Some properties of latin squares - Study of mutually orthogonal latin squares

Jeranfer Bermúdez
University of Puerto Rico, Río Piedras
Computer Science Department

Lourdes M. Morales
University of Puerto Rico, Río Piedras
Computer Science Department

December 2009

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 orthogonal if, when superimposed, all the pairs that are formed are different. In our research we look for new constructions of maximal sets of mutually orthogonal latin squares (MOLS). We present some partial results and conjectures related to this.

1 Preliminaries

Here we give some necessary background. First we start with some types of latin squares.

1.1 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 $n = 5$.

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

Then,

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

Note that $A = A^T$ whereas $B \neq B^T$. Thus, A is a symmetric latin square and B is not.

Also, note that the latin square of order $n = 4$ in Example 1 is also an example of a symmetric latin square.

1.2 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 $0 \leq i < n$. 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.

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.

1.3 Mutually orthogonal latin squares

In our work we focused on constructing sets of mutually orthogonal latin squares, so here are a few definitions and some known facts.

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

Example 6. Let L_1, L_2 and L_3 be three latin squares of order $n = 4$:

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

Then,

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

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

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.

Definition 5. A set of $t \geq 2$ MOLLS 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].

2 Constructing sets of MOLS

2.1 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 7. 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 $q = 4$.

2.2 Isomorphic latin squares

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 $q - 1$ MOLS of order q that are different from the desarguesian set. We shall consider two sets different if, as matrices, the squares are different. Here we present some of the concepts discussed in [2] concerning this matter. The first is a definition that presents the fact that we can take a complete set of MOLS of order q and get another distinct complete set of MOLS of order q 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.

2.3 Transversals

In our research we worked with transversals in latin squares to find permutation matrices.

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 8. 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 9. Let L be the latin square of order $n = 5$ and T be the transversal in L from Example **8**. 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 lefthand 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 righthand 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 lefthand operand we are permuting the rows of L and if the permutation matrix is the righthand operand we are permutation the columns of L.

Since we are looking for permutation matrices with special characteristics we must first see if there exists transversals for any given n. In [5] they discuss some important facts about transversals that help us determine whether or not there will exist a transversal in a latin square of order n. Here we present the ones that are essential to our research.

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

So, some latin squares have no transversals at all.

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.*

Note that the addition tables of $\mathbb{Z}_{2n}$, with $n \geq 1$, have an even order and zero transversals (Proposition 1), which agrees with theorem 4 because zero is an even number. So, 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.

2.4 MOLS generating matrix

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.

Example 10. 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 a 5×5 permutation matrix (see Examples **8** and **9**).

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

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.

In [1] the following conjecture was proposed:

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.

Later in §3 we'll present a counterexample to this conjecture.

3 Main results

In our work we focused 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. So, we begin this section with the following result:

3.1 $q = 5$

So far when we take a symmetric RLS of order $q = 5$ we get 14 transversals (15 if we count the identity matrix $I_{5\times 5}$), ten of which satisfy the conditions for Conjecture 3 and generate complete sets of MOLS of order $n = 5$. We have only worked with the symmetric RLSs of order $q = 5$ contained in the sets $MOLS_1$ (the Cayley Table of order $q = 5$) and $MOLS_4$ from [1]. But, we still haven't worked with all the symmetric RLSs from the complete sets of MOLS in [1] ($MOLS_2$, $MOLS_6$, $MOLS_3$ and $MOLS_5$).

3.2 $q = 7$

For $q = 7$ we only worked with the Cayley Table of order $q = 7$ (CT_7), but it was important because it proved 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 a permutation matrix G for CT_7 with one 1 in 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.

4 Future Work

One of our future goals is to come up with a way to construct or find the biggest possible sets of MOLS, specifically for $n = 6$, so that maybe someday we can generalize for all n. Another of our goals is to improve the MOLS Generating Matrix Conjecture.

5 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 support of the NSF through the S-STEM and The Puerto Rico Luis Stokes Alliance for Minority Participation (PR-LSAMP) programs.

6 Appendix: Maple Procedures

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

6.1 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:
```

6.2 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:
```

6.3 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 righthand 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.