Critical and forcing sets related to the autotopism group of a Latin square

Scientific Section of ICM 2006: 14. Combinatorics.
Poster Number: 774
MSC 2000: 05B15, 05C70, 94A62

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

ABSTRACT: In Cryptography, critical sets of any Latin square L can be used to get the access structure of a secret sharing scheme [2, 6] having triples of L as shares. In such a scheme, further information about the symmetry of L can be obtained by keeping in mind the autotopism group $\mathcal{U}(L)$ [4]. Because the size of an autotopism is generally much larger than that of a triple of L, we propose in this paper an algorithm which allows to decompose any principal autotopism $\Theta \in \mathcal{U}(L)$ into triples of a partial Latin square P_Θ. Critical sets of P_Θ are then used to define the access structure of the new scheme. In this way, we propose an algorithm depending on the order of L which allows to give an upper bound of the size of the smallest set of triples equivalent to Θ. Finally, as Latin squares of order n are equivalent to perfect matchings of $K_{n,n}$ [1], we relate the previous critical sets with the forcing sets of the perfect matching associated to L. A classification of these forcing sets is then obtained.

1 Introduction

A Latin square L of order n is a $n \times n$ array with elements chosen from a set $N = \{x_1, ..., x_n\}$, such that each symbol occurs precisely once in each row and each column. In other words, a Latin square is the multiplication table of a quasigroup in abstract algebra. The set of Latin squares of order n is denoted by $LS(n)$.

$$\begin{pmatrix} a & b & c & d \\ b & a & d & c \\ c & d & b & a \\ d & c & a & b \end{pmatrix} \in LS(4)$$

n	2	3	4	5	6	7	8	...
$\lvert LS(n)\rvert$	2	12	576	161280	812851200	61479419904000	108776032459082956800	...

In this paper we will consider $N = \{0, 1, ..., n-1\}$. So, if $L = (l_{ij})$, the orthogonal array representation of L is the set of n^2 triples $\{(i, j, l_{ij}) : i, j \in N\}$. 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.

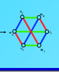
$$\begin{cases} L = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} & \Rightarrow L^\Theta = \begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 0 & 2 \\ 2 & 0 & 3 & 1 \end{pmatrix} \\ \Theta = ((0\ 1)(2\ 3), (1\ 2), \epsilon) & \end{cases}$$

If $\gamma = \epsilon$, the identity map on N, Θ is called a principal isotopism. An isotopism which maps L to itself is an autotopism. $(\epsilon, \epsilon, \epsilon)$ is called the trivial 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 $\Delta(\Theta)$.

n	k	$\Delta(\Theta)$	n	k	$\Delta(\Theta)$
2	1	2	6	1	720
				2	25920
				3	160800
3	1	12	7	1	5040
4	1	24	8	1	40320
	2	96		2	23224320
				4	88355635200
5	1	120	9	1	362880
				3	948109639680

Fixed a graph $G = (V, E)$, a 1-factor f of G is a subgraph of G with the same set V of vertices that G and whose edges are a subset E_f of E such that every vertex has exactly one edge incident on it. If E can be partitioned into disjoint subsets decomposing G into 1-factors, then G is said to be 1-factorizable and this partition F is said to be a 1-factorization or a perfect matching of G. A forcing set for a 1-factorization F of G is a subset S of F such that S is not contained in any other 1-factorization of G. Every Latin square $L \in LS(n)$ is equivalent to a 1-factorization $\mathcal{F}(L)$ of a bipartite graph $K_{n,n}$ [7]:

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

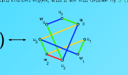


A partial Latin square P of order n is a $n \times n$ array with elements chosen from a set of n symbols, such that each symbol occurs at most once in each row and in each column. It is therefore the multiplication table of a partial quasigroup in abstract algebra.

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

The size of P is the number of its filled cells, that is, the number of triples $(i, j, k) \in P$ such that $k \neq \emptyset$. 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. Finally, fixed $P \in PLS(n)$, we can associate to it a subgraph of $K_{n,n}$ with colored edges, which we will denote by $\mathcal{F}(P)$:

$$\begin{pmatrix} - & - & 2 \\ 2 & - & 1 \\ 1 & 2 & - \end{pmatrix} \longleftrightarrow$$



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 $P \in UC(L)$.

$$\begin{pmatrix} 0 & & & 3 \\ - & 0 & 3 & - \\ 2 & - & 1 & 0 \\ 3 & 2 & 0 & - \end{pmatrix} \text{ uniquely completed to } L = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix}$$

Besides, 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 $P \in CS(L)$.

