ON SELF-INVERSE BINARY MATRICES OVER THE BINARY GALOIS FIELD

Ali Muhammad Ali Rushdi and Fares Ahmad Muhammad Ghaleb

Department of Electrical and Computer Engineering, Faculty of Engineering,
King Abdulaziz University, P. O. Box 80204, Jeddah 21589, Saudi Arabia

ABSTRACT

An important class of square binary matrices over the simplest finite or Galois Field GF(2) is the class of involutory or self-inverse (SI) matrices. These matrices are of significant utility in prominent engineering applications such as the study of the Preparata Transformation or the analysis of synchronous Boolean Networks. Therefore, it is essential to devise appropriate methods, not only for understanding the properties of these matrices, but also for characterizing and constructing them. We survey square binary matrices of orders 1, 2 and 3 to identify primitive SI matrices among them. Larger SI matrices are constructed as (a) the direct sum, or (b) the Kronecker product, of smaller ones. Illustrative examples are given to demonstrate the construction and properties of binary SI matrices. The intersection of the sets of SI and permutation binary matrices is studied. We also study higher-order SI binary matrices and describe them via recursive relations or Kronecker products. Our work culminates in an exposition of the two most common representations of Boolean functions via two types of Boolean SI matrices. A better understanding of the properties and methods of constructing SI binary matrices over GF (2) is achieved. A clearer picture is attained about the utility of binary matrices in the representation of Boolean functions.

Keywords: Involutory or Self-Inverse Matrices, Galois Field GF (2), Direct Sums, Kronecker Products, Recursive Relations, Preparata or Reed-Müller Transformation, Synchronous Boolean Networks

1. INTRODUCTION

Binary matrices play an important role in system modeling (Warfield, 1973). A prominent class of these matrices over the simplest finite or Galois field GF (2) is the class of involutory or Self-Inverse (SI) matrices, which are matrices for which an inverse exists and is equal to the original matrix. This class of matrices is of intrinsic mathematical interest besides being of great utility in many important engineering applications. Two of the most notable such applications are.

1.1. Preparata Transformation

The Preparata (Reed-Müller) Transformation (Preparata, 1964; Saluja and Ong, 1979; Green, 1987; 1994; Stankovic *et al.*, 1996; Kim *et al.*, 1999; Quintana and Avedillo, 2001; Sasao and Butler, 2007; Rushdi and Ghaleb, 2013) for a Boolean function

$f_n(\vec{X}) = f_n(x_1, x_2, ..., x_n)$ of n variables typically takes the form Equation 1a and 1b:

$$\vec{M}_n = [S_n]\vec{L}_n, \ n \geq 0 \tag{1a}$$

$$\vec{L}_n = [S_n]\vec{M}_n \ n \geq 0 \tag{1b}$$

where, $\vec{M}_n$ and $\vec{L}_n$ are vectors of 2^n elements each and the square matrix $[S_n]$ has $2^n \times 2^n$ elements. This matrix is a self-inverse binary transformation matrix that relates the vector $\vec{M}_n$ (which is a basis of a truth-table representation for the function f_n) and the vector $\vec{L}_n$ (which is a basis for a linear (Reed-Müller) representation for the function f_n). Here, we adopt the notation (commonly employed in the literature) of using

Corresponding Author: Ali Muhammad Ali Rushdi, Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, P. O. Box 80204, Jeddah 21589, Saudi Arabia

a single subscript n to denote a $2^n \times 2^n$ square matrix. In the conventional double-script notation, the matrix $[S_n]$ would be written as $[S_{2^n \times 2^n}]$. The vectors $\vec{M}_n$ and $\vec{L}_n$ and the matrix $[S_n]$ in Equation (1) are defined herein for n = 3 as Equation 2-4:

$$\vec{M}_3 = [\bar{x}_1\bar{x}_2\bar{x}_3 \quad \bar{x}_1\bar{x}_2x_3 \quad \bar{x}_1x_2\bar{x}_3 \quad \bar{x}_1x_2x_3$$
$$x_1\bar{x}_2\bar{x}_3 \quad x_1\bar{x}_2x_3 \quad x_1x_2\bar{x}_3 \quad x_1x_2x_3]^T \tag{2}$$

$$\vec{L}_3 = [1 \quad x_3 \quad x_2 \quad x_2x_3 \quad x_1$$
$$x_1x_3 \quad x_1x_2 \quad x_1x_2x_3]^T \tag{3}$$

$$[S_3] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{4}$$

A formal definition of the general matrix $[S_n]$ and the general vectors $\vec{M}_n$ and $\vec{L}_n$ are given later.

1.2. Synchronous Boolean Networks

The $2^n \times 2^n$ transition Matrix [T] of a Synchronous Boolean Network is obtained (Cull, 1971; Rushdi and Al-Otaibi, 2007) from its $2^n \times 2^n$ Function Matrix [A] via a double matrix multiplication of the following form Equation 5a and 5b:

$$[T] = [S_n]^{-1}[A][S_n] \tag{5a}$$

$$= [S_n][A][S_n] \tag{5b}$$

in which a state matrix $[S_n]$ is used. This state matrix is exactly the same as the transformation matrix in (1) and thanks to its self-inverse property, it was possible to go from (5a) to (5b).

The topic of self-inverse binary matrices over GF (2) is interrelated with other interesting topics in mathematics including those of binary matrices over real arithmetic (Harary and Minc, 1976) and nonnegative integer matrices (Plemmons and Cline, 1972; Berman, 1974; Borobia and Moro, 1977; Lewin, 1977; Berman and Plemmons, 1979; Haynsworth and Wall, 1979; Hanson, 1985; Minc, 1988; Bellman, 1997; Laffey, 1998; Siddhartha, 2010).

