Study of Critical Sets in Latin Squares by using the Autotopism Group

R. M. Falcón [1]

Departamento de Matemática Aplicada I.
E. T. S. de Arquitectura. Universidad de Sevilla.
Avda. Reina Mercedes 2. 41012 - Sevilla (Spain).

Abstract

Given a Latin square L and a subset $\mathfrak{F}$ of its autotopism group $\mathcal{U}(L)$, we study in this paper some properties and results which partial Latin squares contained in L inherit from $\mathcal{U}(L)$, by using $\mathfrak{F}$. In particular, we define the concept of $\mathfrak{F}$-critical set of L and we ask ourselves about the smallest one contained in L.

Keywords: Latin Square, Autotopism Group.

1 Introduction

A *Latin square* L of order n is a $n \times n$ array with elements chosen from the set $N = \{0, 1, ..., n-1\}$, such that each symbol occurs precisely once in each row and each column. The set of Latin squares of order n is denoted by $LS(n)$. If $L = (l_{i,j}) \in LS(n)$, the *orthogonal array representation of* L is the set of n^2 triples $\{(i, j, l_{i,j}) : i, j \in N\}$. The previous set is identified with L and so, it is written $(i, j, l_{i,j}) \in L$, for all $i, j \in N$. It is said that L is an *entropic Latin square* if $l_{l_{ij}l_{st}} = l_{l_{is}l_{jt}}$, for all $i, j, s, t \in N$.

[1] Email: `rafalgan@us.es`

Preprint of: Electronic Notes in Discrete Mathematics 29 (2007), pp. 503-507. DOI 10.1016/j.endm.2007.07.078

Let S_n be the symmetric group on N. An *isotopism of Latin squares of order* n is then a triple $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n = S_n \times S_n \times S_n$. If we apply Θ to a Latin square $L \in LS(n)$, it is verified that 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. In particular, if $L = (l_{i,j})$, then $L^\Theta = \{(i, j, \gamma\left(l_{\alpha^{-1}(i),\beta^{-1}(j)}\right) : 0 \leq i, j \leq n-1\}$. An isotopism which maps L to itself is an *autotopism*. The stabilizer subgroup of L in S_n^3 is its *autotopism group*, $\mathcal{U}(L) = \{\Theta \in \mathcal{I}_n : L^\Theta = L\}$.

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 $PLS(n)$. The *size* of P, $|P|$, is the number of non-blank cells. If $L \in LS(n)$ we will denote by $L_{i,j}$ the partial Latin square contained in L such that the unique filled cell of $L_{i,j}$ is $(i, j, l_{i,j})$. Thus, given $P \in PLS(n)$ we can ever find a subset $I_P \subseteq N \times N$ such that $P = \bigcup_{(i,j) \in I_P} L_{i,j}$.

It is said that P can be *completed* to a Latin square $L \in LS(n)$ if $P \subseteq L$. If L is the unique one in such conditions, it is said that P is *uniquely completable to* L and it is denoted $P \in UC(L)$. If besides any proper subset of P can be completed at least to two distinct Latin squares it is said that P is a *critical set* of L and it is denoted $P \in CS(L)$. Given $L \in LS(n)$, $scs(L)$ denotes the size of the smallest critical set of L and $scs(n)$ denotes the minimum of $scs(L)$ for all $L \in LS(n)$. Analogously, $lcs(L)$ denotes the size of the largest critical set of L and $lcs(n)$ denotes the maximum of $lcs(L)$ for all $L \in LS(n)$.

2 Extended autotopisms of partial Latin squares

An *isotopism of partial Latin squares of order* n will be a triple $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$, where $\gamma(\emptyset) = \emptyset$.

Lemma 2.1 *Let $P \in PLS(n)$ be contained in a Latin square $L \in LS(n)$ and let $\Theta \in \mathcal{I}_n$. The following asserts are verified:*

a) P^Θ is also in $PLS(n)$ and $\left|P^\Theta\right| = |P|$,

b) If $Q \in PLS(n)$ verifies that $P \subseteq Q$, then $P^\Theta \subseteq Q^\Theta$.

