A computational algebraic geometry approach to analyze pseudo-random sequences based on Latin squares

Raúl M. Falcón[1] **Víctor Álvarez**[1] **Félix Gudiel**[1]

Abstract

Latin squares are used as scramblers on symmetric-key algorithms that generate pseudo-random sequences of the same length. The robustness and effectiveness of these algorithms are respectively based on the extremely large key space and the appropriate choice of the Latin square under consideration. It is also known the importance that isomorphism classes of Latin squares have to design an effective algorithm. In order to delve into this last aspect, we improve in this paper the efficiency of the known methods on computational algebraic geometry to enumerate and classify partial Latin squares. Particularly, we introduce the notion of affine algebraic set of a partial Latin square $L = (l_{ij})$ of order n over a field $\mathbb{K}$ as the set of zeros of the binomial ideal $\langle\, x_i\, x_j - x_{l_{ij}} \colon (i,\ j)$ is a non-empty cell in$L\,\rangle \subseteq \mathbb{K}[x_1, \ldots,\ x_n]$. Since isomorphic partial Latin squares give rise to isomorphic affine algebraic sets, every isomorphism invariant of the latter constitutes an isomorphism invariant of the former. In particular, we deal computationally with the problem of deciding whether two given partial Latin squares have either the same or isomorphic affine algebraic sets. To this end, we introduce a new pair of equivalence relations among partial Latin squares: being partial transpose and being partial isotopic.

Keywords

Symmetric-key algorithm · Image pattern · Partial Latin square · Affine algebraic set · Isomorphism

✉ Raúl M. Falcón
rafalgan@us.es

Víctor Álvarez
valvarez@us.es

Félix Gudiel
gudiel@us.es

[1] Department Applied Mathematics I, University of Seville, Seville, Spain

1 Introduction

A *partial Latin square of order n* is an $n \times n$ array in which each cell is either empty or contains an element of a finite set S of n symbols so that each symbol occurs at most once in each row and in each column. This is a *Latin square* if all its cells are non-empty. Every Latin square constitutes the multiplication table of a *quasigroup* $Q = (S, \cdot)$ endowed with a binary operation $\cdot$ so that the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions for x and y in S, for all $a, b \in S$. Equivalently, Q has left- and right-division, which we denote respectively $\backslash$ and $/$. That is, $x = a\backslash b$ in the first equation, and $y = b/a$ in the second one. Currently, it is only known the number of Latin squares of order $n \leq 11$ [24, 31, 37] and that of partial Latin squares of order $n \leq 7$ [13–15].

Quasigroups and Latin squares are commonly used in cryptography [38, 39, 41]. In symmetric cryptography, Latin squares are used as *scramblers* that generate ciphered pseudo-random strings with the same length than a given plaintext, but with a remarkable *period growth* [26, 27, 33]. That is, they increase considerably the maximum number of consecutive distinct bits within the plaintext. More specifically, given a quasigroup $Q = (S, \cdot)$, a *leader symbol* $s \in S$ and a plaintext $T = t_1 t_2 \dots t_m$, the former enables one to generate the encrypted string $E_s(T) = e_1 e_2 \dots e_m$, where $e_1 = s \cdot t_1$ and $e_i = e_{i-1} \cdot t_i$, for all $1 < i \leq m$. The sequences of the ciphered text follow a uniform distribution [34, 36]. The decryption map $D_s(E_s(T))$ is, in turn, based on the left-division within Q. In particular, $t_1 = s\backslash e_1$ and $t_i = e_{i-1}\backslash e_i$, for all $1 < i \leq m$. This encryption-decryption process acts, therefore, as a symmetric-key algorithm having the underlying Latin square related to the quasigroup as its cryptographic key. The latter can in turn be decomposed into disjoint partial Latin squares as shares describing a secret sharing scheme [4, 5, 12, 44].

The huge number of Latin squares ensures the robustness of this algorithm against brute force and statistical attacks, even if the ciphered text and the leader symbol are known. In any case, an appropriate choice of the Latin square under consideration is especially relevant to design effective symmetric-key algorithms producing high period growths [9]. In order to optimize this choice, the distribution of Latin squares into isomorphism classes play a fundamental role. This is due to the fact that any two isomorphic Latin squares always generate the same number of consecutive distinct bits starting from a same plaintext. Reciprocally, the analysis of pseudo-random sequences derived from non-isomorphic Latin squares enables one to discover certain algebraic and even geometrical properties that they have in common [32, 35]. Remark in this last regard how Dimitrova and Markovski [10, 11] introduced the distribution of quasigroups into fractals and non-fractals, depending on the image patterns that result after disposing as rows of a rectangular array the ciphered texts derived from an iterative application of the described encryption process. Let us remark that counting, enumerating, and analyzing isomorphism classes constitute indeed main problems in the theory of (partial) Latin squares. Currently, it is known the number of isomorphism classes of Latin squares of order $n \leq 11$ [24, 31, 37] and that of partial Latin squares of order $n \leq 6$ [17, 19].

Computational algebraic geometry has revealed to be a good alternative to deal with the enumeration and classification of (partial) Latin squares of small order [1, 2,

13–17, 19], but further work is necessary to deal with higher orders. This is mainly due to the cost of computation that is required to determine the reduced Gröbner basis of the ideal associated to each partial Latin square. Such a computation is extremely sensitive to the number of involved variables, and the length and degree of the generators [20–22, 28].

In order to reduce the mentioned cost, we introduce in this paper the notion of affine algebraic set of a partial Latin square. Within the framework of the character theory of finite quasigroups, Johnson [30] introduced the determinant of a Latin square $L = (l_{ij})$ as that one of the square matrix $X_L = (x_{l_{ij}})$. We deal with the analogous matrix that is related to a partial Latin square, but focus on the affine algebraic set of the zero-dimensional binomial ideal whose generators are of the form $x_i x_j - x_{l_{ij}}$, for all non-empty cell (i, j). We expose how the isomorphism invariants of such an affine algebraic set reduce the cost of computation that is required to distribute partial Latin squares into isomorphism classes. The study of new invariants to facilitate the classification of partial Latin squares is currently an active research area [6, 18, 43].

The paper is organized as follows. Section 2 deals with some preliminary concepts and results on partial Latin squares and computational algebraic geometry that are used throughout the paper. Sections 3 and 4 focus on those conditions under which two given partial Latin squares have, respectively, the same or isomorphic affine algebraic sets. In particular, we prove that isomorphic Latin squares give rise to isomorphic affine algebraic sets, but the reciprocal is not true in general. As an illustrative example, we enumerate the isomorphism classes of the affine algebraic sets of all partial Latin squares of order up to three. In Section 5, we expose how the computation of affine algebraic sets of partial Latin squares lowers the computational cost that is required to determine their distribution into isomorphism classes. Due to the high dependence on notation, a glossary of symbols is shown in Appendix.

2 Preliminaries

Let us review some basic concepts and results on partial Latin squares and Computational Algebraic Geometry that are used throughout the paper. We refer the reader to the monographs [8, 25] for more details on both topics.

2.1 Partial Latin squares

Let $\mathcal{L}_n$ denote the set of partial Latin squares of order n having the set

$$[n] := \{1, \ldots, n\}$$

as set of symbols. Every partial Latin square $L = (l_{ij}) \in \mathcal{L}_n$ is determined by its *set of entries*

$$E(L) := \{(i, j, l_{ij}) \colon\ i, j, l_{ij} \in [n]\}.$$

The cardinality of this set constitutes the *weight* of L, which coincides with the number of its non-empty cells. Thus, for instance, the partial Latin square

$$L_1 \equiv \begin{array}{|c|c|c|}\hline & 2 & 3 \\ \hline 1 & & \\ \hline & 1 & \\ \hline \end{array} \in \mathcal{L}_3$$

has set of entries $E(L_1) = \{(1, 2, 2), (1, 3, 3), (2, 1, 1), (3, 2, 1)\}$ and weight four. A partial Latin square is said to be *trivial* if its weight is zero.

Let S_n denote the symmetric group on n elements. Permutations of rows, columns, and symbols of partial Latin squares preserve the set $\mathcal{L}_n$. Thus, two partial Latin squares $L = (l_{ij})$ and $L' = (l'_{ij})$ in $\mathcal{L}_n$ are called *isotopic* if there exists a triple $\Theta = (f, g, h) \in S_n \times S_n \times S_n$ such that $E(L') = \{(f(i), g(j), h(l_{ij})) \colon (i, j, l_{ij}) \in E(L)\}$. In such a case, we denote $L^{\Theta} = L'$. The triple (f, g, h) is an *isotopism* from L to L'. This constitutes an *isomorphism* if $f = g = h$, in which case, the partial Latin squares under consideration are called *isomorphic*. In such a case, we denote $L^f = L'$. Thus, for instance, the previously mentioned partial Latin square L_1 is isotopic to the partial Latin square

$$L_2 \equiv \begin{array}{|c|c|c|}\hline 3 & & \\ \hline 2 & & 1 \\ \hline & 3 & \\ \hline \end{array} \in \mathcal{L}_3$$

by means of the isotopism $((123), (12)(3), (13)(2)) \in S_3 \times S_3 \times S_3$. Further, two partial Latin squares L and L' of the same order are said to be *conjugate* if there exists a permutation $\pi \in S_3$ such that $E(L') = \{(i_{\pi(1)}, i_{\pi(2)}, i_{\pi(3)}) \colon (i_1, i_2, i_3) \in E(L)\}$. Every partial Latin square has, therefore, six conjugates (not necessarily distinct from each other). Thus, for instance, the partial Latin square

$$L_3 \equiv \begin{array}{|c|c|c|}\hline & 3 & \\ \hline & 1 & \\ \hline 1 & & 2 \\ \hline \end{array} \in \mathcal{L}_3$$

is conjugate of the previously mentioned partial Latin square L_2 by means of the permutation $(123) \in S_3$. Finally, two partial Latin squares are said to be *paratopic* if one of them is isotopic to a conjugate of the other. Thus, for instance, the previously mentioned partial Latin squares L_1 and L_3 are paratopic. Remark that to be isotopic, isomorphic, conjugate, or paratopic are equivalence relations among partial Latin squares.

