Available online at www.sciencedirect.com
ScienceDirect

Journal of Symbolic Computation 42 (2007) 1142–1154

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Gröbner bases and the number of Latin squares related to autotopisms of order ≤ 7

R.M. Falcón[a,*], J. Martín-Morales[b]

[a] Department of Geometry and Topology, University of Seville, Avda. Reina Mercedes s/n - 41080, Seville, Spain
[b] Department of Mathematics, University of Zaragoza, C/ Pedro Cerbuna, 12 - 50009, Zaragoza, Spain

Received 11 December 2006; accepted 15 July 2007
Available online 1 September 2007

Abstract

Latin squares can be seen as multiplication tables of quasigroups, which are, in general, non-commutative and non-associative algebraic structures. The number of Latin squares having a fixed isotopism in their autotopism group is at the moment an open problem. In this paper, we use Gröbner bases to describe an algorithm that allows one to obtain the previous number. Specifically, this algorithm is implemented in SINGULAR to obtain the number of Latin squares related to any autotopism of Latin squares of order up to 7.
© 2007 Elsevier Ltd. All rights reserved.

Keywords: Autotopism group; Gröbner basis; Latin square

1. Introduction

A *quasigroup* (Albert, 1943) is a nonempty set G endowed with a product $\cdot$, such that if any two of the three symbols a, b, c in the equation $a \cdot b = c$ are given as elements of G, the third one is uniquely determined as an element of G. This is equivalent to saying that G is endowed with left and right division. Specifically, quasigroups are, in general, non-commutative and non-associative algebraic structures. Two quasigroups $(G, \cdot)$ and $(H, \circ)$ are *isotopic* (Bruck, 1944) if there are three bijections α, β, γ from H to G, such that $\gamma(a \circ b) = \alpha(a) \cdot \beta(b)$, for all $a, b \in H$. The triple $\Theta = (\alpha, \beta, \gamma)$ is called an *isotopism* from $(G, \cdot)$ to $(H, \circ)$.

* Corresponding author. Tel.: +34 954559941; fax: +34 954557878.
E-mail addresses: rafalgan@us.es (R.M. Falcón), jorge@unizar.es (J. Martín-Morales).
URLs: http://www.personal.us.es/raufalgan (R.M. Falcón), http://www.grupo.us.es/gmcedm (J. Martín-Morales).

0747-7171/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2007.07.004

Table 1
Number of Latin squares of order $2 \leq n \leq 7$

n	2	3	4	5	6	7
N_n	2	12	576	161280	812851200	61479419904000

$$\begin{cases} L_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\ \\ \Theta = ((12)(34), (23), \epsilon) \in \mathcal{I}_4((0,2,0,0),(2,1,0,0),(4,0,0,0)) \end{cases} \Rightarrow L_1^{\Theta} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 3 & 2 & 4 \\ 4 & 2 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

Fig. 1. Isotopism permuting 1st with 2nd and 3rd with 4th rows and 2nd with 3rd columns.

The multiplication table of a quasigroup is a Latin square. A *Latin square* L of order n is an $n \times n$ array with elements chosen from a set of n distinct symbols $\{x_1, \ldots, x_n\}$, such that each symbol occurs precisely once in each row and each column. The set of Latin squares of order n is denoted by $LS(n)$. The number of Latin squares of order n is denoted by N_n (Table 1). 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 as $PLS(n)$. An exhaustive study as regards Latin squares and their applications is given by Laywine and Mullen (1998).

In this paper, for any given $n \in \mathbb{N}$, we denote by $[n]$ the set $\{1, 2, \ldots, n\}$. Specifically, we assume that the set of symbols of any Latin square of order n is $[n]$. The symmetric group on $[n]$ is denoted by S_n. Given a permutation $\delta \in S_n$, there is defined the set of its *fixed points* $\mathrm{Fix}(\delta) = \{i \in [n] \mid \delta(i) = i\}$. The *cycle structure of* δ is the sequence $\mathbf{l}_\delta = (\mathbf{l}_1^\delta, \mathbf{l}_2^\delta, \ldots, \mathbf{l}_n^\delta)$, where $\mathbf{l}_i^\delta$ is the number of cycles of length i in δ, for all $i \in \{1, 2, \ldots, n\}$. On the other hand, given $L = (l_{i,j}) \in LS(n)$, the *orthogonal array representation of* L is the set of n^2 triples $\{(i, j, l_{i,j}) \mid i, j \in [n]\}$. The previous set is identified with L and then one writes $(i, j, l_{i,j}) \in L$, for all $i, j \in [n]$. Analogously, any $P \in PLS(n)$ will be identified with the set $\{(i, j, l_{i,j}) \mid i, j \in [n], l_{i,j} \neq \emptyset\}$. Given $\sigma \in S_3$, one defines the *conjugate Latin square* $L^\sigma \in LS(n)$ of L, such that if $T = (i, j, l_{i,j}) \in L$; then $(\pi_{\sigma(1)}(T), \pi_{\sigma(2)}(T), \pi_{\sigma(3)}(T)) \in L^\sigma$, where π_i gives the ith coordinate of T, for all $i \in [3]$. In this way, each Latin square L has six conjugate Latin squares associated with it: $L^{Id} = L$, $L^{(12)} = L^t$, $L^{(13)}$, $L^{(23)}$, $L^{(123)}$ and $L^{(132)}$.

Since a Latin square is the multiplication table of a quasigroup, an *isotopism* of a Latin square $L \in LS(n)$ is therefore a triple $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n = S_n \times S_n \times S_n$. In this way, α, β and γ are permutations of rows, columns and symbols of L, respectively. The resulting square L^Θ is also a Latin square and it is said to be *isotopic* to L (Fig. 1). In particular, if $L = (l_{i,j})$, then $L^\Theta = \{(i, j, \gamma(l_{\alpha^{-1}(i), \beta^{-1}(j)}) \mid i, j \in [n]\}$. If $\gamma = \epsilon$, the identity map on $[n]$, Θ is called a *principal isotopism*. The *cycle structure* of an isotopism $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ is the triple $(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$, where $\mathbf{l}_\delta$ is the cycle structure of δ, for all $\delta \in \{\alpha, \beta, \gamma\}$. The set of isotopisms of Latin squares of order n having $(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$ as their cycle structures is denoted by $\mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$.

An isotopism which maps L to itself is an *autotopism*. $(\epsilon, \epsilon, \epsilon)$ is called the *trivial autotopism*. The possible cycle structures of the set of non-trivial autotopisms of Latin squares of order up to 11 have been obtained by Falcón (in press). The stabilizer subgroup of L in $\mathcal{I}_n$ is its *autotopism group*, $\mathcal{U}(L) = \{\Theta \in \mathcal{I}_n \mid L^\Theta = L\}$. Given $L \in LS(n)$, $\Theta = (\alpha, \beta, \gamma) \in \mathcal{U}(L)$ and $\sigma \in S_3$, it is verified that $\Theta^\sigma = (\pi_{\sigma(1)}(\Theta), \pi_{\sigma(2)}(\Theta), \pi_{\sigma(3)}(\Theta)) \in \mathcal{U}(L^\sigma)$, where π_i gives the ith component of Θ, for all $i \in [3]$. Given $\Theta \in \mathcal{I}_n$, the set of all Latin squares L such that $\Theta \in \mathcal{U}(L)$

is denoted by $LS(\Theta)$ and the cardinality of $LS(\Theta)$ is denoted by $\Delta(\Theta)$. The computation of $\Delta(\Theta)$ for any isotopism $\Theta \in \mathcal{I}_n$ is at the moment an open problem having relevance in secret sharing schemes related to Latin squares and only studied in some cases where Θ is a principal autotopism (Falcón, 2006).

