Some properties of latin squares - Study of maximal sets of latin squares

Lourdes M. Morales

University of Puerto Rico, Río Piedras

Computer Science Department

September 2010

Abstract

A latin square of order n is an $n \times n$ matrix containing n distinct symbols (usually denoted by the non-negative integers from 0 to $n-1$) such that each symbol appears in each row and column exactly once. Latin squares have various applications in Coding Theory, Cryptography, Finite Geometries and in the design of statistical experiments, to name a few. Two latin squares of the same order are said to be r-orthogonal if you get r distinct ordered pairs when you superimpose them. In our research we look for new constructions of maximal sets of latin squares. We present some partial results and conjectures related to this.

1 Introduction

A *latin square of order n* is an $n \times n$ matrix containing n distinct symbols (ususally denoted by the non-negative integers from 0 to $n-1$) such that each symbol appears in each row and column exactly once. Latin squares have various applications in the fields of Coding Theory, Cryptography, Finite Geometries and in the design of statistical experiments, to name a few.

In our previous work [1], we were looking for patterns or tendencies that could relate latin squares, or sets of latin squares, that would give maximum orthogonality. This is a continuation of our previous work, but with a focus on the generating matrices and the construction of maximal sets of latin squares. Here we give some necessary background. First we start with a brief description of the different types of latin squares.

Definition 1. A *reduced latin square* (RLS) of order n is a latin square that has its first row and column in the standard order (0,1, ... ,$n-1$).

Example 1. Reduced latin square of order $n = 4$:

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

Definition 2. A *semi-reduced latin square* (SRLS) of order n is a latin square that has its first row in the standard order.

Example 2. Semi-reduced latin square of order $n = 4$:

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

Note that reduced latin squares are semi-reduced, but not all semi-reduced latin squares are reduced.

Definition 3. Let L be a latin square of order n. If $L = L^T$, L^T being the transpose of L, then L is said to be a *symmetric latin square* of order n.

Example 3. Let A and B denote two latin squares of order $n = 5$.

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} = A^T$$

and

$$B = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 3 & 4 & 1 & 2 \\ 1 & 4 & 0 & 2 & 3 \\ 2 & 0 & 1 & 3 & 4 \\ 3 & 1 & 2 & 4 & 0 \\ 4 & 2 & 3 & 0 & 1 \end{pmatrix} = B^T$$

Thus, A is a symmetric latin square and B is not.

The latin square of order $n = 4$ in Example 1 is also an example of a symmetric latin square.

1.1 Orthogonality

When superimposing two latin squares of order n, say L_1 and L_2, we get an $n \times n$ array $S_{(L_1,L_2)}$ of ordered pairs, where the $(i,j) - th$ entry is defined by $S_{(L_1,L_2)}(i,j) = (L_1(i,j), L_2(i,j))$ for $0 \leq i < n$.

Now let $r = P(L_1, L_2)$ denote the number of distinct ordered pairs you get when you superimpose L_1 and L_2. Then, L_1 and L_2 are said to be *r-orthogonal* if you get r distinct ordered pairs when you superimpose them.

Example 4. Let L_1 and L_2 be two latin squares of order $n = 4$, and let $S_{(L_1,L_2)}$ be the superimposition of L_1 and L_2,

$$L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \quad L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

$$S_{(L_1,L_2)} = \begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,2) & (2,3) & (3,0) & (0,1) \\ (2,3) & (3,0) & (0,1) & (1,2) \\ (3,1) & (0,2) & (1,3) & (2,0) \end{pmatrix}$$

Since there are 12 distinct ordered pairs in $S_{(L_1,L_2)}$, we say that L_1 and L_2 are 12-orthogonal and that $r = P(L_1, L_2) = 12$.

Note that $r = P(L_i, L_j) = P(L_j, L_i)$**.**

Two latin squares of order n are *orthogonal* if when the squares are superimposed each of the n^2 ordered pairs appears exactly once, that is, if they are n^2-orthogonal.