We deal now with the use of Latin squares as scramblers within the context of the encryption-decryption process described in the introductory section. Particularly, we focus on the construction of the mentioned image patterns introduced by Dimitrova and Markovski [10, 11]. To this end, let us consider a Latin square $L = (l_{ij}) \in \mathcal{L}_n$, a pair of positive integers $m, r \in \mathbb{N}$, a sequence $S = (s_1, \ldots, s_{r-1})$, and a plaintext $T = t_1 \ldots t_m$, with $s_i, t_j \in [n]$, for all $1 \leq i < r$ and $1 \leq j \leq m$. Let us denote $T_1 = T$ and $T_i = E_{s_{i-1}}(T_{i-1})$, for all $1 < i \leq r$.

Then, the $r \times m$ *image pattern* derived from L, S, and T is the $r \times m$ array satisfying that, for each $i \in [r]$, the entries of its i^{th} row coincide sequentially with the characters of T_i. We denote $\mathcal{I}_{S,T}(L)$ this array.

Example 1 Let us consider the Latin square

$$L \equiv \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 2&3&1\\\hline 3&1&2\\\hline\end{array} \in \mathcal{L}_3,$$

the sequence $S = (1, 2, 2, 3, 3, 3)$ and the plaintext $T = 123123$. Then,

$$\mathcal{I}_{S,T}(L) \equiv \begin{array}{|c|c|c|c|c|c|}\hline 1&2&3&1&2&3\\\hline 1&2&1&1&2&1\\\hline 2&3&3&3&1&1\\\hline 3&2&1&3&3&3\\\hline 2&3&3&2&1&3\\\hline 1&3&2&3&3&2\\\hline 3&2&3&2&1&2\\\hline\end{array}.$$

◁

The following result implies that, in order to analyze the set of image patterns of the set $\mathcal{L}_n$, it is enough to focus on a representative Latin square of each one of its isomorphism classes. It follows straightforwardly from the notion of isomorphism of Latin squares and the described encryption process.

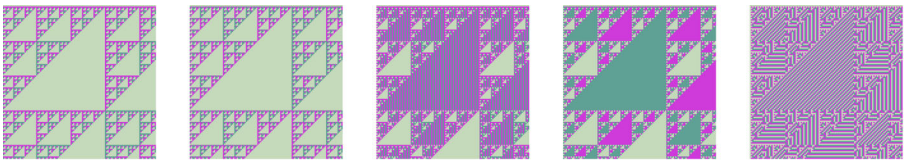
Lemma 1 *Let f be an isomorphism between two Latin squares $L, L^f \in \mathcal{L}_n$, and let us consider a sequence $S = (s_1, \ldots, s_{r-1})$ and a plaintext $T = t_1 \ldots t_m$, with $s_i, t_j \in [n]$, for all $i < r$ and $j \leq m$. Let $f(S) = (f(s_1), \ldots, f(s_{r-1}))$ and $f(T) = f(t_1) \ldots f(t_m)$. Then, the image patterns $\mathcal{I}_{S,T}(L)$ and $\mathcal{I}_{f(S),f(T)}(L^f)$ coincide up to a permutation of their symbols. More specifically, a cell (i, j) in $\mathcal{I}^{r,m}_{S,T}(L)$ contains a symbol $\alpha_{ij} \in [n]$ if and only if the corresponding cell (i, j) in $\mathcal{I}_{f(S),f(T)}(L^f)$ contains the symbol $f(\alpha_{ij})$.*

In practice, image patterns based on Latin squares of order n are represented as pixel arrays so that each symbol in the pattern under consideration is uniquely replaced by a color within a given palette of n colors. In order to illustrate this fact, let us consider the following Latin squares.

$$\begin{array}{|c|c|c|}\hline 1&2&3\\\hline 2&3&1\\\hline 3&1&2\\\hline\end{array}\ L_{3,1} \qquad \begin{array}{|c|c|c|}\hline 1&2&3\\\hline 3&1&2\\\hline 2&3&1\\\hline\end{array}\ L_{3,2} \qquad \begin{array}{|c|c|c|}\hline 1&3&2\\\hline 2&1&3\\\hline 3&2&1\\\hline\end{array}\ L_{3,3} \qquad \begin{array}{|c|c|c|}\hline 1&3&2\\\hline 3&2&1\\\hline 2&1&3\\\hline\end{array}\ L_{3,4} \qquad \begin{array}{|c|c|c|}\hline 2&1&3\\\hline 1&3&2\\\hline 3&2&1\\\hline\end{array}\ L_{3,5}$$

They are respective representatives of the five isomorphism classes of the set $\mathcal{L}_3$. Each pixel array $\mathcal{I}_{3,i}$ in Fig. 1, where $1 \leq i \leq 5$, represents a 120×120 image pattern derived from the Latin square $L_{3,i}$, the constant sequence $S = (2, \ldots, 2)$, and the constant plaintext $T = 1 \ldots 1$.

Lemma 1, together with the fractal character of all the pixel arrays in Fig. 1, implies that every quasigroup of order three is fractal [10]. Observe also from Lemma 1 that all these pixel arrays make easy to distinguish visually all the isomorphism classes of the set $\mathcal{L}_3$ except for the first two arrays, $\mathcal{I}_{3,1}$ and $\mathcal{I}_{3,2}$, which require a more trained eye to distinguish them.



$\mathcal{I}_{3,1}$ $\mathcal{I}_{3,2}$ $\mathcal{I}_{3,3}$ $\mathcal{I}_{3,4}$ $\mathcal{I}_{3,5}$

Fig. 1 Image patterns based on the five isomorphism classes of $\mathcal{L}_3$

We introduce here a general approach to make easier this distinction. This consists of representing separately the contribution of each cell within the Latin square L under consideration on the construction of the corresponding image pattern $\mathcal{I} = (\alpha_{ij})$. To this end, we consider the quasigroup $Q = ([n], \cdot)$ having L as its multiplication table. Then, for each pair $(k, l) \in [n] \times [n]$, we define the $r \times m$ array $\mathcal{A}_{k,l}(\mathcal{I}) = (a_{ij}^{k,l})$ so that $a_{ij}^{k,l} = \alpha_{ij}$ if and only if the encrypted symbol α_{ij} has been obtained as the product $k \cdot l$. Otherwise, $a_{ij}^{k,l} = 0$.

Example 2 In the context of Example 1, we have that

$$\mathcal{A}_{3,1}(\mathcal{I}_{S,T}(L)) \equiv \begin{array}{|c|c|c|c|c|c|}\hline 0&0&0&0&0&0\\\hline 0&0&0&0&0&0\\\hline 0&0&3&3&0&0\\\hline 0&0&0&0&3&3\\\hline 0&0&3&0&0&0\\\hline 0&0&0&0&3&0\\\hline 3&0&0&0&0&0\\\hline\end{array}.$$

◁

We define the *atomic decomposition* of an image pattern $\mathcal{I}$ based on a Latin square of order n as the $n \times n$ array $\mathcal{A}(\mathcal{I})$ so that, for each $i, j \in [n]$, its cell (i, j) contains the array $\mathcal{A}_{i,j}(\mathcal{I})$, which we call an *atom* of $\mathcal{A}(\mathcal{I})$. Thus, for instance, Fig. 2 shows the atomic decomposition of both image patterns $\mathcal{I}_{3,1}$ and $\mathcal{I}_{3,2}$ in Fig. 1. The zero symbols of each atom is colored in black. The following result ensures that the set of atoms within the atomic decompositions of two isomorphic Latin squares coincide up to permutation of their non-zero symbols. It follows straightforwardly from Lemma 1.

Proposition 1 *Under the assumptions of Lemma 1, the atoms* $\mathcal{A}_{i,j}(\mathcal{I}_{S,T}(L))$ *and* $\mathcal{A}_{f(i),f(j)}(\mathcal{I}_{f(S),f(T)}(L^f))$ *coincide up to their non-zero symbols. More specifically, the non-zero symbol of the former is* $\alpha \in [n]$ *if and only if that one of the latter is* $f(\alpha)$.

Proposition 1 makes possible to establish certain conditions that should be satisfied by any possible isomorphism between two given Latin squares. Thus, for instance, we can observe in Fig. 2 that any possible isomorphism f between the Latin squares $L_{3,1}$ and $L_{3,2}$ should map the atom $\mathcal{A}_{1,1}(\mathcal{I}_{3,1})$ into the atom $\mathcal{A}_{1,1}(\mathcal{I}_{3,2})$, because the latter is the only atom within the atomic decomposition $\mathcal{A}(\mathcal{I}_{3,2})$ that coincides with

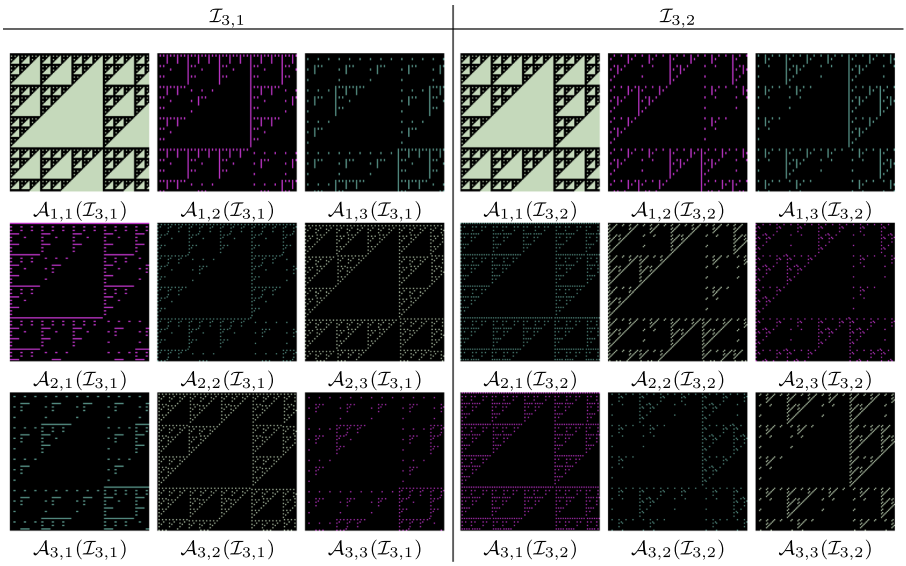


Fig. 2 Atomic decompositions of the image patterns $\mathcal{I}(L_{3,1})$ and $\mathcal{I}(L_{3,2})$

the former, even regardless of the color. As a consequence, it should be $f(1) = 1$. Nevertheless, a detailed inspection of Fig. 2 enables us to ensure that no such an isomorphism exists. Observe to this end that, again even regardless of the color, there are no coincidence among any of the rest of atoms within the atomic decompositions $\mathcal{A}(\mathcal{I}_{3,1})$ and $\mathcal{A}(\mathcal{I}_{3,2})$. Since visual inspections are very difficult to be done in general, alternative approaches are, therefore, required. In this paper, we propose to make use of computational algebraic geometry in this regard.

