Study of Latin Square Generating Polynomials

Jeranfer Bermúdez
University of Puerto Rico, Río Piedras
Dep. Ciencia de Cómputos

July 9, 2009

1 Introduction

A Latin Square of order n is an $n \times n$ matrix of n distinct elements (usually represented with the numbers from 0 to $n-1$), where each element appears in each row and in each column exactly once. Their various applications in Coding Theory, Chryptography and Prossesor Scheduling, just to mention a few, make Latin Squares a very interesting field to study. In a past paper, *Some Properties of Latin Squares*[1], we stated our interest in looking for patterns or tendencies that could relate Latin Squares, or sets of Latin Squares, that would give Maximum Orthogonality. For that reason we look for another way of constructing Latin Squares which we had not studied previously, using polynomials over finite fields.

2 Preliminaries

2.1 Some types of Latin Squares

2.1.1 Reduced Latin Square

A **Reduced Latin Square** of order n is a Latin Square that has its first row and first column in the standard order $(0 \dots n-1)$.

Example 1. *Reduced Latin Square of order* $n = 4$.

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

2.1.2 Semireduced Latin Square

A **Semireduced Latin Square** of order n is a Latin Square that has its first row in the standard order $(0 \dots n-1)$.

Example 2. *Semireduced latin Square of order $n = 4$.*

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

Every Reduced Latin Square is a Semireduced Latin Square, but not all Semireduced latin Squares are Reduced Latin Squares.

2.2 Orthogonality

When superimposing two Latin Squares A and B of the same order, we get a $n \times n$ array $S_{(A,B)}$ of ordered pairs, where $S_{(A,B)}(i,j) = (A(i,j), B(i,j))$ for $0 \leq i, j < n$. If there are r distinct oredered pairs in $S_{(A,B)}$, we say that A and B are **r-Orthogonal**.

Example 3. *Let A and B be two Latin Squares of order $n = 4$, and let $S_{(A,B)}$ be the superimposition of A and B,*

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$

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

Since there are only 8 distinct oredered pairs in $S_{(A,B)}$ then $r = 8$, and we say that A and B are 8-Orthogonal.

2.2.1 Orthogonal Latin Squares

When superimposing two Latin Squares A and B of the same order, if each one of the resulting ordered pairs in $S_{(A,B)}$ are distinct, we say that A and B are **Orthogonal**.

Example 4. *Let A and B be two Latin Squares of order $n = 4$, and let $S_{(A,B)}$ be the superimposition of A and B,*

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix}$$

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

Since every ordered pair in $S_{(A,B)}$ is distinct, we say that A and B are Orthogonal.

To know what r-Orthogonalities exist for a given order n, it is enough to compare every Reduced Latin Square of order n to every Semireduced Latin Square of the same order.

Theorem 1. *[1] For any two Latin Squares A and B of order n, A and B are r-Orthogonal, if and only if there exists a Reduced Latin Square and a Semireduced Latin Square of order n that are r-Orthogonal.*

This is very important from a computational standpoint because instead of superimposing every Latin Square with every Latin Square (26011238400 comparisons for $n = 5$), we only need to superimpose every Reduced Latin Square with every Semmireduced Latin Square (only 75264 comparisons for $n = 5$). This means a great reduction in the number of comparisons we need to study.

2.2.2 Mutually Orthogonal Latin Squares (MOLS)

A set of **Mutually Orthogonal Latin Squares**, or **MOLS**, is a set of 2 or more Latin Squares, all of wich are orthogonal to one another.

Example 5. *Let A, B and C be three Latin Squares of order $n = 4$*

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix} \qquad C = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

Then,

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

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

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

Note that A and B are orthogonal, as well as A with C, and B with C. Therefore A, B and C are MOLS.

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

2.3 Symmetric Latin Square

Let $L1$ be a Latin Square, if $L1 = L1^T$, $L1^T$ being the transposed Latin Square L1, we say that L1 is a **Symmetric Latin Square**.