This study surveys existing methods and contributes new ones for understanding the properties of binary SI matrices and for characterizing and constructing them. Subsequently, it analyzes the two most common representations of Boolean functions, namely, the truth-table representation and the linear or Reed-Müller representation. The analysis makes a clear distinction between a representation and the basis for this representation. Two different types of SI Boolean matrices (that are transposes of one another) are needed in this analysis. This analysis is supported via a mathematical proof by mathematical induction and further illustrated via a detailed example.

The remainder of this study is organized as follows. First, we present preliminary definitions and facts that are borrowed from real algebra, but still apply to GF(2) computations. These are needed herein to make the study self contained. Then, we list all square binary matrices of orders 1 and 2, characterize them and identify the primitive SI ones among them. Later, we present and prove two novel theorems for characterizing SI binary matrices in terms of direct sums and Kronecker products (tensor products). We also demonstrate these two theorems via illustrative examples and consequently list all SI binary matrices of order 3. Moreover, we study and obtain the cardinality of the set SP which is the intersection of the sets of SI binary matrices and permutation matrices. We also study higher-order SI binary matrices and describe them in terms of recursive relations and Kronecker products. Finally, we deal with the truth-table and linear representations of Boolean functions and prove that both these representations and their bases are related via two sets of SI binary matrices that are transposes of one another.

2. PRELIMINARY DEFINITIONS

2.1. A Self-Inverse (Involutory) Matrix

A regular n×n matrix [A] is self inverse (SI) iff $[A]^{-1}$ exists and equals [A], i.e., iff Equation 6:

$$[A]^{-1} = [A]: \tag{6}$$

or equivalently iff Equation 7:

$$[A]^2 = [I]. \tag{7}$$

where, $[I] = [I_{n \times n}]$ is the n×n identity matrix and here we stick to the common policy of subscripting a matrix by

its row dimension crossed by its column dimension. The determinant of a self- inverse matrix equals 1 and its even and odd powers $[A]^{2k}$ and $[A]^{2k+1}$ are $[I]$ and $[A]$, respectively.

2.2. A Periodic Matrix

A square matrix $[A]$ is periodic iff Equation 8:

$$[A]^{k+1} = [A] \tag{8}$$

where, k is a positive integer. If k is the least integer for which (8) in satisfied, $[A]$ is said to be of period k. If k = 1, then $[A]$ is idempotent.

2.3. A Nilpotent Matrix

A square matrix $[A]$ is nilpotent iff Equation 9:

$$[A]^p = [0] \tag{9}$$

where, $[0] = [0_{n \times n}]$ is the n×n null matrix and the index p is a positive integer. If p is the least integer for which (9) is satisfied, $[A]$ is said to be nilpotent of index p.

2.4. Direct Sum of Two Square Matrices

The direct sum of the two square matrices $[A_{m \times m}]$, $[B_{n \times n}]$ is the square matrix Equation 10:

$$[C_{(m+n) \times (m+n)}] = \begin{bmatrix} [A_{m \times m}] & [0_{m \times n}] \\ [0_{n \times m}] & [B_{n \times n}] \end{bmatrix} \tag{10}$$

This is a generalization of the concept of a diagonal matrix and hence is labeled by diagonal($[A]$, $[B]$), or simply diag($[A]$, $[B]$). Similarly, the direct sum of several square matrices $[X]$, $[Y]$, $[Z]$, …, $[W]$ is given by the form: diag($[X]$, $[Y]$, $[Z]$, …, $[W]$). The product of two direct sums of matrices of the same respective orders is the direct sum of the products of the respective matrices, i.e., Equation 11:

$$\text{diag}([A], [B], …, [D]) \, \text{diag}([X], [Y], …, [W])$$
$$= \text{diag}([A][X], [B][Y], …, [D][W]) \tag{11}$$

Here, the respective matrices $[A]$, $[X]$, $[A][X]$ are square matrices of the same order. In particular, the square of the direct sum of some matrices is the direct sum of their squares, namely Equation 12:

$$[\text{diag}([A],[B],[C],..,[D])]^2$$
$$= \text{diag}([A]^2,[B]^2,[C]^2,..,[D]^2) \tag{12}$$

2.5. Kronecker Product

Let $[A_{m \times n}] = \{a_{ij}\}$, $(1 \leq i \leq m, 1 \leq j \leq n)$ be a matrix of m rows and n columns and $[B_{p \times q}]$ be a matrix of p rows and q columns. The Kronecker product (KP) of $[A]$ and $[B]$, also called the tensor product, is denoted by the operator "$\otimes$" and is defined as Equation 13 (Brewer, 1978):

$$([A] \otimes [B])_{mp \times nq} =$$
$$\begin{bmatrix} a_{11}[B] & a_{12}[B] & … & a_{1n}[B] \\ a_{21}[B] & a_{22}[B] & … & a_{2n}[B] \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}[B] & a_{m2}[B] & … & a_{mn}[B] \end{bmatrix} \tag{13}$$

2.6. Permutation Matrix

The square matrix $[P_{n \times n}]$ is a permutation matrix if it results from interchanging (swapping) some rows (or columns) of the identity matrix $[I_{n \times n}]$. Alternatively, in the linear transformation $\vec{Y}_{n \times 1} = [P_{n \times n}]\vec{X}_{n \times 1}$, one has $y_{ij} = x_j$ (j =1,2,..,n) where $i_1, i_2,..,i_n$ is a permutation of 1,2,..,n. Hence, all the elements of $[P_{n \times n}]$ are 0's and 1's, with exactly a single 1 in each row and in each column, namely Equation 14:

$$[P_{n \times n}] = [\vec{\delta}_n^{i_1} \ \vec{\delta}_n^{i_2} ... \vec{\delta}_n^{i_n}] \tag{14}$$

where, $\vec{\delta}_n^{i_j}$ is a column vector of dimension n, whose elements are all 0's except the element at row i_j which is 1. The inverse $[P]^{-1}$ of a permutation matrix is its transpose $[P]^T$. There are (n)! permutation matrices $[P_{n \times n}]$ of order n.

