



NEW ADVANCES IN THE STUDY OF GRÖBNER BASES AND THE NUMBER OF LATIN SQUARES RELATED TO AUTOTOPISMS



Jorge Martín-Morales

Department of Mathematics-I.U.M.A.

University of Zaragoza (Spain)

jorge@unizar.es

Raúl M. Falcón

Department of Applied Mathematic I

University of Seville (Spain)

rafalgan@us.es

Dpto. Álgebra

Abstract

Gröbner bases has been used in [4] to describe an algorithm that allows one to obtain the number of Latin squares of order up to 7 having a given isotopism in their autotopism group. In order to improve the time of computation of this algorithm, we study in this poster a possible combination between Gröbner bases and some combinatorial tools. Specifically, we add to the ideal of polynomials defining a Latin square L , some polynomials related to the permutations of rows, columns and symbols corresponding to the given autotopism of L . Using this method we could obtain the number of some Latin squares of order 8 having an isotopism in their autotopism group.

Introduction and notation

• A **Latin square** L of order n is an $n \times n$ array with elements chosen from a set of n distinct symbols $\{x_1, \dots, x_n\}$, such that each symbol occurs precisely once in each row and each column. The set of Latin squares of order n is denoted by $\mathbf{LS}(n)$. 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 as $\mathbf{PLS}(n)$.

• For any given $n \in \mathbb{N}$, we denote by $[n]$ the set $\{1, 2, \dots, n\}$ and 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 $\delta \in S_n$, it is defined the set of its **fixed points** $\text{Fix}(\delta) = \{i \in [n] \mid \delta(i) = i\}$. The **cycle structure of a permutation** δ is the sequence $\mathbf{l}_\delta = (l_1^\delta, l_2^\delta, \dots, l_n^\delta)$, where l_i^δ is the number of cycles of length i in δ , for all $i \in \{1, 2, \dots, n\}$. On the other hand, given $L = (l_{i,j}) \in \mathbf{LS}(n)$, 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, it is written $(i, j, l_{i,j}) \in L$, for all $i, j \in [n]$.

• An **isotopism** of a Latin square $L \in \mathbf{LS}(n)$ is 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 . If $L = (l_{i,j})$, then $L^\Theta = \{(\alpha(i), \beta(j), \gamma(l_{i,j})) \mid i, j \in [n]\}$. 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}_δ is the cycle structure of δ , for all $\delta \in \{\alpha, \beta, \gamma\}$. An isotopism which maps L to itself is an **autotopism**. The possible cycle structures of the set of non-trivial autotopisms of Latin squares of order up to 11 were obtained in [3].

• The stabilizer subgroup of L in \mathcal{I}_n is its **autotopism group**, $\mathfrak{A}(L) = \{\Theta \in \mathcal{I}_n \mid L^\Theta = L\}$. Given $\Theta \in \mathcal{I}_n$, the set of all Latin squares L such that $\Theta \in \mathfrak{A}(L)$ is denoted by $\mathbf{LS}(\Theta)$ and the cardinality of $\mathbf{LS}(\Theta)$ is denoted by $\Delta(\Theta)$. If Θ_1 and Θ_2 are two autotopisms with the same cycle structure, then $\Delta(\Theta_1) = \Delta(\Theta_2)$. Now, given $P \in \mathbf{PLS}(n)$, the number $c_P = \Delta(\Theta)/|\mathbf{LS}_P(\Theta)|$ is called **P -coefficient of symmetry** of Θ , where $\mathbf{LS}_P(\Theta) = \{L \in \mathbf{LS}(\Theta) \mid P \subseteq L\}$.

• Gröbner bases were used in [4] to describe an algorithm that allows one to obtain the number $\Delta(\Theta)$ in a computational way. This algorithm was implemented in SINGULAR [6] to get the number of Latin squares of order ≤ 7 related to any autotopism of a given cycle structure [5]. The authors have seen that, in order to improve the time of computation, it is convenient to combine Gröbner bases with some combinatorial tools.

Cycle structures of Latin square autotopisms

Every permutation $\delta \in S_n$ can be uniquely written as a composition of pairwise disjoint cycles, $\delta = C_1^{\delta} \circ C_2^{\delta} \circ \dots \circ C_{k_\delta}^{\delta}$, where:

- $\forall i \in [k_\delta], C_i^{\delta} = (c_{i,1}^{\delta} c_{i,2}^{\delta} \dots c_{i,\lambda_i^{\delta}})$, with $\lambda_i^{\delta} \leq n$ and $c_{i,1}^{\delta} = \min_j \{c_{i,j}^{\delta}\}$.
- $\sum_i \lambda_i^{\delta} = n$.
- For all $i, j \in [k_\delta]$, one has $\lambda_i^{\delta} \geq \lambda_j^{\delta}$, whenever $i \leq j$.
- Given $i, j \in [k_\delta]$, with $i < j$ and $\lambda_i^{\delta} = \lambda_j^{\delta}$, one has $c_{i,1}^{\delta} < c_{j,1}^{\delta}$.

