Graphs related to principal autotopisms of Latin squares

Falcón Ganfornina, R.M.

Department of Geometry and Topology
University of Seville
Seville
rafalgan@us.es

Abstract. Latin squares of order n are equivalent to 1-factorizations of $K_{n,n}$. In this way, fixed a principal isotopism $\Theta = (\alpha, \beta, \varepsilon) \in S_n^3$, where S_n is the symmetric group of the set $N = \{0, 1, ..., n-1\}$, we are going to study in this paper the set of graphs related to Θ when this last one is a principal autotopism of a Latin square. To do it, the number $\Delta_R(\Theta)$ of reduced Latin squares having Θ as a principal autotopism is studied.

Keywords. Latin square, Autotopism group, 1-factorization.

1. Introduction

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 of* G. An *isomorphism* from a 1-factorization $F = [f_0, f_1, ..., f_{n-1}]$ of a graph G to a 1-factorization $F' = [f'_0, f'_1, ..., f'_{n-1}]$ of a graph G' is a pair (Φ, π), where Φ is a bijection between the vertices of G and G' and $\pi : S \rightarrow S$ is a permutation of the elements of the set $S = \{0, 1, ..., n-1\}$, such that $\Phi(E_{f_i}) = E_{f'_{\pi(i)}}$ for all $i \in N$.

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. The set of Latin squares of order n is denoted by $LS(n)$. 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 $\{(i, j, l_{ij}) : i, j \in N\}$. By permuting in the same way the coordinates in each one of these triples, it is obtained one of the six *conjugate* Latin squares associated to L. $L = (l_{ij})$ is a *reduced Latin square* if $l_{0k} = k = l_{k0}$ for all $k \in N$. The set of reduced Latin squares of order n is denoted by $RLS(n)$. 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 $PLS(n)$. An *isotopism* of a Latin square L is a triple $\Theta = (\alpha, \beta, \gamma) \in \mathscr{I}_n = S_n \times S_n \times S_n$, where S_n is the symmetric group of N and so, 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. If $\gamma = \varepsilon$, the identity map on N, Θ is called a *principal isotopism*. An isotopism which maps L to itself is an *autotopism*. $(\varepsilon, \varepsilon, \varepsilon)$ is called the *trivial autotopism*. The stabilizer subgroup of L in $\mathscr{I}_n$ is its *autotopism group*, $\mathscr{U}(L) = \{\Theta \in \mathscr{I}_n : L^{\Theta} = L\}$. Fixed $\Theta \in \mathscr{I}_n$, the set of all Latin squares L such that $\Theta \in \mathscr{U}(L)$ is denoted by $LS(\Theta)$. The *main class* of L is the set of all Latin squares isotopic to some conjugate of L.

Every Latin square of order n is equivalent to a 1-factorization of a bipartite graph $K_{n,n}$ [3]. In particular, given a Latin square $L \in LS(n)$ and fixed a set of n colors $\{c_0, c_1, ..., c_{n-1}\}$, it can be defined a bipartite graph $G = (V, E)$ with colored edges. To do it, V is partitioned into two subsets U and W, where $|U| = |W| = n$ and U and W represent, respectively, the rows and columns in L. Besides, if $(i, j, k) \in L$, then there will be an edge of color c_k joining the vertices $i \in U$ and $j \in W$. Each symbol of L determines therefore a monochromatic 1-factor of G and so, we obtain a 1-factorization $\mathscr{F}(L) = [f_0, f_1, ..., f_{n-1}]$ of G, where each 1-factor f_i is associated to the color c_i. The reciprocal construction is also possible in a similar way and we can then construct a Latin square $\mathscr{L}(F)$ associated to each 1-factorization F of $K_{n,n}$. Indeed, $\mathscr{F}(\mathscr{L}(F)) = F$ and $\mathscr{L}(\mathscr{F}(L)) = L$. In particular, F and F' are two isomorphic 1-factorizations if and only if $\mathscr{L}(F)$ and $\mathscr{L}(F')$ are in the same main class.

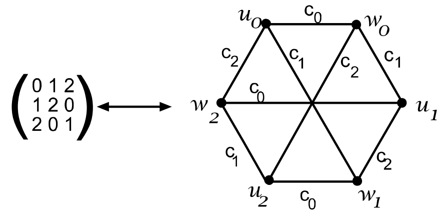


Figure 1: 1-factorization of $K_{3,3}$ starting from a Latin square.