Although $\Delta(\Theta)$ can be studied in a combinatorial way, in this paper we see that Gröbner bases turn out to be useful for obtaining this number. Specifically, given a $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$, we see that, if $k_\alpha \leq n$ is the number of cycles of α, then $LS(\Theta)$ can be obtained starting from a set of *Latin rectangles* of order $k_\alpha \cdot n$, that is to say, a set of $k_\alpha \times n$ arrays, with elements chosen from $[n]$, such that each symbol occurs precisely once in each row. This set of Latin rectangles can be seen as the vector space associated with the solution of an algebraic system of polynomial equations related to the isotopism Θ, which can be solved using Gröbner bases (Buchberger, 1965). We follow the ideas implemented by Bayer (1982) (see also Adams and Loustaunau (1994)) to solve the problem of an n-colouring a graph, since every Latin square of order n is equivalent to an n-coloured bipartite graph $K_{n,n}$ (Laywine and Mullen, 1998). A similar argument has been used by Gago et al. (2006) (see also Martín-Morales (2006)) to give an algorithm for solving Sudokus, which are indeed particular cases of Latin squares.

The structure of the paper is as follows. In Section 2, we study the set of Latin squares having an isotopism with a given cycle structure in their autotopism group. Specifically, we prove that $\Delta(\Theta)$ only depends on the cycle structure of Θ. In Section 3, we use Gröbner bases to define an algorithm that allows one to obtain $\Delta(\Theta)$. Finally, in Section 4, this algorithm is implemented in SINGULAR (Greuel et al., 2005) to get the number of Latin squares of order ≤ 7 related to any autotopism.

2. Cycle structures of Latin square autotopisms

Every permutation of S_n can be written as the composition of pairwise disjoint cycles. So, from now on, given $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$, we will assume that, for all $\delta \in \{\alpha, \beta, \gamma\}$,

$$\delta = C_1^\delta \circ C_2^\delta \circ \cdots \circ C_{k_\delta}^\delta, \tag{1}$$

where:

(i) For all $i \in [k_\delta]$, one has $C_i^\delta = (c_{i,1}^\delta \; c_{i,2}^\delta \; \cdots \; c_{i,\lambda_i^\delta}^\delta)$, with $\lambda_i^\delta \leq n$ and $c_{i,1}^\delta = \min_j\{c_{i,j}^\delta\}$. If $\lambda_i^\delta = 1$, then C_i^δ is a cycle of length 1 and so $c_{i,1}^\delta \in \mathrm{Fix}(\delta)$.
(ii) $\sum_i \lambda_i^\delta = n$.
(iii) For all $i, j \in [k_\delta]$, one has $\lambda_i^\delta \geq \lambda_j^\delta$ whenever $i \leq j$.
(iv) Given $i, j \in [k_\delta]$, with $i < j$ and $\lambda_i^\delta = \lambda_j^\delta$, one has $c_{i,1}^\delta < c_{j,1}^\delta$.

From now on, for a given $\delta \in \{\alpha, \beta, \gamma\}$ and $i \in [k_\delta]$, we will write $a \in C_i^\delta$ if there exists $j \in [\lambda_i^\delta]$ such that $a = c_{i,j}^\delta$. The following results hold:

Proposition 1. *Let $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be such that $\Delta(\Theta) > 0$. Let $L = (l_{i,j}) \in LS(\Theta)$ be such that all the triples of one of the following two Latin subrectangles of L are known:*

(i) $R_L = \left\{ (c_{r,1}^\alpha, c_{s,v}^\beta, l_{c_{r,1}^\alpha, c_{s,v}^\beta}) \mid r \in [k_\alpha], s \in [k_\beta] \text{ and } v \in \begin{Bmatrix} [\lambda_s^\beta], \text{ if } \lambda_r^\alpha > 1, \\ [1], \text{ if } \lambda_r^\alpha = 1. \end{Bmatrix} \right\}$.

(ii) $R'_L = \left\{ (c_{r,u}^\alpha, c_{s,1}^\beta, l_{c_{r,u}^\alpha, c_{s,1}^\beta}) \mid r \in [k_\alpha], s \in [k_\beta] \text{ and } u \in \begin{Bmatrix} [\lambda_r^\alpha], \text{ if } \lambda_s^\beta > 1, \\ [1], \text{ if } \lambda_s^\beta = 1. \end{Bmatrix} \right\}$.

Then, all the triples of L are known.

Proof. We will prove the result in the case where the elements of R_L are known; the other case follows analogously. Let $(i, j, l_{i,j}) \in L$ be such that $i \notin \mathrm{Fix}(\alpha)$ and let $r_0 \in [k_\alpha]$, $u_0 \in [\lambda^\alpha_{r_0}]$, $s_0 \in [k_\beta]$ and $v_0 \in [\lambda^\beta_{s_0}]$ be such that $c^\alpha_{r_0,u_0} = i$ and $c^\beta_{s_0,v_0} = j$. From the hypothesis, the triple $(c^\alpha_{r_0,1}, \beta^{1-u_0}(c^\beta_{s_0,v_0}), l_{c^\alpha_{r_0,1},\beta^{1-u_0}(c^\beta_{s_0,v_0})})$ is known. Thus, $l_{i,j} = l_{c^\alpha_{r_0,u_0},c^\beta_{s_0,v_0}} = \gamma^{u_0-1}(l_{c^\alpha_{r_0,1},\beta^{1-u_0}(c^\beta_{s_0,v_0})})$ and therefore, the triple $(i, j, l_{i,j})$ is known.

Alternatively, let $(i, j, l_{i,j}) \in L$ be such that $i \in \mathrm{Fix}(\alpha)$ and let $r_0 \in [k_\alpha]$, $s_0 \in [k_\beta]$ and $v_0 \in [\lambda^\beta_{s_0}]$ be such that $c^\alpha_{r_0,1} = i$ and $c^\beta_{s_0,v_0} = j$. From the hypothesis, the triple $(c^\alpha_{r_0,1}, c^\beta_{s_0,1}, l_{c^\alpha_{r_0,1},c^\beta_{s_0,1}})$ is known. Thus, $l_{i,j} = l_{c^\alpha_{r_0,1},c^\beta_{s_0,v_0}} = \gamma^{v_0-1}(l_{c^\alpha_{r_0,1},c^\beta_{s_0,1}})$ and therefore, the triple $(i, j, l_{i,j})$ is known. $\square$

Proposition 2. *Let $(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$ be the cycle structure of a Latin square isotopism and let us consider $\Theta_1 = (\alpha_1, \beta_1, \gamma_1)$, $\Theta_2 = (\alpha_2, \beta_2, \gamma_2) \in \mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$. Then, $\Delta(\Theta_1) = \Delta(\Theta_2)$.*

Proof. Since Θ_1 and Θ_2 have the same cycle structure, we can consider the isotopism $\Theta = (\sigma_1, \sigma_2, \sigma_3) \in \mathcal{I}_n$, where:

(i) $\sigma_1(c^{\alpha_1}_{i,j}) = c^{\alpha_2}_{i,j}$ for all $i \in [k_{\alpha_1}]$ and $j \in [\lambda^{\alpha_1}_i]$,
(ii) $\sigma_2(c^{\beta_1}_{i,j}) = c^{\beta_2}_{i,j}$ for all $i \in [k_{\beta_1}]$ and $j \in [\lambda^{\beta_1}_i]$,
(iii) $\sigma_3(c^{\gamma_1}_{i,j}) = c^{\gamma_2}_{i,j}$ for all $i \in [k_{\gamma_1}]$ and $j \in [\lambda^{\gamma_1}_i]$.