2.2 Computational algebraic geometry

Let $\mathbb{K}[X_n]$ be the multivariate polynomial ring over a given field $\mathbb{K}$ that is defined on the finite set of variables $X_n := \{x_1, \ldots, x_n\}$. A *zero* of a set of polynomials $S \subseteq \mathbb{K}[X_n]$ is any point $P \in \mathbb{K}^n$ such that $f(P) = 0$, for all $f \in S$. An *affine algebraic set* in the affine space $\mathbb{K}^n$ is any subset $V \subseteq \mathbb{K}^n$ formed by all the zeros of a set of polynomials in $\mathbb{K}[X_n]$. This is *irreducible* if it is not the union of two non-empty proper affine algebraic subsets. Every affine algebraic set is uniquely decomposed into a finite union of irreducible components so that none of them is a proper subset of another one. The *dimension* of an affine algebraic set V is the maximal length of any chain of irreducible components of V minus one. This is denoted $\dim(V)$.

A *morphism* between two affine algebraic sets V_1 and V_2 in $\mathbb{K}^n$ is any map $\phi : V_1 \to V_2$ such that there exist n polynomial functions, $f_1, \ldots, f_n \in \mathbb{K}[X_n]$, satisfying that $\phi(P) = (f_1(P), \ldots, f_n(P))$, for all $P \in V_1$. This is an *isomorphism* if ϕ is a bijection whose inverse is a morphism from V_2 to V_1. In this case, both affine algebraic sets are said to be *isomorphic*. Any property of affine algebraic sets that

is preserved by isomorphisms is said to be an *isomorphism invariant*. Examples of isomorphism invariants of an affine algebraic set are its dimension, its cardinality in case of being zero-dimensional, and the number of irreducible components.

An *ideal* is a subset $I \subseteq \mathbb{K}[X_n]$ satisfying that $0 \in I$; $p + q \in I$, for all $p, q \in I$; and $p \cdot q \in I$, for all $p \in I$ and $q \in \mathbb{K}[X_n]$. The ideal *generated by* a finite set of polynomials $\{p_1, \ldots, p_k\} \subseteq \mathbb{K}[X_n]$ is defined as

$$\langle\, p_1, \ldots, p_k \rangle := \left\{ \sum_{i=1}^{k} q_i \cdot p_i : \; q_i \in \mathbb{K}[X_n] \right\}.$$

It is *binomial* if all its generators are. Further, it is *radical* if every polynomial $p \in \mathbb{K}[X_n]$ belongs to I whenever there exists a positive integer $m \in \mathbb{N}$ such that $p^m \in I$. The affine algebraic set that is formed by all the zeros of the polynomials within I is denoted $\mathcal{V}(I)$. The ideal I is *zero-dimensional* if $\dim(\mathcal{V}(I)) = 0$.

The *leading monomial* of a polynomial in $\mathbb{K}[X_n]$ is its largest monomial with respect to a given multiplicative well-ordering whose smallest element is the constant monomial 1. A *Gröbner basis* of an ideal $I \subseteq \mathbb{K}[X]$ is any subset $G \subseteq I$ whose leading monomials generate the same ideal that is generated in turn by all the leading monomials of the non-zero polynomials of I. This is *reduced* if all its polynomials are monic and no monomial of a polynomial in G is generated by the leading monomials of the rest of polynomials in the basis. The reduced Gröbner basis of I is unique and can always be computed from Buchberger's algorithm [3]. Its decomposition into finitely disjoint subsets enables one to determine the irreducible components of $\mathcal{V}(I)$ [23, 29, 40].

The computation of a reduced Gröbner basis is extremely sensitive to the number of variables, and the length and degree of polynomials in the ideal [20–22, 28]. The following two results illustrate this fact in case of dealing with the field $\mathbb{Q}$ of rational numbers or a finite field $\mathbb{F}_q$, with q a power prime.

Theorem 1 ([28]) *The complexity to compute the reduced Gröbner basis of a zero-dimensional radical ideal over the field $\mathbb{Q}$ of rational numbers is $d^{O(n)}$, where d is the maximal degree of the polynomials of the ideal, and n is the number of variables.*

Theorem 2 ([20]) *The complexity time that is required to compute the reduced Gröbner basis of an ideal $\langle\, p_1, \ldots, p_m, p_1^q - p_1, \ldots, p_m^q - p_m \,\rangle$ over a polynomial ring $\mathbb{F}_q[X_n]$, where $p_1, \ldots, p_m$ are polynomials given in sparse form and have longest length l, is $q^{O(n)} + O(m^2 l)$. Here, sparsity refers to the number of monomials.*

3 The affine algebraic set of a partial Latin square

Let $\mathbb{K}$ be a field and let $L = (l_{ij})$ be a partial Latin square in $\mathcal{L}_n$. We define the *affine algebraic set* of L over $\mathbb{K}$ as the affine algebraic set $\mathcal{V}_{\mathbb{K}}(L) \subseteq \mathbb{K}^n$ of the binomial ideal

$$I(L) := \langle\, x_i x_j - x_{l_{ij}} : \; (i, j, l_{ij}) \in E(L) \,\rangle. \tag{1}$$

Particularly, if L is the trivial partial Latin square of order n, then $I(L) = \{0\}$ and hence, $\mathcal{V}_{\mathbb{K}}(L) = \mathbb{K}^n$. Throughout this paper, we consider the first three variables x_1, x_2, and x_3 to be, respectively, x, y, and z.

Example 3 Let us consider the Latin square $L_{3,2} \in \mathcal{L}_3$ described in Section 2, and let $\mathbb{K}$ be a field. According to (1), each entry of the Latin square $L_{3,2}$ maps into a binomial in $\mathbb{K}[x, y, z]$. Thus, for instance, the triples $(1, 1, 1)$ and $(1, 2, 2)$ in the set of entries $E(L_{3,2})$ map, respectively, into the binomials $x^2 - x$ and $xy - y$. The complete map is schematically represented as follows, where we take into account that the product of variables is commutative.

$$\begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline \end{array} \rightarrow \begin{array}{|c|c|c|} \hline x^2 - x & xy - y & z - z \\ \hline xy - z & y^2 - x & yz - y \\ \hline xz - y & yz - z & z^2 - x \\ \hline \end{array}$$

The nine binomials appearing as entries within the last array constitute the generators of the binomial ideal $I(L_{3,2})$. Observe in particular that the binomial $y - z$ belongs to such an ideal, because

$$y - z = (xy - z) - (xy - y).$$

Then, the binomial $x - z$ also belongs to the ideal, because

$$x - z = y(y - z) + (yz - z) - (y^2 - x).$$

As a consequence, $x = y = z$ in the coordinate ring $\mathbb{K}[x, y, z]/I(L_{3,2})$. Thus, we have, for instance, that

$$I(L_{3,2}) = \langle\, x - z,\ y - z,\ z^2 - z \,\rangle.$$

The set $\{x - z,\ y - z,\ z^2 - z\}$ constitutes indeed a reduced Gröbner basis of the ideal $I(L_{3,2})$ with respect to the lexicographical ordering. Further, the affine algebraic set of the Latin square $L_{3,2}$ over the $\mathbb{K}$ is, therefore, the set

$$\mathcal{V}_{\mathbb{K}}(L_{3,2}) = \{(0, 0, 0), (1, 1, 1)\}.$$

A similar study can be made for the rest of representative classes of the set $\mathcal{L}_3$, which we showed in Section 2. In particular,

$$\mathcal{V}_{\mathbb{K}}(L_{3,1}) = \{(0, 0, 0)\} \cup \{(a^3, a^2, a) \colon\ a \in \mathbb{K} \text{ such that } a^3 = 1\}$$

and

$$\mathcal{V}_{\mathbb{K}}(L_{3,3}) = \mathcal{V}_{\mathbb{K}}(L_{3,4}) = \mathcal{V}_{\mathbb{K}}(L_{3,5}) = \{(0, 0, 0), (1, 1, 1)\}.$$

Thus, it seems that there is not a clear relationship among affine algebraic sets and isomorphism classes of Latin squares. The goal of the rest of the paper consists of establishing this relationship, together with the characterization and analysis of these new algebraic structures.

Let us start our analysis by illustrating in the following example the dependence that affine algebraic sets of Latin squares have on the base field.

Example 4 Let us consider the partial Latin square

$$L \equiv \begin{array}{|c|c|}\hline 1 & \\ \hline & 1 \\ \hline \end{array} \in \mathcal{L}_2.$$

Then, $I(L) = \langle\, x^2 - x,\, y^2 - x \,\rangle \subset \mathbb{K}[x, y]$ and $\mathcal{V}_{\mathbb{K}}(L) = \{(0, 0), (1, 1), (1, -1)\}$. The latter is formed by three different elements unless the base field $\mathbb{K}$ has characteristic two, in which case the points $(1, 1)$ and $(1, -1)$ coincide. $\triangleleft$

In what follows, we focus on the study of the set

$$\mathcal{V}_{\mathbb{K}}(\mathcal{L}_n) := \{\mathcal{V}_{\mathbb{K}}(L) \colon\ L \in \mathcal{L}_n\}.$$

Firstly, we characterize the case $n = 1$.