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

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

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, 7]: 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 $\Gamma = \{P \in PLS(n) : P \subseteq \bigcup_S \{(i, j, l_{ij})\} \subseteq L$ and $\exists C \in CS(L)$ such that $C \subseteq P\}$.

$$\begin{cases} \underline{\text{Secret Key}}: K = L = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix} \\ S = \begin{pmatrix} 0 & - & - & 3 \\ - & 0 & 3 & - \\ 2 & & 1 & 0 \\ 3 & 2 & 0 & - \end{pmatrix} \end{cases} \Rightarrow \underline{\text{Authorized Groups}}: \begin{cases} \begin{pmatrix} 0 & - & - & 3 \\ - & 0 & - & - \\ 2 & - & 1 & - \end{pmatrix} \\ \begin{pmatrix} 0 & - & - & - \\ - & - & 3 & - \\ 2 & & & 0 \\ - & 2 & - & - \end{pmatrix} \\ \ldots \end{cases}$$

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

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

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 if $P \in UC_{\mathfrak{F}}(L)$ and $Q \notin UC_{\mathfrak{F}}(L)$ for all $Q \subset P$.

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

The study of the size $scs_{\mathfrak{F}}(L)$ of the smallest $\mathfrak{F}$-critical set of L is then an open problem [3]. Analogously to critical sets, it is expected that $\mathfrak{F}$-critical sets will have applications in Cryptography, specially as secret sharing schemes. In this way, in [4], 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 I 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 $\mathfrak{F} \subseteq I$, by sharing its corresponding triples and principal autotopisms, they will obtain as consequence the secret key L.

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

So, the number of participants can be increased with respect to the above model and besides, they can get information about the symmetry of L by obtaining the set $LS(\Theta)$, which is easily computable by following the canonical construction path method (CCPM) [8]. Although the weight of information given by Θ is usually greater than that given by the triples of L, the size of an isotopism is, however, much larger than that of a triple. As this problem rises with n, it is necessary to identify any autotopism with a set of shares of a smaller size. In this way, we give in this paper an algorithm to decompose any non-trivial principal autotopism into triples of a Latin square. It is useful to tackle the calculus of the number $scs_{\{\Theta\}}(L)$ and so, the calculus of $scs_{\mathfrak{F}}(L)$.

2 The Canonical Construction Path Method (CCPM)

From now on, $\Theta = (\alpha, \beta, \epsilon) \in \mathcal{I}_n$ will be a non-trivial principal isotopism, such that $\Delta(\Theta) > 0$. From [1], this is equivalent to say that α and β have all their cycles of the same length and without fixed points, that is:

$$\alpha = C_0^\alpha \circ C_1^\alpha \circ ... \circ C_{k-1}^\alpha; \qquad \beta = C_0^\beta \circ C_1^\beta \circ ... \circ C_{k-1}^\beta;$$

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 $\frac{n}{k} \neq 1$ for all $\delta \in \{\alpha, \beta\}$ and $i \in \{0, 1, ..., k-1\}$, being $\begin{cases} c_{i,j}^\delta \in N, \text{ for all } j \in \{0, 1, ..., \frac{n}{k}-1\}, \\ c_{i,j}^\delta \neq c_{k,l}^\delta, \text{ for all } (i,j) \neq (k,l), \\ c_{0,0}^\alpha = c_{0,0}^\beta = 0. \end{cases}$ 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 $i, j \in \{0, 1, ..., k-1\}$.