Now, let us see that $\Delta(\Theta_1) \leq \Delta(\Theta_2)$. If $\Delta(\Theta_1) = 0$, the result is immediate. Otherwise, let $L_1 = (l_{i,j}) \in LS(\Theta_1)$ and let us see that $L_1^\Theta = (l'_{i,j}) \in LS(\Theta_2)$. Specifically, we must prove that $(\alpha_2(i), \beta_2(j), \gamma_2(l'_{i,j})) \in L_1^\Theta$, for all $(i, j, l'_{i,j}) \in L_1^\Theta$. So, let us consider $(i_0, j_0, l'_{i_0,j_0}) \in L_1^\Theta$ and let $r_0 \in [k_{\alpha_2}]$, $u_0 \in [\lambda^{\alpha_2}_{r_0}]$, $s_0 \in [k_{\beta_2}]$, $v_0 \in [\lambda^{\beta_2}_{s_0}]$, $t_0 \in [k_{\gamma_2}]$ and $w_0 \in [\lambda^{\gamma_2}_{t_0}]$ be such that $c^{\alpha_2}_{r_0,u_0} = i_0$, $c^{\beta_2}_{s_0,v_0} = j_0$, and $c^{\gamma_2}_{t_0,w_0} = l'_{i_0,j_0}$. Thus,

$$(c^{\alpha_1}_{r_0,u_0}, c^{\beta_1}_{s_0,v_0}, c^{\gamma_1}_{t_0,w_0}) = (\sigma_1^{-1}(i_0), \sigma_2^{-1}(j_0), \sigma_3^{-1}(l'_{i_0,j_0})) \in L_1.$$

Next, since $L_1 \in LS(\Theta)$, we have that $(\alpha_1(c^{\alpha_1}_{r_0,u_0}), \beta_1(c^{\beta_1}_{s_0,v_0}), \gamma_1(c^{\gamma_1}_{t_0,w_0})) \in L_1$. Therefore,

$$\begin{aligned}(\alpha_2(i_0), \beta_2(j_0), \gamma_2(l'_{i_0,j_0})) &= (\alpha_2(c^{\alpha_2}_{r_0,u_0}), \beta_2(c^{\beta_2}_{s_0,v_0}), \gamma_2(c^{\gamma_2}_{t_0,w_0})) \\ &= (\sigma_1(\alpha_1(c^{\alpha_1}_{r_0,u_0})), \sigma_2(\beta_1(c^{\beta_1}_{s_0,v_0})), \sigma_3(\gamma_1(c^{\gamma_1}_{t_0,w_0})) \in L_1^\Theta.\end{aligned}$$

Analogously, it is verified that $L_2^{(\sigma_1^{-1},\sigma_2^{-1},\sigma_3^{-1})} \in LS(\Theta_1)$, for all $L_2 \in LS(\Theta_2)$, and hence, the result follows. $\square$

From Proposition 2, the number of Latin squares having a fixed isotopism $\Theta \in \mathcal{I}_n$ in its autotopism group only depends on the cycle structure of Θ. Hence, from now on, $\Delta(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$ will denote the number of Latin squares having a fixed autotopism $\Theta \in \mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$ in its autotopism group. Specifically, the following results are verified:

Proposition 3. *Let $(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$ be the cycle structure of a Latin square autotopism $\Theta = (\alpha, \beta, \gamma)$ and let us consider $\sigma \in S_3$. Then, $\Delta(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma) = \Delta(\mathbf{l}_{\pi_{\sigma(1)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(2)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(3)}(\Theta)})$, where π_i gives the ith component of Θ, for all $i \in [3]$.*

Proof. Since Θ is a Latin square autotopism, we must have $\Delta(\Theta) > 0$. Let $L \in LS(\Theta)$ and consider the isotopism $\Theta^{\sigma} = (\pi_{\sigma(1)}(\Theta), \pi_{\sigma(2)}(\Theta), \pi_{\sigma(3)}(\Theta))$; then it is verified that $\Theta^{\sigma} \in \mathcal{I}_n(\mathbf{l}_{\pi_{\sigma(1)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(2)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(3)}(\Theta)})$ and $L^{\sigma} \in LS(\Theta^{\sigma})$. Thus, $\Delta(\Theta) \leq \Delta(\Theta^{\sigma})$. Moreover, if $L' \in LS(\Theta^{\sigma})$, then $L'^{\sigma^{-1}} \in LS(\Theta)$. Therefore, $\Delta(\Theta) = \Delta(\Theta^{\sigma})$ and thus, from Proposition 2, $\Delta(\mathbf{l}_{\alpha}, \mathbf{l}_{\beta}, \mathbf{l}_{\gamma}) = \Delta(\mathbf{l}_{\pi_{\sigma(1)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(2)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(3)}(\Theta)})$. □

Corollary 4. $(\mathbf{l}_{\alpha}, \mathbf{l}_{\beta}, \mathbf{l}_{\gamma})$ *is the cycle structure of a Latin square autotopism if and only if there exists a permutation* $\sigma \in S_3$ *such that* $(\mathbf{l}_{\pi_{\sigma(1)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(2)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(3)}(\Theta)})$ *is the cycle structure of a Latin square autotopism, such that* $k_{\pi_{\sigma(1)}(\Theta)} \leq k_{\pi_{\sigma(2)}(\Theta)} \leq k_{\pi_{\sigma(3)}(\Theta)}$.

Proof. Since $(\mathbf{l}_{\alpha}, \mathbf{l}_{\beta}, \mathbf{l}_{\gamma})$ is the cycle structure of a Latin square autotopism if and only if $\Delta(\mathbf{l}_{\alpha}, \mathbf{l}_{\beta}, \mathbf{l}_{\gamma}) > 0$, the result is an immediate consequence of Proposition 3. □

Remark 5. From Proposition 2 and Corollary 4, if we want to obtain the number $\Delta(\Theta)$ related to an autotopism $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$, we can suppose that $k_{\alpha} \leq k_{\beta} \leq k_{\gamma}$. Otherwise, we would find a permutation $\sigma \in S_3$ such that $(\mathbf{l}_{\pi_{\sigma(1)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(2)}(\Theta)}, \mathbf{l}_{\pi_{\sigma(3)}(\Theta)})$ is the cycle structure of a Latin square autotopism, such that $k_{\pi_{\sigma(1)}(\Theta)} \leq k_{\pi_{\sigma(2)}(\Theta)} \leq k_{\pi_{\sigma(3)}(\Theta)}$, and we would work with the autotopism Θ^{σ}. Moreover, from Proposition 2, we can suppose that the autotopism Θ is such that $c^{\delta}_{r,1} = r$, for all $r \in [k_{\alpha}]$ and for all $\delta \in \{\alpha, \beta, \gamma\}$.

To simplify the calculation of $\Delta(\Theta)$, it is useful to study first the symmetry of the autotopism Θ. Specifically, we can find a partial Latin square $P \in PLS(n)$ such that there exists $c_P > 0$ verifying that $\Delta(\Theta) = c_P \cdot |LS_P(\Theta)|$, where $LS_P(\Theta) = \{L \in LS(\Theta) \mid P \subseteq L\}$. The number c_P will be called the *P-coefficient of symmetry of* Θ. The following result is immediate:

Lemma 6. *Let* $\Theta \in \mathcal{I}_n$. *Given* $i, j \in [n]$, *it is verified that*

$$LS(\Theta) = \bigsqcup_{k\in[n]} LS_{\{(i,j,k)\}}(\Theta) = \bigsqcup_{k\in[n]} LS_{\{(i,k,j)\}}(\Theta) = \bigsqcup_{k\in[n]} LS_{\{(k,i,j)\}}(\Theta).$$

$$\Delta(\Theta) = \sum_{k\in[n]} |LS_{\{(i,j,k)\}}(\Theta)| = \sum_{k\in[n]} |LS_{\{(i,k,j)\}}(\Theta)| = \sum_{k\in[n]} |LS_{\{(k,i,j)\}}(\Theta)|. \quad \square$$

The following results will be useful in our study:

Proposition 7. *Let* $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ *be such that* $\Delta(\Theta) > 0$ *and* $\mathbf{l}^{\alpha}_1 \cdot \mathbf{l}^{\beta}_1 > 0$ *and let us consider* $L_0 = (l_{i,j}) \in LS(\Theta)$. *Let* $i \in \mathrm{Fix}(\alpha)$ *and* $j \in \mathrm{Fix}(\beta)$. *Then,* $l_{i,j} \in \mathrm{Fix}(\gamma)$. *As a consequence,* $\Delta(\Theta)$ *is a multiple of the number of Latin squares of order* $\mathbf{l}^{\alpha}_1$.