Cardinalities of autotopism groups have been studied to obtain the number of Latin squares of order up to 11 [5], where computer programs incorporating two methods of approach to generation are used: the orderly approach method [2] and the canonical construction path method (CCPM) [4]. In particular, this last one allows to construct a Latin square one *row block* at a time, where a row block consists of the rows corresponding to a cycle of α. Besides, fixed an isotopism

$\Theta = (\alpha, \beta, \gamma) \in \mathscr{I}_n$, the CCPM has been also used [1] to study the number $\Delta(\Theta)$ of Latin squares $L \in LS(n)$ such that $L \in LS(\Theta)$:

Proposition 1. *Let $\Theta = (\alpha, \beta, \gamma) \in \mathscr{I}_n$ 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 $\frac{n}{k}$.*

Theorem 1. *Fixed $k \in \mathbb{N}$, let $\Theta = (\alpha, \beta, \varepsilon) \in \mathscr{I}_n$, where $n > k$ is a multiple of k, be such that α and β are both the composition of k cycles of length $\frac{n}{k}$. Then:*

$$\Delta(\Theta) = n! \cdot \left(\frac{n}{k}!\right)^{k(k-1)} \cdot \Omega(\Theta),$$

where $\Omega(\Theta)$ is 1, if $k = 1$, and the number of different ways in which the row blocks can be chosen in the CCPM, if $k > 1$.

n	k	$\Omega(\Theta)$	$\Delta(\Theta)$	n	k	$\Omega(\Theta)$	$\Delta(\Theta)$
2	1	1	2	6	1	1	720
					2	1	25920
					3	10	460800
3	1	6	12	7	1	1	5040
4	1	1	24	8	1	1	40320
	2	1	96		2	1	23224320
					4	535	88355635200
5	1	1	120	9	1	1	362880
					3	56	948109639680

Table 1: Values of $\Omega(\Theta)$ and $\Delta(\Theta)$ when $2 \leq n \leq 9$.

The number $\Delta(\Theta)$ is useful in Cryptography, when a Latin square L and a family $\mathfrak{F} \subseteq \mathscr{U}(L)$ are used to get a *secret-sharing system*, that 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. Specifically, in this case, $K = L$ and the shares are the triples of L and the isotopisms of $\mathfrak{F}$. In this way, the weight of information given by the latter is usually greater than that given by the former. On the contrary, the size of an isotopism is much larger than that of a triple. As this problem rises with n, it is necessary to identify an isotopism with a share of a smaller size. In this paper we study one possibility in this sense, when Θ is a principal isotopism such that the number $\Delta_R(\Theta)$ of reduced

Latin squares having Θ as an autotopism is positive. In this way, we study the set of 1-factorizations associated to these reduced Latin squares and we identify Θ with a graph $\mathscr{G}_\Theta$ of smallest size with colored vertices and edges.

2. The canonical construction path method.

Fixed $n \in \mathbb{N}$ and $\Theta \in \mathscr{I}_n$, $\Delta_R(\Theta)$ will denote the cardinal of the set $RLS(\Theta)$ of reduced Latin squares of order n such that Θ is an autotopism of all of them. In this paper, we are interested in the value of $\Delta_R(\Theta)$ if Θ is a non-trivial principal isotopism. From Proposition 1, it suffices to study those isotopisms $\Theta = (\alpha, \beta, \varepsilon)$, such that α and β have all their cycles of the same length and without fixed points:

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

where $C_i^\delta = \left(c_{i,0}^\delta \; c_{i,1}^\delta \; \ldots \; c_{i,\frac{n}{k}-1}^\delta\right)$ is a cycle of length $\frac{n}{k}$ for all $\delta \in \{\alpha, \beta\}$ and $i \in \{0,1,...,k-1\}$, being $c_{i,j}^\delta \in N$, for all $j \in \{0,1,...,\frac{n}{k}-1\}$. Besides, it must be $c_{i,j}^\delta \neq c_{k,l}^\delta$, for all $(i,j) \neq (k,l)$. From now on, we will suppose that $c_{0,0}^\alpha = c_{0,0}^\beta = 0$.

Lemma 1. *If* $C_0^\beta \neq \left(C_0^\alpha\right)^{-1}$*, then* $\Delta_R(\Theta) = 0$.