Lemma 2 *The set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_1)$ is formed by the affine space $\mathbb{K}$ and the set $\{0, 1\}$. Both sets are isomorphic if and only if $\mathbb{K}$ is the finite field $\mathbb{F}_2$.*

Proof The only non-trivial partial Latin square in $\mathcal{L}_1$ is

$$L \equiv \boxed{1} \in \mathcal{L}_1.$$

Then, $I(L) = \langle\, x^2 - x \,\rangle \subset \mathbb{K}[x]$ and $\mathcal{V}_{\mathbb{K}}(L) = \{0, 1\}$. The last assertion is straightforwardly verified. $\square$

The following result enables us to ensure that $\mathcal{V}_{\mathbb{K}}(L) \neq \emptyset$, for all $L \in \mathcal{L}_n$.

Lemma 3 *Let $\mathbb{K}$ be a field. Then,*

$$\bigcap_{V \in \mathcal{V}_{\mathbb{K}}(\mathcal{L}_n)} V = \{(0, \ldots, 0), (1, \ldots, 1)\} \subseteq \mathbb{K}^n.$$

Proof The case $n = 1$ follows readily from Lemma 2. Thus, suppose that $n \geq 2$. From (1), it is verified that $\{(0, \ldots, 0), (1, \ldots, 1)\} \subseteq \mathcal{V}_{\mathbb{K}}(L)$, for all $L \in \mathcal{L}_n$. In order to prove the equality, we describe a partial Latin square of order n whose affine algebraic set coincides with the pair of points under consideration. In this regard, let $L \in \mathcal{L}_n$ be such that $E(L) = \{(1, j, j), (j, 1, j-1) \colon\ j \in \{2, \ldots, n\}\}$. Then, $I(L) = \langle\, x_1 x_j - x_j,\ x_j x_1 - x_{j-1} \colon\ j \in \{2, \ldots, n\} \,\rangle \subset \mathbb{K}[X_n]$. Since the product of variables is commutative, we have that $x_1 = \ldots = x_n$ in the coordinate ring $\mathbb{K}[X_n]/I(L)$. As a consequence, $x_1^2 - x_1 \in I(L)$ and hence, $\mathcal{V}_{\mathbb{K}}(L) = \{(0, \ldots, 0), (1, \ldots, 1)\} \subseteq \mathbb{K}^n$. $\square$

Lemma 4 *Let $L \in \mathcal{L}_m$ and $L' \in \mathcal{L}_n$ be such that $m \leq n$. If $E(L) \subseteq E(L')$, then $\mathcal{V}_{\mathbb{K}}(L') \subseteq \mathcal{V}_{\mathbb{K}}(L) \times \mathbb{K}^{n-m}$. The equality holds when $E(L) = E(L')$.*

Proof The result follows readily because every generator of the ideal $I(L)$ in the polynomial ring $\mathbb{K}[X_m]$ is also a generator of the ideal $I(L')$ in $\mathbb{K}[X_n]$. $\square$

The following pair of questions arise in a natural way from the definition of affine algebraic set of a partial Latin square.

Problem 1 When do two partial Latin squares determine the same affine algebraic set?

Problem 2 When do two partial Latin squares determine isomorphic affine algebraic sets?

Let us focus on Problem 1. Firstly, we study which entries can be removed from a partial Latin square so that the resulting partial Latin square has the same affine algebraic set than the former. To this end, for each partial Latin square $L = (l_{ij}) \in \mathcal{L}_n$, we consider the set of non-empty cells of L,

$$C(L) := \{(i, j) \in [n] \times [n] \colon (i, j, l_{ij}) \in E(L)\}.$$

Then, for each subset $S \subseteq C(L)$, we define the partial Latin square $L_S \in \mathcal{L}_n$ so that

$$E(L_S) = \{(i, j, l_{ij}) \in E(L) \colon (i, j) \in C(L) \setminus S\}.$$

Example 5 According to the previous definition, we have, for instance, that

$$(L_{3,2})_{\{(1,1),(2,3),(3,3)\}} \equiv \begin{array}{|c|c|c|}\hline & 2 & 3 \\ \hline 3 & 1 & \\ \hline 2 & 3 & \\ \hline \end{array}$$

◁

Based on the commutativity of the product of variables, the following result enables us to ensure that, in order to determine the same affine algebraic set of a partial Latin square, we can remove from the latter a cell of every pair of symmetric cells (i, j) and (j, i) containing the same symbol.

Lemma 5 *Let $L \in \mathcal{L}_n$ be such that there exist two different positive integers $i, j \leq n$ satisfying that $l_{ij} = l_{ji} \in [n]$. Then, $\mathcal{V}_{\mathbb{K}}(L) = \mathcal{V}_{\mathbb{K}}(L_{\{(i,j)\}})$.*

Proof The result follows straightforwardly from the fact that the only generator of the binomial ideal $I(L)$ that would not be explicitly a generator of the binomial ideal $I(L_{\{(i,j)\}})$ would be $x_i x_j - x_{l_{ij}}$, but this coincides with $x_j x_i - x_{l_{ji}}$. Since $i \neq j$, the latter is a generator of the second ideal. □

In a similar way, the following lemma deals with triples of cells of a partial Latin square from which we can remove one of them in order to preserve its related affine algebraic set.

Lemma 6 *Let $n > 2$. Let $L \in \mathcal{L}_n$ be such that there exist three different positive integers $i, j, k \leq n$ such that $\{(i, j, k), (k, j, i), (j, k, k)\} \subseteq E(L)$. Then, $\mathcal{V}_{\mathbb{K}}(L) = \mathcal{V}_{\mathbb{K}}(L_{\{(i,j)\}})$.*

Proof Since $x_k x_j = x_j x_k$ in $\mathbb{K}[X_n]$, we have that $x_i - x_k \in I(L_{\{(i,j)\}})$. Then, the binomial $x_i x_j - x_k$, which is related to the triple $(i, j, k) \notin E(L_{\{(i,j)\}})$, is equivalent in the ideal $I(L_{\{(i,j)\}})$ to the binomial $x_k x_j - x_i$, which is associated to the triple $(k, j, i) \in E(L_{\{(i,j)\}})$. □

Example 6 From Lemma 6, the following two partial Latin squares determine the same affine algebraic set. In the context of that result, we consider here $(i, j, k) = (1, 3, 2)$.

$$L \equiv \begin{array}{|c|c|c|}\hline & & 2 \\ \hline & & 1 \\ \hline & 2 & \\ \hline \end{array} \qquad\qquad L_{\{(1,3)\}} \equiv \begin{array}{|c|c|c|}\hline & & \\ \hline & & 1 \\ \hline & 2 & \\ \hline \end{array}$$

In particular, for any given field $\mathbb{K}$, we have that

$$\mathcal{V}_{\mathbb{K}}(L) = \mathcal{V}_{\mathbb{K}}(L_{\{(1,3)\}}) = \{(0, 0, a) \colon a \in \mathbb{K}\} \cup \{(a, a, 1) \colon a \in \mathbb{K}\}. \qquad \triangleleft$$

The following result deals with partial Latin squares having pair of cells containing the same pair of different symbols.

Lemma 7 *Let $L = (l_{ij}) \in \mathcal{L}_n$ be such that $n > 2$. Let $i, j \in [n]$ be such that $l_{ij}, l_{ji} \in [n]$ are different. If there exists a cell $(i', j') \in C(L)$ such that $(i', j') \neq (i, j)$, $l_{i'j'} = l_{ij}$ and $l_{j'i'} = l_{ji}$, then $\mathcal{V}_{\mathbb{K}}(L) = \mathcal{V}_{\mathbb{K}}(L_{\{(i',j')\}}) = \mathcal{V}_{\mathbb{K}}(L_{\{(j',i')\}})$.*

Proof The result follows readily from the fact that $x_{l_{ij}} - x_{l_{ji}} \in I(L)$, because of the hypothesis. □

Example 7 Let $\mathbb{K}$ be a field. From Lemma 7, we have that

$$\mathcal{V}_{\mathbb{K}}(L_{3,2}) = \mathcal{V}_{\mathbb{K}}((L_{3,2})_{\{(3,1)\}}) = \mathcal{V}_{\mathbb{K}}((L_{3,2})_{\{(3,1),(3,2)\}}). \qquad \triangleleft$$

Let us introduce now a new concept that enables us to determine new cases of partial Latin squares having the same affine algebraic set. To this end, let L and L' be two partial Latin squares of the same order and weight. We say that L' is a *partial transpose* of L if, for each entry $(i, j, k) \in E(L') \setminus E(L)$, the set $E(L)$ contains the entry (j, i, k). Particularly, the transpose of a partial Latin square is also a partial transpose of the latter. Furthermore, being partial transpose is an equivalence relation among partial Latin squares of the same order and weight.

Example 8 The following two partial Latin squares are partial transpose of each other.

$$\begin{array}{|c|c|c|}\hline & 1 & 3 \\ \hline 2 & & 1 \\ \hline & & \\ \hline \end{array} \qquad\qquad \begin{array}{|c|c|c|}\hline & 2 & 3 \\ \hline 1 & & \\ \hline & 1 & \\ \hline \end{array} \qquad \triangleleft$$

Lemma 8 *If two partial Latin squares of the same order and weight are partial transpose of each other, then their affine algebraic sets coincide.*

Proof Let $L = (l_{ij})$ and $L' = (l'_{ij})$ be the partial Latin squares under consideration. The result follows straightforwardly from the fact that the generators of both binomial ideals $I(L)$ and $I(L')$ coincide. Specifically, for each non-empty cell $(i, j) \in C(L')$, it is

$$x_i x_j - x_{l'_{ij}} = \begin{cases} x_j x_i - x_{l_{ji}}, & \text{if } (i, j, l'_{ij}) \notin E(L_1), \\ x_i x_j - x_{l_{ij}}, & \text{otherwise.} \end{cases}$$

□

Two partial Latin squares that are partial transpose of each other can be considered to be "almost" conjugate in the sense that only a subset of cells of the corresponding partial Latin square are switched. More formally, two partial Latin squares L_1 and L_2 in $\mathcal{L}_n$ are partial transpose if there exists a third partial Latin square $L_3 \in \mathcal{L}_n$ such that $E(L_3) \subseteq E(L_1)$, $E(L_3^t) \subseteq E(L_2)$, and $E(L_1) \setminus E(L_3) = E(L_2) \setminus E(L_3^t)$. Thus, in Example 8, the corresponding third partial Latin square would have $\{(1, 2, 1), (2, 1, 2), (2, 3, 1)\}$ as set of entries. In a similar way, we can ask ourselves about the existence of "almost" isotopic partial Latin squares whose affine algebraic sets coincide. In this regard, we say that two partial Latin squares L_1 and L_2 in $\mathcal{L}_n$ are *partial isotopic* if there exists a third partial Latin square $L_3 \in \mathcal{L}_n$ and an isotopism $\Theta = (f, g, h) \in S_n^3$ such that $E(L_3) \subseteq E(L_1)$, $E(L_3^\Theta) \subseteq E(L_2)$ and $E(L_1) \setminus E(L_3) = E(L_2) \setminus E(L_3^\Theta)$. In particular, if L_1 and L_2 are isotopic by means of an isotopism Θ', then they are partial isotopic. To see it, it is enough to consider $L_3 = L_1$ and $\Theta = \Theta'$.