Proof. It is enough to observe that $\gamma(l_{i,j}) = l_{\alpha(i),\beta(j)} = l_{i,j}$. To prove the consequence, let us observe that, from Theorem 1 of McKay et al. (2007), since $\mathbf{l}^{\alpha}_1 \cdot \mathbf{l}^{\beta}_1 > 0$, we must have $\mathbf{l}_{\alpha} = \mathbf{l}_{\beta} = \mathbf{l}_{\gamma}$. Specifically, $\mathbf{l}^{\alpha}_1 = \mathbf{l}^{\beta}_1 = \mathbf{l}^{\gamma}_1$ is the number of fixed points of α, β and γ. Therefore, the subsquare $R_0 = (r_{i,j})$ of L_0 verifying that its row indices are fixed points of α and its column indices are fixed points of β must be a Latin subsquare of L_0 with elements chosen from the set $\mathrm{Fix}(\gamma)$ of fixed points of γ. Moreover, if we interchange in L_0 the subsquare R_0 with any Latin subsquare $R_1 \in LS(\mathbf{l}^{\alpha}_1)$ of the same order with elements chosen from $\mathrm{Fix}(\gamma)$, we obtain a different Latin square of $LS(\Theta)$. Indeed, it must be that $|LS_{R_0}(\Theta)| = |LS_{R_1}(\Theta)|$ and, therefore, we finally obtain that $\Delta(\Theta) = N_{\mathbf{l}^{\alpha}_1} \cdot |LS_{R_0}(\Theta)|$. □

Theorem 8. *Let $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be a non-trivial autotopism verifying the conditions of Remark 5 such that $\Delta(\Theta) > 0$. Given $\delta \in \{\alpha, \beta, \gamma\}$, let h_δ be the cardinality of the set $\{i \in [n] \mid \mathbf{l}_i^\delta > 0\}$. The following assertions are verified:*

(a) *If $h_\alpha = h_\beta = 1$, then $\Delta(\Theta) = n \cdot |LS_{\{(1,1,1)\}}(\Theta)|$.*

(b) *Let us suppose that there exists $i_0 \in [n] \setminus \{1\}$ such that $\mathbf{l}_{i_0}^\alpha = \mathbf{l}_{i_0}^\beta \neq 0$. If $\mathbf{l}_1^\alpha = \mathbf{l}_1^\beta > 0$ and $h_\alpha = h_\beta = 2$, then*

$$\Delta(\Theta) = \prod_{k=0}^{\mathbf{l}_{i_0}^\alpha - 1} (n - \mathbf{l}_1^\alpha - k \cdot i_0)^2 \cdot |LS_{\{(i,i,k_\alpha),(k_\alpha,i,i) \mid i \in [k_\alpha - \mathbf{l}_1^\alpha]\}}(\Theta)|.$$

$$\Delta(\Theta) = \prod_{k=0}^{\mathbf{l}_{i_0}^\alpha - 1} (n - \mathbf{l}_1^\alpha - k \cdot i_0)^2 \cdot |LS_{\{(i,i,k_\alpha),(i,k_\alpha,i) \mid i \in [k_\alpha - \mathbf{l}_1^\alpha]\}}(\Theta)|.$$

Proof. Let $L = (l_{i,j}) \in LS(\Theta)$. The first assertion is immediate because, in this case, $|LS_{\{(1,i,1)\}}(\Theta)| = |LS_{\{(1,j,1)\}}(\Theta)|$, for all $i, j \in [n]$. Let us see the second assertion. We will prove the first expression; the other one follows analogously. Since $\mathbf{l}_1^\alpha \cdot \mathbf{l}_1^\beta > 0$ and Θ verifies the conditions of Remark 5, it must be that $k_\alpha \in \mathrm{Fix}(\alpha) = \mathrm{Fix}(\beta) = \mathrm{Fix}(\gamma)$. Now, from Proposition 7 and the symmetry of Θ, $|LS_{\{(1,i,k_\alpha)\}}(\Theta)| = 0$ for all $i \in \mathrm{Fix}(\beta)$ and $|LS_{\{(1,i,k_\alpha)\}}(\Theta)| = |LS_{\{(1,j,k_\alpha)\}}(\Theta)|$ for all $i, j \notin \mathrm{Fix}(\beta)$. Thus, from Lemma 6, $\Delta(\Theta) = (n - \mathbf{l}_1^\alpha) \cdot |LS_{\{(1,1,k_\alpha)\}}(\Theta)|$. Now, it must be that $|LS_{\{(1,1,k_\alpha),(2,i,k_\alpha)\}}(\Theta)| = 0$ for all $i \in \mathrm{Fix}(\beta) \cup C_1^\beta$ and $|LS_{\{(1,1,k_\alpha),(2,i,k_\alpha)\}}(\Theta)| = |LS_{\{(1,1,k_\alpha),(2,j,k_\alpha)\}}(\Theta)|$ for all $i, j \notin \mathrm{Fix}(\beta) \cup C_1^\beta$. So, $\Delta(\Theta) = (n - \mathbf{l}_1^\alpha) \cdot (n - \mathbf{l}_1^\alpha - i_0) \cdot |LS_{\{(1,1,k_\alpha),(2,2,k_\alpha)\}}(\Theta)|$. Analogously, it can be proven that $\Delta(\Theta) = \prod_{k=0}^{\mathbf{l}_{i_0}^\alpha - 1} (n - \mathbf{l}_1^\alpha - k \cdot i_0) \cdot |LS_{\{(i,i,k_\alpha) \mid i \in [k_\alpha - \mathbf{l}_1^\alpha]\}}(\Theta)|$. Let $P = \{(i, i, k_\alpha) \mid i \in [k_\alpha - \mathbf{l}_1^\alpha]\} \in PLS(n)$. Next, it must be that $l_{k_\alpha,1} \notin \mathrm{Fix}(\gamma)$ and $|LS_{P \cup \{(k_\alpha,1,i)\}}(\Theta)| = |LS_{P \cup \{(k_\alpha,1,j)\}}(\Theta)|$, for all $i, j \notin \mathrm{Fix}(\gamma)$. So, $\Delta(\Theta) = (n - \mathbf{l}_1^\alpha) \cdot \prod_{k=0}^{\mathbf{l}_{i_0}^\alpha - 1} (n - \mathbf{l}_1^\alpha - k \cdot i_0) \cdot |LS_{P \cup \{(k_\alpha,1,1)\}}(\Theta)|$. Now, it must be that $l_{k_\alpha,2} \notin \mathrm{Fix}(\gamma) \cap C_1^\gamma$ and $|LS_{P \cup \{(k_\alpha,1,1),(k_\alpha,2,i)\}}(\Theta)| = |LS_{P \cup \{(k_\alpha,1,1),(k_\alpha,2,j)\}}(\Theta)|$, for all $i, j \notin \mathrm{Fix}(\gamma) \cap C_1^\gamma$. So, $\Delta(\Theta) = (n - \mathbf{l}_1^\alpha) \cdot (n - \mathbf{l}_1^\alpha - i_0) \cdot \prod_{k=0}^{\mathbf{l}_{i_0}^\alpha - 1} (n - \mathbf{l}_1^\alpha - k \cdot i_0) \cdot |LS_{P \cup \{(k_\alpha,1,1),(k_\alpha,2,2)\}}(\Theta)|$. Analogously, it can be finally proven that $\Delta(\Theta) = \prod_{k=0}^{\mathbf{l}_{i_0}^\alpha - 1} (n - \mathbf{l}_1^\alpha - k \cdot i_0)^2 \cdot |LS_{P \cup \{(k_\alpha,i,i) \mid i \in [k_\alpha - \mathbf{l}_1^\alpha]\}}(\Theta)|$. $\square$