Example 5. Let L_1 and L_2 be two latin squares of order $n = 4$, and let $S_{(L_1,L_2)}$ be the superimposition of L_1 and L_2,

$$L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \quad L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

$$S_{(L_1,L_2)} = \begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \\ (3,2) & (2,3) & (1,0) & (0,1) \end{pmatrix}$$

Since there are 16 distinct ordered pairs in $S_{(L_1,L_2)}$, we say that L_1 and L_2 are orthogonal.

Let $\{LS_1, \ldots, LS_t\}$ be a set of $t \geq 2$ latin squares of order n. Then, $r_t = P(LS_1, \ldots, LS_t)$ is the sum of all the $r = P(L_i, L_j)$, with $1 \leq i, j \leq t$ and $i \neq j$. We call this sum the $r_t - orthogonality$.

Example 6. Let $\{L_1, L_2, L_3\}$ be a set of $t = 3$ latin squares of order $n = 4$.

$$L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 \\ 2 & 0 & 3 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \; L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \; L_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 1 & 2 & 3 & 0 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

Then,

$$S_{(L_1,L_2)} = \begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,1) & (3,2) & (0,3) & (2,0) \\ (2,2) & (0,3) & (3,0) & (1,1) \\ (3,3) & (2,0) & (1,1) & (0,2) \end{pmatrix} \; S_{(L_1,L_3)} = \begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,2) & (3,3) & (0,0) & (2,1) \\ (2,1) & (0,2) & (3,3) & (1,0) \\ (3,3) & (2,0) & (1,1) & (0,2) \end{pmatrix}$$

$$S_{(L_2,L_3)} = \begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,2) & (2,3) & (3,0) & (0,1) \\ (2,1) & (3,2) & (0,3) & (1,0) \\ (3,3) & (0,0) & (1,1) & (2,2) \end{pmatrix}$$

Since $P(L_1, L_2) = 9$, $P(L_1, L_3) = 9$ and $P(L_2, L_3) = 12$, $r_3 = P(L_1, L_2, L_3) = 30$.

1.2 Mutually orthogonal latin squares

We focus on *maximal sets* of latin squares of order n, that is, sets of t latin squares of order n that give the maximum $r_t - orthogonality$. In our research we study maximal sets of latin squares of small orders in hopes of finding how to generate them for all orders. We started studying how to construct sets of mutually orthogonal latin squares (MOLS). In this section we present some important facts about MOLS and known ways to construct them.

Definition 4. A set of *mutually orthogonal latin squares* is a set of two or more latin squares of the same order, all of which are orthogonal to one another.

Example 7. Let L_1, L_2 and L_3 be three latin squares of order $n = 4$:

$$L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \; L_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix} \; L_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

Then,

$$S_{(L_1,L_2)} = \begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \\ (3,2) & (2,3) & (1,0) & (0,1) \end{pmatrix} \; S_{(L_1,L_3)} = \begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,2) & (0,3) & (3,0) & (2,1) \\ (2,3) & (3,2) & (0,1) & (1,0) \\ (3,1) & (2,0) & (1,3) & (0,2) \end{pmatrix}$$

$$S_{(L_2,L_3)} = \begin{pmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (3,2) & (2,3) & (1,0) & (0,1) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \end{pmatrix}$$

Since L_1 and L_2 are orthogonal, as well as L_1 with L_3, and L_2 with L_3. We say that L_1, L_2 and L_3 are MOLS of order $n = 4$.

Note that sets of MOLS are maximal sets.

Definition 5. A set of $t \geq 2$ MOLS of order n is called a *complete set* if $t = n - 1$.

There are various results on how big a set of MOLS can be in [4], but here we present the ones that are vital to our work.

First, let $N(n)$ denote the size of the largest collection of MOLS of order n (that exist).

Theorem 1. *$N(n) \leq n - 1$ for any $n \geq 2$.*
Theorem 2. *If q is a prime power, then $N(q) = q - 1$.*
Theorem 3. *$N(n) \geq 2$ for all n except 2 and 6.*

What the last theorem means is that a pair of MOLS exist for every $n \neq 2, 6$.