Example 9 The following partial Latin squares are non-isotopic (in fact, they are non-paratopic), but they are, however, partial isotopic by means of the partial Latin square in $\mathcal{L}_3$ with set of entries $\{((1, 1, 1), (2, 2, 2), (3, 1, 2))\}$ and the isotopism $((123), (123), \mathrm{Id}) \in S_3^3$. Here, Id denotes the trivial permutation.

1		3
	2	
2		

	2	3
	1	
		2

◁

The following question arises in a natural way.

Problem 3 Given two partial Latin squares that are partial isotopic, when do they determine the same affine algebraic set?

In order to answer this question, a previous definition is required. For each partial Latin square $L = (l_{ij}) \in \mathcal{L}_n$ and each positive integer $m \leq n$, we define the set

$$S(L; m) := \{k \in [n] \colon x_m - x_k \in I(L)\}. \tag{2}$$

In particular, $m \in S(L; m)$. Besides, from (1), if $k \neq m$, then the binomial $x_m - x_k$ belongs to the ideal $I(L)$ if and only if there exists a subset of non-empty cells $\{(i_1, j_1), \ldots, (i_s, j_s)\} \subseteq C(L)$, such that

a) $\{(j_1, i_1), \ldots, (j_s, i_s)\} \subseteq C(L)$,
b) $l_{i_1 j_1} = m$ and $l_{j_s i_s} = k$, and
c) $l_{j_t i_t} = l_{i_{t+1} j_{t+1}}$, for all positive integer $t < s$.

As a consequence, $l_{i_t j_t} \in S(L; m)$, for all positive integer $t \leq s$.

Example 10 Let us consider the partial Latin square

$$L = (l_{ij}) \equiv \begin{array}{|c|c|c|c|}\hline 3 & 4 & & 1 \\ \hline 4 & 2 & 3 & \\ \hline & 1 & 4 & 2 \\ \hline & & 1 & 3 \\ \hline \end{array} \in \mathcal{L}_4.$$

Then, $S(L; 2) = \{1, 2, 3\}$, because of the existence of the subset $\{(3, 4), (3, 2)\} \subset C(L)$, which is associated to the symbols $l_{3,4} = 2$, $l_{4,3} = l_{3,2} = 1$ and $l_{2,3} = 3$. Similarly, we have that $S(L; 1) = S(L; 3) = \{1, 2, 3\}$ and $S(L; 4) = \{4\}$. $\lhd$

Observe that the sets $S(L; 1) = S(L; 2) = S(L; 3)$ and $S(L; 4)$ constitute a partition of the set of symbols of the partial Latin square in Example 10. The next result establishes that this fact always occurs. It follows straightforwardly from (2) and the subsequent remark.

Proposition 2 *Let us consider a partial Latin square $L \in \mathcal{L}_n$ and a positive integer $m \leq n$. Then,*

a) $S(L; k) = S(L; m)$, *for all* $k \in S(L; m)$.
b) $S(L; k) \cap S(L; m) = \emptyset$, *for all* $k \in [n] \setminus S(L; m)$.
c) *The set* $\{S(L; k) \colon k \leq n\}$ *constitutes a partition of the set* $[n]$, *for all* $L \in \mathcal{L}_n$.

From here on, the partition described in Proposition 2 is denoted as $\mathcal{P}(L)$. Thus, for instance, the partial Latin square L in Example 10 satisfies that $\mathcal{P}(L) = \{\{1, 2, 3\}, \{4\}\}$.

Proposition 3 *Let $L \in \mathcal{L}_n$ be such that $\mathcal{P}(L) = \{[n]\}$. Then, $\mathcal{V}_{\mathbb{K}}(L) = \{(0, \ldots, 0), (1, \ldots, 1)\} \subseteq \mathbb{K}^n$.*

Proof Since $S(L; k) = [n]$, for all $k \in [n]$, it must be $x_1 = \ldots = x_n$ in the coordinate ring $\mathbb{K}[X_n]/I(L)$. Besides, the partial Latin square L has to be non-trivial. Otherwise, $\mathcal{P}(L) = \{\{i\} \colon i \in [n]\}$. Let $(i, j, k) \in E(L)$. Then, the result follows from the fact that both binomials $x_i x_j - x_k$ and $x_1^2 - x_1$ are equivalent in $\mathbb{K}[X_n]/I(L)$. $\square$

The following result enables us to answer Problem 3.

Proposition 4 *Let $L_1, L_2 \in \mathcal{L}_n$ be such that $\mathcal{P}(L_1) = \mathcal{P}(L_2)$. If L_1 and L_2 are partial isotopic by means of an isotopism $\Theta = (f, g, h) \in S_n^3$ so that f, g, and h preserve the mentioned partition, then $\mathcal{V}_{\mathbb{K}}(L_1) = \mathcal{V}_{\mathbb{K}}(L_2)$, whatever the field $\mathbb{K}$ is.*

Proof Let $\mathbb{K}$ be a field. From the hypothesis, there exists a third partial Latin square $L_3 \in \mathcal{L}_n$ such that $E(L_3) \subseteq E(L_1)$, $E(L_3^{\Theta}) \subseteq E(L_2)$ and $E(L_1) \setminus E(L_3) =$

$E(L_2) \setminus E(L_3^{\Theta})$. Hence, the generators of the ideal $I(L_2)$ coincide with those of the ideal $I(L_1)$ except for, at most, those binomials in the set $\{x_i x_j - x_k \colon (i, j, k) \in E(L_1) \setminus E(L_3)\}$. More specifically, every such a generator of the ideal $I(L_1)$ gives rise to a unique generator of the ideal $I(L_2)$ in the set $\{x_{f(i)}x_{g(j)} - x_{h(k)} \colon (i, j, k) \in E(L_1) \setminus E(L_3)\}$. Since the three permutations f, g, and h preserve the partition $\mathcal{P}(L_1) = \mathcal{P}(L_2)$, both sets of binomials coincide. Thus, both ideals $I(L_1)$ and $I(L_2)$ have the same set of generators and hence, $\mathcal{V}_{\mathbb{K}}(L_1) = \mathcal{V}_{\mathbb{K}}(L_2)$. □

Example 11 The non-isotopic partial Latin squares

$$L_1 \equiv \begin{array}{|c|c|c|c|}\hline 3&4& &1\\\hline 4&2&3& \\\hline &1&4&2\\\hline & &1&3\\\hline\end{array} \qquad \text{and} \qquad L_2 \equiv \begin{array}{|c|c|c|c|}\hline &4& &1\\\hline 4&2&3& \\\hline 3&1&4&2\\\hline & &1&3\\\hline\end{array}$$

are partial isotopic by means of the partial Latin square $L_3 \in \mathcal{L}_4$ of weight one such that $E(L_3) = \{(1, 1, 3)\}$ and the isotopism $((13), \mathrm{Id}, \mathrm{Id}) \in S_4^3$. Since all the components of this isotopism preserves the partition $\mathcal{P}(L_1) = \mathcal{P}(L_2) = \{\{1, 2, 3\}, \{4\}\}$, Proposition 4 enables us to ensure that $\mathcal{V}_{\mathbb{K}}(L_1) = \mathcal{V}_{\mathbb{K}}(L_2)$, whatever the field $\mathbb{K}$ is. More specifically, both affine algebraic sets coincide with the set $\{(0, 0, 0, 0), (1, 1, 1, 1)\}$. ◁

4 Algebraic sets of isomorphic partial Latin squares

Let us focus now on answering Problem 2 and hence, on the distribution of the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_n)$ into isomorphism classes. In this regard, Lemma 2 dealt with the distribution of the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_1)$ into two isomorphism classes. For higher orders, the next result enables us to focus on the set of affine algebraic sets associated to a representative Latin square of each isomorphism class of the set $\mathcal{L}_n$.

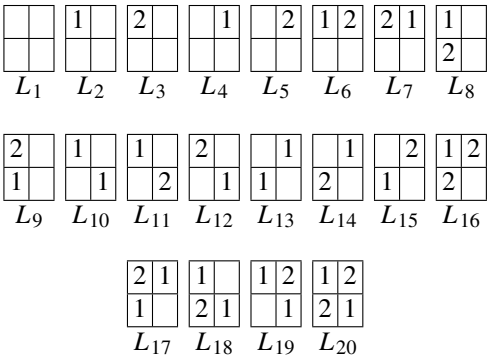
Lemma 9 *If two partial Latin squares $L, L' \in \mathcal{L}_n$ are isomorphic, then the affine algebraic sets $\mathcal{V}_{\mathbb{K}}(L)$ and $\mathcal{V}_{\mathbb{K}}(L')$ are also isomorphic.*

Proof Let f be an isomorphism between the partial Latin squares $L = (l_{ij})$ and $L' = (l'_{ij})$. This gives rise to a bijective map between the generators of the ideals $I(L)$ and $I(L')$. Particularly, each binomial $x_i x_j - x_{l_{ij}} \in I(L)$ maps to the binomial $x_{f(i)}x_{f(j)} - x_{f(l_{ij})} = x_{f(i)}x_{f(j)} - x_{l'_{f(i)f(j)}} \in I(L')$. Hence, a point $(a_1, \ldots, a_n) \in \mathbb{K}^n$ belongs to the affine algebraic set $\mathcal{V}_{\mathbb{K}}(L)$ if and only if $(a_{f(1)}, \ldots, a_{f(n)}) \in \mathcal{V}_{\mathbb{K}}(L')$. □

As an illustrative example, we determine the distribution into isomorphism classes of the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_n)$, for $n \in \{2, 3\}$, whatever the base field $\mathbb{K}$ is.

