Θ-critical sets of Latin squares having Θ as a principal autotopism

R. M. Falcón Ganfornina
rafalgan@us.es
Department of Geometry and Topology
University of Seville (Spain).

ABSTRACT: Any principal autotopism Θ of a Latin square $L \in LS(n)$, whose elements are in a set N of n symbols, gives a significant information about the symmetry of L. Although Θ-critical sets of L can be then used in Cryptography to get the access structure of a secret sharing scheme [1, 3, 7], the size of the smallest one is still an open problem. Because Θ can be decomposed into triples of a partial Latin square [6], we propose in this paper an algorithm depending on the order of L allowing to give an upper bound of the previous size. This algorithm reduces the previous problem to the calculus of the size of the smallest critical set of a Latin subrectangle of L of order $k \times n$, which can be decomposed at the same time into k regions, each of them having all the symbols of N.

1 Introduction

A Latin square $L = (l_{ij})$ of order n is a $n \times n$ array with elements chosen from a set $N = \{0, 1, ..., n-1\}$, such that each symbol occurs precisely once in each row and each column. The orthogonal array representation of L is the set of n^2 triples $\{(i, j, l_{ij}) : i, j \in N\}$. The set of Latin squares of order n is denoted by $LS(n)$.

$$\begin{pmatrix} 1 & 2 & 0 & 3 \\ 3 & 1 & 2 & 0 \\ 0 & 3 & 1 & 2 \\ 2 & 0 & 3 & 1 \end{pmatrix} \in LS(4)$$

An isotopism of a Latin square L is a triple $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n = S_n \times S_n \times S_n$, where S_n is the symmetric group on N and α, β and γ are respectively, permutations of rows, columns and symbols of L. The resulting square L^Θ is also a Latin square and it is said to be isotopic to L.

$$\begin{cases} L = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \\ \\ \Theta = ((0\ 1)(2\ 3), (1\ 2), \epsilon) \end{cases} \Rightarrow L^\Theta = \begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 2 & 0 & 3 & 1 \end{pmatrix}$$

If $\gamma = \epsilon$, the identity map on N, Θ is called a principal isotopism. An isotopism which maps L to itself is an autotopism. The stabilizer subgroup of L in $\mathcal{I}_n$ is its autotopism group, $\mathcal{U}(L) = \{\Theta \in \mathcal{I}_n : L^\Theta = L\}$. Fixed $\Theta \in \mathcal{I}_n$, the set of all Latin squares L such that $\Theta \in \mathcal{U}(L)$ is denoted by $LS(\Theta)$. Finally, the cardinality of $LS(\Theta)$ is denoted by $\Delta(\Theta)$.

A partial Latin square P of order n is a $n \times n$ array with elements chosen from a set of n symbols, such that each symbol occurs at most once in each row and in each column. The set of partial Latin squares of order n is denoted by $PLS(n)$. Isotopisms of partial Latin squares are defined in a similar way than that of Latin squares, although now $\gamma(\emptyset) = \emptyset$. In particular, the sets $\mathcal{U}(P)$ and $PLS(\Theta)$ are similarly defined.

$$\begin{pmatrix} 0 & - & - & 3 \\ - & 0 & 3 & - \\ 2 & - & 1 & 0 \\ 3 & 2 & 0 & - \end{pmatrix} \in PLS(4)$$

It is said that a fixed $P \in PLS(n)$ can be uniquely completed to a Latin square $L \in LS(n)$ if L is the unique Latin square such that $P \subseteq L$ and it is denoted $P \in UC(L)$. If any proper subset of P can be completed to two distinct Latin squares, it is said that P is a critical set of L and it is denoted $P \in CS(L)$.

$$\begin{pmatrix} 0 & - & - & 3 \\ - & 0 & - & - \\ 2 & - & 1 & - \\ - & - & - & - \end{pmatrix} \in CS(L) \rightarrow \begin{pmatrix} 0 & - & - & 3 \\ - & 0 & - & - \\ 2 & 3 & 1 & 0 \\ - & - & - & - \end{pmatrix} \rightarrow \begin{pmatrix} 0 & - & - & 3 \\ - & 0 & 3 & - \\ 2 & 3 & 1 & 0 \\ 3 & - & 0 & - \end{pmatrix} \rightarrow \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix}$$

Fixed $L \in LS(n)$, $scs(L)$ denotes the size of the smallest critical set of L and $scs(n)$ denotes the minimum of $scs(L)$ for all $L \in LS(n)$.