These subsquares can be considered either as partial Latin squares contained in L or as Latin squares of order $\frac{n}{k}$. In this way, to find L, it is enough to determine $\frac{n}{k}$ triples of each subsquare $R_L^{i,j}$, because of the following:

> **Lemma 1 ([5]).** *Let $\left(c_{i,s}^\alpha, c_{j,t}^\beta, l_{c_{i,s}^\alpha c_{j,t}^\beta}\right)$ be a triple of $R_L^{i,j}$. Then, the $\frac{n}{k}$ cells (u, v, l_{uv}) of $R_L^{i,j}$ such that $l_{uv} = l_{c_{i,s}^\alpha c_{j,t}^\beta}$ are known.*

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

$$\downarrow$$

$$\begin{Bmatrix} \underline{\text{Step 1}}: L \in LS(4) \to L = \begin{pmatrix} l_{00} & l_{01} & l_{02} & l_{03} \\ l_{10} & l_{11} & l_{12} & l_{13} \\ l_{20} & l_{21} & l_{22} & l_{23} \\ l_{30} & l_{31} & l_{32} & l_{33} \end{pmatrix} \\ \underline{\text{Step 2}}: \text{From the cycles (01) and (03)}: \begin{cases} l_{00} = l_{13} = a \\ l_{03} = l_{10} = d \end{cases} \Rightarrow R_L^{0,0} = \begin{pmatrix} a & & & d \\ d & - & - & a \\ - & - & - & - \end{pmatrix} \\ \underline{\text{Step 3}}: \text{From the cycles (01) and (12)} \begin{cases} l_{01} = l_{12} = b \\ l_{02} = l_{11} = c \end{cases} \Rightarrow R_L^{0,1} = \begin{pmatrix} - & b & c & - \\ - & c & b & - \\ - & - & - & - \end{pmatrix} \\ \underline{\text{Step 4}}: \text{From the cycles (23) and (03)} \begin{cases} l_{30} = l_{23} = e \\ l_{20} = l_{33} = h \end{cases} \Rightarrow R_L^{0,1} = \begin{pmatrix} - & - & - & - \\ - & - & - & - \\ e & - & - & h \\ h & - & - & e \end{pmatrix} \\ \underline{\text{Step 5}}: \text{From the cycles (23) and (12)} \begin{cases} l_{21} = l_{32} = f \\ l_{22} = l_{31} = g \end{cases} \Rightarrow R_L^{0,1} = \begin{pmatrix} - & - & - & - \\ - & - & - & - \\ - & f & g & - \\ - & g & f & - \end{pmatrix} \end{Bmatrix} \to L = \begin{pmatrix} a & b & c & d \\ d & c & b & a \\ e & f & g & h \\ h & g & f & e \end{pmatrix}$$

$$\downarrow$$

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

3 Partial Latin squares related to principal isotopisms

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

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

Let us observe that, given $L \in LS(n)$, we can extend the previous definitions to any Latin subsquare S of L by identifying it with the partial Latin square of order n such that its unique filled cells are those corresponding to S. In this way, keeping in mind the CCPM, the following result is immediate:

> **Lemma 2 ([5]).** $R_L^{i,j} \in PLS_1(C_i^\alpha) \cap PLS_2(C_j^\beta)$*, for all $i, j \in \{0, 1, ..., k-1\}$.*

We will consider a particular case of Latin square included in $LS(\Theta)$. Specifically, we are interested in a Latin square $L_\Theta = (l_{ij}) \in LS(n)$ verifying the following conditions:

$$(1) \begin{cases} (1.1)\ l_{0j} = j \text{ for all } j \in N. \\ (1.2) \text{ Fixed } i \notin S_0^\alpha \cup S_0^\beta, \text{ we impose } l_{i0} = i. \\ (1.3) \text{ We put in the natural order the elements of } S_0^\alpha \setminus S_0^\beta \text{ and we assign them consecutively} \\ \quad \text{to the elements } l_{i0} \text{ (also in the natural order) which are still without an assigned value.} \end{cases}$$

In this way, keeping in mind Lemma 1 and the previous conditions, we can define the partial Latin square:

$$P_\Theta = \bigcup_i R_{L_\Theta}^{i,0} \bigcup \bigcup_j R_{L_\Theta}^{0,j} \in PLS(n).$$

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

We can 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, $|[\Theta]| = (\frac{n}{k} - 1)!$.

> **Theorem 3 ([5]).** *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 $(2k-1) \cdot (\frac{n}{k})^2$, 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 $\Theta \to P_\Theta$. Specifically, keeping in mind the CCPM, it is immediate that P_Θ is a partial Latin square which verifies all the properties of the theorem.