Example 6. *Let A and B denote two Latin Squares of order $n = 5$.*

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}$$

Then:

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

Note that $A = A^T$ whereas $B \neq B^T$. Therefore A is a symmetric Latin Square and B is not.

3 MOLS Generating Permutation Sets

By the data obtained for our previous paper [1], we now that there are six sets of MOLS for $n = 5$ where each set consists of one Reduced Latin Square and $n - 2$ Semireduced Latin Squares. Interestingly, every Reduced Latin Square that is part of these sets of MOLS is symmetric and, in fact, these are the only Reduced Symmetric Latin Squares. This could lead us to a possible conjecture, that every Reduced Symmetric Latin Square produces MOLS. Unfortunately, this proposition was disprooved when the Symmetric Reduced Latin Square of order $n = 4$ in Example 3 failed to generate a set MOLS.

For the moment, we will focus on the study of the six sets of MOLS we had obtained for our previous paper. Theese set of MOLS are:

$$MOLS_1 = \left\{ \begin{pmatrix} 01234 \\ 12340 \\ 23401 \\ 34012 \\ 40123 \end{pmatrix}, \begin{pmatrix} 01234 \\ 23401 \\ 40123 \\ 12340 \\ 34012 \end{pmatrix}, \begin{pmatrix} 01234 \\ 34012 \\ 12340 \\ 40123 \\ 23401 \end{pmatrix}, \begin{pmatrix} 01234 \\ 40123 \\ 34012 \\ 23401 \\ 12340 \end{pmatrix} \right\}$$

$$MOLS_2 = \left\{ \begin{pmatrix} 01234 \\ 12403 \\ 24310 \\ 30142 \\ 43021 \end{pmatrix}, \begin{pmatrix} 01234 \\ 24310 \\ 30142 \\ 43021 \\ 12403 \end{pmatrix}, \begin{pmatrix} 01234 \\ 30142 \\ 43021 \\ 12403 \\ 24310 \end{pmatrix}, \begin{pmatrix} 01234 \\ 43021 \\ 12403 \\ 24310 \\ 30142 \end{pmatrix} \right\}$$

$$MOLS_3 = \left\{ \begin{pmatrix} 01234 \\ 13042 \\ 20413 \\ 34120 \\ 42301 \end{pmatrix}, \begin{pmatrix} 01234 \\ 20413 \\ 13042 \\ 42301 \\ 34120 \end{pmatrix}, \begin{pmatrix} 01234 \\ 34120 \\ 42301 \\ 20413 \\ 13042 \end{pmatrix}, \begin{pmatrix} 01234 \\ 42301 \\ 34120 \\ 13042 \\ 20413 \end{pmatrix} \right\}$$

$$MOLS_4 = \left\{ \begin{pmatrix} 01234 \\ 13420 \\ 24103 \\ 32041 \\ 40312 \end{pmatrix}, \begin{pmatrix} 01234 \\ 24103 \\ 40312 \\ 13420 \\ 32041 \end{pmatrix}, \begin{pmatrix} 01234 \\ 32041 \\ 13420 \\ 40312 \\ 24103 \end{pmatrix}, \begin{pmatrix} 01234 \\ 40312 \\ 32041 \\ 24103 \\ 13420 \end{pmatrix} \right\}$$

$$MOLS_5 = \left\{ \begin{pmatrix} 01234 \\ 14023 \\ 20341 \\ 32410 \\ 43102 \end{pmatrix}, \begin{pmatrix} 01234 \\ 20341 \\ 14023 \\ 43102 \\ 32410 \end{pmatrix}, \begin{pmatrix} 01234 \\ 32410 \\ 43102 \\ 20341 \\ 14023 \end{pmatrix}, \begin{pmatrix} 01234 \\ 43102 \\ 32410 \\ 14023 \\ 20341 \end{pmatrix} \right\}$$

$$MOLS_6 = \left\{ \begin{pmatrix} 01234 \\ 14302 \\ 23140 \\ 30421 \\ 42013 \end{pmatrix}, \begin{pmatrix} 01234 \\ 23140 \\ 30421 \\ 42013 \\ 14302 \end{pmatrix}, \begin{pmatrix} 01234 \\ 30421 \\ 42013 \\ 14302 \\ 23140 \end{pmatrix}, \begin{pmatrix} 01234 \\ 42013 \\ 14302 \\ 23140 \\ 30421 \end{pmatrix} \right\}$$