The concept of MOLS of a given order is important, because if there are $n-1$ MOLS of order n we can say that there exists a projective plane $PG(2, n)$ (Bose's Equivalence Theorem) [4].

1.3 Constructing sets of MOLS

1.3.1 The desarguesian set

The *desarguesian set* is a complete set of MOLS of prime power order $q = p^m$, where p is a prime and $m \geq 1$ is an integer, which is constructed using linear polynomials over a finite field of order q.

Here we present a way to construct such a set given in [4]: Let $\mathbb{F}_q^* = \{a_1, a_2, ..., a_{q-1}\}$ be the nonzero elements of the field. Label the rows and columns of a $q \times q$ matrix with the elements of the field $\mathbb{F}_q$, listed in order. For each $1 \leq i \leq q - 1$ we construct a latin square L_i as follows. Let $f_i(x, y)$ be the linear polynomial $f_i(x, y) = \alpha_i x + y$. In the location (x, y) in the square L_i place the field element $f_i(x, y)$. In this cases addition is done modulo p.

Example 8. Here we construct the desarguesian set of MOLS of order $q = 4 = 2^2$ (addition is done modulo $p = 2$). Let $\mathbb{F}_4^* = \{1, \alpha, \alpha^2 = \alpha + 1\}$.

For $a_1 = 1$, $f_1(x, y) = x + y$.

$$L_1 = \begin{pmatrix} 0 & 1 & \alpha & \alpha+1 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha & 1 & 0 \end{pmatrix}$$

For $a_2 = \alpha$, $f_2(x, y) = \alpha x + y$.

$$L_2 = \begin{pmatrix} 0 & 1 & \alpha & \alpha+1 \\ \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha & 1 & 0 \\ 1 & 0 & \alpha+1 & \alpha \end{pmatrix}$$

For $a_3 = \alpha^2$, $f_3(x, y) = \alpha^2 x + y$.

$$L_3 = \begin{pmatrix} 0 & 1 & \alpha & \alpha+1 \\ \alpha+1 & \alpha & 1 & 0 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha+1 & 0 & 1 \end{pmatrix}$$

Thus, $\{L_1, L_2, L_3\}$ is the desarguesian set of MOLS of order $q = 4$.

Since we have a way of constructing the desarguesian set we want to know if for a given prime power q there exist other complete sets of MOLS of order q that are different from the desarguesian set. We shall consider two sets different if, as matrices, the squares are different. Next we will present some of the concepts discussed in [2] concerning this matter.

1.3.2 Isomorphic sets of MOLS

It is known that for some prime power orders we can take a complete set and get a different complete set through permutations.

Definition 6. Two complete sets of MOLS of the same order are said to be *isomorphic* if the latin squares of one set can be obtained from the latin squares of the other set by applying a fixed permutation to the rows of all the latin squares of the first set, then by similarly applying a fixed permutation to the columns of the resulting latin squares, and finally by applying a third permutation to the symbols.

The key point is that the three permutations must be applied to each of the latin squares in the first set. They also state that for all prime powers $q = p^m > 8$ with $m > 1$, there are at least two non-isomorphic sets of MOLS of order q. Thus, for such q there is always at least one non-desarguesian complete set of MOLS of order q.

On the other hand, they say that for each prime power $q = 2, 3, 4, 5, 7, 8$, any complete set of MOLS of order q is isomorphic to the desarguesian set of MOLS of order q.

Therefore, for $q = 2, 3, 4, 5, 7, 8$ we can get all the complete sets of MOLS of order q by permuting the MOLS in the desarguesian set.

They also present the following well-known conjecture that, if true, it would mean that all the complete sets of MOLS of order p, where p is a prime, can be found by applying permutations to the MOLS of order p in the desarguesian set.

Conjecture 1. In the case of latin squares of prime order p, any two complete sets of $p - 1$ MOLS of order p are indeed isomorphic.

1.3.3 Transversals and permutation matrices

In our previous work we used permutation matrices generated from the transversals of latin squares contained in complete sets to permute and generate different complete sets.