c) If P can be completed to L, then P^Θ can be completed to L^Θ. □

Lemma 2.2 *Given $L \in LS(n)$, let $\Theta_1, \Theta_2 \in \mathcal{U}(L)$ be two distinct autotopisms of L. Let us consider $L_{i_1,j_1}, L_{i_2,j_2} \in PLS(n)$ with $(i_1, j_1) \neq (i_2, j_2)$. Then $L_{i_1,j_1}^{\Theta_1} \neq L_{i_2,j_2}^{\Theta_1}$ and $L_{i_1,j_1}^{\Theta_1} \neq L_{i_1,j_1}^{\Theta_2}$.* □

Now, let us consider $L \in LS(n)$ and let $\mathfrak{F} \subseteq \mathcal{U}(L)$. If $P \in PLS(n)$ can be completed to L, we will define $P^{\mathfrak{F}} \in PLS(n)$ as $P^{\mathfrak{F}} = \bigcup_{\Theta \in \mathfrak{F}} P^{\Theta}$. Then, we will say that $P^{\mathfrak{F}}$ is an *extended autotopy* of P.

Lemma 2.3 *Let us suppose $L \in LS(n)$, $P \in PLS(n)$ contained in L and $\mathfrak{F} \subseteq \mathcal{U}(L)$. Then, $\left|P^{\mathfrak{F}}\right| \leq |P| \cdot |\mathfrak{F}|$.* □

Example 2.4 Let $L = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in LS(2)$. So, $\mathcal{U}(L) = \{(Id, Id, Id), ((Id, (01), (01)), ((01), Id, (01)), ((01), (01), Id)\}$. Let us take now by example $\mathfrak{F} = \{(Id, Id, Id), (Id, (01), (01))\}$, $P = \begin{pmatrix} 0 & * \\ * & * \end{pmatrix} \in PLS(2)$ and $Q = \begin{pmatrix} 0 & * \\ * & 1 \end{pmatrix} \in PLS(2)$. Then, we can prove that $P^{\mathfrak{F}} = \begin{pmatrix} 0 & 1 \\ * & * \end{pmatrix}$ and $P^{\mathcal{U}(L)} = L = Q^{\mathfrak{F}} = Q^{\mathcal{U}(L)}$. ◁

In general, given $L \in LS(n)$, there does not exist a subset $\mathfrak{F}$ of $\mathcal{U}(L)$ and $P \in PLS(n)$ such that $P \subset L$ and $P^{\mathfrak{F}} = L$. This is due to that the most of Latin squares has only the trivial autotopism group [1], $\mathcal{U}(L) = \{(Id, Id, Id)\}$. We can therefore ask ourselves about conditions under which we can obtain a similar result to Example 2.4:

Theorem 2.5 *Every entropic Latin square is an extended autotopy of each of its proper partial Latin squares.* □

Example 2.6 Let $L = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \in LS(3)$. It is entropic and verifies that $|\mathcal{U}(L)| = 18$ [1]. Let $\mathfrak{F} = \{(\alpha_s, \alpha_t, \alpha_{l_{st}})\}_{s,t \in N}$, where $\alpha_0 = Id$, $\alpha_1 = (012), \alpha_2 = (021)$. So, $|\mathfrak{F}| = 9$ and $P^{\Theta} = L$ for all $P \in PLS(3)$ contained in L. ◁

3 Critical sets by considering $\mathcal{U}(L)$

Given $L \in LS(n)$ and $\mathfrak{F} \subseteq \mathcal{U}(L)$, let $< \mathfrak{F} >$ be the subgroup of $\mathcal{U}(L)$ generated by composing the elements of $\mathfrak{F} \cup \mathfrak{F}^{-1}$, where $\mathfrak{F}^{-1} = \{\Theta^{-1} = (\alpha^{-1}, \beta^{-1}, \gamma^{-1}) : \Theta = (\alpha, \beta, \gamma) \in \mathfrak{F}\} \subseteq \mathcal{U}(L)$. Now, given $P \in PLS(n)$ contained in L, let us denote by $\mathfrak{F}(P)$ the partial Latin square $P^{<\mathfrak{F}>}$. We will then say that P is *uniquely $\mathfrak{F}$-completable to* L and it will be denoted by $P \in UC_{\mathfrak{F}}(L)$ if $\mathfrak{F}(P) \in UC(L)$. We will say that C is a *$\mathfrak{F}$-critical set of* L if $C \in UC_{\mathfrak{F}}(L)$ and $P \notin UC_{\mathfrak{F}}(L)$ for all $P \subset C$. So, we are interested in the smallest size $scs_{\mathfrak{F}}(L)$ of a $\mathfrak{F}$-critical set of L.