A secret sharing scheme is a method of sharing a secret key K, by giving n pieces of information called shares to n participants, in such a way that K can be reconstructed from certain authorized groups of shares and it cannot be done from unauthorized groups of them. The access structure Γ is the set of all the previous authorized groups. An example of this by using Latin squares is the following [2, 8]: Fixed a Latin square $L = (l_{ij}) \in LS(n)$ as the secret key and made public its order n, each share is then a triple $(i, j, l_{ij}) \in L$ and the set of all the used triples is denoted by S. So, if some participants get a critical set of L by sharing its corresponding triples, they will obtain as consequence the secret key L. The access structure is then $\Gamma = \{P \in PLS(n) : P \subseteq \bigcup_S \{(i, j, l_{ij})\} \subseteq L \text{ and } \exists C \in CS(L) \text{ such that } C \subseteq P\}$.

$$K = L = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix}; \qquad S = \begin{pmatrix} 0 & - & - & 3 \\ - & 0 & 3 & - \\ 2 & - & 1 & 0 \\ 3 & 2 & 0 & - \end{pmatrix} \Rightarrow \Gamma = \left\{ \begin{pmatrix} 0 & - & - & 3 \\ - & 0 & - & - \\ 2 & - & 1 & - \\ - & - & - & - \end{pmatrix}, \begin{pmatrix} 0 & - & - & - \\ - & - & 3 & - \\ 2 & - & - & 0 \\ - & 2 & - & - \end{pmatrix}, ... \right\}$$

Given $P \in PLS(n)$, contained in L, and $\mathfrak{F} \subseteq \mathcal{U}(L)$, it is defined the extended autotopy $P^{\mathfrak{F}} = \bigcup_{\Theta \in \mathfrak{F}} P^\Theta \in PLS(n)$.

$$\begin{cases} P = \begin{pmatrix} 0 & - & - & - \\ - & - & - & - \\ - & - & - & - \\ - & - & - & - \end{pmatrix} \\ \\ \Theta_1 = (\epsilon, (0\ 1\ 2\ 3), (0\ 3\ 2\ 1)) \\ \Theta_2 = ((0\ 1\ 2\ 3), \epsilon, (0\ 3\ 2\ 1)) \end{cases} \Rightarrow P^{\{\Theta_1, \Theta_2\}} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & - & - & - \\ 2 & - & - & - \\ 3 & - & - & - \end{pmatrix}$$

Fixed $L \in LS(n)$, $P \in PLS(n)$ contained in L and $\mathfrak{F} \subseteq \mathcal{U}(L)$, it is defined $\mathfrak{F}(P) = P^{<\mathfrak{F}>}$, where $<\mathfrak{F}>$ is the subgroup of $\mathcal{U}(L)$ generated by $\mathfrak{F}$. Then, P is uniquely $\mathfrak{F}$-completable to L, which is denoted as $P \in UC_{\mathfrak{F}}(L)$, if $\mathfrak{F}(P) \in UC(L)$. Furthermore, P is a $\mathfrak{F}$-critical set of L if $P \in UC_{\mathfrak{F}}(L)$ and $Q \notin UC_{\mathfrak{F}}(L)$ for all $Q \subset P$.