2.7. The Finite or Galois Field GF (2)

Let F be a set of objects on which two operations: addition (+) and multiplication (represented by (*) or juxtapositioning) are defined. F is said to be a field if and only if:

- F forms a commutative group under addition. The additive identity element is labeled "0"
- F-{0} (the set F with the additive identity removed) forms a commutative group under multiplication. The multiplicative identity element is labeled "1"

Multiplication is distributed by addition Equation 15:

$$a*(b+c) = (a*b) + (a*c) \tag{15}$$

A field can also be defined as a commutative ring with identity in which every element has a multiplicative inverse. Well known examples of fields include the real field (field of real numbers) and the complex field (field of complex numbers) and fields of a finite order (number of elements) q, called the Galois fields GF(q). The simplest finite field GF(2), also called the binary field or the mod-2 field, has only two elements: the additive identity (0) and the multiplicative identity (1). The field operations of GF(2) are defined by the following axioms Equation 16a-16d:

$$0+0 = 1+1 = 0 \tag{16a}$$

$$1+0 = 0+1 = 1 \tag{16b}$$

$$0*0 = 0*1 = 1*0 = 0 \tag{16c}$$

$$1*1 = 1 \tag{16d}$$

Note that the addition (+) operation is a modulo-2 operation that resembles the exclusive-OR operation ($\oplus$) in switching algebra or bigger Boolean algebras. Any function $f(\vec{X})$ of n variables over GF(2) is a polynomial of 2^n terms (called a Taylor or a positive polarity Reed-Müller polynomial) which involves only un-complemented literals, namely Equation 17:

$$f_n\left(\vec{X}\right) = f_n\left(x_1, x_2, \cdots, x_n\right) = \vec{E}_n^T \vec{L}_n = e_0 + e_n x_n e_{(n-1)} x_{(n-1)} + e_{(n-1)n} x_{(n-1)} x_n + \cdots + e_{12\cdots n} x_1 x_2 \cdots x_n \tag{17}$$

and hence $f_n(\vec{X})$ can be expressed by a vector $\vec{E}_n$ of length 2^n called the Reed-Müller spectrum (Sasao and Butler, 2007), which is referenced in the basis vector $\vec{L}_n$.

It is also possible to express similar fixed-polarity Reed-Müller polynomials in which each variable x_i has a fixed polrity (i.e., it appears only as an uncomplemented literal x_i or a complemented one $\bar{x}_i$).

The function $f_n(\vec{X})$ might also be viewed as a logic or switching function over switching algebra (the two-valued Boolean algebra) $B_2 = \{0,1\}$ and could be expressed by another 2^n vector, namely its truth or minterm vector $\vec{F}_n = [f_0 \ f_1 \cdots f_{2^n-1}]^T$ referenced in the basis

$\vec{M}_n$ which is used in the XOR sum-of-products expansion:

$$f_n\left(\vec{X}\right) = \vec{F}_n^T \vec{M}_n = f_0 \bar{x}_1 \bar{x}_2 \cdots \bar{x}_n + f_1 \bar{x}_1 \bar{x}_2 \cdots x_n + \cdots + f_{2^n-1} x_1 x_2 \cdots x_n \tag{18}$$

The expansion in Equation (18) is a disjoint sum in which the mod-2 or XOR operator (+) might be replaced by the OR operator (V) to produce a conventional sum-of-products expression for $f_n(\vec{X})$.

3. SQUARE BINARY MATRICES OF ORDERS 1 AND 2

There are only two binary matrices of order 1 (1-square matrices), namely (a) the matrix $[N_0] = [0]$, the null matrix and the additive identity, which is nilpotent and idempotent and (b) the matrix $[U_0] = [1]$, the multiplicative identity, which is idempotent and involutory (self-inverse).

Figure 1 illustrates all 16 binary matrices of order 2 (2-square matrices), i.e., matrices of the form $\{a_{ij}\}$ where $1 \le i, j \le 2$ and $a_{ij} \in B_2 = \{0,1\}$. Among these 16 matrices, there are four Self-Inverse (SI) matrices (that we name $[S_1]$, $[R_1]$, $[U_1]$ and $[V_1]$), six matrices that are idempotent, five matrices that are nilpotent of index 2 and two matrices $[T_1]$ and $[Q_1]$ that are periodic of period 4. Note that the null matrix $[N_1]$ is both idempotent and nilpotent of index 2. In addition to the four SI matrices, the two matrices $[T_1]$ and $[Q_1]$ are also invertible and are inverses of one another. The determinant of each of the six invertible matrices is 1. Out of the four SI matrices, we label $[S_1]$, $[R_1]$ and $[V_1]$ as primitive ones, while the matrix $[U_1]$ (the 2-square identity matrix) is non-primitive since it is expressible as a direct sum Equation 19:

$$[U_1] = \text{diag}([U_0],[U_0]) \tag{19}$$

in terms of the 1-square SI matrix $[U_0]$, which is considered primitive by default. We use the abbreviation PSI to denote the set of primitive 1-square and 2-square SI matrices, i.e. Equation 20:

$$PSI = \{[U_0],[V_1],[S_1],[R_1]\} \tag{20}$$

In **Fig. 1**, we note that the matrix $[T_1] = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ is periodic of period 4, i.e., $[T_1]^4 = [T_1]$. This matrix is self-inverse in disguise, in the sense that it becomes a self-inverse matrix if we interchange its two rows, for then it becomes $[S_1]$, or if we interchange its two columns as this changes it into $[R_1]$.