3. Gröbner bases and Latin square autotopisms

Gröbner bases can be used to obtain the set $LS(n)$ of Latin squares of order n by following the ideas of Bayer (1982) (see also Adams and Loustaunau (1994)), since every Latin square of order n is equivalent to an n-coloured bipartite graph $K_{n,n}$ (Laywine and Mullen, 1998). In particular, given a generic Latin square $L = (l_{i,j}) \in LS(n)$, we can consider the set of n^2 variables $\{x_{i,j} \mid i, j \in [n]\}$, where $x_{i,j}$ corresponds to the triple $(i, j, l_{i,j}) \in L$, for all $i, j \in [n]$. Then, we define

$$F(x) = \prod_{m=1}^{n} (x - m), \qquad G(x, y) = \frac{F(x) - F(y)}{x - y}.$$

Thus, given $i, i', j, j' \in [n]$ such that $i \neq i'$ and $j \neq j'$, it must follow that $F(l_{i,j}) =$

$0 = G(l_{i,j}, l_{i',j}) = G(l_{i,j}, l_{i,j'})$, because $L \in LS(n)$. Thus, if we define the following ideal of $\mathbb{Q}[\mathbf{x}] = \mathbb{Q}[x_{1,1}, \ldots, x_{n,n}]$:

$$I = \langle\, F(x_{i,j}), G(x_{i,j}, x_{i',j}), G(x_{i,j}, x_{i,j'}) \mid i, i', j, j' \in [n],\ i \neq i' \text{ and } j \neq j' \,\rangle$$

generated by $n^2 + \sum_{(i,j)\in[n]\times[n]}((n-i)+(n-j))$ polynomials, it is verified that the set of zeros of I, denoted by $V(I)$, corresponds to the set $LS(n)$.

Remark 9. Once we know that the polynomial $F(x_{1,1}) \in I$, it is easy to see that the rest of the polynomials $F(x_{i,j})$, $(i, j) \neq (1, 1)$, are redundant, so we can delete them. The ideal I can be generated by $1 + \sum_{(i,j)\in[n]\times[n]}((n-i)+(n-j))$ polynomials.

Remark 10. It is well know that, as ideals I produced by Latin squares are radical (Cox et al., 1997, Ch. 2, Prop. 2.7.), the number of elements in $V(I)$ is equal to the dimension of the $\mathbb{Q}$-vector space $\mathbb{Q}[\mathbf{x}]/I$, and this number can be computed with any Gröbner basis with respect to any term ordering.

Now, let $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n(\mathbf{l}_\alpha,\ \mathbf{l}_\beta,\ \mathbf{l}_\gamma)$ be a Latin square autotopism verifying the conditions of Remark 5. In this section, we are interested in obtaining the number $\Delta(\Theta)$. The following set will be useful:

$$S_\Theta = \left\{ (i, j) \ \mid\ i \in [k_\alpha],\ j \in \begin{Bmatrix} [n], & \text{if } i \notin \operatorname{Fix}(\alpha), \\ [k_\beta], & \text{if } i \in \operatorname{Fix}(\alpha). \end{Bmatrix} \right\}.$$

Remark 11. From Proposition 1, we can eliminate some of the polynomials defining the above-defined ideal I to obtain the Latin squares of $LS(\Theta)$. In particular, if we consider the first case of that result, we can restrict our study to those polynomials in which there only appear some of the $(k_\alpha - \mathbf{l}_1^\alpha)\cdot n + \mathbf{l}_1^\alpha \cdot k_\beta$ variables $x_{i,j}$, where $(i, j) \in S_\Theta$. Hence, we are interested in the following ideal of $\mathbb{Q}[x_{i,j} \mid (i, j) \in S_\Theta]$:

$$\begin{aligned} I' = {} & \langle\, F(x_{1,1}), G(x_{i,j}, x_{i',j}), G(x_{i,j}, x_{i,j'}) \mid i, i' \in [k_\alpha],\ j, j' \in [n],\ i \neq i' \text{ and } j \neq j' \,\rangle \\ & + \langle\, G(x_{i,j}, x_{i',j}), G(x_{i,j}, x_{i,j'}) \mid i \in \operatorname{Fix}(\alpha), i' \in [n],\ j, j' \in [k_\beta],\ i \neq i' \text{ and } j \neq j' \,\rangle. \end{aligned}$$

Next, let $P = (p_{i,j}) \in PLS(n)$ be such that $p_{i,j} = \emptyset$ for all $(i, j) \notin S_\Theta$ and let c_P be the P-coefficient of symmetry of Θ. Thus, we know that $\Delta(\Theta) = c_P \cdot |LS_P(\Theta)|$ and we will calculate $|LS_P(\Theta)|$ starting from the set of solutions of an algebraic system of polynomial equations related to Θ and P. Specifically, we obtain Algorithm 1.

Proof (*Correctness of Algorithm* 1).

(i) Given a partial Latin square $P \in PLS(n)$ such that $p_{i,j} = \emptyset$, for all $(i, j) \notin S_\Theta$, we will consider the vector v such that

$$\begin{cases} v_{(i-1)\cdot n+j} = \begin{cases} p_{i,j}, & \text{if } p_{i,j} \neq \emptyset, \\ 0, & \text{if } p_{i,j} = \emptyset, \end{cases} & \text{and } i \notin \operatorname{Fix}(\alpha),\ j \in [n] \\ v_{(k_\alpha - \mathbf{l}_1^\alpha)\cdot n + (i - k_\alpha + \mathbf{l}_1^\alpha - 1)\cdot k_\beta + j} = \begin{cases} p_{i,j}, & \text{if } p_{i,j} \neq \emptyset, \\ 0, & \text{if } p_{i,j} = \emptyset, \end{cases} & \text{and } i \in \operatorname{Fix}(\alpha),\ j \in [k_\beta] \end{cases}$$

(ii) The first definition of I' corresponds to the ideal defined in Remark 11. The second one is obtained by adding the polynomials associated with the filled cells of P.

Algorithm 1. LST (computing the number of Latin squares having a fixed isotopism)

Input: $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$, an isotopism verifying the conditions of Remark 5;
k_α, the number of cycles of α;
$v = \left(v_1, v_2, \ldots, v_{(k_\alpha - \mathbf{l}_1^\alpha)\cdot n + \mathbf{l}_1^\alpha \cdot k_\beta}\right)$ corresponding to triples of a partial Latin square $P \in PLS(n)$ such that $p_{i,j} = \emptyset$, for all $(i, j) \notin S_\Theta$;
c, the P-coefficient of symmetry of Θ.

Output: $\Delta(\Theta)$, the number of Latin squares having Θ as an autotopism;

$I' := \langle F(x_{1,1}), G(x_{i,j}, x_{i',j}), G(x_{i,j}, x_{i,j'}) \mid i, i' \in [k_\alpha],\ j, j' \in [n],\ i \neq i' \text{and } j \neq j' \rangle +$
$\langle G(x_{i,j}, x_{i',j}), G(x_{i,j}, x_{i,j'}) \mid i \in \text{Fix}(\alpha),\ i' \in [n],\ j, j' \in [k_\beta],\ i \neq i' \text{and } j \neq j' \rangle$;
$I' := I' + \langle x_{i,j} - v_{i,j} \mid (i, j) \in S_\Theta, v_{i,j} \neq 0 \rangle$;
GI' := Gröbner basis of I' with respect to any term ordering;
$t := \dim_{\mathbb{Q}}(\mathbb{Q}[\mathbf{x}]/I)$; ▷ t is the cardinality of $V(I')$
SOL := $V(I')$; ▷ list of all elements in $V(I')$
Delta := 0; ▷ the output is $c \cdot$ Delta
for $l = 1$ to t **do**
  L := the $n \times n$ array associated with SOL[l]; ▷ see Proposition 1
  if L is a Latin square **then**
    Delta ← Delta + 1;
  end if
end for
return $c \cdot$ Delta;

(iii) From Proposition 1, we are not interested in $V(I')$, but in the subset $\{R_L \mid L \in LS_P(\Theta)\} \subseteq V(I')$, because its cardinality is equal to $|LS_P(\Theta)|$. Thus, finally, once we have obtained $V(I')$, we must check how many of its elements are in the previous subset. Specifically:
  (iii.1) Given an element of $V(I')$, we follow the proof of Proposition 1 to define the $n \times n$ array associated with it.
  (iii.2) Then, the array obtained belongs to the set $LS_P(\Theta)$ if and only if it is a Latin square.

