Constructions of Orthomorphisms of $\mathbb{Z}_2^n$

Solomon W. Golomb[1], Guang Gong[2], Lothrop Mittenthal[3]

[1] Communication Sciences Institute
University of Southern California
Electrical Engineering-Systems, EEB#500
Los Angeles, CA 90089-2565
milly@usc.edu
[2] Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
ggong@cacr.math.uwaterloo.ca
[3] Teledyne Electronic Technologies
649 Lawrence Dr.
Newbury Park, CA 91320

Abstract. A permutation σ on $\mathbb{Z}_2^n$, the linear space consisting of n-bit numbers, is an orthormorphism iff the mapping is also a permutation on $\mathbb{Z}_2^n$, as x takes all values in $\mathbb{Z}_2^n$. It is a linear orthomorphism iff σ is a linear transformation on $\mathbb{Z}_2^n$. This paper contains two parts. In the first part, first, in terms of the isomorphism between the linear space $\mathbb{Z}_2^n$ and the finite field $GF(2^n)$, an algebraic method of constructing linear orthomorphisms with the maximal cycles is provided. Then two algorithms to implement this type of linear orthomorphisms are presented. In the second part, by using this type of linear orthomorphisms, a special type of Latin squares, called *Bar Sinister Latin squares* are constructed and nonlinear orthomporphisms, which can be represented as transversals, are constructed. Some discussion on nonlinearity of this type of nonlinear orthomorphisms and a construction of arbitarty nonlinear orthormorphisms are included in this part. A motivation is to use such mappings for encryption of digital data.

Key Words: Linear/nonlinear orthomorphism, Latin square, algorithm, finite field.

1 Introduction

Encryption and decryption algorithms play an important role in the information age. Mathematically, to design these kinds of algorithms is to construct permutations of a finite set with specific properties. In [5] [6], Mittenthal discussed this concept by using the orthomorphisms of $\mathbb{Z}_2^n$ to design the cryptographic algorithms. This paper will discuss how to construct and implement the linear orthomorphisms with the maximal cycles and how to construct nonlinear orthomorphisms from such kind of linear orthomorphisms. The paper contains two parts. In the first part, in terms of the isomorphism between the linear space $\mathbb{Z}_2^n$ and the finite field $GF(2^n)$ [4] [9], we provide an algebraic method of constructing linear orthomorphisms with the maximal cycles. Then we present two algorithms to implement this type of linear orthomorphisms. In the second part, by using this type of linear orthomorphisms, we construct a special type of Latin squares, called *Bar Sinister Latin squares.* Finally, nonlinear orthomporphisms, which can be represented as transversals, are constructed in terms of the Bar Sinister Latin squares.

This paper is organized as follows. In Section 2, we will give an algebraic method for constructing linear orthomorphisms. In Sections 3, we will give two algorithms to implement this type of linear orthomorphisms of $\mathbb{Z}_2^n$. One is to use matrix transformation where a basis of $GF(2^n)/GF(2)$ is fixed. The other is to use the characteristic m-sequences of period $2^n - 1$ where altering bases of $GF(2^n)/GF(2)$ is possible. In Sections 4 and 5, in terms of this type of linear orthomorphisms, we construct a special type of Latin squares, called the *Bar Sinister Latin squares* and show a method to construct nonlinear orthomorphisms from the Bar Sinister Latin squares. Some discussions for constructing arbitrary nonlinear orthomorphisms are provided in Section 6.

2 A Class of Linear Orthmorphisms of $\mathbb{Z}_2^n$

We will specify the following notation used through out this paper.

- $\mathbb{F}_q = GF(q)$,
- $\mathbb{Z}_2^n = \{(x_0, x_1, \cdots, x_{n-1}) | x_i \in F_2, 0 \leq i < n\}$, and
- $p = 2^n - 1$ and $q = 2^n$.

Definition 1. *A permutation σ on $\mathbb{Z}_2^n$ is an orthormorphism iff the mapping $x \mapsto x + \sigma(x)$ is also a permutation on $\mathbb{Z}_2^n$, as x takes all values in $\mathbb{Z}_2^n$. It is a linear orthomorphism iff σ is a linear transformation on $\mathbb{Z}_2^n$.*

Define $S(x) = x + \sigma(x)$. Then $S(x)$ is a permutation of $\mathbb{Z}_2^n$ if σ is an orthomorphism of $\mathbb{Z}_2^n$. Therefore S is a linear permutation of if and only if σ is a linear permutation of $\mathbb{Z}_2^n$.

2.1 An Isomorphism between $\mathbb{Z}_2^n$ and $\mathbb{F}_{2^n}$

Let $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ be a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2 (= \mathbb{Z}_2)$. Let $x = (x_0, x_1, \cdots, x_{n-1}) \in \mathbb{Z}_2^n$, then the following map

$$x = (x_0, x_1, \cdots, x_{n-1}) \mapsto x_0\alpha_0 + x_1\alpha_1 + \cdots + x_{n-1}\alpha_{n-1}$$

is an isomorphism between $\mathbb{Z}_2^n$ and $\mathbb{F}_{2^n}$ when both of them are regarded as vector spaces over $\mathbb{F}_2 = \mathbb{Z}_2$. Note that there is a one-to-one correspondence between $\mathbb{Z}_2^n$ and $\mathbb{Z}_{2^n}$ via

$$x = (x_0, x_1, \cdots, x_{n-1}) \mapsto x_0 + x_1 2 + x_2 2^2 + \cdots + x_{n-1} 2^{n-1} \in \mathbb{Z}_{2^n}.$$

Thus in this paper, we use the same symbol x for $x \in \mathbb{F}_{2^n}$, $\mathbb{Z}_2^n$ or $x \in \mathbb{Z}_{2^n}$. So, the exact meaning of x depends on the context.