Now, if we want to find a reduced Latin square $L = (l_{ij}) \in RLS(\Theta)$, we will use the CCPM. So, we define the following subrectangles of L:

$$R^{i,j} = \left\{ \left(c_{i,s}^\alpha, c_{j,t}^\beta, l_{c_{i,s}^\alpha \, c_{j,t}^\beta} \right) : s,t \in \{0,1,...,\frac{n}{k}-1\} \right\},$$

for all $i,j \in \{0,1,...,k-1\}$. When all these subrectangles are known, then L is determined. Due to it, it is useful to define also the following sets:

$$S^{i,j} = \left\{ l_{st} : (s,t,l_{st}) \in R^{i,j} \right\}, \text{ for all } i,j \in \{0,1,...,k-1\}.$$

Lemma 2. *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* $j \in \{0,1,...,k-1\}$.

c) $\bigcup_{j=0}^{k-1} S^{i,j} = N$*, for all* $i \in \{0,1,...,k-1\}$.

d) If $(i,j) \neq (s,t)$*, then* $S^{i,j} \cap S^{s,t} = \emptyset$ *whenever* $i = s$ *or* $j = t$.

e) $S^{i,0} = S^{0,i} = \left\{ i \cdot \frac{n}{k}, i \cdot \frac{n}{k} + 1, ..., (i+1) \cdot \frac{n}{k} - 1 \right\}$*, for all* $i \in \{0,1,..., k-1\}$.

- *f) If l_{st} is known, being $(s,t,l_{st}) \in R^{i,j}$, then the $\frac{n}{k}$ cells (u,v,l_{uv}) of $R^{i,j}$ such that $l_{uv} = l_{st}$ are known.*
- *g) If $S^{i,j}$ is known then $R^{i,j}$ can be chosen of $\frac{n}{k}!$ ways.*

As a consequence, the subrectangles $R^{i,0}$ and $R^{0,j}$ are known for all $i,j \in \{0,1,...,k-1\}$ and we can define the following partial Latin square:

$$P_\Theta = \bigcup_i R^{i,0} \cup \bigcup_j R^{0,j} \in PLS(n),$$

which is common to all Latin squares of $RLS(\Theta)$. Indeed, to determine L, we only must fix the $(k-1)^2$ subrectangles $R^{i,j}$ with $i \neq 0 \neq j$.

Theorem 2. $\Delta_R(\Theta) = \left(\frac{n}{k}!\right)^{(k-1)^2} \cdot \Omega_R(\Theta)$, *where $\Omega_R(\Theta)$ denotes the number of different ways in which the elements of all sets $S^{i,j}$ can be chosen.*

In particular, the cases $k \in \{1,2,3,4\}$ of Table 1 are easily computable by following the CCPM. The following result is then verified:

Theorem 3. *Fixed $k \in \{1,2,3,4\}$, let $\Theta = (\alpha,\beta,\varepsilon) \in \mathscr{I}_n$, where $n > k$ is a multiple of k, be such that α and β are both the composition of two cycles of length $\frac{n}{k}$, being $C_0^\beta = (C_0^\alpha)^{-1}$. Then:*

a) If $k \neq 4$: $\Omega_R(\Theta) = 1, \quad \Delta_R(\Theta) = \begin{cases} 1, \text{ if } k = 1, \\ \frac{n}{2}!, \text{ if } k = 2, \\ \left(\frac{n}{3}!\right)^4, \text{ if } k = 3. \end{cases} \quad .$

b) If $k = 4$:

$$\Omega_R(\Theta) = \textstyle\sum_{a,b} \begin{pmatrix} \frac{n}{4} \\ a \end{pmatrix} \begin{pmatrix} \frac{n}{4} \\ b \end{pmatrix} \begin{pmatrix} \frac{n}{4} \\ a+b \end{pmatrix} \cdot \textstyle\sum_c \begin{pmatrix} \frac{n}{4}-a \\ c \end{pmatrix} \begin{pmatrix} a+b \\ \frac{n}{4}-c \end{pmatrix} \cdot$$
$$\cdot \textstyle\sum_d \begin{pmatrix} \frac{n}{4}-a \\ d \end{pmatrix} \begin{pmatrix} a+b+c-\frac{n}{4} \\ c-d \end{pmatrix} \cdot \textstyle\sum_e \begin{pmatrix} \frac{n}{4}-c-d \\ e \end{pmatrix} \begin{pmatrix} \frac{n}{4} \\ d+e \end{pmatrix}.$$