Lemma 3.1 *Let $L \in LS(n)$. The next assertions are verified:*

a) Given $\mathfrak{F}_1, \mathfrak{F}_2 \subseteq \mathcal{U}(L)$ such that $\mathfrak{F}_1 \subseteq \mathfrak{F}_2$, then $scs_{\mathfrak{F}_2}(L) \leq scs_{\mathfrak{F}_1}(L)$.

b) If $\mathfrak{F} \subseteq \mathcal{U}(L)$ is such that $| < \mathfrak{F} > | \geq lcs(L)$, then $scs_{\mathfrak{F}}(L) = 1$. □

Lemma 3.2 *Let $L \in LS(n)$, $P \in PLS(n)$ contained in L and $\mathfrak{F} \subseteq \mathcal{U}(L)$. Let $C \in CS(L)$ be such that $|C| = scs(L)$. If $C \subseteq \mathfrak{F}(P)$ then, $scs_{\mathfrak{F}}(L) \leq |P|$. So, $scs_{\mathfrak{F}}(L) \leq scs(L)$, for all $\mathfrak{F} \subseteq \mathcal{U}(L)$, such that $\mathfrak{F} \neq \emptyset$.* $\square$

Proposition 3.3 *Let $L \in LS(n)$, $P \in PLS(n)$ contained in L and $\mathfrak{F} \subseteq \mathcal{U}(L)$. Then, $scs_{\mathfrak{F}}(L) = \min_{P \in PLS(n)} \{|P| : \exists C \in CS(L)$ such that $C \subseteq \mathfrak{F}(P)\}$.* $\square$

Example 3.4 Let $L = \begin{pmatrix} 0&1&2&3&4 \\ 1&2&3&4&0 \\ 2&3&4&0&1 \\ 3&4&0&1&2 \\ 4&0&1&2&3 \end{pmatrix} \in LS(5)$, $C = \begin{pmatrix} 0&1&*&*&* \\ 1&*&*&*&* \\ *&*&*&*&* \\ *&*&*&*&2 \\ *&*&*&2&3 \end{pmatrix} \in CS(L)$ and $P = \begin{pmatrix} 0&1&*&*&* \\ *&*&*&*&* \\ *&*&*&*&* \\ *&*&*&1&2 \\ *&*&*&*&* \end{pmatrix} \in PLS(5)$. Let $\mathfrak{F} = \{((04321), Id, (04321))\} \subseteq \mathcal{U}(L)$. So, $C \subseteq P \cup P^{\mathfrak{F}} = \begin{pmatrix} 0&1&*&*&* \\ 1&2&*&*&* \\ *&*&*&*&* \\ *&*&*&1&2 \\ *&*&*&2&3 \end{pmatrix}$ and therefore, $scs_{\mathfrak{F}}(L) \leq 4 < 6 = scs(L)$. $\lhd$

3.1 An algorithm to obtain an upper bound of $scs_{\mathfrak{F}}(L)$

Lemma 3.5 *Let $L = (l_{ij}) \in LS(n)$, $\mathfrak{F} \subseteq \mathcal{U}(L)$, $P \in PLS(n)$ be contained in L such that $|P| = scs_{\mathfrak{F}}(L)$ and $C \in CS(L)$ be contained in $\mathfrak{F}(P)$. For all $i, j \in N$, there exist $(s, t, l_{st}) \in C$ and $\Theta \in <\mathfrak{F}>$ such that $L^{\Theta}_{i,j} = L_{s,t}$.* $\square$

Lemma 3.6 *Let $L \in LS(n)$, $\mathfrak{F} \subseteq \mathcal{U}(L)$, $P \in PLS(n)$ be contained in L such that $|P| = scs_{\mathfrak{F}}(L)$ and $C \in CS(L)$ be contained in $\mathfrak{F}(P)$. Then $P \subseteq \mathfrak{F}(C)$.* $\square$