Let $\{\eta_0, \eta_1, \cdots, \eta_{n-1}\}$ be the dual basis of $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$. Then

$$(x_0, x_1, \cdots, x_{n-1}) = (Tr(\eta_0 x), Tr(\eta_1 x), \cdots, Tr(\eta_{n-1} x)), \forall x \in \mathbb{F}_{2^n}$$

where $Tr(x) = x + x^2 + \cdots + x^{2^{n-1}}$ is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

2.2 An Algebraic Construction

Proposition 1. *Let α be a primitive element in $\mathbb{F}_{2^n}$. Let s be a fixed positive integer in the range of $1 \leq s < p$. Let*

$$\sigma(x) = \alpha^s x, x \in \mathbb{F}_{2^n}.$$

Then $\sigma(x)$ is a linear orthomorphism of $\mathbb{F}_{2^n}$. Moreover, $\sigma(x)$ has a maximal cycle when it is regarded as a permutation.

Proof. Let α be a primitive element of $\mathbb{F}_{2^n}$. Then we can write $\mathbb{F}_{2^n}^*$, the multiplication group of $\mathbb{F}_{2^n}^*$, as follows

$$\mathbb{F}_{2^n}^* = \{\alpha^i | 0 \leq i < p\}.$$

For any $0 \leq i \neq j < p$, there is an integer k: $0 \leq k < p$ such that

$$\alpha^i + \alpha^j = \alpha^k.$$

Therefore, there exists τ: $0 \leq \tau < p$ such that $1 + \alpha^s = \alpha^\tau$. Consequently,

$$S(x) = x + \sigma(x) = (1 + \alpha^s)x = \alpha^\tau x$$

which is a linear permutation of $\mathbb{F}_{2^n}$. Note that $\sigma(\alpha^i) = \sigma^{s+i}, 0 \leq i < p$. This shows that $\sigma(x)$ has the maximal cycle when it is regarded as a permutation.

□

In the following, we will assume that $R(x) = \alpha x$. Then $\sigma(x) = R^s(x) = \alpha^s x$. Let $S(x) = x + R^s(x)$. Then $S(x)$ can be represented as a number in Z_2^n for any $x \in \mathbb{F}_{2^n}$ as follows

$$S(x) = (Tr(\eta_0 \alpha^\tau x), Tr(\eta_1 \alpha^\tau x), \cdots, Tr(\eta_{n-1} \alpha^\tau x)) \in Z_2^n \quad (1)$$

where $1 + \alpha^s = \alpha^\tau$. So the *implementation problem* is how to compute $S(x)$ from a given integer in Z_2^n using the above formula (1).

3 Implemention of Linear Orthomorphisms

In this section, we will give two algorithms to implement $S(x)$ represented by (1).

3.1 Implementation in Terms of Matrix Transformations

Let $(a_0, a_1, \cdots, a_s)^T$ be the transpose of the vector $(a_0, a_1, \cdots, a_s)$.

Algorithm 1: Procedure for Implementation of $S(x) = x + R^s(x)$ on Z_2^n.
Input: $m = (m_0, m_1, \cdots, m_{n-1}) \in Z_2^n$.
Output: $S(m) \in Z_2^n$.

1. Generate a finite field $\mathbb{F}_{2^n}$ and choose α is a primitive element of $\mathbb{F}_{2^n}$.
2. Compute $\tau : 0 < \tau < N$ such that $1 + \alpha^s = \alpha^\tau$. (I.e., compute the discrete logarithm of $\tau = log_\alpha^\beta$ where $\beta = 1 + \alpha^s$.)
3. Choose a basis of $\mathbb{F}_{2^n}/\mathbb{F}_2 : \{1, \alpha, \cdots, \alpha^{n-1}\}$.
4. Pack the matrix form $B = (b_{ij})_{n\times n}$ of $S(x)$ by computing
$$(\alpha^\tau, \alpha^{\tau+1}, \cdots, \alpha^{\tau+n-1})^T = B(1, \alpha, \cdots, \alpha^{n-1})^T.$$
5. Evaluate mB which is $S(m)$.

Note. This algorithm can only easily change the value of s, but it can not easily change the basis involved here.

Example 1. Let $n = 4$, $s = 1$, and α be a primitive element of $\mathbb{F}_{2^4}$ with $f(\alpha) = 0$ where $f(x) = x^4 + x + 1$.

Input: $m = 12 = (0, 0, 1, 1) \in \mathbb{Z}_2^4$.
Output: $S(12) \in Z_2^4$.

1. Generate $\mathbb{F}_{2^4}$ in Table 1.
2. From Table 1, $1 + \alpha = \alpha^4 \Longrightarrow \tau = 4$.
3. Choose the basis of $\mathbb{F}_{2^4}/\mathbb{F}_2$: $\{1, \alpha, \alpha^2, \alpha^3\}$.
4. Pack the matrix form of $S(x)$ by computing $(\alpha^4, \alpha^5, \alpha^6, \alpha^7)^T = B(1, \alpha, \alpha^2, \alpha^3)^T$. So
$$B = \begin{pmatrix} 1\,1\,0\,0 \\ 0\,1\,1\,0 \\ 0\,0\,1\,1 \\ 1\,1\,0\,1 \end{pmatrix}.$$
5. Compute
$$mB = (0, 0, 1, 1)B = (1, 1, 1, 0) = 7$$
which gives $S(m) = 7$.