(iv) The final output is therefore $\Delta(\Theta) = c_P \cdot |LS_P(\Theta)|$. □

Let us see some examples:

Example 12. Let $\Theta = ((1234), (1234), (12)) \in \mathcal{I}_4((0, 0, 0, 1), (0, 0, 0, 1), (2, 1, 0, 0))$. Let us define

$$F(x) = \prod_{m=1}^{4} (x - m), \qquad G(x, y) = \frac{F(x) - F(y)}{x - y}.$$

Then, let us consider the ideal of $\mathbb{Q}[x_{11}, x_{12}, x_{13}, x_{14}]$:

$$\begin{aligned} I' = \langle & F(x_{11}), G(x_{11}, x_{12}), G(x_{11}, x_{13}), G(x_{11}, x_{14}), \\ & G(x_{12}, x_{13}), G(x_{12}, x_{14}), G(x_{13}, x_{14})\rangle. \end{aligned}$$

The following is a Gröbner basis of I' with respect to the degree reverse lexicographical ordering:

$$\begin{aligned} \{x_{13}^3 + x_{13}^2 x_{14} + x_{13}x_{14}^2 + x_{14}^3 - 10x_{13}^2 - 10x_{13}x_{14} - 10x_{14}^2 + 35x_{13} + 35x_{14} - 50, \\ x_{12}^2 + x_{12}x_{13} + x_{13}^2 + x_{12}x_{14} + x_{13}x_{14} + x_{14}^2 - 10x_{12} - 10x_{13} - 10x_{14} + 35, \\ x_{14}^4 - 10x_{14}^3 + 35x_{14}^2 - 50x_{14} + 24, x_{11} + x_{12} + x_{13} + x_{14} - 10\}. \end{aligned}$$

It can be proven that the algebraic system of polynomial equations given by the previous Gröbner basis has 24 solutions. However, only 8 of them correspond to a Latin square, by following the proof of Proposition 1. Therefore, $\Delta(\Theta) = 8$. Moreover,

$$\Delta((0, 0, 0, 1), (0, 0, 0, 1), (2, 1, 0, 0)) = 8.$$

Example 13. Let $\Theta = (\epsilon, (12345), (12345)) \in \mathcal{I}_5((5, 0, 0, 0, 0), (0, 0, 0, 0, 1), (0, 0, 0, 0, 1))$. In this case, $k_\alpha = 5 > 1 = k_\beta = k_\gamma$. Let us consider, for example, the permutation $(13) \in S_3$ and let us define the principal isotopism $\Theta' = \Theta^{(13)} = ((12345), (12345), \epsilon) \in \mathcal{I}_5((0, 0, 0, 0, 1), (0, 0, 0, 0, 1), (5, 0, 0, 0, 0))$. From Proposition 3, we have that $\Delta(\Theta) = \Delta(\Theta')$. Let us define

$$F(x) = \prod_{m=1}^{5} (x - m), \qquad G(x, y) = \frac{F(x) - F(y)}{x - y}.$$

Then, let us consider the ideal of $\mathbb{Q}[x_{11}, x_{12}, x_{13}, x_{14}, x_{15}]$:

$$\begin{aligned} I' = \langle &F(x_{11}), G(x_{11}, x_{12}), G(x_{11}, x_{13}), G(x_{11}, x_{14}), G(x_{11}, x_{15}), G(x_{12}, x_{13}), \\ &G(x_{12}, x_{14}), G(x_{12}, x_{15}), G(x_{13}, x_{14}), G(x_{13}, x_{15}), G(x_{14}, x_{15})\rangle. \end{aligned}$$

The following is a Gröbner basis of I' with respect to the degree reverse lexicographical ordering:

$$\begin{aligned} &\{x_{13}^3 + x_{13}^2x_{14} + x_{13}x_{14}^2 + x_{14}^3 + x_{13}^2x_{15} + x_{13}x_{14}x_{15} + x_{14}^2x_{15} + x_{13}x_{15}^2 + x_{14}x_{15}^2 + x_{15}^3 \\ &-15x_{13}^2 - 15x_{13}x_{14} - 15x_{14}^2 - 15x_{13}x_{15} - 15x_{14}x_{15} - 15x_{15}^2 + 85x_{13} + 85x_{14} \\ &+ 85x_{15} - 225, x_{12}^2 + x_{12}x_{13} + x_{13}^2 + x_{12}x_{14} + x_{13}x_{14} + x_{14}^2 + x_{12}x_{15} + x_{13}x_{15} \\ &+ x_{14}x_{15} + x_{15}^2 - 15x_{12} - 15x_{13} - 15x_{14} - 15x_{15} + 85, x_{15}^5 - 15x_{15}^4 + 85x_{15}^3 \\ &-225x_{15}^2 + 274x_{15} - 120, x_{14}^4 + x_{14}^3x_{15} + x_{14}^2x_{15}^2 + x_{14}x_{15}^3 + x_{15}^4 - 15x_{14}^3 - 15x_{14}^2x_{15} \\ &-15x_{14}x_{15}^2 - 15x_{15}^3 + 85x_{14}^2 + 85x_{14}x_{15} + 85x_{15}^2 - 225x_{14} - 225x_{15} + 274, \\ &x_{11} + x_{12} + x_{13} + x_{14} + x_{15} - 15\}. \end{aligned}$$

It can be proven that the algebraic system of polynomial equations given by the previous Gröbner basis has 120 solutions. Indeed, each one of them corresponds to a Latin square, by following the proof of Proposition 1. Therefore, $\Delta(\Theta) = \Delta(\Theta') = 120$. Moreover, $\Delta((5, 0, 0, 0, 0), (0, 0, 0, 0, 1), (0, 0, 0, 0, 1)) = 120$.

Remark 14. In the previous examples, the Gröbner basis obtained has the same number of elements as variables. However, this does not happen in general. So, for example, the Gröbner basis that we obtained corresponding to the autotopism $\Theta = ((134), (134), (134)) \in \mathcal{I}_4((1, 0, 1, 0), (1, 0, 1, 0), (1, 0, 1, 0))$ with respect to the degree reverse lexicographical has nine elements, but there are only six variables.

4. Number of Latin squares related to a cycle structure of order ≤ 7

Let $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be a Latin square autotopism of order up to 7 verifying the conditions of Remark 5. In this section, Algorithm 1 is implemented to obtain the number $\Delta(\Theta)$ in a procedure for the computer algebra system for polynomial computations Singular 3-0-2. A Singular library called latinSquare.lib has been created and it is available on the Internet.[1] The

[1] http://www.personal.us.es/raufalgan/LS/latinSquare.lib.