$$\mathfrak{F} = \{(\epsilon, (0\ 1\ 2\ 3)), (0\ 3\ 2\ 1))\} \Rightarrow \begin{pmatrix} 0 & - & - & - \\ - & 0 & - & - \\ 2 & - & - & - \\ - & - & - & - \end{pmatrix} \text{ is uniquely } \mathfrak{F}-\text{completable to } \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix}$$

In [5], fixed a Latin square $L = (l_{ij}) \in LS(n)$ as the secret key and made public its order n, it is allowed to consider triples $(i, j, l_{ij}) \in L$ and a set $\digamma$ of principal autotopisms $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{U}(L)$ as shares of a secret sharing scheme. So, if some participants get a $\mathfrak{F}$-critical set of L, being $\mathfrak{F} \subseteq \digamma$, by sharing its corresponding triples and principal autotopisms, they will obtain as consequence the secret key L.

$$K = L = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix}; \qquad S = \left\{ \begin{pmatrix} 0 & - & - & 3 \\ - & 0 & 3 & - \\ 2 & - & 1 & 0 \\ 3 & 2 & 0 & - \end{pmatrix} \right\} \Rightarrow \begin{cases} \text{Authorized Groups:} \\ \\ \{\Theta_1, \Theta_2\} \bigcup \{(i_0, j_0, l_{i_0 j_0})\} \\ \\ \{\Theta_1\} \bigcup \begin{pmatrix} 0 & - & - & - \\ - & 0 & - & - \\ 2 & - & - & - \\ - & - & - & - \end{pmatrix} \end{cases}$$

2 The Canonical Construction Path Method (CCPM)

Proposition 1 ([5]). *Let $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be a non-trivial isotopism. If one of the permutations α, β or γ is equal to ϵ, then $\Delta(\Theta) > 0$ if and only if the other two permutations are both the composition of k cycles of length $\frac{n}{k}$.*

From now on, $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$ will be a non-trivial principal isotopism, such that $\Delta(\Theta) > 0$. So, $\alpha = C_0^\alpha \circ C_1^\alpha \circ ... \circ C_{k-1}^\alpha$ and $\beta = C_0^\beta \circ C_1^\beta \circ ... \circ C_{k-1}^\beta$, where $C_i^\delta = \left(c_{i,0}^\delta\ c_{i,1}^\delta\ ...\ c_{i,\frac{n}{k}-1}^\delta\right)$ is a cycle of length $\frac{n}{k}$ for all $\delta \in \{\alpha, \beta\}$. Now, fixed $i \in \{0, 1, ..., k-1\}$ and $\delta \in \{\alpha, \beta\}$, we will define the set $S_i^\delta = \{c_{i,j}^\delta : j \in \{0, 1, ..., \frac{n}{k} - 1\}\}$. If we want to find a Latin square $L = (l_{ij}) \in LS(\Theta)$, then we can use the CCPM. This algorithm allows to decompose L in the subsquares $R_L^{i,j} = \{(c_{i,s}^\alpha, c_{j,t}^\beta, l_{c_{i,s}^\alpha\ c_{j,t}^\beta}) : s, t \in \{0, 1, ..., \frac{n}{k} - 1\}\}$, for all $i, j \in \{0, 1, ..., k-1\}$. Finally, it is useful to define also the following sets $S^{i,j} = \left\{l_{st} : (s, t, l_{st}) \in R_L^{i,j}\right\}$, for all $i, j \in \{0, 1, ..., k-1\}$.