3.2 Implementation in Terms of M-sequences

Let $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + 1$ be a primitive polynomial of degree n over $\mathbb{F}_2$ and α be a root of $f(x)$ in the extension $\mathbb{F}_{2^n}$. A sequence $A = \{a_i\}$ whose elements are given by

$$a_i = Tr(\beta\alpha^i), \beta \in \mathbb{F}_{2^n}, i = 0, 1, \cdots$$

Table 1. $\mathbb{F}_{2^4}$ Generated by $\alpha^4 + \alpha + 1 = 0$

Index $i = log_\alpha^\beta$	1	α	α^2	α^3
0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	1	0	0
5	0	1	1	0
6	0	0	1	1
7	1	1	0	1
8	1	0	1	0
9	0	1	0	1
10	1	1	1	0
11	0	1	1	1
12	1	1	1	1
13	1	0	1	1
14	1	0	0	1

is an m-sequence of degree n. I.e., A satisfies that following recursive relation

$$a_{i+n} = \sum_{k=0}^{n-1} c_k a_{i+k}, i \geq 0.$$

If $\beta = 1$, then A is called *the characteristic m-sequence.*

Algorithm 2: Procedure for Implementation of $S(x) = x + R^s(x)$ on Z_2^n.
Input: $m = m_0 + m_1 2 + \cdots + m_{n-1} 2^{n-1}$, an integer in $\mathbb{Z}_q$, i.e., $0 \leq m < q$.
Output: $S(m)$, an integer in $\mathbb{Z}_q$.

1. Generate a finite field $\mathbb{F}_q$ be a primitive polynomial $f(x)$ with $f(\alpha) = 0$.
2. Compute $\tau : 0 < \tau < p$ such that $1 + \alpha^s = \alpha^\tau$.
3. Choose $t = (t_0, t_1, \cdots, t_{n-1}) \in \mathbb{Z}_p^n$ so that $\{\alpha^{t_0}, \alpha^{t_1}, \cdots, \alpha^{t_{n-1}}\}$ is a basis of $\mathbb{F}_{2^n}/\mathbb{F}_2$.
4. Generate the characteristic m-sequence $A = \{a_i\}$ by $f(x)$.
5. Pack the one-to-one correspondence table from $\mathbb{Z}_p$ to $\mathbb{Z}_q$:
$$\begin{pmatrix} 0 & 1 & \cdots p-1 \\ r_0 & r_1 & \cdots r_{p-1} \end{pmatrix}$$
where $r_i = a_{i+t_0} + a_{i+t_1} 2 + \cdots + a_{i+t_{n-1}} 2^{n-1} \in Z_q, i = 0, 1, \cdots, p-1$.
6. Look up the table for finding an i such that $m = r_i$.
7. Output $S(m) = r_{i+\tau}$.

Example 2. With the same notation as Example 1.

1. See Table 1.

2. $\tau = 4$ from Example 1.
3. Choose $t = (t_0, t_1, t_2, t_3) = (0, 1, 2, 3)$. It is clear that $\{1, \alpha, \alpha^2, \alpha^3\}$ is a basis of $\mathbb{F}_{2^4}/\mathbb{F}_2$.
4. From Table 1, we have $Tr(1) = 0, Tr(\alpha) = 0, Tr(\alpha^2) = 0$, and $Tr(\alpha^3) = 1$. Therefore the characteristic m-sequence generated by $f(x) = x^4 + x + 1$ is as follows.
$$A = 000100110101111.$$
5. Compute $r_i = a_i + a_{i+1}2 + a_{i+2}2^2 + a_{i+3}2^3$, $0 \leq i < 15$. Then We have the following 1-1 correspondence from $\mathbb{Z}_{15}$ to $\mathbb{Z}_{16}$.

Table 2

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
8	4	2	9	12	6	11	5	10	13	14	15	7	3	1

6. Look up Table 2, we have $m = 12 = r_4 \Longrightarrow i = 4$.
7. Output $S(m) = S(12) = r_{4+4} = r_8 = 10$.

Remark 1. Algorithm 2 can generate all linear orthomorphisms when different bases are plugged in at step 3. Since different bases may result in the same linear orthomorphisms. This procedure can not distinguish them. A solution for this problem and the number of different linear orthomorphisms on $\mathbb{Z}_2^n$ are given by Dai, Golomb and Gong in a separate paper [1].

Remark 2. In applications of encryption, the steps 1-4 of Algorithm 1 and the steps 1-5 of ALgorithm 2 can be put into pre-computing units. The parameter s should be kept as secret key and used for a short time when the orthomorphism is used as an enciphering function. If s is exposed, the system will be broken. In fact, as an attacker has a cipher $c = S(m)$ where m is a message, and if the attacker knows s, then he can obtain by using the same primitive polynomial for generating the finite field. From $c = \alpha^k$ the attacker can compute the message m by $m = \alpha^{k-\tau}$. Notice that the process for computing cipher involves solving a discrete logarithm. So, the parameter n can not be large. Therefore it is difficult to keep the generating polynomial $f(x)$ as a secret key.

4 Constructing Nonlinear Orthomorphisms

For many applications, linear mappings including orthomorphisms, are unsatisfactory. To construct nonlinear orthomorphisms directly requires discarding some of the tools that were so useful in the linear case.