Table 2
Number of Latin squares related to autotopisms of $\mathcal{I}_n$, for $2 \leq n \leq 5$

n	$\mathbf{l}_\alpha$	$\mathbf{l}_\beta$	$\mathbf{l}_\gamma$	$\Theta \in \mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$	P	c_P	Δ	r.t. (s)
2	(0,1)	(0,1)	(2,0)	((12), (12), ϵ)	–	1	2	0
3	(0,0,1)	(0,0,1)	(0,0,1)	((123),(123),(123))	–	1	3	0
			(3,0,0)	((123),(123),ϵ)	–	1	6	0
	(1,1,0)	(1,1,0)	(1,1,0)	((13),(13),(13))	–	1	4	0
4	(0,0,0,1)	(0,0,0,1)	(0,2,0,0)	((1234),(1234),(12)(34))	–	1	8	0
			(2,1,0,0)	((1234), (1234),(14))	–	1	8	0
			(4,0,0,0)	((1234),(1234),ϵ)	–	1	24	0
	(0,2,0,0)	(0,2,0,0)	(0,2,0,0)	((13)(24),(13)(24),(13)(24))	{(1, 1, 1)}	4	32	0
			(2,1,0,0)	((13)(24), (13)(24),(14))	{(1, 1, 1)}	4	32	0
			(4,0,0,0)	((13)(24),(13)(24), ϵ)	{(1, 1, 1)}	4	96	0
	(1,0,1,0)	(1,0,1,0)	(1,0,1,0)	((134), (134),(134))	{(2, 2, 2)}	1	9	0
	(2,1,0,0)	(2,1,0,0)	(2,1,0,0)	((14),(14),(14))	{(2, 2, 2), (2, 3, 3)}	2	16	0
5	(0,0,0,0,1)	(0,0,0,0,1)	(0,0,0,0,1)	((12345),(12345),(12345))	{(1, 1, 1)}	5	15	0
			(5,0,0,0,0)	((12345),(12345),ϵ)	{(1, 1, 1)}	5	120	0
	(1,0,0,1,0)	(1,0,0,1,0)	(1,0,0,1,0)	((1345), (1345),(1345))	{(1, 1, 2), (2, 2, 2)}	4	32	1
	(1,2,0,0,0)	(1,2,0,0,0)	(1,2,0,0,0)	((15)(24),(15)(24),(15)(24))	{(1, 1, 3), (1, 3, 1), (2, 2, 3), (2, 3, 2), (3, 3, 3)}	64	256	2
	(2,0,1,0,0)	(2,0,1,0,0)	(2,0,1,0,0)	((145), (145),(145))	{(1, 1, 3), (1, 3, 1), (2, 2, 2), (2, 3, 3), (3, 2, 3), (3, 3, 2)}	18	144	0

authors are going to submit this library to the Singular distribution. The main procedure has been called LST, from the initials of *"Latin Squares of Theta"*. Specifically, LST depends on the permutations α, β and γ, given respectively by the n-vectors $A = [\alpha(1), \alpha(2), \ldots, \alpha(n)]$, $B = [\beta(1), \beta(2), \ldots, \beta(n)]$, and $C = [\gamma(1), \gamma(2), \ldots, \gamma(n)]$. LST also depends on the number k_α of cycles of α, denoted by kA, on a vector v corresponding to a partial Latin square $P \in PLS(n)$ and on the P-coefficient of symmetry, denoted by c. From (Falcón, in press), it is verified that $k_\alpha \leq 5$ and if $\mathbf{l}_1^\alpha \cdot \mathbf{l}_1^\beta > 0$, then $k_\alpha = k_\beta$ and $\mathbf{l}_1^\alpha = \mathbf{l}_1^\beta \leq 3$.

Let us see in the following example how to use this library in SINGULAR.

Example 15. To compute, for example, $\Delta((0, 0, 0, 0, 0, 1), (0, 0, 0, 0, 0, 1), (4, 1, 0, 0, 0, 0))$, let us consider the autotopism $\Theta((123456), (123456), (16))$ and $P = \{(1, 1, 1)\} \in PLS(6)$.

```
LIB "latinSquare.lib";
intvec A = 2,3,4,5,6,1;
intvec B = 2,3,4,5,6,1;
intvec C = 6,2,3,4,5,1;
int kA = 1;
intvec v = 1,0,0,0,0,0;
int c = 6;
LST(A,B,C,kA,v,c);
  //-> 288
```

Table 3
Number of Latin squares related to autotopisms of $\mathcal{I}_6$

$\Theta \in \mathcal{I}_6((0,0,0,0,0,1),(0,0,2,0,0,0),(0,3,0,0,0,0))$	P	c_P	Δ	r.t. (s)
((123456), (156)(234), (16)(25)(34))	$\{(1,1,1)\}$	6	288	2

$\mathbf{l}_\alpha = \mathbf{l}_\beta$	$\mathbf{l}_\gamma$	$\Theta \in \mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$	P	c_P	Δ	r.t. (s)
(0, 0, 0, 0, 0, 1)	(0, 0, 2, 0, 0, 0)	((123456), (123456), (156)(234))	$\{(1,1,1)\}$	6	72	2
	(1, 1, 1, 0, 0, 0)	((123456), (123456), (156)(24))	$\{(1,1,1)\}$	6	72	2
	(2, 2, 0, 0, 0, 0)	((123456), (123456), (15)(26))	$\{(1,1,1)\}$	6	144	2
	(3, 0, 1, 0, 0, 0)	((123456), (123456), (156))	$\{(1,1,1)\}$	6	144	2
	(4, 1, 0, 0, 0, 0)	((123456), (123456), (16))	$\{(1,1,1)\}$	6	288	2
	(6, 0, 0, 0, 0, 0)	((123456), (123456), ϵ)	$\{(1,1,1)\}$	6	720	3
(0, 0, 2, 0, 0, 0)	(0, 0, 2, 0, 0, 0)	((156)(234), (156)(234), (156)(234))	$\{(1,1,1),(1,2,2),(2,3,j),(2,5,i)\}$ $(i \neq 2;\ j \neq 5)$	54	1296	55
	(3, 0, 1, 0, 0, 0)	((156)(234), (156)(234), (156))	$\{(1,i,i),(1,5,j),(2,1,2)\}_{i\in[n];\ j=3,4,6}$	162	5184	28
	(6, 0, 0, 0, 0, 0)	((156)(234), (156)(234), ϵ)	$\{(1,i,i)\}_{i\in[n]}$	720	25920	9
(1, 0, 0, 0, 1, 0)	(1, 0, 0, 0, 1, 0)	((13456), (13456), (13456))	$\{(i,i,2)\}_{i=1,2}$	5	75	7
(0, 3, 0, 0, 0, 0)	(2, 2, 0, 0, 0, 0)	((16)(25)(34), (16)(25)(34), (16)(25))	$\begin{pmatrix} 1 & 6 & \ast & \ast & \ast & \ast \\ 6 & \ast & i & \ast & j & \ast \\ \ast & \ast & \ast & k & \ast & l \end{pmatrix}$ $(i, j \neq 6;\ k, l \in [n])$	96	36864	252
	(4, 1, 0, 0, 0, 0)	((16)(25)(34), (16)(25)(34), (16))	$\begin{pmatrix} 1 & 6 & 3 & 4 & 5 & 2 \\ 6 & \ast & \ast & \ast & \ast & 4 \\ 3 & \ast & \ast & \ast & \ast & 5 \end{pmatrix}$	13824	110592	2
	(6, 0, 0, 0, 0, 0)	((16)(25)(34), (16)(25)(34), ϵ)	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & \ast & i & \ast & \ast & \ast \\ \ast & \ast & \ast & \ast & j & \ast \end{pmatrix}$ $(i \neq 2, 3;\ j \neq 2, 5)$	2880	460800	92
(2, 0, 0, 1, 0, 0)	(2, 0, 0, 1, 0, 0)	((1456), (1456), (1456))	$\begin{pmatrix} 3 & \ast & 1 & \ast & \ast & \ast \\ \ast & 2 & 3 & \ast & \ast & \ast \\ \ast & 3 & 2 & \ast & \ast & \ast \end{pmatrix}$	32	768	2
(2, 2, 0, 0, 0, 0)	(2, 2, 0, 0, 0, 0)	((16)(25), (16)(25), (16)(25))	$\begin{pmatrix} 4 & \ast & \ast & 1 & i & \ast \\ \ast & 4 & \ast & 2 & \ast & j \\ \ast & \ast & 4 & 3 & \ast & \ast \\ \ast & \ast & 3 & 4 & \ast & \ast \end{pmatrix}$ $(i \neq 1, 4;\ j \neq 2, 4)$	128	20480	137
(3, 0, 1, 0, 0, 0)	(3, 0, 1, 0, 0, 0)	((156), (156), (156))	$\begin{pmatrix} 2 & \ast & \ast & \ast & \ast & \ast \\ \ast & 2 & 3 & 4 & \ast & \ast \\ \ast & 3 & 4 & 2 & \ast & \ast \\ \ast & 4 & 2 & 3 & \ast & \ast \end{pmatrix}$	36	2592	1