Definition 7. A *transversal* in a latin square of order n is a set of n cells, one from each row and column containing each of the n symbols exactly once.

Example 9. Let L be latin square of order $n = 5$.

$$L = \begin{pmatrix} \mathbf{0} & 1 & 2 & 3 & 4 \\ 1 & 2 & \mathbf{3} & 4 & 0 \\ 2 & 3 & 4 & 0 & \mathbf{1} \\ 3 & \mathbf{4} & 0 & 1 & 2 \\ 4 & 0 & 1 & \mathbf{2} & 3 \end{pmatrix}$$

Then, $T = \{L_{1,1} = 0, L_{2,3} = 3, L_{3,5} = 1, L_{4,2} = 4, L_{5,4} = 2\}$ is a transversal in L.

Setting the value of each of the cells in the transversal to 1 and the rest of the cells to 0 gives a *permutation matrix* of order n. If we multiply a latin square of order n by a permutation matrix of order n we get a different latin square of order n.

Example 10. Let L be the latin square of order $n = 5$ and T be the transversal in L from Example **9**. Also, let G be the permutation matrix of order $n = 5$ that results from setting the values of the cells in T to 1 and the rest of the cells to 0.

First, we have the permutation matrix as the left-hand operand.

$$G \times L = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix}$$

Note that the resulting matrix is a latin square of order $n = 5$ and that it is not equal to L.

Now we have the permutation matrix as the right-hand operand.

$$L \times G = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 3 & 1 & 4 & 2 \\ 1 & 4 & 2 & 0 & 3 \\ 2 & 0 & 3 & 1 & 4 \\ 3 & 1 & 4 & 2 & 0 \\ 4 & 2 & 0 & 3 & 1 \end{pmatrix}$$

Again the resulting matrix is a latin square of order $n = 5$ not equal to L.

Moreover, note that if the permutation matrix is the left-hand operand we are permuting the rows of L and if the permutation matrix is the right-hand operand we are permutation the columns of L.

Now, we know how to get a permutation matrix from the transversal of a latin square, but first we need to know if there exists a transversal for a latin square of any given order. Here are some important results about the existence of transversals [5]:

Proposition 1. *The addition tables of $\mathbb{Z}_{2n}$, with $n \geq 1$, are a class of latin squares that do not have transversals.*

Proposition 2. *If a latin square has a transversal, then any latin square isomorphic to that square has a transversal.*

Theorem 4. *Every latin square of even order has an even number of transversals.*

So, some latin squares have no transversals at all. The addition tables of $\mathbb{Z}_{2n}$, with $n \geq 1$, for example, have an even order and zero transversals (Proposition 1), which agrees with theorem 4 because zero is an even number. Therefore, theorem 4 also implies that some latin squares of even number may not have transversals.

Conjecture 2. Every latin square of odd order has a transversal.

2 MOLS generating matrix

In [1] the concept of MOLS generating matrices was introduced to describe a very special kind of permutation matrix.

Definition 8. Let L be a latin square of order n, and let G be an $n \times n$ permutation matrix. We say that G is a *MOLS generating matrix* if $\{G \times L, G^2 \times L, ..., G^{n-1} \times L\}$ is a complete set of MOLS of order n.

Example 11. Let L be a latin square of order $n = 5$, $T = \{L_{1,1} = 0, L_{2,3} = 3, L_{3,5} = 1, L_{4,2} = 4, L_{5,4} = 2\}$ be a transversal in L and G be the 5×5 permutation matrix

given by T (see Examples **9** and **10**).

$$L = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} \quad G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

then,

$$G \times L = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix} = L_1$$

$$G^2 \times L = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix} = L_2$$

$$G^3 \times L = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix} = L_3$$

$$G^4 \times L = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} = L = L_4$$

The set $\{L_1, L_2, L_3, L_4\}$ is a complete set of MOLS of order $n = 5$. Thus, G is a MOLS generating matrix.

Since we can construct a permutation matrix from a transversal, it is natural to ask if every transversal gives a MOLS generating matrix. The answer is no, take for instance this next example.