We can see that every Semireduced Latin Square in a given set can be obtained by permuting the last $n-1$ rows of the Reduced Latin Square in that same set. Let us denote the set of these permutations as **MOLS Generating Permutation Sets**.

Example 7. *Let A be the following set of $n-1$ MOLS of order $n=4$:*

$$A = \left\{ \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{pmatrix} \right\}$$

Since each Latin Square in the set is composed of different permutations of the same rows, we label each distinct row by its first element. In this case:

$$\begin{gathered} 0 = 0\ 1\ 2\ 3 \\ 1 = 1\ 0\ 3\ 2 \\ 2 = 2\ 3\ 0\ 1 \\ 3 = 3\ 2\ 1\ 0 \end{gathered}$$

Then, by taking into consideration only the row labels of each Latin Square in the set we obtain a set of row permutations:

$$P: \left\{ \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 1 \\ 2 \end{pmatrix} \right\}$$

so that when these permutations are applied to the Reduced Latin Square:

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

we will obtain the set of MOLS A.

This way of labeling the rows is particularly useful since we only need to look at the first column of the Latin Square to determine its permutation.

For the 6 sets of MOLS of order $n = 5$ previously stated, we found that each one of them could be constructed by applying one of the following three different MOLS Generating Permutation Sets:

$$P_A : \left\{ \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 4 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 1 \\ 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \\ 3 \\ 2 \\ 1 \end{pmatrix} \right\}$$

$$P_B : \left\{ \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 3 \\ 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 4 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \\ 1 \\ 2 \\ 3 \end{pmatrix} \right\}$$

$$P_C : \left\{ \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \\ 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 4 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 4 \\ 3 \\ 1 \\ 2 \end{pmatrix} \right\}$$

Furthermore, each one of the MOLS Generating Permutation Sets is associated to exactly 2 of the 6 sets of MOLS previously mentioned at the beginning of this section. If 2 or more set of MOLS can be obtained by applying the same MOLS Generating Permutation Set to different Reduced Latin Squares, we say that these MOLS are **Permutation Equivalent**.

$MOLS_1$ and $MOLS_4$ use P_A
$MOLS_2$ and $MOLS_6$ use P_B
$MOLS_3$ and $MOLS_5$ use P_C

Then,

$MOLS_1$ and $MOLS_4$ are Permutation Equivalent.
$MOLS_2$ and $MOLS_6$ are Permutation Equivalent.
$MOLS_3$ and $MOLS_5$ are Permutation Equivalent.

This means that when the P_A permutation is applied to the Reduced Latin Sqaures of $MOLS_1$ and $MOLS_4$, the row permutations specified will produce $MOLS_1$ and $MOLS_4$ respectively.

4 Latin Square Generating Polynomials

As we have previously stated, the elements of a Latin Squares of order n are usually represented with numbers from 0 to $n-1$. These numbers can be associated to the elements in a finite field $\mathbb{F}_q$, given that $n = q$ is a prime power.

A Latin Square can be constructed by evaluating a bivariate polynomial $p(x, y)$ over $\mathbb{F}_q^2$. Such polynomial is called a **Latin Square Generating Polynomial**.