$$[N_1] = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

Idempotent and nilpotent of index 2

$$\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

Idempotent

$$[U_1] = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

Self-inverse and permutation

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

Nilpotent of index 2

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

Nilpotent of index 2

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

Idempotent

$$[R_1] = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

Self-inverse

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

Idempotent

$$[V_1] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Self-inverse

$$[T_1] = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

Periodic of period 4 and invertible

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

Nilpotent of index 2

$$[Q_1] = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Periodic of period 4 and invertible

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

Nilpotent of index 2

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

Idempotent

$$[S_1] = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Self-inverse

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

Idempotent

Fig. 1. All 2×2 matrices of the form $\{a_{ij}\}$, where $1 \leq i, j \leq 2$ and $a_{ij} \in B_2 = \{0,1\}$. The six invertible matrices are highlighted in bold.

Similarly $[Q_1] = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ is periodic of period 4, i.e., $[Q_1]^4$ = $[Q_1]$ and again it is self-inverse in disguise. It is related to $[T_1]$ as $[T_1]^2 = [Q_1]$, $[Q_1] = [T_1]^2$.

4. SELF-INVERSE BINARY MATRICES

Assuming real addition, Harary and Minc (1976) state that a square binary matrix [A] is self-inverse if and only if there exists a permutation matrix [P] such that $[P][A][P]^T$ is a direct sum of 1-square matrices $[U_0]$ and 2-square matrices $[V_1]$. The result remains valid if we use 2-square matrices $[U_1]$ also. However, $[U_1]$ is not a primitive SI matrix and could be replaced in a direct-sum matrix by two $[U_0]$ matrices thanks to (19).

Inspired by the Harary-Minc result for real operations on binary matrices, we set out to obtain an analogous result for GF(2) operations on binary matrices. Unlike the Harary-Minc result, which is a bi-conditional or equivalence (IFF) statement, our result is only a conditional (IF) statement. Also, while the Harary-Minc result utilizes only two primitive SI matrices $[U_0]$ and $[V_1]$, our result involves not only these two matrices, but it uses all the four elements of the PSI set in (20). Both results rely on the introduction of the similarity transformation Equation 21:

$[P^{(j)}]$ \ $[A^{(i)}]$	$[P^{(1)}] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$[P^{(2)}] = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	$[P^{(3)}] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$	$[P^{(4)}] = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$[P^{(5)}] = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$	$[P^{(6)}] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$
$[A^{(1)}] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$	$[A^{(1)}]$	$[A^{(4)}]$	$[A^{(3)}]$	$[A^{(5)}]$	$[A^{(2)}]$	$[A^{(6)}]$
$[A^{(2)}] = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$[A^{(2)}]$	$[A^{(3)}]$	$[A^{(5)}] = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$[A^{(4)}]$	$[A^{(6)}]$	$[A^{(1)}]$
$[A^{(3)}] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$	$[A^{(3)}]$	$[A^{(2)}]$	$[A^{(1)}]$	$[A^{(6)}]$	$[A^{(4)}]$	$[A^{(5)}]$
$[A^{(4)}] = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$[A^{(4)}]$	$[A^{(1)}]$	$[A^{(6)}] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$	$[A^{(2)}]$	$[A^{(5)}]$	$[A^{(3)}]$

Fig. 2. Products of the form $[P^{(j)}] [A^{(i)}] [P^{(j)}]^T$, $1 \leq i \leq 4$, $1 \leq j \leq 6$. The ten SI 3-square binary matrices are highlighted in bold.

$$[B] = [P][A][P]^T \tag{21}$$

where [P] is a permutation matrix of the same size as the two n×n matrices [A] and [B]. Let row i of [P] have a single 1 at (i, j_i), then [C] = [P] [A], which is a row-permutation of [A], is such that row i of [C] is row j_i of [A]. Similarly, row i of $[D] = [P][C]^T$ is row j_i of $[C]^T$, which is column j_i of [C]. Hence, $[B] = [C] [P]^T = [D]^T$, which is a column-permutation of [C], is such that column i of [B] is column j_i of [C]. This means that [B] defined by (21) is obtained from [A] by permuting both its rows and columns according to the permutation dictated by the matrix [P], i. e., the one from $(1, 2, …, n)$ to $(j_1, j_2, …, j_n)$.

The similarity transformation in Equation (21) preserves the matrix property of being self inverse. We make use of the fact that the transpose of a permutation matrix equals its inverse $([P]^T = [P]^{-1})$, to rewrite (21) as Equation 22 and 23:

$$[B] = [P][A][P]^{-1} \tag{22}$$

$$[A = [P]^{-1}[B][P] \tag{23}$$

Now, if we assume that the matrix [B] is self-inverse, i.e., it satisfies (7), then the matrix [A] is also self-inverse, as shown below Equation 24:

$$\begin{aligned} [A]^2 &= [A][A] \\ &= ([P]^{-1}[B][P])([P]^{-1}[B][P]) \\ &[P]^{-1}[B]([P][P]^{-1})[B][P] \\ &= [P]^{-1}[B]^2[P] \\ &= [P]^{-1}[I][P] = [I] \end{aligned} \tag{24}$$

Similarly, if we assume that the matrix [A] is self-inverse, then the matrix [B] is also self-inverse. Now, we present our result formally as Theorem 1 below.