In general, given $L = (l_{ij}) \in LS(n)$, $P = \bigcup_{(i,j) \in I_P} L_{i,j} \in PLS(n)$ contained in L and $\mathfrak{F} \subseteq \mathcal{U}(L)$, we must be interested in an algorithm which allows us to obtain the number $scs_{\mathfrak{F}}(L)$. To do it, let $\mathfrak{F}(P) = \bigcup_{(i,j) \in I_{\mathfrak{F}(P)}} L_{i,j} \in PLS(n)$, which is contained in L. Given $(i, j, l_{ij}) \in \mathfrak{F}(P)$, let us consider:

$$S^P_{i,j} = \{(s, t, l_{st}) \in P \text{ such that } L_{i,j} \subseteq \mathfrak{F}(L_{s,t})\} \subseteq P.$$

Lemma 3.7 *Let $L \in LS(n)$, $P, Q \in PLS(n)$ be both contained in L and $\mathfrak{F} \subseteq \mathcal{U}(L)$. If $Q \subseteq \mathfrak{F}(P)$ and $P \subseteq \mathfrak{F}(Q)$, then $P = \bigcup_{(i,j) \in I_Q} S^P_{i,j}$ and $Q = \bigcup_{(i,j) \in I_P} S^Q_{i,j}$.* $\square$

Theorem 3.8 *Let $L \in LS(n)$ and $\mathfrak{F} \subseteq \mathcal{U}(L)$. Then $scs_{\mathfrak{F}}(L)$ is equal to:*

$$\min_{C \in CS(L)} \left\{ \min \left\{ |P| : \exists I_P \subseteq I_{\mathfrak{F}(C)} \text{ being } P = \bigcup_{(i,j) \in I_P} L_{i,j},\ C = \bigcup_{(i,j) \in I_P} S^C_{i,j} \right\} \right\}.$$

Proof. Let $C \in CS(L)$ and $I_P \subseteq I_{\mathfrak{F}(C)}$ be such that $C = \bigcup_{(i,j)\in I_P} S_{i,j}^C$, being $P = \bigcup_{(i,j)\in I_P} L_{i,j} \subseteq \mathfrak{F}(C)$. So, given $(s,t,l_{st}) \in C$, there exists $\Theta \in <\mathfrak{F}>$ and $(i,j) \in I_P$ such that $L_{s,t}^{\Theta} = L_{i,j}$. Then, $L_{i,j}^{\Theta^{-1}} = L_{s,t}$ and so, $(s,t,l_{st}) \in \mathfrak{F}^{-1}(P) = \mathfrak{F}(P)$. Therefore, we have that $C \subseteq \mathfrak{F}(P)$. So, from Proposition 3.3, $scs_{\mathfrak{F}}(L)$ is smaller than the signaled minimum. Now, let $P \in PLS(n)$ contained in L be such that $|P| = scs_{\mathfrak{F}}(L)$. From Proposition 3.3, there exist $C \in CS(L)$ contained in $\mathfrak{F}(P)$. Besides, from Lemma 3.6, $P \subseteq \mathfrak{F}(C)$. So, Lemma 3.7 involves $C = \bigcup_{(i,j)\in I_P} S_{i,j}^C$, being $I_P \subseteq I_{\mathfrak{F}(C)}$, and therefore, by using Proposition 3.3 again, $scs_{\mathfrak{F}}(L)$ is bigger than the signaled minimum. $\square$