Now, 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 $N \setminus \bigcup_{l=0}^{j-1} S_l^\beta$. 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 $(N, \cdot)$.*

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. In this way, the following result is useful:

> **Lemma 5.** *If we denotes $m_0^\alpha = 0 = m_0^\beta$, then:*
> *i) $S_l^\alpha = \{i \in N : \exists j \in N$ such that $(i, j, m_l^\beta) \in P_\Theta\}$, for all $l \in N$.*
> *ii) $S_l^\beta = \{j \in N : \exists i \in N$ such that $(i, j, m_l^\alpha) \in P_\Theta\}$, for all $l \in N$.*

So, we obtain an upper bound of the size of the smallest set of triples equivalent to Θ. Indeed, if we denotes this last size as $scs(\Theta)$, we have the following:

> **Proposition 6.** $scs(\Theta) < (\frac{n}{k} - 1) \cdot (2k - 1)$.

		$\Theta = (\alpha, \beta, \epsilon) \in [\Theta]$	
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) $\alpha = ((0\ 1)(2\ 5)(3\ 4))$ $\beta = ((0\ 1)(2\ 3)(4\ 5))$	

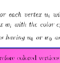
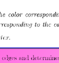
Let us observe that Step 4 is not necessary in the previous example. Due to it, we can reduce the size of the partial Latin square corresponding to Lemma 5. In our case, we can find the following:

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

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.

4 Forcing sets associated to principal autotopisms of reduced Latin squares

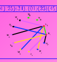
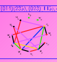
Let Θ be a principal autotopism such that $\Delta(\Theta) > 0$. In this section we will study the 1-factorizations corresponding to the partial Latin square P_Θ associated to $[\Theta]$.

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

As all the cells of the first row and column of P_Θ are always filled, we can reduce the number of edges of $\mathcal{F}(P_\Theta)$, by following the next algorithm:

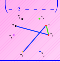
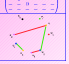
> **Algorithm 7.**
> *i) Fixed $i \neq 0$, we color each vertex u_i with the color corresponding to the edge $\overline{u_i w_0}$ and each vertex w_i with the color c_i corresponding to the edge $\overline{u_0 w_i}$.*
> *ii) We remove the edges having u_0 or w_0 as vertex.*

The resulting graph has therefore colored vertices and edges and determines $[\Theta]$. This graph will be denoted by $\mathcal{G}_{[\Theta]}$ and it will be called the graph related to $[\Theta]$.

Θ	$((01)(25)(34), (01)(23)(45), \epsilon)$	$((014)(235), (023)(145), \epsilon)$
$\mathcal{G}_{[\Theta]}$		

The graph $\mathcal{G}_{[\Theta]}$ allows to recover P_Θ and so, the class $[\Theta]$. In this way, we can consider a set of vertices and edges of $\mathcal{G}_{[\Theta]}$ as shares in a secret sharing scheme. So, the size of these shares would be smaller than that of Θ. It would allow to increase the number of participants in such a scheme and to adjust the weight of information of the used shares. Anyway, it is possible to find a graph of smaller size than $\mathcal{G}_{[\Theta]}$. To do it, let us observe that, fixed a vertex in this graph, its color must be different of those of its incident edges. Furthermore, these last ones have also different colors between themselves. So, keeping in mind these properties, we can eliminate some vertices and edges of $\mathcal{G}_{[\Theta]}$ and we can therefore obtain a graph of the smallest size allowing to recover $[\Theta]$. Such a graph will be called a forcing set of $[\Theta]$. The sets of forcing sets of $[\Theta]$ will be denoted by $FS([\Theta])$.

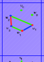
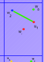
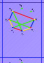
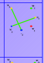
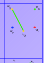
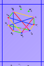
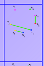
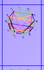
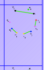
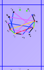
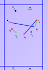
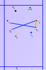
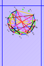
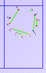
It is possible to get forcing sets of $[\Theta]$ by considering critical sets of $[\Theta]$. Specifically, fixed $C \in CS([\Theta])$, it is enough to remove those edges of $\mathcal{G}_{[\Theta]}$ not corresponding to C. In the resulting graph we remove those isolated vertices u_i. Let us observe that the vertices w_i must be all in the final graph $\mathcal{G}_{[\Theta], C}$ to know what color corresponds to each element of N.