We list the elements of $\mathbb{Z}_2^n$ as

$$Z_2^n = \{0, x_i, i = 1, 2, \cdots, p\}$$

Any orthomorphisms on $\mathbb{Z}_2^n$ can be expressed as a set of equations and without loss of generality, the necessary single fixed point can be 0. The equations are of the form:

$$x_{k-1} + x_k = z_k$$

except for $0+0=0$. (Note that 0 is zero in $\mathbb{F}_{2^n}$ or in $\mathbb{Z}_{2^n}$ or a vector in $\mathbb{Z}_2^n$ depends on the context.)

A non trivial pair of equations when added component-wise will not be another equation in the same orthomorphism unless the orthormorphism is linear or linear when restricted to some subgroup of the domain. However, the nonlinear orthomorphism can be expressed as an ordered set of equations:

$$\begin{array}{cllll}
RowNumber & L & M & R \\
0 & 0 & +0 & =0 \\
1 & x_p & +x_1 & =z_1 \\
2 & x_1 & +x_2 & =z_2 \\
\vdots & & & \\
k & x_{k-1} & +x_k & =z_k \\
\vdots & & & \\
p & x_{p-1} & +x_p & =z_p
\end{array}$$

Figure 1

An orthomorphic permutation is one in which the pairs of successive numbers in the permutation have distinct sums.

The left (L) and middle (M) columns represent an orthomorphic permutation but the right (R) column in general is not an orthomorphic permutation. In most cases there are also some cycles. In what follows, we show a method of deriving nonlinear orthomorphisms as illustrated in Figure 1, from a linear orthomorphism $S(x)=x+R^s(x)$ which is defined in (1) in Section 2, as illustrated in Figure 2. As before, a linear orthomorphism on $\mathbb{Z}_2^n$ can be written as:

$$\begin{array}{cllll}
RowNumber & L & M & R \\
0 & 0 & +0 & =0 \\
1 & x_p & +x_1 & =x_{1-\tau} \\
2 & x_1 & +x_2 & =x_{2-\tau} \\
\vdots & & & \\
k & x_{k-1} & +x_k & =x_{k-\tau} \\
\vdots & & & \\
p & x_{p-1} & +x_p & =x_{p-\tau}
\end{array}$$

Figure 2

For our purposes, namely the generation of nonlinear orthomorphisms, it is sufficient that the linear orthomorphism be maximal. It will have the single fixed point 0, and a cycle of length p as illustrated in Figure 2. These linear orthomorphisms can be generated by the methods presented in Section 2. Figure 2 represents a family of linear orthomorphisms corresponding to a particular primitive polynomial over $\mathbb{F}_2$ of degree n. Any complete linearly independent set in $\mathbb{Z}_2^n$ can be used to generate a particular orthomorphism in that family. The shift τ is uniquely associated with the primitive polynomial.

For simplicity of notation, we can use $x_{k-1} = L_k$ in the left column; $x_k = M_k$ in the middle column; and $x_{k-\tau} = R_k$ in the right right column. In that case, Fig. 2 can be rewritten as:

$$\begin{array}{cl}
RowNumber & L \quad\;\; M \quad\;\; R \\
0 & \underline{0} \;\; + \underline{0} \quad = \underline{0} \\
1 & L_1 + M_1 = R_1 \\
2 & L_2 + M_2 = R_2 \\
\vdots & \\
k & L_k + M_k = R_k \\
\vdots & \\
p & L_p + M_p = R_p
\end{array}$$

Figure 3

If columns L and M can be permuted, leaving column R fixed, and maintaining equality, a new and generally nonlinear orthomorphism will have been generated. This means finding a consistent set of equations:

$$L_i + M_j = R_k \tag{2}$$

where the indices refer to the row numbers in Fig. 3. The index k is a function of indices i and j, so that one can write:

$$k_{ij} = k(i, j).$$

From Fig. 2, $L_i + M_{i-1} = R_0 = 0$ for all i so that $k(i, i-1) = 0$. $L_i + M_i = R_i$ so that $k(i, i) = i$. $L_0 + M_i = R_{i+\tau}$, from Fig. 2, where τ is the shift between the middle and right columns determined by the generating function for the linear orthomorphism. Thus, $k(0, i) = i + \tau$ and $k(i, 0) = i + \tau - 1$. The possible combinations in equation (2) can be expressed in Table 3.

Each row and each column in Table 3 contains each index in the set $\mathbb{Z}_{2^n}$ exactly once. An orthormorphism will be generated by selecting one entry from each rwo and column without duplicateds. That is, by selecting a transversal. It is known that for a group which has an orthomorphism, its multiplication table (Cayley table) has a transversal. (See reference [2]). However, Table 3, while related to $\mathbb{Z}_2^n$, is not its Cayley Table but a table of indicies for a specific maximal linear orthomorphism. The principal diagonal which is a transversal, represents that linear orthomorphism. Every other othormorphism can be represented by a transversal in this table. As can be seen form the numerical examples below, the table actually represents the muptiplication table of a quasi-group as the operation represented is non-associative.