Theorem 1:

A square binary matrix [A] is self inverse in GF (2) if there exists a permutation matrix [P] such that [A] has a similar matrix [B], defined by (21) which is a direct sum of the form Equation 25:

$$[B] = \operatorname{diag}\left([B^{(1)}], [B^{(2)}], \cdots, [B^{(m)}]\right) \tag{25}$$

where, $[B^{(i)}] \in$ PSI for $1 \leq i \leq m$ and the set PSI is defined in (20).

Proof of Theorem 1:

First, we prove that [B] defined in (25) is a self-inverse matrix. We prove that [B] satisfies (7) by making use of (12) and the fact that the $[B^{(i)}]$'s are SI matrices as follows Equation 26:

$$[B]^2 = [\mathrm{diag}([B^{(1)}],[B^{(2)}],\cdots,[B^{(m)}])]^2$$
$$= \mathrm{diag}\left([B^{(1)}]^2,[B^{(2)}]^2,\cdots,[B^{(m)}]^2\right) \qquad (26)$$
$$= \mathrm{diag}([I],[I],\cdots,[I]) = [I]$$

Since [B] is SI, then thanks to (24), [A] is also SI. QED.

Now, we argue that the converse of Theorem 1 does not hold by finding a counter-example self-inverse [A] for which not even a single [B] can be cast in the form (25). One such counter-example is $[A] = [S_3]$ given in (4). This [A] has a row of all 1's. Any [B] produced from it via (21) is obtained through certain permutations of rows and columns. Hence, this [B] will still have a row of all 1's and consequently cannot be written as a direct sum of 1-square and 2-square matrices.

Now, we move another step further in the characterization of SI matrices using the concept of Kronecker products, in the following theorem.

Theorem 2:

If the two matrices [A] and [B] are binary SI matrices, then their Kronecker product $[C] = ([A] \otimes [B])$ is also a binary SI matrix. Conversely, if the square SI matrix [C] could be written as the Kronecker product of two matrices $[A_{m \times m}]$ and $[B_{n \times n}]$ then both [A] and [B] are SI.

Proof of Theorem 2:

The fact that $([A] \otimes [B])$ is binary when [A] and [B] are binary results immediately from (13). The inverse of a Kronecker product is the Kronecker product of the inverses given in the same order (Brewer, 1978; Rushdi and Ghaleb, 2013), i.e., Equation 27:

$$([A] \otimes [B])^{-1} = [A]^{-1} \otimes [B]^{-1} \qquad (27)$$

Since [A] and [B] are SI matrices, then by virtue of (6), we have $[A]^{-1} = [A]$ and $[B]^{-1} = [B]$ and hence (27) becomes $([A] \otimes [B])^{-1} = [A]^{-1} \otimes [B]^{-1} = [A] \otimes [B]$, which means that $([A] \otimes [B])$ is also SI.

To prove the converse part of the theorem, let the SI matrix be equal to $([A] \otimes [B])$. The fact $[C] = [C]^{-1}$ yields Equation 28:

$$[A]_{m \times m} \otimes [B]_{n \times n} = ([A]_{m \times m} \otimes [B]_{n \times n})^{-1} \qquad (28)$$

So by virtue of (28), one obtains:

$$[A]_{m \times m} \otimes [B]_{n \times n} = [A]_{m \times m}^{-1} \otimes [B]_{n \times n}^{-1}$$

Which means that $[A] = [A]^{-1}$ and $[B] = [B]^{-1}$ and hence both [A] and [B] are SI. QED.

Example 1:

According to Theorem 1, the two matrices:

$$[P^{(3)}] = \mathrm{diag}(U_0, V_1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

$$[P^{(4)}] = \mathrm{diag}(V_1, U_0) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

are both SI. Their Kronecker product:

$$[C] = [P^{(3)}] \otimes [P^{(4)}] = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

is also SI by virtue of Theorem 2.

Example 2:

Among the six 3-square permutation matrices $[P^{(i)}]$, $1 \leq i \leq 6$ shown in **Fig. 2**, there are four SP matrices $[P^{(i)}]$, $1 \leq i \leq 4$. The two permutation matrices $[P^{(5)}]$ and $[P^{(6)}]$ are not SI, as can be easily verified by finding $[P^{(5)}]^2 = [P^{(6)}] \neq [I]$ and $[P^{(6)}]^2 = [P^{(5)}] \neq [I]$.

We now utilize Theorem 1 to find binary 3-square matrices which are not permutation matrices. The SI 3-square matrices of the form (22) are given by diag ([C], (D)], where $[C] = [U_0]$ and $[D] \in \{[V_1],[S_1],[T_1],[U_1]\}$ or $[D] \in \{[V_1],[S_1],[T_1],[U_1]\}$ and $[D] = [U_0]$.

Out of these 3-square matrices, there are only 4 non-permutation matrices, namely:

$$[A^{(1)}] = \text{diag}([U_0], [S_1])$$
$$[A^{(2)}] = \text{diag}([S_1], [U_0])$$
$$[A^{(3)}] = \text{diag}([U_0], [R_1])$$
$$[A^{(4)}] = \text{diag}([R_1], [U_0])$$

So we add the 4 matrices $[A^{(i)}]$, $1 \leq i \leq 4$ to the set of SI 3-square matrices. To check whether there are other SI square matrices, we form matrix products of the form $[P^{(j)}][A^{(i)}][P^{(j)}]^T$, $1 \leq i \leq 4$, $1 \leq j \leq 6$, as shown in **Fig. 2**. We obtain only two more SI 3-square matrices, namely $[A^{(5)}]$ and $[A^{(6)}]$, shown in **Fig. 2**. Therefore, there are exactly ten SI 3-square binary matrices.