Therefore, $\Delta((0,0,0,0,0,1),(0,0,0,0,0,1),(4,1,0,0,0,0)) = \Delta(\Theta) = 288$. Alternatively, to compute $\Delta((2,2,0,0,0,0),(2,2,0,0,0,0),(2,2,0,0,0,0))$, we have used

```
intvec A = 6,5,3,4,2,1;
intvec B = 6,5,3,4,2,1;
intvec C = 6,5,3,4,2,1;
int kA,c = 4,128;
int i,j,a; intvec v;
for (i=2; i<=6; i++)
{
  for (j=1; j<=6; j++)
  {
    if (i!=4 and j!=4 and j!=2)
    {
      v = 4,0,0,1,i,0,0,4,0,2,0,j,0,0,4,3,0,0,3,4;
      a = a + LST(A,B,C,kA,v,c);
    }
  }
}
print(a);
  //-> 20480
```

Table 4
Number of Latin squares related to autotopisms of $\mathcal{I}_7$

$\Theta \in \mathcal{I}_7((0,0,0,0,0,0,1),(0,0,0,0,0,0,1),(7,0,0,0,0,0,0))$	P	c_P	Δ	r.t. (s)
$((1234567),(1234567),\epsilon)$	$\{(1,1,1)\}$	7	5040	17

$\mathbf{l}_\alpha = \mathbf{l}_\beta = \mathbf{l}_\gamma$	$\Theta \in \mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$	P	c_P	Δ	r.t. (s)
(0, 0, 0, 0, 0, 0, 1)	((1234567), (1234567), (1234567))	$\{(1,1,1)\}$	7	133	5
(1, 0, 0, 0, 0, 1, 0)	((134567), (134567), (134567))	$\{(1,1,2),(1,2,1),(2,2,2)\}$	36	288	4
(1, 0, 2, 0, 0, 0, 0)	((167)(245), (167)(245), (167)(245))	$\begin{pmatrix} 3 & * & * & * & i & * & j \\ * & 3 & * & k & * & l & * \\ 1 & 2 & 3 & * & * & * & * \end{pmatrix}$ $(i,j,k,l \in [n] \setminus \{3\})$	324	42768	253
(1, 1, 0, 1, 0, 0, 0)	((1456)(27), (1456)(27), (1456)(27))	$\begin{pmatrix} 3 & * & * & 2 & * & 7 & * \\ * & 3 & 2 & * & * & * & 7 \\ 1 & 7 & 3 & * & * & * & * \end{pmatrix}$	128	512	3
(2, 0, 0, 0, 1, 0, 0)	((14567), (14567), (14567))	$\{(1,1,3),(2,2,2),(2,3,3),(3,1,1),(3,2,3),(3,3,2)\}$	50	4000	16
(1, 3, 0, 0, 0, 0, 0)	((17)(26)(35), (17)(26)(35), (17)(26)(35))	$\begin{pmatrix} 4 & i & * & j & * & k & * \\ * & 4 & l & * & p & * & q \\ r & * & 4 & * & * & * & * \\ 1 & 2 & 3 & 4 & * & * & * \end{pmatrix}$ $(i \neq 2,4;\ j,k,p,q \neq 4,6;\ l \neq 3,4;\ r \neq 1,4)$	2304	6045696	4512
(3, 0, 0, 1, 0, 0, 0)	((1567), (1567), (1567))	$\begin{pmatrix} 2 & * & * & * & * & * & * \\ * & 2 & 3 & 4 & * & * & * \\ * & 3 & 4 & 2 & * & * & * \\ * & 4 & 2 & 3 & * & * & * \end{pmatrix}$	36	41472	53
(3, 2, 0, 0, 0, 0, 0)	((17)(26), (17)(26), (17)(26))	$\begin{pmatrix} 5 & 4 & 1 & 2 & 6 & 7 & 3 \\ * & * & 2 & 1 & 7 & * & j \\ i & * & 5 & 4 & 3 & * & * \\ * & * & 3 & 5 & 4 & * & * \\ * & * & 4 & 3 & 5 & * & * \end{pmatrix}$ $(i \neq 3,4,5;\ j = 4,5,6)$	27648	1327104	40

Therefore, $\Delta((2,2,0,0,0,0),(2,2,0,0,0,0),(2,2,0,0,0,0)) = 20480$.

To finish this section, we have used the previous procedure and the results of Section 2 to obtain, in Tables 2–4, the number of Latin squares of order up to 7 having a given autotopism in their autotopism groups. For each case, we show the autotopism, partial Latin squares and coefficient of symmetry used. The running time (r.t.) is measured in seconds and has been taken from an *Intel Core 2 Duo Processor T5500, 1.66 GHz* with *Windows Vista* operating system. We follow the classification of such autotopisms given by Falcón (in press).

5. Final remarks

The algorithm given in Section 3 can be used to obtain the number of Latin squares related to autotopisms of Latin squares of any order. However, after applying it to the 36 possible cases of autotopisms of Latin squares of order 8 or to the 22 possible ones of order 9, we have seen that, in order to improve the time of computation, it is convenient to combine Gröbner bases with some combinatorial tools improving the results of Section 2, specifically, with autotopisms $\Theta = (\alpha, \beta, \gamma)$ in which $k_\alpha > 3$. So, for example, the computation corresponding to cycle structures $(\mathbf{l}_\alpha, \mathbf{l}_\beta, \mathbf{l}_\gamma)$, where $\mathbf{l}_\alpha = \mathbf{l}_\beta = (0, 4, 0, 0, 0, 0, 0, 0)$ would turn out to be too expensive using this method.

References

Adams, W., Loustaunau, P., 1994. An Introduction to Gröbner Bases. In: Graduate Studies in Mathematics, vol. 3. American Mathematical Society, Providence, RI.

Albert, A.A., 1943. Quasigroups I. Transactions of the American Mathematical Society 54, 507–519.

Bayer, D., 1982. The division algorithm and the Hilbert scheme. Ph. D. Thesis. Harvard University.

Bruck, R.H., 1944. Some results in the theory of quasigroups. Transactions of the American Mathematical Society 55, 19–54.

Buchberger, B., 1965. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph. D. Thesis. University of Innsbruck. English translation 2006: An algorithm for finding the basis elements in the residue class ring modulo a zero dimensional polynomial ideal. (Logic, mathematics, and computer science: Interactions). Journal of Symbolic Computation. 41 (3–4), 475–511 (special issue).

Cox, D., Little, J., O'Shea, D., 1997. Ideals, Varieties and Algorithms. Springer, Berlin.

Falcón, R.M., 2006. Latin squares associated to principal autotopisms of long cycles. Application in Cryptography. In: Proceedings of Transgressive Computing 2006: A Conference in Honor of Jean Della Dora. Granada. pp. 213–230.

Falcón, R.M., 2007. Cycle structures of autotopisms of the Latin squares of order up to 11. Ars Combinatoria (in press). http://arxiv.org/abs/0709.2973.

Gago-Vargas, J., Hartillo-Hermoso, I., Martín-Morales, J., Ucha-Enríquez, J.M., 2006. Sudokus and Gröbner bases not only a divertimento. In: CASC 2006. In: Lecture Notes in Computer Science, vol. 4194. pp. 155–165.

Greuel, G.-M., Pfister, G., Schönemann, H., 2005. SINGULAR 3.0. A computer algebra system for polynomial computations. Centre for Computer Algebra, University of Kaiserlautern. http://www.singular.uni-kl.de.

Laywine, C.F., Mullen, G.L., 1998. Discrete Mathematics Using Latin Squares. In: Series in Discrete Mathematics and Optimization, Wiley-Interscience, ISBN: 0-471-24064-8.

Martín-Morales, J., 2006. Sudoku and Gröbner bases. In: Proceedings of Transgressive Computing 2006: A Conference in Honor of Jean Della Dora. Granada. pp. 303–310.

McKay, B.D., Meynert, A., Myrvold, W., 2007. Small Latin squares, quasigroups and loops. Journal of Combinatorial Designs 15, 98–119.