Example 12. Consider for example the same latin square of order $n = 5$ from Example 11. Let $T = \{L_{1,2} = 1, L_{2,3} = 3, L_{3,4} = 0, L_{4,5} = 2, L_{5,1} = 4\}$ be a transversal in L and G be a 5×5 permutation matrix given by T.

$$L = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} \quad G = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

then,

$$G \times L = \begin{pmatrix} 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix} = L_1$$

$$G^2 \times L = \begin{pmatrix} 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix} = L_2$$

$$G^3 \times L = \begin{pmatrix} 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix} = L_3$$

$$G^4 \times L = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} = L = L_4$$

The set $\{L_1, L_2, L_3, L_4\}$ is not a complete set of MOLS of order $n = 5$. Thus, G is not a MOLS generating matrix. What is more, note that $r_4 = 30$ which is the minimum $r_4(5)$-orthogonality for sets of 4 latin squares of order $n = 5$.

The next conjecture was proposed in [1]. Are goal in this research was to improve it, since, as we will show later in §4, we already found a counterexample for the $q = 7$ case.

Conjecture 3. Let L be a symmetric RLS contained in a set of MOLS. If G is a permutation matrix given by a transversal of L with exactly one 1 on its diagonal, then G is a MOLS generating matrix.

3 Permutation Polynomials

Definition 9. A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the associated polynomial function $f : c \to f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.

So, if f is a permutation polynomial of $\mathbb{F}_q$, then the equation $f(x) = a$ has exactly one solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$. Another way to say this is expressed in the next Lemma.

Lemma 1. *The polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ iff one of the following conditions holds:*

(i) the function $f :\to f(c)$ is onto;

(ii) the function $f :\to f(c)$ is one-to-one;

(iii) $f(x) = a$ has a solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$;

(iv) $f(x) = a$ has a unique solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$;

4 Main results

In our work we focused on constructing maximal sets of latin sqaures. First, we worked on constructing complete sets of mutually orthogonal latin squares of prime power orders $q = p^m$, where p is a prime and $m \geq 1$ is an integer, using permutation matrices derived from the transversals of symmetric reduced latin sqaures and then with permutation polynomials.

4.1 MOLS generating matrix

First, we constructed complete sets of mutually orthogonal latin squares of prime power orders $q = p^m$, where p is a prime and $m \geq 1$ is an integer, using Conjecture **3**. Here are our results:

4.1.1 $q = 5$

There are 56 RLSs of order $q = 5$, **6** of which are symmetric and are contained in sets of MOLS [3].

When we take any of these **6** symmetric RLS of order $q = 5$ we get **15** transversals: the identity matrix $I_{5\times5}$ (we ignore this one), plus **4** that don't have ones on their diagonal and **10** that have one **1** on their diagonal.

These **10** transversals satisfy the conditions for Conjecture 3 and they give MOLS generating matrices; on the other hand, the four that don't have ones on their diagonals give permutation matrices that generate sets of 4 distinct LSs of order $q = 5$ with $r_4(5) = 30$.

Note that $r_4(5) = 30$ is the minimum $r_4(5)$-orthogonality, for there are six possible superimpositions of pairs of distinct LSs and the minimum $r(5)$-orthogonality is 5 (see [6] for a table with the spectrum and frequency for r-orthogonalities when $n = 4, 5, 6$).

So for $q = 5$ Conjecture **3** is true.

4.1.2 $q = 7$

For $q = 7$ we only worked with the Cayley Table of order $q = 7$ (CT_7), but it was enough to prove that Conjecture **3** was false.

First of all, note that CT_7 is a symmetric RLS of order $q = 7$ and that it is contained in the desarguesian set of order $q = 7$.

We found the next permutation matrix G for CT_7 with one **1** on its diagonal:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Nevertheless, the set $\{G \times CT_7, G^2 \times CT_7, G^3 \times CT_7, G^4 \times CT_7, G^5 \times CT_7, G^6 \times CT_7\}$ is not a complete set of MOLS (see the Appendix for the maple procedure we used to compute the $r_6 - orthogonality$).