5. INTERSECTION OF SI AND PERMUTATION BINARY MATRICES

We digress a little bit to study binary matrices that belong to the set SP of matrices that are both SI binary matrices and permutation matrices. The identity matrix [I] and the three matrices in Example 1 are examples of these matrices. If exactly two rows (or two columns) in the identity matrix [I] are swapped, then the resulting matrix still belongs to SP. If two more rows (columns) that are distinct from the earlier ones are swapped, then the new matrix still belongs to SP and so on. Therefore, the cardinality of the set SP as a function of n, denoted by $N_{SP}(n)$ is given by:

$$N_{SP}(n) = 1 + \frac{1}{1!}\binom{n}{2} + \frac{1}{2!}\binom{n}{2}\binom{n-2}{2} +$$
$$\frac{1}{3!}\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2} + \cdots + \qquad (29)$$
$$\frac{1}{m!}\binom{n}{2}\binom{n-2}{2}\cdots\binom{n-2(m-1)}{2}$$

where, $n - 2(m-1) \geq 2$ or $\left(m \leq \frac{n}{2}\right)$.

Table 1. Cardinalities $N_B(n)$, $N_{SI}(n)$, $N_P(n)$ and $N_{SP}(n)$ versus n for small n

	$N_B(n) = 2^{n^2}$	$N_{SI}(n)$	$N_P(n) = n!$	$N_{PS}(n)$ Eq. (29)
1	2	1	1	1
2	16	4	2	2
3	512	10	6	4

Table 1 lists, for small n, the numbers $N_B(n)$, $N_{SI}(n)$, $N_P(n)$ and $N_{SP}(n)$ of elements in the set B of binary n-order matrices, its subsets SI and P of self-inverse and permutation matrices and the intersection SP of these two latter subsets.

6. LARGER SI BINARY MATRICES

The 2^n-square SI binary matrices $[S_n]$ and $[R_n]$ are defined recursively by Equation 30a-31b (Preparata, 1964; Saluja and Ong. 1979; Green, 1987; 1994; Stankovic *et al.*, 1996; Quintana and Avedillo, 2001; Kim *et al.*, 1999; Sasao and Butler, 2007; Rushdi and Fares, 2013; Rushdi and Al-Otaibi, 2007):

$$[S_0] = [1] \qquad (30a)$$

$$[S_n] = \begin{bmatrix} [S_{n-1}] & [S_{n-1}] \\ [0] & [S_{n-1}] \end{bmatrix} \qquad (30b)$$

$$[R_0] = [1] \qquad (31a)$$

$$[R_n] = \begin{bmatrix} [R_{n-1}] & [0] \\ [R_{n-1}] & [R_{n-1}] \end{bmatrix} \qquad (31b)$$

where [0] is the $2^{n-1} \times 2^{n-1}$ null matrix. These definitions include the 2-square SI binary matrices $[S_1]$ and $[R_1]$ in **Fig. 1** as special cases. Mathematical induction can be used (Rushdi and Al-Otaibi, 2007) to prove that $[S_n]^2 = [R_n]^2 = [I]$ and to show that $[R_n] = [S_n]^T$.

Alternatively, the higher-order SI binary matrices can be defined recursively via Kronecker products as follows Equation 32a-33b:

$$[S_1] = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad (32a)$$

$$[S_n] = [S_1] \otimes [S_{n-1}] = [S_{n-1}] \otimes [S_1] \qquad (32b)$$

$$[R_1] = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \qquad (33a)$$

$$[R_n] = [R_1] \otimes [R_{n-1}] = [R_{n-1}] \otimes [R_1] \qquad (33b)$$

It is interesting to note that while Kronecker products are generally not commutative (Rushdi and Ghaleb, 2013; Brewer, 1978), the Kronecker product of $[S_{n-1}]$ and $[S_1]$ is commutative and its transpose, the Kronecker product of $[R_{n-1}]$ and $[R_1]$ is also commutative. Equations (32b) can be restated to say that $[S_n]$ is the Kronecker product of $[S_1]$ with itself (n-1) times, i.e., $[S_n]$ is

obtained through the Kronecker multiplication of n copies of $[S_1]$. The transpose of (32b) is (33b) which says that $[R_n]$ is the Kronecker product of $[R_1]$ with itself (n-1) times.

Beside the 2^n-square SI binary matrices $[S_n]$ and $[R_n]$, which are particularly useful, as we will see in Section 7, other higher-order SI binary matrices can be constructed from various combinations of all four types of 2-square SI binary matrices. The 2-square binary matrix $[T_1]$ (respectively, $[Q_1]$), which is self-inverse in disguise, can also be Kronecker-multiplied with itself (n-1) times to produce the 2^n-square binary matrix $[T_n]$ (respectively, $[Q_n]$), which is again self-inverse in disguise. The matrix $[T_n]$ is used frequently in the semi-tensor product representation of Boolean functions (Rushdi and Ghaleb, 2013; Cheng et al., 2010).

