of the size of $R$ with all entries 1 and $\mathbf{0}$ has the same meaning as in previous definition.*

**Theorem 2** *Reed-Muller and AND-OR operators result in nonsingular matrices of a higher dimension.*

*Proof:* This follows from the fact that both $\boldsymbol{\rho}(R)$and $\boldsymbol{\alpha}(R)$ are block triangular matrices of the form

$$\begin{bmatrix} R & \mathbf{0} \\ * & R \end{bmatrix} \tag{8}$$

[2]Although the $\alpha\rho$ family is the generalization of Reed-Muller family of expressions, we do not call them "Generalized Reed-Muller" forms since this name is already reserved and also these forms are an order of magnitude more general.

with determinant $det(R)^2$. The value of the matrix denoted by * is irrelevant. *QED*

The starting matrix for a single variable, used in the generation of the positive polarity $\boldsymbol{\alpha\rho}$ family of bases, is:

$$T_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \quad (9)$$

This matrix essentially gives the basis

$$\begin{bmatrix} a \\ 1 \end{bmatrix}. \quad (10)$$

A special case of applying the $\boldsymbol{\rho}$ operator is the generation of the Reed-Muller Transform. In this case the repetitive application of the $\boldsymbol{\rho}$ operator is the same as the Kronecker tensor product of the generated nonsingular matrices.

Table 1 shows the basis functions of the Reed-Muller, AND/OR, and Reed-Muller/AND/OR expansions for three input variables.

The Reed-Muller/AND/OR expansion is constructed by $\boldsymbol{\alpha}(\boldsymbol{\rho}(T_1))$. Other similar constructs are possible - incorporating different orders of application of $\boldsymbol{\alpha}$ and $\boldsymbol{\rho}$ operators - which give rise to various AND/OR/wire connections in the complex plane of CMLA. While the order of variables is irrelevant for Reed-Muller basis, for AND/OR and all other combinations of the $\boldsymbol{\alpha}$ and $\boldsymbol{\rho}$ operators, it gives rise to a new basis.

**Definition 7** *The family of bases generated by applications of $\boldsymbol{\alpha}$ and $\boldsymbol{\rho}$ operators in all possible orders and all possible permutations of the variables is the* positive polarity $\boldsymbol{\alpha\rho}$ family of bases.

**Example 3** *The nonsingular transition matrix of AND/OR expansion for a 2-input function is given as:*

$$\boldsymbol{\alpha}[T_1] = \begin{bmatrix} T_1 & \mathbf{0} \\ \mathbf{1} & T_1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \quad (11)$$

*The transition matrix above results in the following basis functions:*

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} ab \\ \bar{a}b \\ a\bar{b} \\ \bar{a}\bar{b} \end{bmatrix} = \begin{bmatrix} ab \\ b \\ a+b \\ 1 \end{bmatrix}. \quad (12)$$

## 5.2 Consistent Generalized $\alpha\rho$ Family of Bases

The transformation of the Reed-Muller basis to any other polarity and generation of $2^n$ Consistent Generalized Reed-Muller bases is well known [3, 14]. Here, every variable is allowed to take either positive or negative polarity. Hence there are $2^n$ possible forms for an $n$ variable function. It is similarly possible to generalize all members of the $\boldsymbol{\alpha\rho}$ family of bases to $2^n$ different fixed polarities. This family will be called the *Consistent Generalized $\boldsymbol{\alpha\rho}$ ($\boldsymbol{CG\alpha\rho}$) family of forms.* In terms of the Complex Maitra Logic Arrays, this would lead to the inclusion of an additional bus for each inverted input signal. Alternatively, the inverter on the inputs can be taken as another possible gate in the CMLA.

| Reed-Muller | AND/OR | Reed-Muller/AND/OR |
|---|---|---|
| abc | abc | abc |
| bc | bc | bc |
| ac | (a + b)c | ac |
| c | c | c |
| ab | ab + c | ab + c |
| b | b + c | b + c |
| a | a + b + c | a + c |
| 1 | 1 | 1 |

Table 1: Examples of Bases for 3-Input Functions

In order to introduce negation of variables, two negation operations and a new starting transformation matrix need to be introduced. Notice that similar to Equation (9), it is possible to define a negative polarity basis of a single element. This is given as $T_2$ below:

$$T_2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad (13)$$

which gives essentially the basis

$$\begin{bmatrix} \bar{a} \\ 1 \end{bmatrix}. \quad (14)$$

Now, corresponding to the $\boldsymbol{\rho}$ and $\boldsymbol{\alpha}$ operators, $\bar{\boldsymbol{\rho}}$ and $\bar{\boldsymbol{\alpha}}$ operators are defined as the following:

**Definition 8** *Let $R$ be a nonsingular matrix. The* Negative Reed-Muller Operator $\bar{\boldsymbol{\rho}}$ *on $R$ is:*

$$\bar{\boldsymbol{\rho}}(R) = \begin{bmatrix} \mathbf{0} & R \\ R & R \end{bmatrix}. \quad (15)$$

**Definition 9** *Let $R$ be a nonsingular matrix. The* Negative AND-OR Operator $\bar{\boldsymbol{\alpha}}$ *on $R$ is:*

$$\bar{\boldsymbol{\alpha}}(R) = \begin{bmatrix} \mathbf{0} & R \\ R & \mathbf{1} \end{bmatrix}. \quad (16)$$

**Theorem 3** *The $\bar{\boldsymbol{\rho}}$ and $\bar{\boldsymbol{\alpha}}$ operators result in nonsingular matrices of a higher dimension.*

*Proof:* As in the proof of Theorem 2, the determinants of both $\bar{\boldsymbol{\rho}}(R)$ and $\bar{\boldsymbol{\alpha}}(R)$ are $det(R)^2$, thus nonzero. To this end, column exchanges will transform each of the above matrices into a block triangular matrix of the form (8). Moreover, since $-1 = +1$

in $GF(2)$, column exchanges do not alter the determinant. *QED*

Again, each variable can take either a positive or a negative operation and thus there exist $2^n$ possible Consistent Generalized forms for each positive $\boldsymbol{\alpha\rho}$ family of bases.

**Example 4** *In the following, a $\boldsymbol{CG\alpha\rho}$ basis of three variables will be shown. Here, the order and the polarity of the variables is given as: $\bar{b}\bar{c}a$, where the "natural" order of variables is assumed to be abc. First, the transition matrix for the natural order is generated and then the corresponding transition matrix for the given order will be shown.*

$$\boldsymbol{\rho}\bar{\boldsymbol{\alpha}}(T_2) = \begin{bmatrix} \bar{\boldsymbol{\alpha}}(T_2) & \mathbf{0} \\ \bar{\boldsymbol{\alpha}}(T_2) & \bar{\boldsymbol{\alpha}}(T_2) \end{bmatrix}; \; \bar{\boldsymbol{\alpha}}(T_2) = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \tag{17}$$

*The transition matrix above results in the following basis functions:*

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} abc \\ \bar{a}bc \\ a\bar{b}c \\ \bar{a}\bar{b}c \\ ab\bar{c} \\ \bar{a}b\bar{c} \\ a\bar{b}\bar{c} \\ \bar{a}\bar{b}\bar{c} \end{bmatrix} \tag{18}$$

$$= \begin{bmatrix} \bar{a}\bar{b}c \\ \bar{b}c \\ (\bar{a}+\bar{b})c \\ c \\ \bar{a}\bar{b} \\ \bar{b} \\ \bar{a}+\bar{b} \\ 1 \end{bmatrix}. \tag{19}$$

*The corresponding transition matrix for the "bca" ordering will be:*

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} abc \\ \bar{a}bc \\ a\bar{b}c \\ \bar{a}\bar{b}c \\ ab\bar{c} \\ \bar{a}b\bar{c} \\ a\bar{b}\bar{c} \\ \bar{a}\bar{b}\bar{c} \end{bmatrix} \tag{20}$$

$$= \begin{bmatrix} \bar{b}\bar{c}a \\ \bar{c}a \\ (\bar{b}+\bar{c})a \\ a \\ \bar{b}\bar{c} \\ \bar{c} \\ \bar{b}+\bar{c} \\ 1 \end{bmatrix}. \tag{21}$$

The comparison between Equations (18) and (20) shows that different orderings are achieved by swapping of appropriate columns in the transition matrix.

### 5.3 Generalized $\alpha\rho$ Family of Bases

The members of the $\boldsymbol{\alpha\rho}$ family of bases need not be confined to fixed polarities in order to provide new bases. The polarity of the literals can be "inconsistently" varied and still result in a new basis. This will be shown by the following example:

**Example 5** *The basis generated in Example 4 can now be inconsistently changed for polarity of literals to give the following new basis:*

$$\begin{bmatrix} b\bar{c}a \\ ca \\ (\bar{b}+\bar{c})\bar{a} \\ a \\ \bar{b}c \\ \bar{c} \\ \bar{b}+\bar{c} \\ 1 \end{bmatrix}. \tag{22}$$

As it can be observed, the literals $a$, $b$, and $c$ take different polarities in different basis functions.

This larger family of bases will be termed *Generalized* $\boldsymbol{\alpha\rho}$ ($\boldsymbol{G\alpha\rho}$).