4.2 Permutation Polynomials

Using linear and cubic permutation polynomials, we constructed sets of $t = 3, 4, 5$ LSs of order $n = 5$ and calculated the spectrum and frequency of the $r_t - orthogonality$ for these sets to provide more information that will later help us determine the best method for constructing maximal sets of latin squares in general.

4.2.1 Linear Permutation Polynomials

Here we generated 20 linear polynomials of the form $ax + b$, where $a \neq 0$, $b \in F_5$, and verified that they were permutation polynomials. Then, we generated a list of 20 LSs of order $n = 5$ with those polynomials using the following construction:

1. If the index set of a LS of order n (LS will be an $n \times n$ array) is $\{0, 1, ..., n-1\}$ and $f(x)$ is the permutation polynomial, then $LS(i, j) = (f(i) + j) mod n$.
2. It contains the Cayley Table of order $q = 5$.

Next, we calculated the spectrum and the frequency for the following data:

1. The $r - orthogonality$ between each pair of LSs in the list (the list includes the Cayley Table of order $q = 5$ because it was generated by one of the linear

permutation polynomials):

r	$frequency$
5	40
25	150

2. The $r-orthogonality$ between the Cayley Table of order $q=5$ and the rest of the LSs in the list:

r	$frequency$
5	5
25	15

3. The $r_t-orthogonality$ for sets of $t=3$ and $t=4$ LSs that are $5-orthogonal$ to the Cayley Table of order $q=5$ and to each other:

t	r_t	$frequency$
3	15	6
4	30	4

4. The $r_t-orthogonality$ for sets of $t=3$ and $t=4$ LSs that are *orthogonal* to the Cayley Table of order $q=5$ and to each other (i.e., sets of MOLS of order $n=5$ that contain the Cayley Table of order $q=5$):

t	r_t	$frequency$
3	75	75
4	150	125

5. The $r_t-orthogonality$ for sets of $t=3$ and $t=4$ LSs that are $5-orthogonal$ to each other but they don't contain the Cayley Table of order $q=5$:

t	r_t	$frequency$
3	15	34
4	30	16

6. The $r_t-orthogonality$ for sets of $t=3$ and $t=4$ LSs that are *orthogonal* to each other but they don't contain the Cayley Table of order $q=5$ (i.e., sets of MOLS of order $n=5$ that don't contain the Cayley Table of order $q=5$):

t	r_t	$frequency$
3	75	425
4	150	500

4.2.2 Cubic Permutation Polynomials

Finally, we generated 100 cubic polynomials of the form $a(x+b)^3+c$, where $a \neq 0, b, c \in F_5$, and verified that they were permutation polynomials. Next, we generated a list of 100 LSs of order $n=5$ with those polynomials using the following construction:

1. If the index set of a LS of order n (LS will be an $n \times n$ array) is $\{0,1,...,n-1\}$ and $f(x)$ is the permutation polynomial, then $(i,j) = (f(i)+j) mod n$.
2. It **doesn't** contain the Cayley Table of order $q=5$.

Then, we calculated the spectrum and the frequency for the following data:

1. The $r-orthogonality$ between each pair of LSs in the list (this doesn't include the Cayley Table of order $q=5$):

r	$frequency$
5	200
15	4,000
25	750

2. The $r-orthogonality$ between the Cayley Table of order $q=5$ and the 100 LSs in the list:

r	$frequency$
15	100

3. The $r_t-orthogonality$ for sets of $t=3$ and $t=4$ LSs (from the list, so none of them contain the Cayley Table of order $q=5$) that are $5-orthogonal$ to each other:

t	r_t	$frequency$
3	15	200
4	30	100

4. The $r_t-orthogonality$ for sets of $t=3$ and $t=4$ LSs (from the list and with the Cayley Table of order $q=5$ as the first LS) that are $15-orthogonal$ to the Cayley Table of order $q=5$ and each other:

t	r_t	$frequency$
3	45	4,000
4	90	80,000

5. The $r_t-orthogonality$ for sets of $t=3$ and $t=4$ LSs (from the list, so none of them contain the Cayley Table of order $q=5$) that are $orthogonal$ to each other:

t	r_t	$frequency$
3	75	2,500
4	150	3,125

5 Future Work

We would like to improve the MOLS Generating Matrix Conjecture (Conjecture **3**) and gather more information on other methods for constructing maximal sets of LSs, because our goal is to come up with the best way to construct or find the biggest maximal sets of latin squares of order n possible for all n.