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

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

Then, all the triples of L are known. \square

Gröbner bases and Latin square autotopisms

Given a generic Latin square $L = (l_{i,j}) \in \mathbf{LS}(n)$, 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:

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

Now, given an autotopism $\Theta = (\alpha, \beta, \gamma) \in \mathfrak{A}(L)$, let $H(x)$ be a polynomial such that $H(x) = \gamma(x)$, for all $x \in [n]$. Following the ideas implemented by Bayer [2] (see also [1]) to solve the problem of an n -colouring a graph, we have:

Theorem 2. Let $I \subseteq \mathbb{Q}[x] = \mathbb{Q}[x_{1,1}, \dots, x_{n,n}]$ be the ideal generated by $F(x_{i,j}), G(x_{i,j}, x_{i',j'}), G(x_{i,j}, x_{i',j'}), H(x_{i,j}) - x_{\alpha(i),\beta(j)}$, where $i, i', j, j' \in [n], i \neq i', j \neq j'$. Then $V(I) = \mathbf{LS}(\Theta)$. \square

Let S_Θ the following set of multi-indices:

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

Let $P = (p_{i,j}) \in \mathbf{PLS}(n)$ 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 $\Delta(\Theta) = c_P \cdot |\mathbf{LS}_P(\Theta)|$ and we will

calculate $|\mathbf{LS}_P(\Theta)|$ starting from the set of solutions of an algebraic system of polynomial equations associated with Θ and P . Specifically, we obtain the following algorithm that we implemented in SINGULAR and got the table below.

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

Input: $\Theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$; $P = (p_{i,j}) \in \mathbf{PLS}(n)$; c_P , the P -coefficient of symmetry of Θ .
Output: $\Delta(\Theta)$, the number of Latin squares L such that $\Theta \in \mathfrak{A}(L)$;
 $I :=$ the ideal in $\mathbb{Q}[x]$ in \mathcal{I}_n ;
 $J := I + \langle x_{i,j} - p_{i,j} \mid (i, j) \in S_\Theta \rangle$; $V(J) = \mathbf{LS}_P(\Theta)$
 $G :=$ Gröbner basis of J w.r.t. **ANY** term ordering;
 $\Delta_P := \dim_{\mathbb{Q}}(\mathbb{Q}[x]/J)$; $[\Delta_P]$ is the cardinality of $V(J)$
return $c_P \cdot \Delta_P$;

Computational Remark 3. Algorithm 1 has several advantages comparing to the algorithm that we presented in [4], (see the table below):

- Gröbner bases with respect to elimination orderings were needed in [4]. Here, any term ordering can be chosen.
- When the polynomial H , which satisfies $H(x) = \gamma(x)$ for all $x \in [n]$, has rational coefficients, Gröbner bases over fields of positive characteristic can be used.
- The computation of a Gröbner basis of J could actually be done in the ring $\mathbb{Q}[x_{i,j} \mid (i, j) \in S_\Theta]$.

Gröbner bases on block design

We have just seen that Algorithm 1 allows one to obtain all the elements of the Latin rectangle R_L of Proposition 1. Now, let us observe that R_L is indeed the union of $k_\alpha \cdot k_\beta$ Latin rectangles:

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

Each of these rectangles can be obtained by using an algorithm similar to Algorithm 1. Specifically, given $r \in [k_\alpha]$ and $s \in [k_\beta]$, it is enough to consider λ_s^β variables, $x_{r,c_{s,1}^\beta}, \dots, x_{r,c_{s,\lambda_s^\beta}^\beta}$, corresponding to the elements $l_{r,c_{s,1}^\beta}, \dots, l_{r,c_{s,\lambda_s^\beta}^\beta}$ of the partial Latin square $R_L^{r,s} \in \mathbf{PLS}(\Theta)$. Next, let us consider the set:

$$LS_{r,s}(\Theta) = \left\{ P = (p_{i,j}) \in \mathbf{PLS}(\Theta) \mid |P| = \lambda_r^\alpha \cdot \lambda_s^\beta \text{ and } p_{i,j} = \emptyset, \text{ whenever } (i, j) \notin C_r^\alpha \times C_s^\beta \right\}.$$

The following result holds:

Theorem 3. The set of zeros of the following ideal of $\mathbb{Q}[x] = \mathbb{Q}[x_{r,c_{s,1}^\beta}, \dots, x_{r,c_{s,\lambda_s^\beta}^\beta}]$ corresponds to the set $LS_{r,s}(\Theta)$:

$$I_{r,s} = \langle G(x_{r,j}, x_{r,j'}) \mid j, j' \in C_s^\beta \text{ and } j \neq j' \rangle + \langle P(x_{i,j}) - x_{\alpha(i),\beta(j)} \mid (i, j) \in C_r^\alpha \times C_s^\beta \rangle. \square$$

• In this way, it is possible to decompose Algorithm 1 into $k_\alpha \cdot k_\beta$ similar algorithms. However, it must be observed that, in general, $\bigcup_{r \in [k_\alpha], s \in [k_\beta]} LS_{r,s}(\Theta) \neq \mathbf{LS}(\Theta)$, because, given $r' \in [k_\alpha], s' \in [k_\beta]$ such that $(r', s') \neq (r, s)$, we can find $P' \in LS_{r',s'}(\Theta)$ and $P'' \in LS_{r',s'}(\Theta)$ such that $P \cup P' \in \mathbf{PLS}(\Theta)$.