3. 1-factorizations associated to principal autotopisms of reduced Latin squares

Let $\Theta \in \mathscr{I}_n$ such that $\Delta_R(\Theta) > 0$. By following the CCPM described in the previous section, we can define the set $RLS(\Theta)$, starting from the subrectangles $R^{i,j}$ associated to Θ. So, we can define the set $\mathscr{F}(RLS(\Theta)) = \{\mathscr{F}(L) : L \in RLS(\Theta)\}$. As we have previously observed, all Latin squares of $RLS(\Theta)$ have the partial Latin square P_Θ in common. Due to it, it can be useful to extend to partial Latin

n	2	3	4		5	6			7	8			9	
k	1	1	1	2	1	1	2	3	1	1	2	4	1	3
$\Omega_R(\Theta)^*$	1	1	1	1	1	1	1	1	1	1	1	145	1	1
$\Delta_R(\Theta)^*$	1	1	1	2	1	1	6	16	1	1	24	74240	1	1296

$*$ Being $C_0^{\beta} = \left(C_0^{\alpha}\right)^{-1}$. Otherwise, $\Delta_R(\Theta) = 0$.

Table 2: Values of $\Omega_R(\Theta)$ and $\Delta_R(\Theta)$ when $2 \leq n \leq 9$.

squares the above algorithm which allows to construct a 1-factorization starting from a Latin square. Indeed, it is enough to ignore in the mentioned algorithm those edges corresponding to triples $(i, j, \emptyset)$. In this way, we will obtain a subgraph of $K_{n,n}$ with colored edges. Fixed $P \in PLS(n)$, we will denote this subgraph as $\mathscr{F}(P)$.

Proposition 2. *The following asserts are verified:*

a) $|\mathscr{F}(RLS(\Theta))| = \Delta_R(\Theta)$.

b) $\bigcap_{F \in \mathscr{F}(RLS(\Theta))} F = \mathscr{F}(P_\Theta)$.

Let us see an example:

Example 1. Let $N = \{0,1,2,3\}$. The unique possible isotopisms verifying the conditions of Theorem 3 for $k = 2$ are:

$$\Theta_1 = ((01)(23),(01)(23),\varepsilon); \quad \Theta_2 = ((02)(13),(02)(13),\varepsilon);$$
$$\Theta_3 = ((03)(12),(03)(12),\varepsilon).$$

Now, the graphs $\mathscr{F}(P_{\Theta_i})$ related to each Θ_i are shown in Table 3. Indeed, it can be proved that $\mathscr{F}(P_{\Theta_1})$, $\mathscr{F}(P_{\Theta_2})$ and $\mathscr{F}(P_{\Theta_3})$ are isomorphic 1-factorizations.

However, we can find an other graph related to Θ with smaller size than $\mathscr{F}(P_\Theta)$. To do it, it is enough to observe that the first row and column of P_Θ are fixed with the elements of $N = \{0,1,...,n-1\}$, which determine the colours of $\mathscr{F}(P_\Theta)$. So, we can follow this algorithm:

Algorithm 1.

i) Fixed $i \neq 0$, we colour each pair of vertex u_i and w_i with the color c_i.

ii) We eliminate the vertices $u_0 \in U$, and $w_0 \in W$ and their incident edges.

The resulting graph has therefore colored vertices and edges and determines Θ. This graph will be denoted by $\mathscr{G}_\Theta$ and it will be called the *graph related to* Θ. In Table 4, we can see the case of Example 1.