$$\Theta = ((01)(23), (03)(12), \epsilon); \qquad L \in LS(\Theta)?$$

$$\Downarrow$$

$$\left\{ \begin{array}{l} \underline{\text{Step 1:}}\ L \in LS(4) \Rightarrow L = \begin{pmatrix} l_{00} & l_{01} & l_{02} & l_{03} \\ l_{10} & l_{11} & l_{12} & l_{13} \\ l_{20} & l_{21} & l_{22} & l_{23} \\ l_{30} & l_{31} & l_{32} & l_{33} \end{pmatrix} \\ \\ \underline{\text{Step 2:}}\ \text{From the cycles (01) and (03)}: \begin{cases} l_{00} = l_{13} = a \\ l_{03} = l_{10} = d \end{cases} \Rightarrow R_L^{0,0} = \begin{pmatrix} a & - & - & d \\ d & - & - & a \\ - & - & - & - \\ - & - & - & - \end{pmatrix} \\ \\ \underline{\text{Step 3:}}\ \text{From the cycles (01) and (12)} \begin{cases} l_{01} = l_{12} = b \\ l_{02} = l_{11} = c \end{cases} \Rightarrow R_L^{0,1} = \begin{pmatrix} - & b & c & - \\ - & c & b & - \\ - & - & - & - \\ - & - & - & - \end{pmatrix} \\ \\ \underline{\text{Step 4:}}\ \text{From the cycles (23) and (03)} \begin{cases} l_{20} = l_{33} = e \\ l_{23} = l_{30} = h \end{cases} \Rightarrow R_L^{0,1} = \begin{pmatrix} - & - & - & - \\ - & - & - & - \\ e & - & - & h \\ h & - & - & e \end{pmatrix} \\ \\ \underline{\text{Step 3:}}\ \text{From the cycles (23) and (12)} \begin{cases} l_{21} = l_{32} = f \\ l_{22} = l_{31} = g \end{cases} \Rightarrow R_L^{0,1} = \begin{pmatrix} - & - & - & - \\ - & - & - & - \\ - & f & g & - \\ - & g & f & - \end{pmatrix} \end{array} \right\} \Rightarrow L = \begin{pmatrix} a & b & c & d \\ d & c & b & a \\ e & f & g & h \\ h & g & f & e \end{pmatrix}$$

$$\Downarrow$$

$$LS(\Theta) = \left\{ L_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 3 & 0 & 2 \\ 2 & 0 & 3 & 1 \end{pmatrix}; \qquad L_2 = \begin{pmatrix} 2 & 0 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 0 & 3 & 2 & 1 \\ 1 & 2 & 3 & 0 \end{pmatrix}; \qquad ... \right\}$$

3 Partial Latin squares related to principal isotopisms

It is possible to identify Θ with a partial Latin square $P_\Theta = (p_{ij}) \in PLS(\Theta)$ by following the next:

Algorithm 2.

i) We take $p_{0j} = j$ for all $j \in N$.
ii) Fixed $i \notin S_0^\alpha \cup S_0^\beta$, we impose $p_{i0} = i$.
iii) We put in the natural order the elements of $S_0^\alpha \setminus S_0^\beta$ and we assign them consecutively to the elements p_{i0} (also in the natural order) which are still without an assigned value.
iv) Finally, we follow the CCPM.

Θ	$((01)(25)(34), (01)(23)(45), \epsilon)$	$((014)(235), (023)(145), \epsilon)$
P_Θ	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 2 & 5 & 4 \\ 2 & 5 & - & - & - & - \\ 3 & 4 & - & - & - & - \\ 4 & 3 & - & - & - & - \\ 5 & 2 & - & - & - & - \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 0 & 2 & 1 & 4 \\ 1 & - & 5 & 4 & - & - \\ 4 & - & 1 & 5 & - & - \\ 2 & 4 & 3 & 0 & 5 & 1 \\ 5 & - & 4 & 1 & - & - \end{pmatrix}$

Now, fixed $\delta \in S_n$, we define the sets:

$$\begin{cases} PLS_1(\delta) = \{P \in PLS(n) : \exists \gamma \in S_n \text{ such that } P \in PLS((\delta, \gamma, \epsilon))\}, \\ PLS_2(\delta) = \{P \in PLS(n) : \exists \gamma \in S_n \text{ such that } P \in PLS((\gamma, \delta, \epsilon))\}. \end{cases}$$

We can then consider the equivalence relation in the set of principal isotopisms given by: $\Theta_1 \sim \Theta_2 \Leftrightarrow P_{\Theta_1} = P_{\Theta_2}$. So, if $\Theta_1 \sim \Theta_2$ then $LS(\Theta_1) = LS(\Theta_2)$. The equivalence class of each principal isotopism Θ will be denoted by $[\Theta]$. In particular, $|[\Theta]| = \left(\frac{n}{k} - 1\right)!$.