Example 8. *Let $p(x, y)$ be the bivariate polynomial $x + y$ over $\mathbb{F}_q$, where $q = 2^2$. Then,*

$$\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha + 1 = \alpha^2\}$$

$$\begin{array}{llll} p(0,0) = 0 & p(0,1) = 1 & p(0,\alpha) = \alpha & p(0,\alpha^2) = \alpha^2 \\ p(1,0) = 1 & p(1,1) = 0 & p(1,\alpha) = \alpha^2 & p(1,\alpha^2) = \alpha \\ p(\alpha,0) = \alpha & p(\alpha,1) = \alpha^2 & p(\alpha,\alpha) = 0 & p(\alpha,\alpha^2) = 1 \\ p(\alpha^2,0) = \alpha^2 & p(\alpha^2,1) = \alpha & p(\alpha^2,2) = 1 & p(\alpha^2,\alpha^2) = 0 \end{array}$$

This generates the following Latin Square:

$$\begin{pmatrix} 0 & 1 & \alpha & \alpha^2 \\ 1 & 0 & \alpha^2 & \alpha \\ \alpha & \alpha^2 & 0 & 1 \\ \alpha^2 & \alpha & 1 & 0 \end{pmatrix}$$

Which can be associated to

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

4.1 Finding a Latin Square Generating polynomial.

Any function defined over a finite field can be represented by a polynomial whose coefficients recide in that same field [2]. Lagrange's Interpolation formula provides us with a way to construct such a polynomial. Let L be

a Latin Square of order q, q a prime power, where each Latin Square entry is denoted $L_{c_1c_2}$, for $(c_1, c_2) \in \mathbb{F}_q^2$. Let $f : \mathbb{F}_q^2 \to \mathbb{F}_q$ be a bijective function such that $f(c_1, c_2) = L_{c_1c_2}$. The function $f(c_1, c_2)$ can be represented by a unique polynomial $p(x, y)$ over $\mathbb{F}_q$ of degree at most $q - 1$ in each variable [1]. The following is a variation of Lagrange's Interpolation Formula to obtain a polynomial $p(x, y)$ representing a bivariate function $f(c_1, c_2)$ over a finite field $\mathbb{F}_q^2$.

$$p(x, y) = \sum_{(c_1,c_2)\in\mathbb{F}_q^2} (f(c_1, c_2)(1 - (x - c_1)^{q-1})(1 - (y - c_2)^{q-1}))$$

We used this formula to find the Latin Square Generating Polynomials for the Reduced Latin Squares of each set of MOLS for $n = 5$ previously stated:

- $\begin{pmatrix} 01234 \\ 12340 \\ 23401 \\ 34012 \\ 40123 \end{pmatrix} \Rightarrow x + y$
- $\begin{pmatrix} 01234 \\ 12403 \\ 24310 \\ 30142 \\ 43021 \end{pmatrix} \Rightarrow x + y + x^3y^3 + 2x^3y + x^2y^2 + 3x^2y + 2xy^3 + 3xy^2 + 3xy$
- $\begin{pmatrix} 01234 \\ 13042 \\ 20413 \\ 34120 \\ 42301 \end{pmatrix} \Rightarrow x + y + 3x^3y^3 + 4x^3y + 2x^2y^2 + 2x^2y + 4xy^3 + 2xy^2 + 4xy$
- $\begin{pmatrix} 01234 \\ 13420 \\ 24103 \\ 32041 \\ 40312 \end{pmatrix} \Rightarrow x + y + 3x^3y^2 + 3x^2y^3$

[1] Theorem 1.6.3 in [2]

- $\begin{pmatrix} 01234 \\ 14023 \\ 20341 \\ 32410 \\ 43102 \end{pmatrix} \Rightarrow x + y + 2x^3y^3 + x^3y + 3x^2y^2 + 2x^2y + xy^3 + 2xy^2 + xy$

- $\begin{pmatrix} 01234 \\ 14302 \\ 23140 \\ 30421 \\ 42013 \end{pmatrix} \Rightarrow x + y + 4x^3y^3 + 3x^3y + 4x^2y^2 + 3x^2y + 3xy^3 + 3xy^2 + 2xy$