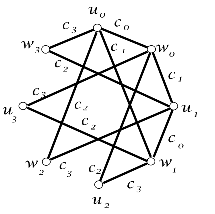
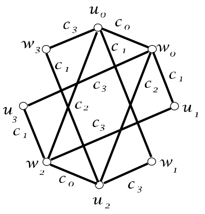
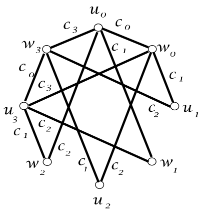
Θ_i	Θ_1	Θ_2	Θ_3
$RLS(\Theta_i)$	$\begin{pmatrix}0&1&2&3\\1&0&3&2\\2&3&0&1\\3&2&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&2&3\\1&0&3&2\\2&3&1&0\\3&2&0&1\end{pmatrix}$	$\begin{pmatrix}0&1&2&3\\1&0&3&2\\2&3&0&1\\3&2&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&2&3\\1&2&3&0\\2&3&0&1\\3&0&1&2\end{pmatrix}$	$\begin{pmatrix}0&1&2&3\\1&0&3&2\\2&3&0&1\\3&2&1&0\end{pmatrix}$ $\begin{pmatrix}0&1&2&3\\1&3&0&2\\2&0&3&1\\3&2&1&0\end{pmatrix}$
P_{Θ_i}	$\begin{pmatrix}0&1&2&3\\1&0&3&2\\2&3&-&-\\3&2&-&-\end{pmatrix}$	$\begin{pmatrix}0&1&2&3\\1&-&3&-\\2&3&0&1\\3&-&1&-\end{pmatrix}$	$\begin{pmatrix}0&1&2&3\\1&-&-&2\\2&-&-&1\\3&2&1&0\end{pmatrix}$
$\mathscr{F}(P_{\Theta_i})$	 u_0 c_3 c_0 w_3 c_1 w_0 c_2 c_1 c_3 u_3 c_2 u_1 c_2 c_0 w_2 c_3 c_2 w_1 c_3 u_2	 u_0 c_3 c_0 w_3 c_1 w_0 c_1 c_3 c_2 c_1 c_2 u_3 u_1 c_1 c_3 w_2 w_1 c_0 c_3 u_2	 u_0 c_3 c_0 w_3 c_1 w_0 c_0 c_3 c_1 u_3 c_2 u_1 c_1 c_2 c_2 w_2 c_1 c_2 w_1 u_2

Table 3: Graphs $\mathscr{F}(P_{\Theta_i})$ related to Θ_i.

4. Final remarks

The graph $\mathscr{G}_\Theta$ allows to recover the isotopism Θ. In this way, we can consider a set of vertices and edges of $\mathscr{G}_\Theta$ as shares in a secret-sharing system. 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 system and to adjust the weight of information of the used shares. Anyway, it is possible to find a graph of smaller size than $\mathscr{G}_\Theta$. 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 $\mathscr{G}_\Theta$ and we can therefore obtain a graph of the smallest size allowing to recover Θ. It would be therefore necessary an analogous study to that of *forcing sets* of a 1-factorization.

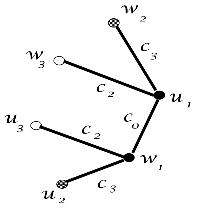
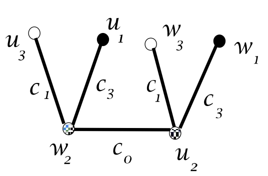
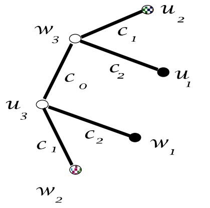
Θ_i	Θ_1	Θ_2	Θ_3
$\mathscr{G}_{\Theta_i}$	 w_2 c_3 w_3 c_2 u_1 c_0 u_3 c_2 w_1 u_2 c_3	 u_3 u_1 w_3 w_1 c_1 c_3 c_1 c_3 w_2 c_0 u_2	 u_2 w_3 c_1 c_2 u_1 c_0 u_3 c_2 c_1 w_1 w_2

Table 4: Graphs $\mathscr{G}_{\Theta_i}$ related to Θ_i.

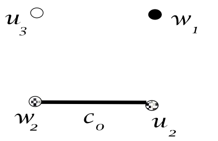


Figure 2: Forcing set related to the isotopism Θ_2 of Example 1.

References

[1] FALCÓN GANFORNINA, R. M. *Latin squares associated to principal autotopisms of long cycles. Application in Cryptography.* Transgressive Computing 2006, Granada (Spain).

[2] FARADZEV, I. A. *Constructive enumeration of combinatorial objects*, Problèmes combinatoires et théorie des graphes. Colloque International. CNRS 260. CNRS Paris (1978) 131 - 135.

[3] 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.

[4] MCKAY, B. D. *Isomorph-free exhaustive generation.* J. Algorithms 26 (1998) 306 - 324.

[5] MCKAY, B. D., MEYNERT, A., MYRVOLD, W. *Small Latin squares, quasigroups and loops.* J. Combinatorial Designs. To appear.