Θ	$((01)(25)(34), (01)(23)(45), \epsilon)$	$((014)(235), (023)(145), \epsilon)$
C	$\begin{pmatrix} - & 0 & - & 2 & - & - \\ & & & & & \\ - & - & - & - & - & - \\ - & - & - & - & - & - \\ - & 2 & - & - & - & - \end{pmatrix}$	$\begin{pmatrix} - & 0 & - & 1 & - & - \\ & & & & & \\ - & 1 & - & - & - & - \\ - & - & 0 & - & - & - \\ - & - & - & - & - & - \end{pmatrix}$
$\mathcal{G}_{[\Theta], C}$		

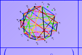
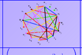
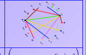
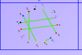
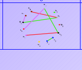
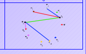
5 Classification of forcing sets of principal autotopisms for $2 \leq n \leq 9$

Fixed a principal autotopism $\Theta \in \mathcal{I}_n$ such that $\Delta(\Theta) > 0$, we have seen in the Introduction that the values of $\Delta(\Theta)$ are known for $2 \leq n \leq 9$. In this last section, we will study those critical and forcing sets associated to these principal autotopisms. Keeping in mind the previous sections, it is enough to give an example in each case.

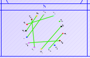
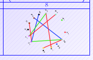
$\underline{2 \leq n \leq 7}$:

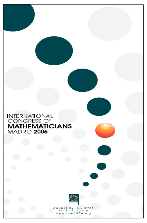
n	k	$\Theta = (\alpha, \beta, \epsilon)$	P_Θ	$\mathcal{G}_{[\Theta]}$	$C \in CS([\Theta])$	$\lvert C\rvert$	$\mathcal{G}_{[\Theta], C}$
2	1	$\alpha = (0\ 1)$ $\beta = (0\ 1)$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$		$\begin{pmatrix} - & - \end{pmatrix}$	0	
3	1	$\alpha = (0\ 1\ 2)$ $\beta = (0\ 2\ 1)$	$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$		$\begin{pmatrix} - & - & 0 \\ - & - & - \end{pmatrix}$	1	
4	1	$\alpha = (0\ 2\ 3\ 1)$ $\beta = (0\ 3\ 1\ 2)$	$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 0 & 1 \\ 2 & 3 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$		$\begin{pmatrix} - & - & 0 & - \\ - & - & - & 0 \\ - & - & - & - \end{pmatrix}$	2	
4	2	$\alpha = (0\ 2)(3\ 1)$ $\beta = (0\ 3)(1\ 2)$	$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & - & - & 2 \\ 3 & 2 & 1 & 0 \\ 2 & & & 1 \end{pmatrix}$		$\begin{pmatrix} - & - & - & - \\ - & - & - & 0 \end{pmatrix}$	1	
5	1	$\alpha = (0\ 1\ 3\ 2\ 4)$ $\beta = (0\ 1\ 2\ 3\ 4)$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}$		$\begin{pmatrix} - & 0 & - & - & - \\ - & - & - & 0 & - \\ - & - & 0 & - & - \end{pmatrix}$	3	
6	1	$\alpha = (0\ 2\ 4\ 1\ 3\ 5)$ $\beta = (0\ 1\ 3\ 5\ 2\ 4)$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 & 0 \\ 4 & 0 & 5 & 1 & 2 & 3 \\ 3 & 5 & 0 & 2 & 1 & 4 \\ 2 & 4 & 3 & 0 & 5 & 1 \\ 0 & 3 & 4 & 5 & 0 & 2 \end{pmatrix}$		$\begin{pmatrix} - & - & - & - & - & 0 \\ & 0 & & & & \\ & & 0 & & & \\ - & - & - & 0 & - & - \\ - & - & - & - & - & - \end{pmatrix}$	4	
6	2	$\alpha = (0\ 2\ 1)(1\ 3\ 5)$ $\beta = (0\ 1\ 3)(5\ 2\ 4)$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & - & 4 & - & - \\ 3 & 0 & 5 & 1 & 2 & 1 \\ 4 & 2 & - & 5 & - & - \\ 1 & 3 & 4 & 0 & 5 & 2 \\ 5 & 1 & - & 2 & - & - \end{pmatrix}$		$\begin{pmatrix} - & - & - & - & - & - \\ - & - & - & - & - & - \\ & 0 & & & 2 & \\ - & 2 & - & - & - & - \\ - & - & - & 0 & - & - \\ - & - & - & - & - & - \end{pmatrix}$	4	
6	3	$\alpha = (0\ 2)(4\ 1)(3\ 5)$ $\beta = (0\ 1)(3\ 5)(2\ 4)$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & - & - & - & - \\ 1 & 0 & 4 & 5 & 2 & 3 \\ 3 & 5 & - & - & - & - \\ 4 & 2 & - & - & - & - \\ 5 & 3 & - & - & - & - \end{pmatrix}$		$\begin{pmatrix} - & - & - & - & - & - \\ - & - & - & - & - & - \\ & 0 & & & 2 & \\ - & 2 & - & - & - & - \\ - & - & - & - & - & - \end{pmatrix}$	3	
7	1	$\alpha = (0\ 2\ 4\ 6\ 1\ 3\ 5)$ $\beta = (0\ 1\ 3\ 5\ 2\ 4\ 6)$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 0 & 4 & 1 & 6 & 3 \\ 6 & 0 & 5 & 1 & 2 & 3 & 4 \\ 3 & 5 & 6 & 2 & 0 & 4 & 1 \\ 4 & 6 & 3 & 0 & 5 & 1 & 2 \\ 1 & 3 & 4 & 5 & 6 & 2 & 0 \\ 2 & 4 & 1 & 6 & 3 & 0 & 5 \end{pmatrix}$		$\begin{pmatrix} - & - & 0 & - & - & - & - \\ - & 0 & - & - & - & - & - \\ - & - & - & - & 0 & - & - \\ & & & 0 & & & \\ - & - & - & - & - & - & 0 \\ - & - & - & - & - & - & - \end{pmatrix}$	5	