The other main diagonal running from lower left to upper right, is not a transversal. But it turns out, as shown below, to be of particular interest. This is known as the Bar Sinister in heraldry, and so, for want of standard terminology, Table 3 is referred to as a *Bar Sinister table.*

Table 3: A Bar Sinister Table Defined by A Family of Maximal Linear Orthomorphisms on $\mathbb{Z}_2^n$

		Index j of M_j, the Middle Column Entry						
		0	1	2	$\cdots$	j	$\cdots$	p
Index i of L_i, the Left Column Entry	0	k_{00}	k_{01}	k_{02}	$\cdots$	k_{0j}	$\cdots$	k_{0p}
	1	k_{10}	k_{11}	k_{12}	$\cdots$	k_{1j}	$\cdots$	k_{1p}
	$\vdots$							
	i	k_{i0}	k_{i1}	k_{i2}	$\cdots$	k_{ij}	$\cdots$	k_{ip}
	$\vdots$							
	p	k_{p0}	k_{p1}	k_{p2}	$\cdots$	k_{pj}	$\cdots$	k_{pp}

The entries $k_{ij} = k(i, j)$ are the indices of the entries R_k in the right column in the linear orthomorphism in Figures 2 and 3.

As mentioned above, if one chooses the principal diagonal, from upper left to lower right, the original linear orthomorphism is obtained. If one chooses $k(0,0)$ and follows with the sub-diagonal from upper left to lower right, $k(i, i-1)$ for $i \geq 2$, it is easy to see that the trivial mapping onto 0 is obtained. This path is not a transversal. As noted above

$$x_{i-1} = L_i \text{ and } x_j = M_j \Longrightarrow x_{i-1} + x_j = x_{k-\tau}$$

This equation corresponds to some power s of the basic orthomorphic permutation where $i - 1 = j - s$ and $k - \tau = j - \tau(s)$. Thus, $s = j - i + 1$ and $k = j + \tau - \tau(s) = j + \tau - \tau(j - i + 1)$. If $\tau(s)$ has been tabulated as a function of s, Table I could be derived this way. Now again start with k(0, 0) and consider any other such diagonal from upper left to lower right, that is, $k(i, i+a)$ for all i and some fixed a where $i > 0$ and $a > 0$. Then $M_{i+a} = x_{i+a}$ and $L_i = x_{i-1} = x_{i+a-(a+1)}$. Let $s = a + 1$ and $L_i = x_{i+a-s}$. Then

$$x_{i+a-s} + x_{i+a} = x_{i+a-\tau(s)} = x_{i+a-\tau(s)+\tau-\tau} = R_{i+a-\tau(s)+\tau}$$

and

$$k(i, i+a) = i + a - \tau(s) + \tau.$$

Thus, the orthomorphism which is generated is the $(a+1)$st power of the original, and is linear again. This is a transversal. In general, we have have the following procedure to finding a nonlinear orthomorphisms from the Bar Sinister Latin square.

Procedure for Finding Nonlinear Orthomorphisms from the Bar Sinister Latin square:

1. Choose a diagonal from upper right to lower right and start with some pair

$$L_a + M_b = R_k \text{ with } k = k(a, b).$$

For $i = a$ and $j = b$ the entry $k(a, b)$ is in the intersection of row a and column b, which corresponds to the equation

$$x_{a-1} + x_b = x_{k-\tau}.$$

So, $k = k(a, b) = b + \tau - \tau(s) = b + \tau(1) - \tau(s)$ and $b - s = a - 1$, so $s = b - a + 1$.
2. Proceeding down the diagonal (bar sinister path), each successive entry is $k(a + i, b - i)$ corresponding to: $x_{a+i-1} + x_{b-i} = x_{b-i-\tau(s)}$. Thus $a + i - 1 = b - i - s$ and $s = b - a - 2i + 1$.
3. Proceeding downward from right to left with successive values:

$$k(a + i, b - i) = b + \tau - \tau(s) - 2i$$

and equations of the form

$$x_{a+i-1} + x_{b-i} = x_{b-i-\tau(s)}$$

where

$$s = b - i - (a + i - 1) \equiv b - a + 1 - 2i \pmod p$$

and the successive values of the index i give equations from different powers of the basic linear orthomorphism.
4. Proceeding along such diagonals from upper right to lower left will eventually lead to a repeated value of $k(i, j)$. This collision will occur when

$$k(a + i, b - i) = k(a, b) \text{ or}$$
$$b + \tau - \tau(b - a + 1) = b - i + \tau - \tau(b - a + 1 - 2i)$$

so that $i = \tau(b-a+1) - \tau(b-a+1-2i)$. One skips over the repeated value or goes to a parallel diagonal.

This process is completed when a full transversal is found. The latter stages this process can be expedited to minimize backtracking by estimating which one of the remaining choices for the next step in the transversal will maximize the probability of success.

5 Constructing the Bar Sinister Latin Square

Because the table will have 2^{2n} entries, it would seem to be a formidable task to contruct one. However, there are some simplifications. The top row and the left column are automatically generated by not needed if 0 is to be maintained as the fixed point. The main diagonal, from upper left to bottom right, and the subdiagonal are also fixed. $k(i + 1, j + 1) = k(i, j) + 1$. So, it is necessary only to determine $2^n - 3$ numbers in the row of index 1.

Remark 3. If there is no need to find transversals, then there is a simple way to construct the Bar Sinister Latin square. I.e., the Bar Sinister Latin square constructed before is the Latin square

$$L(x, y) = (R^s(x) + y)(1 + \alpha^s)^{-1}$$

where the elements in $\mathbb{F}_q$ is listed as a natural order of $(0, 1, \alpha, \alpha^2, ..., \alpha^{p-1})$.

In the following examples, we always suppose that a finite field $\mathbb{F}_{2^4}$ is generated by the primitive polynomial $f(x) = x^4 + x^3 + 1$ and α is a primitive element of $\mathbb{F}_{2^4}$ with $f(\alpha) = 0$. The elements of this field are listed in Table 4.