7. BOOLEAN FUNCTION REPRESENTATIONS

We recall from (17) and (18) that a function over GF (2) or a two-valued Boolean function $f_n(\vec{X})$ can be written as Equation 34:

$$f_n(\vec{x}) = \vec{F}_n^T \overline{M}_n = \vec{E}_n^T \vec{L}_n \tag{34}$$

Here, each of the four vectors $\vec{F}_n, \overline{M}_n, \vec{E}_n$ and $\vec{L}_n$ is a vector of 2^n elements. The vectors $\overline{M}_n$ and $\vec{L}_n$ are variable basis vectors for the truth-table and linear representations of the function. Typically, different fixed versions of these vectors are used implicitly by various authors. The two vectors $\vec{F}_n$ and $\vec{E}_n$ are constant binary vectors representing the truth table and the Reed-Müller spectrum of the function. We stress here that these two vectors are meaningless unless clearly and explicitly referenced to their bases $\overline{M}_n$ and $\vec{L}_n$. Now, we formally define our basis vectors $\overline{M}_n$ and $\vec{L}_n$ recursively as Equation 35a-36b:

$$\overline{M}_0 = [1] \tag{35a}$$

$$\overline{M}_n = \overline{M}_{n-1} \otimes \begin{bmatrix} \overline{x}_n \\ x_n \end{bmatrix} \tag{35b}$$

$$\vec{L}_0 = [1] \tag{36a}$$

$$\vec{L}_n = \vec{L}_{n-1} \otimes \begin{bmatrix} 1 \\ x_n \end{bmatrix} \tag{36b}$$

Note that our expressions (2) and (3) for $\overline{M}_3$ and $\vec{L}_3$ fit into these formal definitions. Again, we stress that the definitions (35) and (36) are not unique, since other definitions are possible with different ordering or polarity of the variables (Sasao and Butler, 2007; Rushdi and Ghaleb, 2013; Rudeanu, 1974; Cheng et al., 2010). We call the Preparata Transformation in (1a) $\{T(n), n \geq 0\}$ and give a novel proof for it by mathematical induction by proving the boundary and inductive cases as follows. The boundary case T(0) states Equation 37:

$$[1] = [1] \ [1] \tag{37}$$

and is obviously and trivially true. In the inductive case $T(k) \to T(k+1)$, $k \geq 0$, we assume the truth of T(k), namely Equation 38:

$$\overline{M}_k = [S_k]\vec{L}_k, \ k \geq 0 \tag{38}$$

and utilize this assumption in proving T(k+1), which is Equation 39:

$$\overline{M}_{k+1} = [S_{k+1}]\vec{L}_{k+1}, \ k \geq 0 \tag{39}$$

We can reduce (39) by virtue of (35b), (32b) and (36b) to Equation 40:

$$\begin{aligned} \left(\overline{M}_k \otimes \begin{bmatrix} \overline{x}_{k+1} \\ x_{k+1} \end{bmatrix} \right) &= ([S_k] \otimes [S_1]) \\ \left(\vec{L}_k \otimes \begin{bmatrix} 1 \\ x_{k+1} \end{bmatrix} \right), & k \geq 0 \end{aligned} \tag{40}$$

A well known property of Kronecker products (Brewer, 1978) is Equation 41:

$$([A] \otimes [B]) \ ([D] \otimes [G]) = [A][D] \otimes [B][G] \tag{41}$$

ascertains the truth of (40) thanks to (38) and the fact that Equation 42:

$$\begin{bmatrix} \overline{x}_{k+1} \\ x_{k+1} \end{bmatrix} = [S_1] \begin{bmatrix} 1 \\ x_{k+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ x_{k+1} \end{bmatrix} \tag{42}$$

which is true since $\overline{x}_{k+1} = 1 + x_{k+1}$. Substitution of (1) into (34) produces Equation 43:

$$\vec{F}_n^T [S_n]\vec{L}_n = \vec{E}_n^T \vec{L}_n \tag{43}$$

which is an identity for all $\vec{L}_n$ requiring:

$$\vec{F}_n^T[S_n] = \vec{E}_n^T,$$

or equivalently Equation 44a and 44b:

$$\vec{E}_n = [S_n]^T \vec{F}_n = [R_n]\vec{F}_n \qquad (44a)$$

$$\vec{F}_n = [R_n]\vec{E}_n \qquad (44b)$$

While the basis vectors $\overline{M}_n$ and $\vec{L}_n$ are related via the SI matrix $[S_n]$, the value vectors $\vec{F}_n$ and $\overline{E}_n$ are related by its transpose SI matrix $[R_n]$.

Example 3:

Consider the 3-variable Boolean function Equation 45a-45d:

$$f_3(x_1, x_2, x_3) = \overline{x}_1 \overline{x}_2 \vee x_2 \overline{x}_3 \vee \overline{x}_2 x_3 \qquad (45a)$$

$$= \overline{x}_1 \overline{x}_2 \overline{x}_3 \vee \overline{x}_1 \overline{x}_2 x_3 \vee \overline{x}_1 x_2 \overline{x}_3 \vee x_1 \overline{x}_2 x_3 \vee \qquad (45b)$$
$$x_1 x_2 \overline{x}_3$$

$$= \overline{x}_1 \overline{x}_2 \overline{x}_3 + \overline{x}_1 \overline{x}_2 x_3 + \overline{x}_1 x_2 \overline{x}_3 + x_1 \overline{x}_2 x_3 + x_1 x_2 \overline{x}_3 \qquad (45c)$$

$$= 1 + x_2 x_3 + x_1 + x_1 x_3 + x_1 x_2 + x_1 x_2 + x_1 x_2 x_3 \qquad (45d)$$

The truth table and Reed-Müller Spectrum of this function are Equation 46a and 46b:

$$\vec{F}_3 = [1\ 1\ 1\ 0\ 0\ 1\ 1\ 0]^T \qquad (46a)$$

$$\vec{E}_3 = [1\ 0\ 0\ 1\ 1\ 1\ 1\ 1]^T \qquad (46b)$$

and can be used together with (2), (3) and (34) to produce its algebraic expressions (45c) and (45d). These two vectors also satisfy (44).

8. CONCLUSION

This study compiled many pieces of information about binary self-inverse matrices over GF(2). The study added also some novel contributions about the characterization and construction of these matrices via the concepts of direct sums and Kronecker products. Self-inverse binary matrices of order 1, 2 and 3 are listed, while those of order 2^n are described in terms of recursive relations and Kronecker products. The utility of binary SI matrices in relating the two most common representations of Boolean functions is also investigated.