$\underline{n = 8}$:

k	1	2	4
$\Theta = (\alpha, \beta, \epsilon)$	$\alpha = (01325467)$ $\beta = (05271634)$	$\alpha = (0132)(5467)$ $\beta = (0527)(1634)$	$\alpha = (01)(32)(54)(67)$ $\beta = (05)(27)(16)(34)$
P_Θ	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 6 & 3 & 0 & 1 & 2 \\ 6 & 5 & 4 & 7 & 1 & 3 & 2 & 0 \\ 3 & 2 & 0 & 1 & 6 & 4 & 7 & 5 \\ 7 & 4 & 6 & 5 & 2 & 1 & 0 & 3 \\ 1 & 0 & 3 & 2 & 7 & 6 & 5 & 4 \\ 2 & 3 & 1 & 0 & 5 & 7 & 4 & 6 \\ 5 & 6 & 7 & 4 & 0 & 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 5 & 6 & 3 & 0 & 1 & 2 \\ 5 & 6 & 7 & 4 & 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\ 4 & & 3 & & & 1 & & 6 \\ 1 & - & 6 & - & - & 3 & - & 4 \\ 6 & - & 1 & - & - & 4 & - & 3 \\ 3 & - & 4 & - & - & 6 & - & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 7 & 4 & 3 & 0 & 1 & 2 \\ 2 & - & - & - & - & 3 & - & - \\ 3 & - & - & - & - & 2 & - & - \\ 4 & & & & & 1 & & \\ 1 & - & - & - & - & 4 & - & - \\ 6 & - & - & - & - & 7 & - & - \\ 7 & - & - & - & - & 6 & - & - \end{pmatrix}$
$\mathcal{G}_{[\Theta]}$			
$C \in CS([\Theta])$	$\begin{pmatrix} - & - & - & - & - & - & 0 & - & - \\ - & - & - & - & - & - & - & - & 0 \\ - & - & 0 & - & - & - & - & - & - \\ & & & & & & & 0 & \\ - & 0 & - & - & - & - & - & - & - \\ - & - & - & - & 0 & - & - & - & - \\ - & - & - & - & - & 0 & - & - & - \end{pmatrix}$	$\begin{pmatrix} - & - & - & - & - & - & 0 & 1 & - \\ - & - & - & - & - & 1 & - & - & 0 \\ - & - & 0 & - & - & - & - & - & - \\ - & - & - & - & - & - & - & - & 4 \\ - & - & - & - & - & - & 4 & - & - \\ - & - & - & - & - & - & - & - & - \end{pmatrix}$	$\begin{pmatrix} - & - & - & - & - & - & 0 & 1 & 2 \\ - & - & - & - & - & - & 2 & - & - \\ - & - & - & - & - & - & 4 & - & - \\ - & - & - & - & - & - & - & - & - \end{pmatrix}$
$\lvert C\rvert$	6	6	6
$\mathcal{G}_{[\Theta], C}$			