Table 4. $\mathbb{F}_{2^4}$ Generated by $\alpha^4 + \alpha^3 + 1 = 0$

Index $i = log_\alpha^\beta$	1	α	α^2	α^3
0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	0	0	0	1
4	1	0	0	1
5	1	1	0	1
6	1	1	1	1
7	1	1	1	0
8	0	1	1	1
9	1	0	1	0
10	0	1	0	1
11	1	0	1	1
12	1	1	0	0
13	0	1	1	0
14	0	0	1	1

Example 3. Table 5 below is an example for block size 4. The original linear orthomorphism is as shown in Figure 2 with $\tau = 4$. The table shows compatible rearrangements of the three columns. For example, L_{10} and M_6 have the corresponding entry $k(10, 6) = 14$ which means that $L_10 + M_6 = R_{14}$ or that

$$x_{10-1} + x_6 = x_{14-4} \text{ i.e., } x_9 + x_6 = x_{10}.$$

The small circles in Table 5 are a selection of values of $k(i, j)$ which are all different and taken from each row and column exactly once. This is a transversal of the Latin square. Equivalently, this represents a 16 x 16 x 16 cube in which each row and column in the X, Y plane and each parallel plane along the Z axis are sampled once. As far as possible, a lower left to upper right diagonal was used.

The circled numbers represent a transversal. The linear orthmorphism defining Table 5 is $\sigma(x) = \alpha^{14}x, x \in \mathbb{F}_{2^4}$ and the nonlinear orthomorphism $g(x)$

Table 5. Bar Sinister Latin Square for Generating Function:

$x_k = x_{k-4} + x_{k-1}$

$n = 4,\ \tau = 4$

$x_{k-1} + x_k = x_{k-\tau}$

Entries are k indices of $x_{k-\tau}$

		j index of $\underline{x}_j$															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	0	5	6	7	8	9	10	11	12	13	14	15	1	$\boxed{2}$	3	4
	1	4	1	13	8	7	14	12	2	10	6	9	3	5	11	15	$\boxed{0}$
	2	5	0	2	14	9	8	15	13	3	11	$\boxed{7}$	10	4	6	12	1
	3	6	2	0	3	15	10	9	1	14	$\boxed{4}$	12	8	11	5	7	13
i	4	7	14	3	0	4	1	11	10	2	15	5	13	9	12	$\boxed{6}$	8
Index	5	8	9	15	4	0	5	2	12	11	3	1	6	$\boxed{14}$	10	13	7
of	6	9	8	10	1	5	0	6	3	$\boxed{13}$	12	4	2	7	15	11	14
$\underline{x}_{i-1}$	7	10	15	9	11	2	6	0	7	4	14	13	$\boxed{5}$	3	8	1	12
	8	11	13	1	10	12	$\boxed{3}$	7	0	8	5	15	14	6	4	9	2
	9	12	3	14	2	$\boxed{11}$	13	4	8	0	9	6	1	15	7	5	10
	10	13	11	4	$\boxed{15}$	3	12	14	5	9	0	10	7	2	1	8	6
	11	14	7	$\boxed{12}$	5	1	4	13	15	6	10	0	11	8	3	2	9
	12	15	$\boxed{10}$	8	13	6	2	5	14	1	7	11	0	12	9	4	3
	13	$\boxed{1}$	4	11	9	14	7	3	6	15	2	8	12	0	13	10	5
	14	2	6	5	12	10	15	$\boxed{8}$	4	7	1	3	9	13	0	14	11
	15	3	12	7	6	13	11	1	$\boxed{9}$	5	8	2	4	10	14	0	15

derived from the above Bar Sinister Latin square is as follows.

$$\begin{aligned}
g(x) + x &= F(x) \\
\alpha^{11} + 0 &= \alpha^{11} \\
\alpha^{10} + 1 &= \alpha^{5} \\
\alpha^{9} + \alpha &= \alpha^{7} \\
\alpha^{8} + \alpha^{2} &= \alpha^{10} \\
\alpha^{7} + \alpha^{3} &= \alpha^{6} \\
\alpha^{6} + \alpha^{4} &= \alpha^{13} \\
\alpha^{12} + \alpha^{5} &= \alpha^{3} \\
\alpha^{13} + \alpha^{6} &= \alpha^{4} \\
\alpha^{4} + \alpha^{7} &= \alpha^{8} \\
\alpha + \alpha^{8} &= \alpha^{14} \\
1 + \alpha^{9} &= \alpha^{2} \\
\alpha^{5} + \alpha^{10} &= 1 \\
\alpha^{3} + \alpha^{11} &= \alpha^{9} \\
0 + \alpha^{12} &= \alpha^{12} \\
\alpha^{2} + \alpha^{13} &= \alpha \\
\alpha^{14} + \alpha^{14} &= 0
\end{aligned}$$

Figure 4

Let the elements in $\mathbb{F}_{2^4}$ be represented by the exponents of α where we write $0 = \alpha^{\infty}$ as convention. The mapping from the left column to the right column of Figure 4 can be represented by the following permutation:

$$(11)(10, 5, 0, 2, 1, 14, \infty, 12, 3, 9, 7, 6, 13, 4, 8).$$

Thus it is maximal except for the single fixed point (11). The orthomorphism in Figure 4 can also be represented by a permutation in which each number is added to its successor to obtain a unique sum in that same permutation. This permutation is the following:

$$(14)(10, 0, 9, 1, 8, 2, 13, 6, 4, 7, 3, 11, \infty, 12, 5)$$

Once again, it is maximal except for the single fixed point which is necessary in every orthomorphism.