Note that each Latin Square Generating Polynomial that generates the Symmetric Reduced Latin Squares is symmetric as well. We define a **Symmetric Polynomial** as a polynomial $p(x, y)$ such that $p(x, y) = p(y, x)$. Since $L_{ij} = p(i, j)$ and $L_{ji} = p(j, i)$, it follows that $L_{ij} = p(i, j) = p(j, i) = L_{ji}$. Then $L_{ij} = L_{ji}$ for every $0 \leq (i, j) < n$ and, consecuently, $L = L^T$. Therefore if $p(i, j)$ is a symmetric Latin Square Generating Polynomial, then L is a Symmetric Latin Square. Likewise, if $L_{i,j}$ is symmetric then $L_{ij} = L_{ji}$, since $p(i, j) = L_{ij}$ and $p(j, i) = L_{ji}$, it follows that $p(i, j) = L_{ij} = L_{ji} = p(j, i)$. Therefore if L is a Symmetric Latin Square, then $p(i, j)$ is a symmetric Latin Square Generating Polynomial.

Proposition 4.1. *Let A be a Latin Square of order q, q a prime power, and let $p(x, y)$ be the Latin square Generating Polynomial associated with A. A is a Symmetric Latin Square if and only if $p(x, y)$ is symmetric.*

4.2 Coefficient Table

Comparing polynomials and looking for paterns can be confusing and sometimes dificult. To facilitate this, we compare instead the coefficient tables generated by each polynomial.

To create the **coefficient table** for a given bivariate polynomial $p(x, y)$, first one must break down the polynomial into terms. We then associate a bivariate polynomial to a 2-dimensional $n \times n$ array by associating the monomial $x^a y^b$ to the entry in column a, row b. This is, the entry in (a, b) is the coefficient C of the term $C \cdot x^a y^b$.

Example 9. *Let* $p(x, y) = 3x + y + 2xy + x^2y + 2x^3$. *This can be rewritten as* $p(x, y) = 3x^1y^0 + x^0y^1 + 2x^1y^1 + x^2y^1 + 2x^3y^0$. *Then the coefficient table for* p *is:*

	0	*1*	*2*	*3*
0		*3*		*2*
1	*1*	*2*	*1*	
2				
3				

The entry in (a, b) *is left blank or is* 0 *if and only if* $C \cdot x^a y^b = 0$.

Appendix A shows the coefficient table representation for $MOLS_1$ through $MOLS_6$ grouped by Permutation Equivalence.

For now we turn our focus on $MOLS_2, MOLS_3, MOLS_5$ and $MOLS_6$. The elements in each MOLS set correspond to one of the following table structures with X in the non-zero monomials:

	0	1	2	3	4
0		X			
1	X	X	X	X	
2		X	X		
3		X		X	
4					

	0	1	2	3	4
0		X	X	X	
1	X	X	X		
2		X	X	X	
3		X		X	
4					

	0	1	2	3	4
0				X	
1	X	X	X	X	
2			X	X	
3		X		X	
4					

	0	1	2	3	4
0		X	X	X	
1	X		X	X	
2		X	X	X	
3		X		X	
4					

Let A and B be coefficient tables. A and B are **coefficient tables of similar structure** if for every non-zero term $C_1 \cdot x^a y^b$ in A there is a non-zero term $C_2 \cdot x^a y^b$ in B (C_1 not necessarily equal to C_2), and every other term in both A and B is zero.

Example 10. *Let* A *and* B *be coefficient tables of similar structure from* $MOLS_2$ *and* $MOLS_6$ *respectively.*

A

	0	1	2	3	4
0		1			
1	1	3	3	2	
2		3	1		
3		2		1	
4					

B

	0	1	2	3	4
0		1			
1	1	2	3	3	
2		3	4		
3		3		4	
4					

Let $C_1 \cdot x^a y^b$ and $C_2 \cdot x^a y^b$ correspond to the terms in A and B respectively. For every marked entry (a, b), $C_1 = C_2$. on the other hand, for every unmarked entry (a, b), $C_1 + C_2 = 5$. This can be seen in **Example 10**. *Appendix A* shows that this pattern occurs for every pair of coefficient tables of similar structure that are in the same permutation equivalent set of MOLS[2].