Theorem 3 ([6]). *There exists a bijection between the set of equivalence classes of non-trivial principal isotopisms Θ such that $\Delta(\Theta) > 0$ and the set of partial Latin squares $P = (p_{ij})$ of order n and size $(2k-1) \cdot \left(\frac{n}{k}\right)^2$, such that:*

i) In P, all the cells of its first row and column are filled. Besides, $p_{0j} = j\ \forall j \in N$.
ii) Indeed, there exist $\frac{n}{k}$ rows and $\frac{n}{k}$ columns in P such that all its cells are filled.
iii) There is an unique way of decomposing P in $2k-1$ disjoint blocks B_0, $B_1^r, ..., B_{k-1}^r$, $B_1^c, ..., B_{k-1}^c$, where the blocks corresponding to the filled rows (columns) of P are denoted with the r (c) index. B_0 denotes the block of the intersection of filled rows and columns.
iv) There exist two $\frac{n}{k}$-cycles C_1 and C_2, such that $B_0 \in PLS((C_1, C_2, \epsilon))$. Besides, for all $i \in \{1, 2, ..., k-1\}$, $B_i^r \in PLS_1(C_1)$ and $B_i^c \in PLS_2(C_2)$.

To prove the previous result, it is enough to consider the map $\Theta \rightarrow P_\Theta$. Indeed, fixed a partial Latin square P verifying these properties, we can find a principal isotopism $\Theta = (\alpha, \beta, \epsilon)$ such that $P_\Theta = P$. To obtain it, let $(N, \cdot)$ be the partial quasigroup having P as its multiplication table. Now, we must keep in mind the next:

Algorithm 4.

i) We take $C_0^\alpha = C_1$ and $C_0^\beta = C_2$, in such a way that $c_{0,0}^\alpha = c_{0,0}^\beta = 0$.
ii) For i from 1 to $k-1$, let $m_i^\alpha = c_{i,0}^\alpha$ be the minimum in the natural order of $N \setminus \bigcup_{j=0}^{i-1} S_j^\alpha$. So, $C_i^\alpha = (c_{i,0}^\alpha\ \ p_{c_{i,0}^\alpha 0}/c_{0,1}^\beta\ \ p_{c_{i,0}^\alpha 0}/c_{0,2}^\beta\ ...\ p_{c_{i,0}^\alpha 0}/c_{0,\frac{n}{k}-1}^\beta)$, where / denotes the right division on $(N, \cdot)$.
iii) For j from 1 to $k-1$, let $m_j^\beta = c_{j,0}^\beta$ be the minimum in the natural order of $N \setminus \bigcup_{i=0}^{j-1} S_i^\beta$. So, $C_j^\beta = (c_{j,0}^\beta\ \ c_{0,1}^\alpha \backslash c_{j,0}^\beta\ \ c_{0,2}^\alpha \backslash c_{j,0}^\beta\ ...\ c_{0,\frac{n}{k}-1}^\alpha \backslash c_{j,0}^\beta)$, where $\backslash$ denotes the left division on $(N, \cdot)$.

4 Critical sets related to principal isotopisms

Keeping in mind Theorem 3, we have found a way to identify any non-trivial principal isotopism Θ such that $\Delta(\Theta) > 0$ with a set of triples: those corresponding to the filled cells of P_Θ. However, from Conditions (1) and Algorithm 4, we can obtain Θ starting from a partial Latin square with a smaller size that P_Θ.