4.1 The set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_2)$

For $n = 2$, it is known [17] the distribution of $\mathcal{L}_2$ into 20 isomorphism classes, for which the following partial Latin squares are class representatives.



In order to determine the isomorphism classes of the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_2)$, we discard the partial Latin squares L_{13}, L_{16}, L_{17}, and L_{20}, because their related affine algebraic sets coincide, from Lemma 5, with those of L_4, L_6, L_7, and L_{19}, respectively. Further, we discard from Lemma 8 the partial Latin squares L_8, L_9, L_{15}, and L_{19}, which are respective transposes of L_6, L_7, L_{14}, and L_{18}. Finally, from Lemmas 8 and 9, we discard the partial Latin square L_5, which is isomorphic to the transpose of L_4. Table 1 shows the affine algebraic sets of those isomorphism classes that have not been discarded.

Table 1 enables us to ensure that the reciprocal of Lemma 9 is not true in general, because the partial Latin squares L_7, L_{10}, and L_{18} give rise to isomorphic affine algebraic sets. The following result also holds from the table.

Theorem 3 *Let $\mathbb{K}$ be a field. If its characteristic is two, then the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_2)$ is distributed into seven isomorphism classes, which correspond to the affine algebraic sets*

Table 1 Algebraic sets of the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_2)$

$\dim(\mathcal{V}_{\mathbb{K}}(L))$	L	$\mathcal{V}_{\mathbb{K}}(L)$
2	L_1	$\mathbb{K}^2$
1	L_2	$\{x = 0\} \cup \{x = 1\}$
	L_3	$\{y = x^2\}$
	L_4	$\{x = 0\} \cup \{y = 1\}$
	L_6	$\{x = 1\} \cup \{(0, 0)\}$
0	L_7	$\{(0, 0), (1, 1), (-1, 1)\}$
	L_{10}	$\{(0, 0), (1, 1), (1, -1)\}$
	L_{11}	$\{(0, 0), (0, 1), (1, 0), (1, 1)\}$
	L_{12}	$\{x = y^2, y^2 + y + 1 = 0\} \cup \{(0, 0), (1, 1)\}$
	L_{14}	$\{(0, 0), (1, 1)\}$
	L_{18}	$\{(0, 0), (1, 1), (1, -1)\}$

of L_1, L_2, L_3, L_4, L_6, L_{11}, and L_{14}. Otherwise, there exists an eighth isomorphism class associated to L_7.

Proof From Table 1, the affine algebraic sets of the partial Latin squares L_7 and L_{14} coincide if and only if the base field has characteristic two. It is then enough to focus on the affine algebraic set of the partial Latin square L_{12}. Depending on the base field $\mathbb{K}$, this consists of two, three, or four different points. Then, a bivariate polynomial interpolation determines an isomorphism between such an affine algebraic set and that one associated, respectively, to the partial Latin square L_{14}, L_7, or L_{11}. □

4.2 The set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_3)$

The following results are useful to study the distribution of the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_n)$ into isomorphism classes, for $n > 2$.

Lemma 10 *Let $n > 2$. Let $L \in \mathcal{L}_n$ be such that there exist three different positive integers $i, j, k \leq n$ satisfying that (a) $\{(i, j, i), (j, i, k)\} \subseteq E(L)$, (b) $C(L) \cap \{(j, k), (k, j)\} = \emptyset$, and (c) there does not exist $i', j' \in [n]$ such that $\{(j, i', i), (k, j', k)\} \subset E(L)$. Then, $\mathcal{V}_{\mathbb{K}}(L)$ coincides with the affine algebraic set of the partial Latin square that is obtained by replacing the entry $(j, i, k) \in E(L)$ by both entries (j, k, i) and (k, j, k).*

Proof Let $L' \in \mathcal{L}_n$ be the new partial Latin square. By the hypothesis, this is well-defined. Observe also that the set of generators of the binomial ideal $I(L')$ coincides with that of $I(L)$ after replacing the generator $x_j x_i - x_k$ in the latter by both binomials $x_j x_k - x_i$ and $x_k x_j - x_k$. All of them are equivalent, because $x_i - x_k \in I(L) \cap I(L')$. □

Proposition 5 *Let $n > 2$. Let $L \in \mathcal{L}_n$ be such that there exist three different positive integers $i, j, k \leq n$ such that $\{(i, j, i), (j, k, i)\} \subseteq E(L)$. Then, $\mathcal{V}_{\mathbb{K}}(L)$ is isomorphic to an affine algebraic set contained in $\mathcal{V}_{\mathbb{K}}(L')$, where $L' \in \mathcal{L}_n$ is such that $E(L') = \{(1, 2, 1), (2, 3, 1)\}$.*

Proof Let f be any permutation on the set $[n]$ that maps, respectively, the elements i, j, and k into 1, 2, and 3. This leads to an isomorphism between L and a partial Latin square $L'' \in \mathcal{L}_n$ such that $E(L'') \subseteq E(L')$. The result follows then from Lemma 4. □

Example 12 Let us consider the following three partial Latin squares.

$$L_1 \equiv \begin{array}{|c|c|c|}\hline & 3 & \\ \hline 2 & & \\ \hline & & \\ \hline \end{array} \qquad L_2 \equiv \begin{array}{|c|c|c|}\hline & & 2 \\ \hline 2 & & \\ \hline 3 & & \\ \hline \end{array} \qquad L_3 \equiv \begin{array}{|c|c|c|}\hline & 1 & \\ \hline & & 1 \\ \hline & 3 & \\ \hline \end{array}$$

From Lemma 10, the affine algebraic sets of L_1 and L_2 coincide, whatever the base field is. Further, from the proof of Proposition 5, both affine algebraic sets are isomorphic to the affine algebraic set of L_3. In the context of both results, we consider here $(i, j, k) = (2, 1, 3)$. In particular, for any given field $\mathbb{K}$, we have that

$$\mathcal{V}_{\mathbb{K}}(L_1) = \mathcal{V}_{\mathbb{K}}(L_2) = \{(a, 0, 0) \colon a \in \mathbb{K}\} \cup \{(1, a, a) \colon a \in \mathbb{K}\}$$

and

$$\mathcal{V}_{\mathbb{K}}(L_3) = \mathcal{V}_{\mathbb{K}}(L_2) = \{(0, a, 0) \colon a \in \mathbb{K}\} \cup \{(a, 1, a) \colon a \in \mathbb{K}\}. \qquad \triangleleft$$

The next result holds from a simple study of cases based on Proposition 5.

Proposition 6 *Let $L \in \mathcal{L}_3$ be such that there exist three different positive integers $i, j, k \leq n$ such that $\{(i, j, i), (j, k, i)\} \subseteq E(L)$. Then, $\mathcal{V}_{\mathbb{K}}(L)$ is isomorphic to one of the following affine algebraic sets in $\mathbb{K}[x, y, z]$, whatever the base field $\mathbb{K}$ is.*

a) *If* $\dim(\mathcal{V}_{\mathbb{K}}(L)) = 1$*:*

- *Two non-concurrent straight lines and a common concurrent line to both of them:* $\{x = y = 0\} \cup \{x = z = 0\} \cup \{x = z, y = 1\}$.
- *Two concurrent straight lines:* $\{x = z = 0\} \cup \{x = z, y = 1\}$.
- *Two non-concurrent straight lines:* $\{x = y = 0\} \cup \{x = z, y = 1\}$.
- *Two concurrent straight lines and an external point:* $\{x = y = 0\} \cup \{x = z = 0\} \cup \{(1, 1, 1)\}$.
- *A straight line and two external points:* $\{x = z = 0\} \cup \{(0, 0, 1), (1, 1, 1)\}$.
- *A straight line and an external point:* $\{x = y = 0\} \cup \{(1, 1, 1)\}$.

b) *If* $\dim(\mathcal{V}_{\mathbb{K}}(L)) = 0$*:*

- *Two points:* $\{(0, 0, 0), (1, 1, 1)\}$.
- *Three points:* $\{(0, 0, 0), (0, 1, 0), (1, 1, 1)\}$.
- *Four points:* $\{(0, 0, 0), (0, 1, 0), (0, 0, 1), (1, 1, 1)\}$.

It is known [17] the distribution of the set $\mathcal{L}_3$ into 2029 isomorphism classes. The results exposed throughout the paper enable us to discard the most of them and focus on only 124 classes. The distribution of their respective affine algebraic sets into 30 isomorphism classes is exposed in Table 2, where we also indicate a partial Latin square from which each one of these classes derives. Each one of them is written row after row in a single line, with empty cells represented by zeros. They are labeled from M_1 to M_{30}.

The following result holds straightforwardly from Table 2.

Theorem 4 *Let $\mathbb{K}$ be a field. If its characteristic is two, then the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_3)$ is distributed into 32 isomorphism classes, which correspond to those affine algebraic sets of the partial Latin squares M_1–M_{28} and M_{33}–M_{36}. Otherwise, it is distributed into the 38 isomorphism classes exposed in* Table 2.