This orthomorphism can also be examined for nonlinearity [7] [8]. A linear function $f(x)$ over a R-module M is defined to be one for which:

$$f(ax + by) = af(x) + bf(y), \forall x, y \in M, a, b \in R.$$

$\mathbb{Z}_2^n$ can be considered as a $\mathbb{Z}_2$ module. We define a *discrepacy function* of a function $f(x)$ of $\mathbb{Z}_2^n$ as

$$D_f(x, y) = f(x) + f(y) + f(x + y), \forall x, y \in \mathbb{Z}_2^n.$$

Then a linear function over $\mathbb{Z}_2^n$ is one for which:

$$D_f(x, y) = 0, \ \forall x, y \in \mathbb{Z}_2^n.$$

$D_f(x, y)$ as defined is a mapping of subgroups of order ≤ 4 into $\mathbb{Z}_2^n$. That is, any additive triple supplemented by 0, $\{x, y, x+y, 0\}$ is a subgroup of $\mathbb{Z}_2^n$. The range of $D_f(x, y)$, donoted by $Im(D_f)$, satisfies that $Im(D_f) \in \mathbb{Z}_2^n$. A reasonable goal for a nonlinear mapping is that

$$Im(D_f) = \mathbb{Z}_2^n.$$

That is, all possible values in $\mathbb{Z}_2^n$ are taken on. In addition, the nonzero values should be approzimately equally distributed. This correlates well with the L_1 and L_4 norms using the Walsh-Fourier transform. In the example above, calculating all 16 x 16 = 256 values of $D_f(x, y)$ shows that $D_f(x, y)$ takes on all values in $\mathbb{Z}_2^4$. In other words, we have

$$Im(D_f) = \mathbb{Z}_2^4$$

where $f(x)$ is the nonlinear orthomorphism given above. Note that if y is fixed in $D_f(x, y)$, then this is the same function discussed in [7].

6 Finding a Transversal for an Arbitrary Orthomorphism

An arbitrary orthomorphism, in particular a nonlinear one, can be written as in Figure 1. Without changing the mapping defined by the orthomorphism, the set of equations defineing the orthomorphism can be permute so that the right column is identical to the right column of the linear orthormorphism in Figure 2, as follows:

$$\begin{array}{cllll}
RowNumber & L & & M & R \\
0 & 0 & + & 0 & = 0 \\
1 & u_1 & + & v_1 & = x_{1-\tau} \\
2 & u_2 & + & v_2 & = x_{2-\tau} \\
\vdots & & & & \\
k & u_k & + & v_k & = x_{k-\tau} \\
\vdots & & & & \\
p & u_p & + & v_p & = x_{p-\tau}
\end{array}$$

Figure 5

The resultant L and M columns in Figure 5 are, respectively, permuations of the L and M columns of Figure 2. $(x_{1-\tau}, x_{2-\tau}, \cdots, x_{p-\tau})$ in column R is a permuation of the original $(z_1, z_2, \cdots, z_p)$ in column 1 and is identical to column R of Figure 2. Consider an arbitrary equation in Figure 5:

$$u_k + v_k = x_{k-\tau}$$

where u_k occurs at some index i and v_k occurs at some index j, respectively, in columns L and M of Figure 3. Thus

$$L_i + M_j = R_k \text{ or } x_{i-1} + x_j = x_{k-\tau}.$$

Note that $k_{ij} = k(i,j) = k$ defines a point in Table 4. The set of 2^n such points defined by comparing Figure 5 with Figure 2 specifies a transversal in Table 3. The following are two examples.

Example 4. Let $g(x)$ be a nonlinear orthomporphism derived by nonlinear shift register logic I [3] which is given as below. The transversal in Table 6, framed numbers, representing this nonlinear orthomorphism.

$$\begin{gathered}
g(x) + x = F(x) \\
0 + 0 = 0 \\
\alpha^3 + 1 = \alpha^4 \\
\alpha^{12} + \alpha = 1 \\
\alpha^5 + \alpha^2 = \alpha^6 \\
\alpha^9 + \alpha^3 = \alpha^{11} \\
\alpha^7 + \alpha^4 = \alpha^8 \\
\alpha^8 + \alpha^5 = \alpha^9 \\
\alpha^4 + \alpha^6 = \alpha^{13} \\
\alpha^{14} + \alpha^7 = \alpha^5 \\
\alpha^{11} + \alpha^8 = \alpha^{12} \\
\alpha^6 + \alpha^9 = \alpha^{10} \\
\alpha^{13} + \alpha^{10} = \alpha^{14} \\
\alpha^{10} + \alpha^{11} = \alpha^7 \\
1 + \alpha^{12} = \alpha \\
\alpha + \alpha^{13} = \alpha^2 \\
\alpha^2 + \alpha^{14} = \alpha^3
\end{gathered}$$

Example 5. The transversal marked in Table 7 is the transversal representing the nonlinear orthomorphism generated by computer search.

Note that Example 4 is clearly "not very nonlinear" as 10 of 16 points in the transversal are on the main diagonal corresponding to a linear orthomorphism. Example 5 has only 2 points on the main diagonal and thus is "more nonlinear".