Another interesting pattern arises when grouping all of the coefficient tables of $MOLS_2$, $MOLS_3$, $MOLS_5$ and $MOLS_6$ by table structure alone. This is, we will clasify the coefficient tables of $MOLS_2$, $MOLS_3$, $MOLS_5$ and $MOLS_6$, not by permutation equivalence like we have been doing so far, but by similar coefficient table structures. *Appendix B* shows this clasification. Let us take the first group of similar structured coefficient tables:

T_1

	0	1	2	3	4
0		1			
1	1	3	3	2	
2		3	1		
3		2		1	
4					

T_2

	0	1	2	3	4
0		1			
1	1	2	3	3	
2		3	4		
3		3		4	
4					

T_3

	0	1	2	3	4
0		1			
1	1	4	2	4	
2		2	2		
3		4		3	
4					

T_4

	0	1	2	3	4
0		1			
1	1	1	2	1	
2		2	3		
3		1		2	
4					

Note that each unhighlighted entry $T_k(i, j)$ where $1 \leq k \leq 4$ and $0 \leq (i, j) \leq 4$, is such that $T_k(i, j) \in \mathbb{Z}_n/\{0\}$ and $T_1(i, j) \neq T_2(i, j) \neq T_3(i, j) \neq T_4(i, j)$.

[2]The coeficient tables in *Appendix A* are organized in such way that tables of the same structure between Permutation Equivalent sets are next to each other.

Example 11. *Consider the four previously stated coefficient tables grouped by table structure alone (T_1, T_2, T_3 and T_4). Note that*

- $T_1(1,1) = 3, \quad T_2(1,1) = 2, \quad T_3(1,1) = 4, \quad T_4(1,1) = 1$
- $T_1(3,1) = 2, \quad T_2(3,1) = 3, \quad T_3(3,1) = 4, \quad T_4(3,1) = 1$
- $T_1(2,2) = 1, \quad T_2(2,2) = 4, \quad T_3(2,2) = 2, \quad T_4(2,2) = 3$
- $T_1(1,3) = 2, \quad T_2(1,3) = 3, \quad T_3(1,3) = 4, \quad T_4(1,3) = 1$
- $T_1(3,3) = 1, \quad T_2(3,3) = 4, \quad T_3(3,3) = 3, \quad T_4(3,3) = 2$

This pattern remains consistant in the other three groups of similar structure coefficient tables.

5 Another MOLS Construction: MOLS Generating Matrices

Previously, we introduced 3 MOLS generating permutation sets (P_A, P_B, P_C), which, when aplied to a given symetric reduced Latin Square, will generate one of the 6 sets of MOLS we are studying. With this in mind we present another form of MOLS construction, permutating the rows of a Latin Square by multiplying by another matrix wich we will call a MOLS Generating Matrix. Let G be a $n \times n$ matrix with exactly one entry 1 in each row and each column, the rest of the entries being 0, and let LS_1 be a Latin Square of order n. G is a **MOLS Generating Matrix** if $\{G \times LS_1 = LS_2, G \times LS_2 = LS_3, \ldots, G \times LS_{n-2} = LS_{n-1}, G \times LS_{n-1} = LS_1\}$ is a set of MOLS.

Example 12. *Let G be an $n \times n$ matrix and let LS_1 be the reduced Latin Square in $MOLS_2$.*

$$G = \begin{pmatrix} 10000 \\ 00100 \\ 00010 \\ 00001 \\ 01000 \end{pmatrix} \qquad LS_1 = \begin{pmatrix} 01234 \\ 12403 \\ 24310 \\ 30142 \\ 43021 \end{pmatrix}$$

then,

- $G \times LS_1 = \begin{pmatrix} 01234 \\ 24310 \\ 30142 \\ 43021 \\ 12403 \end{pmatrix} = LS_2$

- $G \times LS_2 = \begin{pmatrix} 01234 \\ 30142 \\ 43021 \\ 12403 \\ 24310 \end{pmatrix} = LS_3$