Table 2 Distribution of the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_3)$ into isomorphism classes

dim	L	$\mathcal{V}_{\mathbb{K}}(L)$
3	$M_1 \equiv 000\,000\,000$	$\mathbb{K}^3$
2	$M_2 \equiv 100\,000\,000$	$\{x = 0\} \cup \{x = 1\}$
	$M_3 \equiv 010\,000\,000$	$\{x = 0\} \cup \{y = 1\}$
	$M_4 \equiv 120\,000\,000$	$\{x = 1\} \cup \{x = y = 0\}$
	$M_5 \equiv 023\,000\,000$	$\{x = 1\} \cup \{y = z = 0\}$
	$M_6 \equiv 123\,000\,000$	$\{x = 1\} \cup \{(0, 0, 0)\}$
	$M_7 \equiv 200\,000\,000$	$\{y = x^2\}$
	$M_8 \equiv 030\,000\,000$	$\{z = xy\}$
1	$M_9 \equiv 120\,030\,000$	$\{x = 1, z = y^2\} \cup \{(0, 0, 0)\}$
	$M_{10} \equiv 100\,020\,000$	$\{x = y = 0\} \cup \{x = y = 1\} \cup \{x = 0, y = 1\} \cup \{x = 1, y = 0\}$
	$M_{11} \equiv 010\,200\,000$	$\{x = y = 0\} \cup \{x = y = 1\}$
	$M_{12} \equiv 010\,300\,000$	$\{x = z = 0\} \cup \{x = z, y = 1\}$
	$M_{13} \equiv 013\,000\,000$	$\{x = z = 0\} \cup \{x = 1, y = z\}$
	$M_{14} \equiv 010\,001\,000$	$\{x = y = 0\} \cup \{x = z = 0\} \cup \{x = z, y = 1\}$
	$M_{15} \equiv 100\,001\,000$	$\{x = y = 0\} \cup \{x = z = 0\} \cup \{x = 1, yz = 1\}$
	$M_{16} \equiv 013\,000\,000$	$\{x = z = 0\} \cup \{x = y = 1\} \cup \{y = 1, z = 0\}$
	$M_{17} \equiv 100\,002\,000$	$\{x = y = 0\} \cup \{x = z = 1\} \cup \{x = 1, y = 0\} \cup \{x = 0, z = 1\}$
	$M_{18} \equiv 010\,001\,020$	$\{x = y = 0\} \cup \{(1, 1, 1)\}$
	$M_{19} \equiv 130\,003\,000$	$\{x = z = 0\} \cup \{(1, 0, 0), (1, 1, 1)\}$
	$M_{20} \equiv 120\,003\,000$	$\{x = y = 1\} \cup \{x = 1, z = 0\} \cup \{(0, 0, 0)\}$
	$M_{21} \equiv 012\,000\,000$	$\{xz = 1, y = 1\} \cup \{x = y = 0\}$
	$M_{22} \equiv 012\,003\,000$	$\{xz = 1, y = 1\} \cup \{(0, 0, 0)\}$
	$M_{23} \equiv 200\,002\,000$	$\{y = x^2, z = 1\} \cup \{x = y = 0\}$
	$M_{24} \equiv 123\,030\,000$	$\{x = 1, z = y^2\} \cup \{(0, 0, 0)\}$
	$M_{25} \equiv 200\,001\,000$	$\{xz = 1, yz^2 = 1\} \cup \{x = y = 0\}$
	$M_{26} \equiv 100\,030\,000$	$\{x = 0, z = y^2\} \cup \{x = 1, z = y^2\}$
	$M_{27} \equiv 230\,000\,000$	$\{y = x^2, z = x^3\}$
	$M_{28} \equiv 200\,030\,000$	$\{y = x^2, z = x^4\}$
	$M_{29} \equiv 210\,000\,000$	$\{x = y = 0\} \cup \{x = y = 1\} \cup \{x = -1, y = 1\}$
	$M_{30} \equiv 210\,003\,000$	$\{x = y = 1\} \cup \{x = y = -1\} \cup \{(0, 0, 0)\}$
	$M_{31} \equiv 200\,003\,000$	$\{y = x^2, z = 0\} \cup \{x = y = 1\} \cup \{x = y = -1\}$
	$M_{32} \equiv 300\,030\,000$	$\{y = -x, z = x^2\} \cup \{y = x, z = x^2\}$
0	$M_{33} \equiv 012\,200\,300$	$\{(0, 0, 0), (1, 1, 1)\}$
	$M_{34} \equiv 130\,002\,000$	$\{(0, 0, 0), (1, 1, 1), (1, 0, 0)\}$
	$M_{35} \equiv 100\,002\,030$	$\{(0, 0, 0), (1, 1, 1), (1, 0, 0), (0, 1, 1)\}$
	$M_{36} \equiv 100\,020\,003$	$\{(0, 0, 0), (1, 1, 1),$ $(1, 0, 0), (0, 1, 1), (0, 1, 0), (0, 0, 1), (1, 0, 1), (1, 1, 0)\}$
	$M_{37} \equiv 032\,001\,000$	$\{(0, 0, 0), (1, 1, 1), (1, -1, -1), (-1, 1, -1), (-1, -1, 1)\}$
	$M_{38} \equiv 100\,023\,002$	$\{(0, 0, 0), (1, 1, 1), (1, 0, 0), (0, 1, 1), (0, 1, -1), (1, 1, -1)\}$

5 Effectiveness of the method

Let $F = \{\mathfrak{f}_{ij} : i, j \in [n]\}$ and $\mathbb{K}[F]$ respectively denote the set of n^2 variables $\{\mathfrak{f}_{ij} : i, j \in [n]\}$ and the related multivariate polynomial ring over a field $\mathbb{K}$.

Lemma 11 *Two partial Latin squares $L, L' \in \mathcal{L}_n$ are isomorphic if and only if the affine algebraic set of the following ideal in $\mathbb{K}[F]$ is non-empty*

$$\begin{aligned} I(L, L') := & \langle f_{ij}^2 - \mathfrak{f}_{ij} : i, j \in [n] \rangle \\ & + \langle 1 - \sum\nolimits_{i \in [n]} \mathfrak{f}_{ij} : j \in [n] \rangle + \langle 1 - \sum\nolimits_{j \in [n]} \mathfrak{f}_{ij} : i \in [n] \rangle \\ & + \langle f_{ii'} f_{jj'} (f_{kk'} - 1) : (i, j, k) \in E(L), (i', j', k') \in E(L') \rangle. \end{aligned}$$

Proof Let $P = (p_{11}, \ldots, p_{nn})$ be a zero of the ideal $I(L, L')$. The first subideal of $I(L, L')$ involves P to belong to the set $\{0, 1\}^{n^2}$. The second and third ones imply that the map $f : [n] \to [n]$ that is defined so that $f(i) = j$ if $p_{ij} = 1$ is a well-defined permutation of the symmetric group S_n. Finally, the fourth one involves f to be an isomorphism between the partial Latin squares L and L'. To see it, let $(f(i), f(j), k') \in E(L')$ be such that $(i, j, k) \in E(L)$, for some $k \in [n]$. Since $p_{if(i)} = p_{jf(j)} = 1$, the fourth subideal of $I(L, L')$ implies that $p_{kk'} = 1$ and hence, $k' = f(k)$. □

Lemma 11 enables one to make use of computational algebraic geometry in order to distribute a given set of partial Latin squares into isomorphism classes. In particular, the affine algebraic set $\mathcal{V}(I(L, L'))$ can be computed by means of the reduced Gröbner basis of the ideal $I(L, L')$ [23, 29, 40]. The following result shows how the cost of computation that is required to this end is, however, extremely sensitive to the number of variables and the length and degree of the generators of $I(L, L')$.

Proposition 7 *The complexity to compute the reduced Gröbner basis of the ideal $I(L, L')$ in Lemma 11 is*

a) $3^{O(n^2)}$, *if $\mathbb{K} = \mathbb{Q}$, the field of rational numbers.*
b) $q^{O(n^2)} + O(n^5)$, *if $\mathbb{K} = \mathbb{F}_q$, the finite field of order a prime power q.*

Proof The result holds from Theorems 1 and 2 once we prove that the ideal $I(L, L')$ in Lemma 11 is zero-dimensional and radical. The first condition derives from the fact of being $\mathcal{V}(I(L, L')) \subset \{0, 1\}^{n^2}$, whereas the second one follows from Seidenberg's Lemma (see Proposition 3.7.15 in [25]), once we observe that, for any three positive integers $i, j, k \leq n$, the unique monic generator of $I(L, L') \cap \mathbb{K}[F]$ is the square-free polynomial $\mathfrak{f}_{ij}^2 - \mathfrak{f}_{ij}$. □

Algebraic sets of partial Latin squares constitute an efficient alternative to lower this computational cost. Particularly, Lemma 9 implies that, under the assumptions of Lemma 11, none computation is required to ensure that $\mathcal{V}(I(L, L')) = \emptyset$ whenever the affine algebraic sets $\mathcal{V}_{\mathbb{K}}(L)$ and $\mathcal{V}_{\mathbb{K}}(L')$ are not isomorphic. Isomorphism

invariants of affine algebraic sets can, therefore, be considered as new isomorphism invariants of partial Latin squares.

Further, the computational cost that is required to determine the affine algebraic set $\mathcal{V}(I(L, L'))$ is much lower than that one exposed in Proposition 7. More specifically, a similar proof to that one exposed in the mentioned result enables us to ensure that the complexity to compute the reduced Gröbner basis of the ideal defined in (1) is $2^{O(n)}$ over the field $\mathbb{Q}$ and $q^{O(n)} + O(n^4)$ over the finite field $\mathbb{F}_q$, with q a prime power.

We have implemented all the previous results in the open computer algebra system for polynomial computations SINGULAR [7] and we have checked the efficiency of using affine algebraic sets of partial Latin squares to lower the cost of computation exposed in Proposition 7. Figure 3 shows the average run time that both methods (with and without using affine algebraic sets) require, in a system with an *Intel Core i7-2600, with a 3.4-GHz processor and 16 GB of RAM*, to distribute into isomorphism classes a set of 1000 partial Latin squares of order $n \leq 3$ and weight $m \leq n^2$ that are randomly generated in the next way:

1. We begin with a trivial partial Latin square of order n and attempt x times to add an entry (i, j, k) chosen randomly uniform from $[n] \times [n] \times [n]$.
2. If the random entry does not give rise to a partial Latin square (that is, if the pair (i, j) is already in the domain, or adding the entry introduces a repeated symbol in a row or a column of the array), we do nothing.

This way for generating random partial Latin squares has already been used in [42, 43].