Table 6. The Same Bar Sinister Latin Sqaure in Example 3

		k index of x_k															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	$\boxed{0}$	0	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4
	1	4	1	13	8	7	14	$\boxed{12}$	2	10	6	9	3	5	11	15	0
	2	5	0	$\boxed{2}$	14	9	8	15	13	3	11	7	10	4	6	12	1
	3	6	2	0	$\boxed{3}$	15	10	9	1	14	4	12	8	11	5	7	13
k	4	7	14	3	0	$\boxed{4}$	1	11	10	2	15	5	13	9	12	6	8
Index	5	8	9	15	4	0	$\boxed{5}$	2	12	11	3	1	6	14	10	13	7
of	6	9	8	10	1	5	0	6	3	13	12	4	2	7	15	$\boxed{11}$	14
x_{k-1}	7	10	15	9	11	2	6	0	$\boxed{7}$	4	14	13	5	3	8	1	12
	8	11	13	1	10	12	3	7	0	8	5	15	$\boxed{14}$	6	4	9	2
	9	12	3	14	2	11	13	4	8	0	$\boxed{9}$	6	1	15	7	5	10
	10	13	11	4	15	3	12	14	5	9	0	$\boxed{10}$	7	2	1	8	6
	11	14	7	12	5	1	4	13	15	6	10	0	11	$\boxed{8}$	3	2	9
	12	15	10	8	13	6	2	5	14	$\boxed{1}$	7	11	0	12	9	4	3
	13	1	4	11	9	14	7	3	6	15	2	8	12	0	$\boxed{13}$	10	5
	14	2	$\boxed{6}$	5	12	10	15	8	4	7	1	3	9	13	0	14	11
	15	3	12	7	6	13	11	1	9	5	8	2	4	10	14	0	$\boxed{15}$

Table 7. The Same Bar Sinister Latin Sqaure in Example 3

		k index of $\underline{x}_k$															
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	$\boxed{0}$	5	6	7	8	9	10	11	12	13	14	15	1	2	3	4
	1	4	1	13	8	7	14	12	2	10	$\boxed{6}$	9	3	5	11	15	0
	2	5	0	2	14	9	8	15	13	3	11	7	10	4	6	$\boxed{12}$	1
	3	6	2	0	3	15	10	9	1	14	4	12	8	11	5	7	$\boxed{13}$
k	4	7	14	3	0	4	1	11	10	2	15	5	13	$\boxed{9}$	12	6	8
Index	5	8	9	15	4	0	5	2	12	$\boxed{11}$	3	1	6	14	10	13	7
of	6	9	8	10	1	5	0	6	$\boxed{3}$	13	12	4	2	7	15	11	14
x_{k-1}	7	10	$\boxed{15}$	9	11	2	6	0	7	4	14	13	5	3	8	1	12
	8	11	13	1	10	12	3	7	0	8	5	15	14	6	$\boxed{4}$	9	2
	9	12	3	14	2	11	13	4	8	0	9	6	$\boxed{1}$	15	7	5	10
	10	13	11	4	15	3	12	14	5	9	0	$\boxed{10}$	7	2	1	8	6
	11	14	7	12	$\boxed{5}$	1	4	13	15	6	10	0	11	8	3	2	9
	12	15	10	8	13	6	$\boxed{2}$	5	14	1	7	11	0	12	9	4	3
	13	1	4	11	9	$\boxed{14}$	7	3	6	15	2	8	12	0	13	10	5
	14	2	6	5	12	10	15	$\boxed{8}$	4	7	1	3	9	13	0	14	11
	15	3	12	$\boxed{7}$	6	13	11	1	9	5	8	2	4	10	14	0	15

7 Conclusion

In terms of the isomorphism between the linear space $\mathbb{Z}_2^n$ and the finite field $\mathbb{F}_{2^n}$, an algebraic method of constructing linear orthomorphisms on $\mathbb{Z}_2^n$ with maximal cycles and two algorithms for implementation are provided. The linear orthomorphism can be used to construct Bar Sinister Latin squares from which all orthomorphisms, especially, nonlinear orthomorphisms on $\mathbb{Z}_2^n$, can be represented as transversals. If one can count the number of transversals in the Bar Sinister Latin squares, one can determine the number of orthomorphisms in $\mathbb{Z}_2^n$.

Some remaining qustions are: Is there a determinsistic way to find transversals in Bar Sinister Latin squares which are not parallel to the principle diagonal? Can tranversals be categorized as to the cycle structure and degree of nonlinearity of the corresonding orthomorphisms?

References

1. Z.T. Dai, S.W. Golomb, and G. Gong, Generating all linear orthomorphisms without repetitions, *Discrete Mathematics*, 205 (1999) pp. 47-55.
2. J. Denes and A.D. Keedwell, *Latin Squares: New Developments in the Theory and Applications*, North Holland, 1991.
3. S.W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, May 1982, pp. 142.
4. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopaedia of Mathematics and its Applications, Volume 20, Addison-Wesley, 1983.
5. Lothrop Mittenthal, Block substitutions using orthomorphic mappings, *Advances in Applied Mathematics*, Vol. 16, No. 1, March 1995.
6. Lothrop Mittenthal, The algebraic structure of nonlinear orthomorphisms of binary numbers, *Technical report, Teledyne Electronic Technologies*, Feb. 1994.
7. K. Nyberg, Differentially uniform mappings for cryptography, *Advances in Cryptology, Proceedings of EuroCrypt'93*, Lecture Notes in Computer Science, 1993.
8. J.P. Pieprzyk, Nonlinearity of exponent permutations, *Advances in Cryptology, Proceedings of EuroCrypt'89*, pp. 80-92, Lecture Notes in Computer Science, 1989.
9. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, 1977.
10. J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press 1992, pp. 264.