### 5.4 $\alpha\rho\sigma$ Family of Bases

A different generalization of the $\boldsymbol{\alpha\rho}$ family of bases is possible through the introduction of a third operator called the Shannon operator, $\boldsymbol{\sigma}$.

First the starting transformation matrix for this extension will be introduced. Again similar to Equation (10), the basis for a single element is given as $T_3$:

$$T_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{23}$$

**Definition 10** *Let $R$ be a nonsingular matrix. The* Shannon Operator $\boldsymbol{\sigma}$ *on $R$ is:*

$$\boldsymbol{\sigma}(R) = \begin{bmatrix} R & \mathbf{0} \\ \mathbf{0} & R \end{bmatrix}. \tag{24}$$

**Theorem 4** *The $\boldsymbol{\sigma}$ operator results in a nonsingular matrix of a higher dimension.*

*Proof:* As in the proof of Theorem 2, the determinant of $\boldsymbol{\sigma}(R)$ is $det(R)^2$, thus nonzero. *QED*

Notice that $T_1$, $T_2$, and $T_3$ are three possible nonsingular matrices for a single variable function. All other nonsingular matrices for a single variable function can be constructed from swapping the rows of these three matrices and would not result in any new bases. As an example, similar to $\boldsymbol{\alpha}$ and $\boldsymbol{\rho}$ operators, it is possible to define a negative $\boldsymbol{\sigma}$ operator as shown below:

**Definition 11** *Let $R$ be a nonsingular matrix. The* Negative Shannon Operator $\bar{\boldsymbol{\sigma}}$ *on $R$ is:*

$$\bar{\boldsymbol{\sigma}}(R) = \begin{bmatrix} \mathbf{0} & R \\ R & \mathbf{0} \end{bmatrix}. \tag{25}$$

The basis for a single element here is:

$$T_4 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{26}$$

which gives essentially the basis

$$\begin{bmatrix} \bar{a} \\ a \end{bmatrix}. \tag{27}$$

It can be observed that $T_3$ and $T_4$ define essentially the same basis and no new bases will be generated by negative Shannon operator when the corresponding positive operator is present.

Introduction of the $\boldsymbol{\sigma}$ still extends the possibilities of generating new AND/OR bases. Certain other generalizations have been known for the AND/XOR bases in the literature. Those generalizations can also be extended to the AND/OR bases resulting in even larger classes of AND/OR/XOR canonical forms.

## 6 Conclusions

In this paper, a concept of canonical Universal XOR Forms was formulated. It was shown that through defining various bases in the vector space of Boolean functions, it is possible to generate all possible XOR canonical forms. AND/XOR canonical forms, both well-known as well as lesser-known ones, were shown to be special classes of Universal XOR Forms. Since these new canonical forms include all known and not yet known AND/XOR canonical forms, they can never be worse in terms of the number of uxf-terms and therefore are very much worthy of further investigations.

While the number of these forms is huge, the mapping constraints limit the number of canonical forms that can be utilized in a given technology. Two matrix operations of Reed-Muller and AND/OR along with their negations were used to generate the Consistent Generalized $\boldsymbol{\alpha\rho}$ family of forms. They were further generalized by introduction of the positive and negative Shannon operators. These new canonical forms require different AND/OR/wire configurations for their realizations and can find special applications in the Complex Maitra Logic Array realization of Boolean functions [16].

The linear group theoretic approach introduced for the study of XOR canonical forms opens up new areas for research and study. It provides the systematic treatment of all these forms and allows the utilization of linear algebra in the study of these logical forms. It also illuminates the underlying structure of these forms. It was shown through this approach that the number of these forms is huge compared to AND/OR canonical forms. The same approach can be utilized for the identification of minimal XOR canonical representation of the functions.

## References


[1] S. B. Akers, "On a Theory of Boolean Functions", *Journal of SIAM*, Vol. 7, pp. 487-498, December 1959.

[2] E. Artin, *Geometric Algebra*, Interscience Publishers, Inc., 1957.

[3] Ph. W. Besslich, "Efficient Computer method for ExOR logic design", *Proceedings of IEE Pt. E*, Vol. 130, pp. 203-206, 1983.

[4] L. Csanky, M. A. Perkowski and I. Schäfer, "Canonical Restricted Mixed Polarity Exclusive-OR Sums of Products and the Efficient Algorithm for Their Minimization", *Proceedings of IEE Pt. E*, Vol. 140, No. 1, pp. 69-77, October 1992.

[5] M. Davio, J. P. Deschamps, and A. Thayse, *Discrete and Switching Functions*, McGraw-Hill, 1978.