n	$\mathbf{l}_\alpha = \mathbf{l}_\beta$	\mathbf{l}_α	$\Theta \in \mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta)$	P	c_P	Δ	r.t. (1)	r.t. (1)
5	(1,0,0,1)	(1,0,0,1)	((1325), (1345), (1345))	((1,1,2), (2,2,2))	8	106496	1191	1
	(0,0,0,0,1)	(6,0,0,0,0)	((123456), (123456))	((1,1,1))	6	720	0	3
	(1,0,0,0,1)	(1,0,0,0,1)	((13456), (13456), (13456))	((i, i, 2))_{i=1,2}	5	75	1	7
	(1,0,0,0,0)	(4,1,0,0,0)	((16)(25)(34), (16)(25)(34), (16))	$\begin{pmatrix} 1 & 6 & 3 & 4 & 5 & 2 \\ 6 & * & * & * & * & * \\ 3 & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{pmatrix}$	13824	110592	0	2
	(2,2,0,0,0)	(2,2,0,0,0)	((16)(25), (16)(25), (16)(25))	$\begin{pmatrix} 4 & * & * & * & * & * \\ * & 4 & 2 & * & * & * \\ * & * & 3 & 4 & * & * \\ * & * & * & 3 & 4 & * \\ * & * & * & * & 4 & 2 & * \\ * & * & * & * & * & 4 & 2 & * \end{pmatrix}$	128	20480	5	137
(0,0,0,0,0,1)	(7,0,0,0,0,0)	((1234567), (1234567), (1234567))	((1,1,1))	7	5040	2	17	
								(1,0,0,0,0,1)
(1,1,0,1,0,0)	(1,1,0,1,0,0)	((1456)(27), (1456)(27), (1456)(27))	$\begin{pmatrix} 3 & * & 2 & * & * & 7 \\ * & 3 & 2 & * & * & * \\ * & * & 2 & * & * & * \\ * & * & * & 2 & * & * \\ * & * & * & * & 2 & * \\ * & * & * & * & * & 2 \end{pmatrix}$	128	512	2	3	
								(3,0,0,1,0,0)

n	$\mathbf{l}_\alpha = \mathbf{l}_\beta$	\mathbf{l}_α	$\Theta \in \mathcal{I}_n(\mathbf{l}_\alpha, \mathbf{l}_\beta)$	P	c_P	Δ	r.t. (1)	r.t. (1)
8	(0,0,0,2,0,0,0,0)	(0,0,0,2,0,0,0,0)	((12345678), (12345678), (12345678))	((1,1,2), (2,2,2))	8	1152	51	1
	(0,4,0,0,0,0,0,0)	(0,4,0,0,0,0,0,0)	((12345678), (12345678), (18)(27)(36)(45))	((1,1,1), (1,6,2))	48	81008	1119	
								(2,1,0,1,0,0,0,0)
	(0,0,0,2,0,0,0,0)	(3,0,0,0,0,0,0,0)	((12345678), (12345678), (1678)(2345), (1678)(2345), (18)(27)(36)(45))	((1,1,4), (1,6,2), (2,2,2))_{i \in [8]}	8	1007616	610	
								(0,0,0,0,0,0,0,1)
	(4,0,0,1,0,0,0,0)	(4,0,0,1,0,0,0,0)	((12345678), (12345678), (1678)(2345), (1678)(2345), (18)(27)(36)(45))	((1,1,3), (1,6,2), (2,2,2))_{i \in [8]}	32	2727936	770	
								(4,2,0,0,0,0,0,0)
	(6,1,0,0,0,0,0,0)	(6,1,0,0,0,0,0,0)	((12345678), (12345678), (1678)(2345), (1678)(2345), (18)(27)(36)(45))	((1,1,1), (1,6,2), (1,8,3), (2,2,2))	960	7744440	83	
								(1,0,0,0,0,0,1,0)
(0,2,0,1,0,0,0,0)	(0,2,0,1,0,0,0,0)	$\alpha, \beta, \gamma = (1678)(25)(34), (1678)(25), (1678)(25)$	$\begin{pmatrix} 1 & 6 & 8 & 7 & * & * & * & * \\ * & 1 & * & * & 8 & 7 & * & * \\ * & * & * & * & 1 & 8 & 7 & * \end{pmatrix}$	64	16384	1		
							(0,2,0,1,0,0,0,0)	(2,1,0,1,0,0,0,0)
(4,0,0,1,0,0,0,0)	(4,0,0,1,0,0,0,0)	$\alpha, \beta = (1678)(25)(34), \gamma = (1678)$	$\begin{pmatrix} 1 & 6 & 8 & 7 & * & * & * & * \\ * & 1 & * & * & 8 & 7 & * & * \\ * & * & * & * & 1 & 8 & 7 & * \end{pmatrix}$	64	147456	1		
							(2,0,0,0,1,0,0,0)	(2,0,0,0,1,0,0,0)