6 Acknowledgments

This research was done in collaboration with the Latin Square Research Group consisting of: Prof. Rafael Arce, Prof. Francis Castro, Prof. Javier Córdova, Prof. Ivelisse Rubio, University of Puerto Rico in Ro Piedras, and Prof. Gary Mullen, Penn State University. And with the the support from the NSF through the S-STEM program's Alan Turing Fellowship and The Puerto Rico Luis Stokes Alliance for Minority Participation (PR-LSAMP) program.

7 Appendix: Maple Procedures

Note: The package *with(linalg)* is needed for these procedures.

7.1 Computing orthogonality for sets of two latin squares

First we have a procedure that given two latin squares (of the same order) and the order, computes r-orthogonality.

```
rOrt := proc (A, B, n)
local freq, i, j;
freq := Array(0 .. n^2-1);
for i to n do
for j to n do
freq[A[i][j]+n*B[i][j]] := 1
end do;
end do;
freq := convert(freq, list);
return numboccur(freq, 1)
end proc:
```

7.2 Computing orthogonality for sets of two or more latin squares

Here we have a procedure that given a set of $t \geq 2$ latin squares (of the same order) and the order, uses the first procedure to compute the r-orthogonality of every pair of distinct latin squares in the set, and finally adds them all up to give the r_t-orthogonality.

```
rtOrt := proc (SET, n)
local numls, compList, i, r;
numls := nops(SET);
compList := [];
for i to numls do
compList := [op(compList), i]
end do;
with(combinat);
compList := choose(compList, 2);
r := 0;
for i in compList do
r := r+rOrt(SET[i[1]], SET[i[2]], n);
end do;
return r
end proc:
```

7.3 Generating sets of latin squares with permutation matrices

Finally we have two procedures that given a latin square, a permutation matrix and the order, generates a set of latin squares.

The first one does it by permuting rows (the permutation matrix is the lefthand operand):

```
genLSsetPF:=proc(LS::Matrix, T::Matrix, q::integer)
local LSs, LSq, i:
LSs := [LS]:
LSq:=LS:
for i from 1 to q-2 do
LSq := multiply(T, LSq):
LSs := [op(LSs), eval(LSq)]:
end do:
RETURN(LSs)
end proc:
```

The second one does it by permuting columns (the permutation matrix is the right-hand operand):

```
genLSsetPC := proc (LS::Matrix, T::Matrix, n::integer) local LSs, LSn, i:
LSs := [LS]:
LSn:=LS:
for i from 1 to n-2 do
LSn := multiply(LSn, T):
LSs := [op(LSs), eval(LSn)]:
end do:
RETURN(LSs)
end proc:
```

References

[1] J. Bermúdez, *Study of Latin Square Generating Polynomials*, 2009.

[2] C.F. Laywine, & G.L. Mullen, *Discrete Mathematics Using Latin Squares*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons, Inc., New York, 1998.

[3] J. Bermúdez Piñero, & R. García Lebrón, & R. López Roig. *Some Properties of Latin Squares*, 2009.

[4] G. Mullen, & C. Mummert, *Finite Fields and Applications*, Chapter 2: Combinatorics. Section 2: Latin Squares. Pp. 43-59. P.cm-Student mathematical library; v.41, American Mathematical Society, Rhode Island, 2007.

[5] C. J. Colbourn and J. H. Dinitz, The CRC Handbook of Combinatorial Designs. Boca Raton, FL: CRC, 1996.

[6] R. Arce, J. Córdova and I. Rubio. *Consideraciones Computacionales de Latin Squares*. University of Puerto Rico, Río Piedras Campus, Undergraduate Seminar 1 in Computer Science, 2008. (Power Point Presentation)