[6] R. Drechsler, A. Sarabi, M. Theobald, B. Becker and M. A. Perkowski, "Efficient Representation and Manipulation of Switching Functions Based on Ordered Kronecker Functional Decision Diagrams", *Proceedings of DAC '94*, pp. 321-326, San Diego, CA, June 1994.

[7] D. H. Green, "Reed-Muller Canonical Forms With Mixed Polarity and Their Manipulations", *Proceedings of IEE Pt. E*, Vol. 137, No. 1, pp. 103-113, January 1990.

[8] D. H. Green, "Families of Reed-Muller canonical forms", *International Journal of Electronics*, pp. 259-280, February 1991.

[9] D. E. Muller, "Application of Boolean Algebra to Switching Circuit Design and to Error Detection", *IRE Transactions on Electronic Computers*, Vol. EC-3, pp. 6-12, September 1954.

[10] M. A. Perkowski, "The Generalized Orthonormal Expansion of Functions With Multiple-Valued Inputs and Some of its Applications", *Proceedings of the 22nd IEEE International Symposium on Multiple-Valued Logic*, pp. 442-450, June 1992.

[11] M. A. Perkowski, L. Csanky, A. Sarabi, and I. Schäfer, "Fast Minimization of Mixed-Polarity AND/XOR Canonical Networks", *Proceedings of the IEEE International Conference on Computer Design*, pp. 33-36, Cambridge, MA, October 1992.

[12] F. P. Preparata, "State-Logic Relations For Autonomous Sequential Networks", *IEEE Transactions on Electronic Computers*, Vol. EC-15, pp. 898-908, December 1966.

[13] I. S. Reed, "A Class of Multiple-Error-Correcting Codes and Their Decoding Scheme", *IRE Transactions on Information Theory*, Vol. PGIT-4, pp. 38-49, 1954.

[14] A. Sarabi and M. A. Perkowski, "Fast Exact and Quasi-Minimal Minimization of Highly Testable Fixed-Polarity AND/XOR Canonical Networks", *Proceedings of the 29th ACM/IEEE Design Automation Conference*, pp. 30-35, Anaheim, CA, June 1992.

[15] A. Sarabi and M. A. Perkowski, "Design For Testability Properties of AND/XOR Networks", *Proceedings of the IFIP WG 10.5 Workshop on Applications of the Reed-Muller Expansion in Circuit Design*, Hamburg, Germany, September 1993.

[16] A. Sarabi, N. Song, M. Chrzanowska-Jeske, and M. A. Perkowski, "A Comprehensive Approach to Logic Synthesis and Physical Design for Two-Dimensional Logic Arrays", *Proceedings of the 31st ACM/IEEE Design Automation Conference*, pp. 321-326, San Diego, CA, June 1994.

[17] T. Sasao and Ph. W. Besslich, "On the Complexity of MOD-2 Sum PLAs", *IEEE Transactions on Computers*, Vol. 39, No. 2, pp. 262-266, February 1990.

[18] T. Sasao, "EXMIN2: A simplification algorithm for Exclusive-or-Sum-Of-Products expressions for multiple-valued input two-valued output function", *IEEE Transactions on Computer Aided Design*, Vol. 39, No. 2, pp. 262-266, 1990.

[19] T. Sasao, "AND-EXOR Expressions and their Optimization", in Sasao(ed.), *Logic Synthesis and Optimization*, Kluwer Academic Publishers, pp. 287-312, 1993.

[20] N. Song and M. A. Perkowski, "EXORCISM-MV-2: Minimization of Exclusive Sum of Products Expressions for Multiple-Valued Input Incompletely Specified Functions", *Proceedings of the 23rd IEEE International Symposium on Multiple-Valued Logic*, pp. 132-137, May 1993.

[21] H. S. Stone and A. J. Korenjak, "Canonical Form and Synthesis of Two-input Flexible Cells", *IRE Transactions on Electronic Computers*, Vol. EC-11, pp. 136-143, 1962.

[22] S. Swamy, "On Generalized Reed-Muller Expansions", *IEEE Transactions on Computers*, Vol. C-21, pp. 1008-1009, September 1972.

[23] C. C. Tsai, and M. Marek-Sadowska, "Boolean Matching Using Generalized Reed-Muller Forms", *Proceedings of the 31st ACM/IEEE Design Automation Conference*, pp. 339-344, San Diego, CA, June 1994.

[24] I. L. Zhegalkin, "Arifmetizatsiya simbolicheskoĭ logiki (Arithmetization of Symbolic Logic)", *Matematicheskiĭ Sbornik*, Vol. 35, pp. 311-373, 1928 and Vol. 36, pp. 205-338, 1929.