		$\Theta = (\alpha, \beta, \epsilon) \in [\Theta]$	
Step 1	$\begin{pmatrix} - & - & - & - & - & - \\ - & 0 & - & 2 & - & 4 \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & 3 & - & - & - & - \\ - & 2 & - & - & - & - \end{pmatrix}$	$\alpha = ((0\ ...\ ?)...(?\ ...\ ?))$ $\beta = ((0\ ...\ ?)...(?\ ...\ ?))$	By Condition (1.1) $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ - & 0 & - & 2 & - & 4 \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & 3 & - & - & - & - \\ - & 2 & - & - & - & - \end{pmatrix}$
Step 2	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ - & 0 & - & 2 & - & 4 \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & 3 & - & - & - & - \\ - & 2 & - & - & - & - \end{pmatrix}$	By Algorithm 4 (i) + (ii) + (iii) $\alpha = ((0\ 1)(2\ ?)(?\ ?))$ $\beta = ((0\ 1)(2\ ?)(?\ ?))$	By Conditions (1.2) + (1.3) $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & - & 2 & - & 4 \\ 2 & - & - & - & - & - \\ 3 & - & - & - & - & - \\ 4 & 3 & - & - & - & - \\ 5 & 2 & - & - & - & - \end{pmatrix}$
Step 3	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & - & 2 & - & 4 \\ 2 & - & - & - & - & - \\ 3 & - & - & - & - & - \\ 4 & 3 & - & - & - & - \\ 5 & 2 & - & - & - & - \end{pmatrix}$	By Algorithm 4 (ii) + (iii) $\alpha = ((0\ 1)(2\ 5)(3\ ?))$ $\beta = ((0\ 1)(2\ 3)(4\ ?))$	
Step 4	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & - & 2 & - & 4 \\ 2 & - & - & - & - & - \\ 3 & - & - & - & - & - \\ 4 & 3 & - & - & - & - \\ 5 & 2 & - & - & - & - \end{pmatrix}$	By Algorithm 4 (ii) + (iii) $\alpha = ((0\ 1)(2\ 5)(3\ 4))$ $\beta = ((0\ 1)(2\ 3)(4\ 5))$	

Let us observe that Step 4 is not necessary. So, we can reduce the previous partial Latin square to the following one:

$$C = \begin{pmatrix} - & - & - & - & - & - \\ - & 0 & - & 2 & - & - \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & 2 & - & - & - & - \end{pmatrix} \Rightarrow scs(\Theta) \leq 3.$$

In general, if we denotes by $scs(\Theta)$ the size of the smallest set of triples equivalent to Θ, we have therefore the following:

Proposition 5. $scs(\Theta) \leq \begin{cases} n-2, \text{ if } k = 1, \\ \left(\frac{n}{k} - 1\right) \cdot (2k-1) - 2, \text{ if } k \neq 1. \end{cases}$.

By the other way, in the previous example, we can not find a partial Latin subsquare of C such that $[\Theta]$ is obtained from it. We will say then that C is a critical set of $[\Theta]$. The set of critical sets of $[\Theta]$ will be denoted by $CS([\Theta])$. So, the study of critical sets of principal autotopisms will be therefore related to that of the access structure of any secret sharing scheme using Latin squares and principal isotopisms.

Keeping in mind all the previous process, we obtain:

n	k	Upper bound of $scs(\Theta)$	n	k	Upper bound of $scs(\Theta)$
2	1	0	6	1 2 3	4 4 3
3	1	1	7	1	5
4	1 2	2 1	8	1 2 4	6 7 5
5	1	3	9	1 3	7 8

5 Θ-Critical sets of Latin squares

In this section, fixed $\Theta \in \mathcal{I}_n$ such that $\Delta(\Theta) > 0$ and a Latin square $L = (l_{ij}) \in LS(\Theta)$, we want to know an upper bound of the smallest size $scs_\Theta(L)$ of all $\{\Theta\}$-critical sets of L. To obtain it, it can be useful the next result:

Lemma 6. *In the CCPM, the following asserts are verified:*

a) $|S^{i,j}| = \frac{n}{k}$, for all $i, j \in \{0, 1, ..., k-1\}$.
b) $\bigcup_{i=0}^{k-1} S^{i,j} = N$, for all $j \in \{0, 1, ..., k-1\}$ and $\bigcup_{j=0}^{k-1} S^{i,j} = N$, for all $i \in \{0, 1, ..., k-1\}$.
c) If $(i, j) \neq (s, t)$, then $S^{i,j} \cap S^{s,t} = \emptyset$ whenever $i = s$ or $j = t$.
d) If l_{st} is known, being $(s, t, l_{st}) \in R_L^{i,j}$, then the $\frac{n}{k}$ cells (u, v, l_{uv}) of $R_L^{i,j}$ such that $l_{uv} = l_{st}$ are known.

As an immediate consequence of the previous lemma, we obtain the following:

Proposition 7. $scs_\Theta(L) \leq k \cdot n$.

- **Proof:** We can suppose that c_{i0}^α is the minimum in the natural order of S_i^α, for all $i \in \{0, 1, ..., k-1\}$. Then, if we know $l_{c_{i0}^\alpha j}$ for all $i \in \{0, 1, ..., k-1\}$ and $j \in \{0, 1, ..., n-1\}$, we can recover L by using the CCPM with all these elements and the autotopism Θ.

$$\Theta = ((01)(25)(34), (01)(23)(45), \epsilon); \begin{pmatrix} 0 & 4 & 1 & 5 & 3 & 2 \\ - & - & - & - & - & - \\ 1 & 3 & 0 & 2 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 & 0 \\ - & - & - & - & - & - \\ - & - & - & - & - & - \end{pmatrix} \overset{(CCPM)}{\Rightarrow} L = \begin{pmatrix} 0 & 4 & 1 & 5 & 3 & 2 \\ 4 & 0 & 5 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 & 0 \\ 5 & 2 & 3 & 4 & 0 & 1 \\ 3 & 1 & 2 & 0 & 5 & 4 \end{pmatrix}$$

$$\Theta = ((014)(235), (023)(145), \epsilon); \begin{pmatrix} 0 & 4 & 1 & 5 & 3 & 2 \\ - & - & - & - & - & - \\ 2 & 0 & 4 & 3 & 1 & 5 \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & - & - & - & - & - \end{pmatrix} \overset{(CCPM)}{\Rightarrow} L = \begin{pmatrix} 0 & 4 & 1 & 5 & 3 & 2 \\ 5 & 2 & 0 & 1 & 4 & 3 \\ 2 & 0 & 4 & 3 & 1 & 5 \\ 3 & 5 & 2 & 4 & 0 & 1 \\ 1 & 3 & 5 & 0 & 2 & 4 \\ 4 & 1 & 3 & 2 & 5 & 0 \end{pmatrix}$$

Lemma 8. $R_{L,\Theta}^j = \{l_{c_{i0}^\alpha\ c_{jl}^\beta} : i \in \{0, 1, ..., k-1\}, l \in \{0, 1, ..., \frac{n}{k} - 1\}\} = N$, *for all* $j \in \{0, 1, ..., k-1\}$.

So, the calculus of scs_Θ of L can be reduced to the calculus of the size of the smallest critical set of a Latin rectangle of order $k \times n$, which can be decomposed at the same time into k regions, each of them having all the symbols of N. Therefore, if we denotes $R_{L,\Theta} = \bigcup_{j=0}^{k-1} R_{L,\Theta}^j \in LS(k, n)$, we have the following:

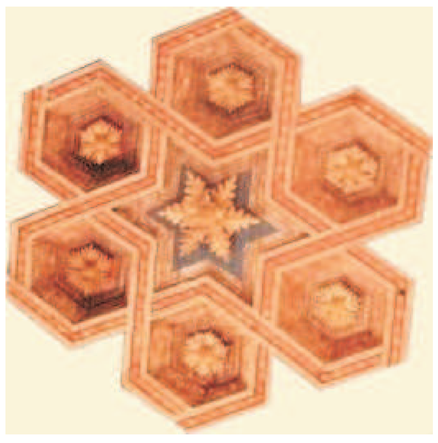
Proposition 9. $scs_\Theta(L) \leq scs(R_{L,\Theta})$.

$$\Theta = ((01)(25)(34), (01)(23)(45), \epsilon); \begin{pmatrix} 0 & 4 & 1 & 5 & 3 & 2 \\ - & - & - & - & - & - \\ 1 & 3 & 0 & 2 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 & 0 \\ - & - & - & - & - & - \\ - & - & - & - & - & - \end{pmatrix} \Rightarrow \text{Critical set: } \begin{pmatrix} 0 & - & - & 5 & - & 2 \\ - & - & - & - & - & - \\ 1 & - & 0 & - & 4 & - \\ - & 5 & - & 3 & 1 & - \\ - & - & - & - & - & - \\ - & - & - & - & - & - \end{pmatrix}$$

$$\Theta = ((014)(235), (023)(145), \epsilon); \begin{pmatrix} 0 & 4 & 1 & 5 & 3 & 2 \\ - & - & - & - & - & - \\ 2 & 0 & 4 & 3 & 1 & 5 \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & - & - & - & - & - \end{pmatrix} \Rightarrow \text{Critical set: } \begin{pmatrix} 0 & 4 & 1 & - & 3 & - \\ - & - & - & - & - & - \\ 2 & 0 & 4 & - & 1 & - \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & - & - & - & - & - \end{pmatrix}$$

By construction, it is immediate that $scs(R_{L,\Theta}) \geq k \cdot (n-k)$. We give then the following conjecture:

Conjecture 10. $scs_\Theta(L) \leq k \cdot (n-k)$. *As a consequence, the smallest size of an authorized group of a secret sharing scheme having Θ and the triples of L as shares is smaller or equal than $2n-3$, if $k = 1$ and smaller or equal than $\left(\frac{n}{k} - 1\right) \cdot (2k-1) - 2 + k \cdot (n-k)$, if $k \neq 1$.*



References

[1] Adams, P., Mahdian, M., Mahmoodian, E.S., On the forced matching numbers of bipartite graphs, *D*iscrete Mathematics **281** (2004), 1–12.

[2] Cooper, J. A., Donovan, D., Seberry, J. *S*ecret Sharing Schemes arising from Latin squares. Bull. Inst. Combin. Appl. 12 (1994) 33 - 43.

[3] Falcón Ganfornina, R. M., *C*ritical and forcing sets related to the autotopism group of a Latin square. International Congress of Mathematicians 2006.

[4] Falcón Ganfornina, R. M., *S*tudy of Critical Sets in Latin Squares by using the Autotopism Group. Submitted (2005).

[5] Falcón Ganfornina, R. M., *L*atin squares associated to principal autotopisms of long cycles. Application in Cryptography. Proceedings of Transgressive Computing 2006: a conference in honor of Jean Della Dora. Granada, 2006, pp. 213 - 230. ISBN: 84-689-8381-0.

[6] Falcón Ganfornina, R. M., *D*ecomposition of principal autotopisms into triples of a Latin square. X Encuentro de Álgebra Computacional y Aplicaciones EACA 2006.

[7] Kościelny, C., Generating quasigroups for cryptographic applications, *I*nternational Journal of Applied Mathematics and Computer Science **12** (4) (2002), 559–569.

[8] Laywine, C. F., Mullen, G. L. *D*iscrete mathematics using Latin Squares. Wiley-Interscience. Series in discrete mathematics and optimization, 1998. ISBN 0-471-24064-8.

[9] McKay, B. D. *I*somorph-free exhaustive generation. J. Algorithms 26 (1998) 306 - 324.