$\underline{n = 9}$:

k	1	2
$\Theta = (\alpha, \beta, \epsilon)$	$\alpha = (025163784)$ $\beta = (047381526)$	$\alpha = (025)(163)(784)$ $\beta = (047)(381)(526)$
P_Θ	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 8 & 0 & 2 & 3 & 1 & 6 & 4 \\ 6 & 8 & 5 & 7 & 0 & 1 & 2 & 4 & 3 \\ 8 & 0 & 7 & 2 & 1 & 4 & 3 & 5 & 6 \\ 4 & 5 & 6 & 8 & 7 & 2 & 0 & 3 & 1 \\ 2 & 3 & 1 & 4 & 6 & 8 & 5 & 0 & 7 \\ 1 & 4 & 3 & 6 & 5 & 7 & 8 & 2 & 0 \\ 3 & 6 & 4 & 5 & 8 & 0 & 7 & 1 & 2 \\ 7 & 2 & 0 & 1 & 3 & 6 & 1 & 8 & 5 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & & & & 3 & & & 6 & \\ 7 & 8 & 5 & 1 & 0 & 6 & 2 & 4 & 3 \\ 3 & - & - & - & 6 & - & - & 1 & - \\ 2 & - & - & - & 8 & - & - & 5 & - \\ 4 & 3 & 6 & 8 & 7 & 2 & 5 & 0 & 1 \\ 6 & - & - & - & 1 & - & - & 3 & - \\ 5 & - & - & - & 2 & - & - & 8 & - \\ 8 & - & - & - & 5 & - & - & 2 & - \end{pmatrix}$
$\mathcal{G}_{[\Theta]}$		
$C \in CS([\Theta])$	$\begin{pmatrix} - & - & - & 0 & - & - & - & - & - \\ - & - & - & - & 0 & - & - & - & - \\ - & 0 & - & - & - & - & - & - & - \\ & & & & & & & 0 & \\ - & - & - & - & - & - & - & 0 & - \\ - & - & - & - & - & - & - & - & 0 \\ - & - & - & - & - & 0 & - & - & - \end{pmatrix}$	$\begin{pmatrix} - & - & - & - & 1 & 0 & - & 2 & - \\ - & - & - & - & - & - & - & 1 & - \\ & & & & & & & & \\ - & - & - & - & - & - & - & 0 & 1 \\ - & - & - & - & 1 & - & - & - & - \\ - & - & - & - & 2 & - & - & - & - \end{pmatrix}$
$\lvert C\rvert$	8	8
$\mathcal{G}_{[\Theta], C}$		



References

[1] Adams, P., Mahdian, M., Mahmoodian, E.S., On the forced matching numbers of bipartite graphs, *Discrete Mathematics* **281** (2004), 1–12.
[2] Cooper, J. A., Donovan, D., Seberry, J. *Secret Sharing Schemes arising from Latin squares.* Bull. Inst. Combin. Appl. 12 (1994) 33 - 43.
[3] Falcón Ganfornina, R. M., *Study of Critical Sets in Latin Squares by using the Autotopism Group.* Submitted (2005).
[4] Falcón Ganfornina, R. M., *Latin 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.
[5] Falcón Ganfornina, R. M., *Decomposition of principal autotopisms into triples of a Latin square.* X Encuentro de Álgebra Computacional y Aplicaciones EACA 2006. Sevilla (September, 2006).
[6] Kościelny, C., Generating quasigroups for cryptographic applications, *International Journal of Applied Mathematics and Computer Science* **12** (4) (2002), 559–569.
[7] Laywine, C. F., Mullen, G. L. *Discrete mathematics using Latin Squares.* Wiley-Interscience. Series in discrete mathematics and optimization, 1998. ISBN 0-471-24064-8.
[8] McKay, B. D. *Isomorph-free exhaustive generation.* J. Algorithms 26 (1998) 306 - 324.