- $G \times LS_3 = \begin{pmatrix} 01234 \\ 43021 \\ 12403 \\ 24310 \\ 30142 \end{pmatrix} = LS_4$

- $G \times LS_4 = \begin{pmatrix} 01234 \\ 43021 \\ 12403 \\ 24310 \\ 30142 \end{pmatrix} = LS_1$

The set formed by $\{LS_1, LS_2, LS_3, LS_4\}$ *is the set* $MOLS_2$*. Therefore* G *is a MOLS Generating Matrix.*

Note: The MOLS Generating Matrix must always be the lefthand operand ($G \times LS$) to pemrute the rows of the Latin Square. If it is the righthand operand it will permute the Latin Square's columns.

Every one of the 6 MOLS is associated with a MOLS Generating Matrix: $\begin{pmatrix} 10000 \\ 00100 \\ 00001 \\ 01000 \\ 00010 \end{pmatrix}$ is a MOLS Generating Matrix for $MOLS_1$ and $MOLS_4$.

$$\begin{pmatrix} 10000 \\ 00100 \\ 00010 \\ 00001 \\ 01000 \end{pmatrix}$$ is a MOLS Generating Matrix for $MOLS_2$ and $MOLS_6$.

$$\begin{pmatrix} 10000 \\ 00010 \\ 00001 \\ 00100 \\ 01000 \end{pmatrix}$$ is a MOLS Generating Matrix for $MOLS_3$ and $MOLS_5$.

The MOLS Generating Matrices mentioned above are not the only ones associated with that particular set of MOLS. If G is a MOLS Generating Matrix for $MOLS_k$ then G^T is also a MOLSGenerating Matrix for $MOLS_k$.

5.1 Finding a MOLS Generating Matrix

Let LS be the symetric reduced Latin Square of $MOLS_3$. We first find a transversal in LS such as:

$$\begin{pmatrix} 0\,1\,234 \\ 13\,0\,42 \\ 2041\,3 \\ 341\,2\,0 \\ 4\,2301 \end{pmatrix}$$

By replacing each entry in the transversal with 1 and every other entry with 0 we get the MOLS Generating Matrix:

$$G = \begin{pmatrix} 010000 \\ 00100 \\ 00001 \\ 00010 \\ 10000 \end{pmatrix}$$

which gives us the set of MOLS:

$$MOLS_G = \left\{ \begin{pmatrix} 01234 \\ 13042 \\ 20413 \\ 34120 \\ 42301 \end{pmatrix}, \begin{pmatrix} 13042 \\ 20413 \\ 42301 \\ 34120 \\ 01234 \end{pmatrix}, \begin{pmatrix} 20413 \\ 42301 \\ 01234 \\ 34120 \\ 13042 \end{pmatrix}, \begin{pmatrix} 42301 \\ 01234 \\ 13042 \\ 34120 \\ 20413 \end{pmatrix} \right\}$$

Note that, although they $MOLS_G$ and $MOLS_3$ share the same symetric reduced Latin Square, $MOLS_G \neq MOLS_3$. Furthermore, every transversal found in a symetric reduced Latin Square of order 5 results in different sets of MOLS.

References

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

[2] G. Mullen, & C. Mummert *Finite Fields and Applications*, p. cm (Student mathematical library; v.41), American Mathematical Society, Rhode Island, 2007.

Appendix A Coefficient table representation for $MOLS_1$ through $MOLS_6$ grouped by Permutation Equivalence.