The computation of the minimum of the previous theorem allows us to obtain $scs_{\mathfrak{F}}(L)$ but it can be an arduous process. In a concrete case, a first upper bound of $scs_{\mathfrak{F}}(L)$ can be given by the following way: let $C \in CS(L)$ be such that $|C| = scs(L)$. Let us obtain $\mathfrak{F}(C)$ and next all the sets $S_{i,j}^C$. If the cardinality of all these sets is one, then we cannot improve the upper bound of $scs(L)$ by using this critical set C. In the other case, let $n_1 > 1$ be the maximum of the mentioned cardinalities and let us take S_{i_1,j_1}^C a set with cardinality n_1. Let us now fixe $(s_1,t_1,l_{s_1t_1}) \in S_{i_1,j_1}^C$ and let $\Theta_1 \in \mathfrak{F}$ be such that $L_{s_1,t_1}^{\Theta_1} = L_{i_1,j_1}$. Let us then consider $C_1 = C \setminus \left(S_{i_1,j_1}^C \setminus \{(s_1,t_1,l_{s_1t_1})\}\right)$ and $P_1 = C_1^{\Theta_1} \subseteq C^{\Theta_1}$. So, $|P_1| = |C_1| < |C|$ and it can be seen that $C \subseteq \mathfrak{F}(P_1)$ and therefore, $scs_{\mathfrak{F}}(L) \leq |C_1| < scs(L)$. Now we can take the same procedure with C_1 instead of C. If the cardinality of all the corresponding $S_{i,j}^{C_1}$ is one, then we cannot improve the upper bound of $scs_{\mathfrak{F}}(L)$ by using this method with C. In the other case, we take $S_{i_2,j_2}^{C_1}$ a set with cardinality $n_2 > 1$, the maximum of the mentioned cardinalities, and we fixe $(s_2,t_2,l_{s_2t_2}) \in S_{i_2,j_2}^{C_1}$. Let us observe that it is necessary to take $(s_2,t_2,l_{s_2t_2}) = (s_1,t_1,l_{s_1t_1})$ whenever it is possible. So, we consider $C_2 = C_1 \setminus \left(S_{i_2,j_2}^{C_1} \setminus \{(s_2,t_2,l_{s_2t_2})\}\right) \subseteq C_1$, being $\Theta_2 \in \mathfrak{F}$ such that $L_{s_2,t_2}^{\Theta_2} = L_{i_2,j_2}$. Let $P_2 = C_2^{\Theta_2} \subseteq C_1^{\Theta_2}$. By construction, $C_1 \subseteq \mathfrak{F}(P_2)$ and so, $P_1 \subseteq \mathfrak{F}(C_1) \subseteq \mathfrak{F}(\mathfrak{F}(P_2)) = \mathfrak{F}(P_2)$. Finally, $C \subseteq \mathfrak{F}(P_1) \subseteq \mathfrak{F}(\mathfrak{F}(P_2)) = \mathfrak{F}(P_2)$. Therefore, $scs_{\mathfrak{F}}(L) \leq |P_2| = |C_2| < |C_1|$. We repeat all this procedure until we find that the maximum cardinality of all the corresponding sets $S_{i,j}$ is one.

Example 3.9 In Example 3.4, where $\mathfrak{F}(C) = \begin{pmatrix} 0 & 1 & * & 3 & 4 \\ 1 & 2 & * & 4 & 0 \\ 2 & 3 & * & 0 & 1 \\ 3 & 4 & * & 1 & 2 \\ 4 & 0 & * & 2 & 3 \end{pmatrix}$, we can see that, for all $i \in N$, $\left|S_{i,j}^C\right| = \begin{cases} 1, \text{ if } j = 1 \text{ or } 3, \\ 2, \text{ if } j = 0 \text{ or } 4. \end{cases}$. Let us then take for example $S_{0,0}^C = \{(0,0,0),(1,0,0)\}$ and let us consider $(0,0,0) \in S_{0,0}^C$. So, $C_1 =$

$C \setminus L_{1,0} = \begin{pmatrix} 0 & 1 & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & 2 \\ * & * & * & 2 & 3 \end{pmatrix}$. Besides, it will be $P_1 = C_1$ because $L_{0,0}^{Id} = L_{0,0}$. So, $C \subseteq \mathfrak{F}(P_1) = \mathfrak{F}(C)$ and $scs_{\mathfrak{F}}(L) \leq |C_1| = 5$. Now, for all $i \in N$, $\left|S_{i,j}^{C_1}\right| = \begin{cases} 1, \text{ if } j = 0, 1 \text{ or } 3, \\ 2, \text{ if } j = 4. \end{cases}$. Let us take $S_{3,4}^{C_1} = \{(3,4,2),(4,4,3)\}$ and let us consider $(3,4,2) \in S_{0,0}^{C}$. So, $C_2 = C_1 \setminus L_{3,4} = \begin{pmatrix} 0 & 1 & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & 2 \\ * & * & * & 2 & * \end{pmatrix} = P_2$, as $L_{3,4}^{Id} = L_{3,4}$. So, $C \subseteq \mathfrak{F}(P_2) = \mathfrak{F}(C)$ and $scs_{\mathfrak{F}}(L) \leq |C_1| = 4$, as we have seen in Example 3.4. Thus, $S_{i,j}^{C_2} = 1$ for all i, j and so, the algorithm finishes. $\lhd$

References

[1] B. D. McKay, A. Meynert and W. Myrvold, Small Latin Squares, Quasigroups and Loops, Journal of Combinatorial Designs 15 (2007) 98-119.