10. REFERENCES

Bellman, R., 1997. Introduction to Matrix Analysis. 1st Edn., SIAM, Philadelphia, ISBN-10: 0898713994, pp: 403.

Berman, A. and R.J. Plemmons, 1979. Nonnegative Matrices in the Mathematical Sciences. 1st Edn., Academic Press, New York, ISBN-10: 0120922509, pp: 316.

Berman, A., 1974. Nonnegative matrices which are equal to their generalized inverse. Linear Algebra Applic., 9: 261-265. DOI: 10.1016/0024-3795(74)90042-1

Borobia, A. and J. Moro, 1977. On the nonnegative matrices similar to positive matrices. Linear Algebra Applic., 266: 365-379. DOI: 10.1016/S0024-3795(97)00362-5

Brewer, J., 1978. Kronecker products and matrix calculus in system theory. IEEE Trans. Circ. Syst., CAS-25, 9: 772-781. DOI: 10.1109/TCS.1978.1084534

Cheng, D., H. Qi and Z. Li, 2010, Analysis and Control of Boolean Networks: A Semi-Tensor Product Approach. 1st Edn., Springer, London, ISBN-10: 0857290975, pp: 488.

Cull, P., 1971. Linear analysis of switching nets. Kybernetik, 8: 31-39. DOI: 10.1007/BF00270831

Green, D.H., 1987. Reed-Müller expansions of incompletely specified functions. IEE Proc. E Comput. Digital Techniques, 134: 228-236. DOI: 10.1049/ip-e.1987.0038

Green, D.H., 1994. Dual forms of Reed-Müller expansions. IEE Proc. Comput. Digital Techniques, 141: 184-192. DOI: 10.1049/ip-cdt:19941097

Hanson, R., 1985. Self-inverse integer matrices. College Mathem. J., 16: 190-198. DOI: 10.2307/2686570

Harary, F. and H. Minc, 1976. Which nonnegative matrices are self-inverse. Mathem. Mag., 49: 91-92. DOI: 10.2307/2689442

Haynsworth, E. and J.R. Wall, 1979. Group inverses of certain nonnegative matrices. Linear Algebra Applic., 25: 271-288. DOI: 10.1016/0024-3795(79)90023-5

Kim, S.W., B.S. Shin, J.H. Kim and H.S. Kim, 1999. The method to generate generalized Reed-Muller coefficients over GF(2) using decision diagram. Proceedings of the IEEE Region 10 Conference, (RN '99), IEEE Xplore Press, Cheju Island, pp: 379-382. DOI: 10.1109/TENCON.1999.818430

Laffey, T.J., 1998. Extreme nonnegative matrices. Linear Algebra Applic., 275: 349-357. DOI: 10.1016/S0024-3795(97)10059-3

Lewin, M., 1977. Nonnegative matrices generating a finite cyclic group. Linear Multilinear Algebra, 5: 91-94. DOI: 10.1080/03081087708817182

Minc, H., 1988. Nonnegative Matrices. 1st Edn., Wiley, New York, ISBN-10: 0471839663, pp: 206.

Plemmons, R.J. and R.E. Cline, 1972. The generalized inverse of a nonnegative matrix. Proc. Am. Mathem. Soc., 31: 46-50. DOI: 10.1090/S0002-9939-1972-0285541-5

Preparata, F.P., 1964. State-logic relations for autonomous sequential networks. IEEE Trans. Elect. Comput., 13: 542-548. DOI: 10.1109/PGEC.1964.263725

Quintana, J.M. and M.J. Avedillo, 2001. Reed-Muller descriptions of symmetric functions. Proceedings of the 2001 IEEE International Symposium on Circuits and Systems, May 6-9, IEEE Xplore Press, Sydney, NSW, pp: 682-685. DOI: 10.1109/ISCAS.2001.922329

Rudeanu, S., 1974. Boolean Functions and Equations. 1st Edn., North-Holland, Amsterdam, ISBN-10: 0720420822, pp: 442.

Rushdi, A.M. and F.A. Ghaleb, 2013. A tutorial exposition of semi-tensor products of matrices with a stress on their representation of Boolean functions.

Rushdi, A.M. and S.O. Al-Otaibi, 2007. On the linear analysis of synchronous switching networks. King Abdulaziz Univ. J. Eng. Sci., 18: 47-78. DOI: 10.4197/Eng.18-2.4

Saluja, K.K. and E.H. Ong, 1979. Minimization of Reed-Muller canonic expansion. IEEE Trans. Comput., 28: 535-537. DOI: 10.1109/TC.1979.1675401

Sasao, T. and J.T. Butler, 2007. The eigenfunction of the Reed-Muller transformation. Proceedings of the Workshop on Applications of the Reed Muller Expansion in Circuit Design and Representation and Methodology of Future Computing Technology. (RM' 07), pp: 31-38.

Siddhartha, S., 2010. A note on the resolvent of a nonnegative matrix and its applications. Linear Algebra Applic., 432: 2524-2528. DOI: 10.1016/j.laa.2009.11.004

Stankovic, R.S., T. Sasao and C. Moraga, 1996. Spectral Transform Decision Diagram. In: Representations of Discrete Functions, Sasao, T. and M. Fujita (Eds.), Kluwer Academic Publishers, Norwell, MA, USA., ISBN-10: 0792397207, pp: 55-92.

Warfield, J.N., 1973. Binary matrices in system modeling. IEEE Trans. Syst. Man Cybernetics, SMC, 3: 441-449. DOI: 10.1109/TSMC.1973.4309270