$MOLS_1$

	0	1	2	3	4
0		1			
1	1				
2					
3					
4					

	0	1	2	3	4
0		2			
1	1				
2					
3					
4					

	0	1	2	3	4
0		3			
1	1				
2					
3					
4					

	0	1	2	3	4
0		4			
1	1				
2					
3					
4					

$MOLS_4$

	0	1	2	3	4
0		1			
1	1				
2				3	
3			3		
4					

	0	1	2	3	4
0		2			
1	1				
2				4	
3			2		
4					

	0	1	2	3	4
0		3			
1	1				
2				1	
3			2		
4					

	0	1	2	3	4
0		4			
1	1				
2				2	
3			3		
4					

$MOLS_2$

	0	1	2	3	4
0		1			
1	1	3	3	2	
2		3	1		
3		2		1	
4					

	0	1	2	3	4
0		1	4	1	
1	1	3	1		
2		4	2	4	
3		3		4	
4					

	0	1	2	3	4
0				3	
1	1	4	2	4	
2			4	4	
3		2		1	
4					

	0	1	2	3	4
0		2	1	1	
1	1		4	4	
2		3	3	2	
3		3		4	
4					

$MOLS_6$

	0	1	2	3	4
0		1			
1	1	2	3	3	
2		3	4		
3		3		4	
4					

	0	1	2	3	4
0		1	1	1	
1	1	2	1		
2		4	3	4	
3		2		1	
4					

	0	1	2	3	4
0				3	
1	1	1	2	1	
2			1	4	
3		3		4	
4					

	0	1	2	3	4
0		2	4	1	
1	1		4	1	
2		3	2	2	
3		2		1	
4					

$MOLS_3$

	0	1	2	3	4
0		1			
1	1	4	2	4	
2		2	2		
3		4		3	
4					

	0	1	2	3	4
0				2	
1	1	2	3	3	
2			3	4	
3		4		3	
4					

	0	1	2	3	4
0		2	2	4	
1	1	4	4		
2		1	4	4	
3		1		2	
4					

	0	1	2	3	4
0		2	3	4	
1	1		1	3	
2		2	1	2	
3		1		2	
4					

$MOLS_5$

	0	1	2	3	4
0		1			
1	1	1	2	1	
2		2	3		
3		1		2	
4					

	0	1	2	3	4
0				2	
1	1	3	3	2	
2			2	4	
3		1		2	
4					

	0	1	2	3	4
0		2	2	4	
1	1	1	4		
2		1	1	4	
3		4		3	
4					

	0	1	2	3	4
0		2	2	4	
1	1		1	2	
2		2	4	2	
3		4		3	
4					

Appendix B Coefficient tables grouped by structure similarity.

Group A:

	0	1	2	3	4
0		1			
1	1	3	3	2	
2		3	1		
3		2		1	
4					

	0	1	2	3	4
0		1			
1	1	2	3	3	
2		3	4		
3		3		4	
4					

	0	1	2	3	4
0		1			
1	1	4	2	4	
2		2	2		
3		4		3	
4					

	0	1	2	3	4
0		1			
1	1	1	2	1	
2		2	3		
3		1		2	
4					

Group B:

	0	1	2	3	4
0		1	4	1	
1	1	3	1		
2		4	2	4	
3		3		4	
4					

	0	1	2	3	4
0		1	1	1	
1	1	2	1		
2		4	3	4	
3		2		1	
4					

	0	1	2	3	4
0		2	2	4	
1	1	4	4		
2		1	4	4	
3		1		2	
4					

	0	1	2	3	4
0		2	3	4	
1	1	1	4		
2		1	1	4	
3		4		3	
4					

Group C:

	0	1	2	3	4
0				3	
1	1	4	2	4	
2			4	4	
3		2		1	
4					

	0	1	2	3	4
0				3	
1	1	1	2	1	
2			1	4	
3		3		4	
4					

	0	1	2	3	4
0				2	
1	1	2	3	3	
2			3	4	
3		4		3	
4					

	0	1	2	3	4
0				2	
1	1	3	3	2	
2			2	4	
3		1		2	
4					

Group D:

	0	1	2	3	4
0		2	1	1	
1	1		4	4	
2		3	3	2	
3		3		4	
4					

	0	1	2	3	4
0		2	4	1	
1	1		4	1	
2		3	2	2	
3		2		1	
4					

	0	1	2	3	4
0		2	3	4	
1	1		1	3	
2		2	1	2	
3		1		2	
4					

	0	1	2	3	4
0		2	2	4	
1	1		1	2	
2		2	4	2	
3		4		3	
4					