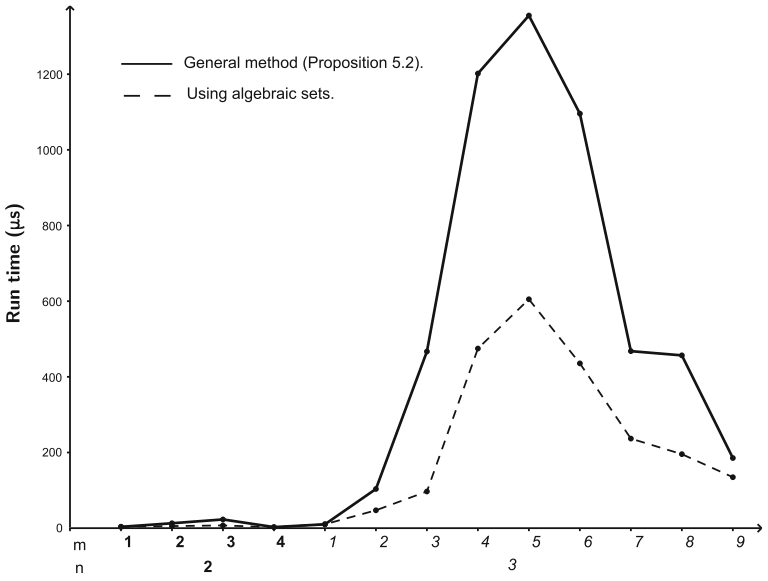


Fig. 3 Computational cost required to distribute the set $\mathcal{L}_n$ into isomorphism classes

6 Conclusion and further studies

In this paper, we have introduced the affine algebraic set of a finite partial Latin square and several results have been exposed to study when two such affine algebraic sets are equal or isomorphic. We have also introduced two new concepts that enable us to deal with new ways of classifying partial Latin squares according to whether they are partial transpose or partial isotopic. Further work is required to delve into both classifications. Particularly, we have determined the isomorphism classes of the set of affine algebraic sets of partial Latin squares of order $n \leq 3$. The following question is also established as further work.

Problem 4 Let V be an affine algebraic set in the set $\mathcal{V}_{\mathbb{K}}(\mathcal{L}_n)$. Which is the smallest weight of a partial Latin square $L \in \mathcal{L}_n$ such that $\mathcal{V}_{\mathbb{K}}(L) = V$?

Finally, remark the fact that Lemmas 1 and 9 enable us to ensure that the common use of image patterns and affine algebraic sets of Latin squares constitutes a good alternative to determine isomorphism classes of Latin squares, with a particular interest to be implemented into the encryption process described into the introductory section. Thus, for instance, the common use of Fig. 1 together with the fact that $\mathcal{V}_{\mathbb{K}}(L_{3,1}) \neq \mathcal{V}_{\mathbb{K}}(L_{3,2})$ (as we showed at the beginning of Section 3) implies in an easy way that the five Latin squares $L_{3,1}$ to $L_{3,5}$ really correspond to different isomorphism classes. Of course, further work dealing with Latin squares of higher orders is required to delve into this implementation.

Appendix: Glossary of symbols

$C(L)$	The set of non-empty cells of a partial Latin square L.
$E(L)$	The set of entries of a partial Latin square L.
$I(L)$	The binomial ideal related to a partial Latin square L.
$\mathcal{L}_n$	The set of partial Latin squares of order n.
L_S	The partial Latin square that results after eliminating a subset $S \subseteq C(L)$.
$\mathcal{P}(L)$	The partition of $[n]$ described in Proposition 2.
$\mathcal{V}(I)$	The affine algebraic set of an ideal of polynomials I.
$\mathcal{V}_{\mathbb{K}}(L)$	The affine algebraic set of a partial Latin square L over a field $\mathbb{K}$.
$\mathcal{V}_{\mathbb{K}}(\mathcal{L}_n)$	The set of affine algebraic sets over a field $\mathbb{K}$ of partial Latin squares of order n.

References

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

2. Bayer, D.: The Division Algorithm and the Hilbert Scheme. PhD Thesis, Harvard University (1982)
3. Buchberger, B.: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. J. Symbolic Comput. **41**, 475–511 (2006)
4. Chum, C.S., Zhang, X.: The Latin squares and the secret sharing schemes. Groups Complex Cryptol. **2**, 175–202 (2010)
5. Cooper, J., Donovan, D., Seberry, J.: Secret sharing schemes arising from Latin squares. Bull. Inst. Combin. Appl. **12**, 33–43 (1994)
6. Danan, E., Falcon, R.M., Kotlar, D., Marbach, T.G., Stones, R.J.: Refining invariants for computing autotopism groups of partial Latin rectangles. Submitted (2018)
7. Decker, W., Greuel, G.M., Pfister, G., Schönemann, H.: Singular 4-1-1. A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2018). Accessed 30 September 2018
8. Dénes, J., Keedwell, A.D.: Latin Squares and Their Applications. Academic Press, New York-London (1974)
9. Dimitrova, V., Markovski, J.: On Quasigroup Pseudo Random Sequence Generator. In: Manolopoulos, Y., Spirakis, P. (eds.) Proceedings of the First Balkan Conference in Informatics, pp. 393–401, Thessaloniki (2004)
10. Dimitrova, V., Markovski, S.: Classification of quasigroups by image patterns. In: Proceedings of the Fifth International Conference for Informatics and Information Technology, pp. 152–160. Bitola, Macedonia (2007)
11. Dimitrova, V., Markovski, S., Mileva, A.: Periodic Quasigroup String Transformations. Quasigroups Related Systems 17, 191–204 (2009) On Quasigroup Pseudo Random Sequence Generator. In: Manolopoulos, Y., Spirakis, P. (eds.) Proceedings of the First Balkan Conference in Informatics, pp. 393–401, Thessaloniki (2004)
12. Falcón, R.M.: Latin squares associated to principal autotopisms of long cycles. Application in Cryptography. In: Dumas, J. (ed.) Proceedings of Transgressive Computing 2006, a conference in honor of Jean Della Dora, pp. 213–230. Universidad de Granada, Granada (2006)
13. Falcón, R.M.: The set of autotopisms of partial Latin squares. Discret. Math. **313**, 1150–1161 (2013)
14. Falcón, R.M.: Enumeration and classification of self-orthogonal partial Latin rectangles by using the polynomial method. Eur. J. Combin. **48**, 215–223 (2015)
15. Falcón, R.M., Falcón, O.J., Núñez, J.: Counting and enumerating partial Latin rectangles by means of computer algebra systems and CSP solvers. Math. Methods Appl. Sci. https://doi.org/10.1002/mma.4820 (2018). Accessed 30 September 2018
16. Falcón, R.M., Martín-Morales, J.: Gröbner bases and the number of Latin squares related to autotopisms of order 7. J. Symbolic Comput. **42**, 1142–1154 (2007)
17. Falcón, R.M., Stones, R.J.: Classifying partial Latin rectangles. Electron. Notes Discret. Math. **49**, 765–771 (2015)
18. Falcón, R.M., Stones, R.J.: Partial Latin rectangle graphs and autoparatopism groups of partial Latin rectangles with trivial autotopism groups. Discret. Math. **340**, 1242–1260 (2017)
19. Falcón, R.M., Stones, R.J.: Enumerating partial Latin rectangles. Submitted (2018)
20. Gao, S.: Counting Zeros over Finite Fields Using Gröbner Bases. Carnegie Mellon University (2009)
21. Hashemi, A.: Nullstellensätze for zero-dimensional Gröbner bases. Comput. Complex. **18**, 155–168 (2009)
22. Hashemi, A., Lazard, D.: Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving. Internat. J. Algebra Comput. **21**, 703–713 (2011)
23. Hillebrand, D.: Triangulierung Nulldimensionaler Ideale - Implementierung Und Vergleich Zweier Algorithmen. Universitaet Dortmund, Fachbereich Mathematik (1999)
24. Hulpke, A., Kaski, P., ÖStergård, P.R.J.: The number of Latin squares of order 11. Math. Comp. **80**, 1197–1219 (2011)
25. Kreuzer, M., Robbiano, L.: Computational commutative algebra 1. Springer, Berlin (2000)
26. Koscielny, C.: A method of constructing quasigroup-based stream-ciphers. Int. J. Appl. Math. Comput. Sci. **6**, 109–121 (1996)
27. Koscielny, C., Mullen, G.L.: A quasigroup-based public-key cryptosystem. Int. J. Appl. Math. Comput. Sci. **9**, 955–963 (1999)
28. Lakshman, Y.N.: On the complexity of computing a Gröbner basis for the radical of a zero dimensional ideal. In: Ortiz, H. (ed.) Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing, STOC'90, pp. 555–563. ACM, New York (1990)

29. Lazard, D.: Solving zero-dimensional algebraic systems. J. Symbolic Comput. **13**, 117–131 (1992)
30. Johnson, K.W.: Latin Square Determinants. In: Algebraic, Extremal and Metric Combinatorics 1986, pp. 146–154. London Math. Soc. Lecture Note Ser. 131 (1988)
31. Kolesova, G., Lam, C.W.H., Thiel, L.: On the number of 88 Latin squares. J. Combin. Theory Ser. A **54**, 143–148 (1990)
32. Markovski, S., Dimitrova, V., Samardjiska, S.: Identity sieves for quasigroups. Quasigroups Relat. Syst. **18**, 149–163 (2010)
33. Markovski, S., Gligoroski, D., Andova, S.: Using quasigroups for one-one secure encoding. In: Proceedings of Eight Conference Logic and Computer Science (LIRA), pp. 157–162. Novi Sad (1997)
34. Markovski, S., Gligoroski, D., Bakeva, V.: Quasigroup string processing: Part 1. In: Proceedings of Macedonian Academy of Sciences and Arts for Mathematical and Technical Sciences XX, 1-2, pp. 13–28 (1999)
35. Markovski, S., Gligoroski Markovski, J.: Classification of quasigroups by random walk on torus. J. Appl. Math. Comput. **19**, 57–75 (2005)
36. Markovski, S., Kusakatov, V.: Quasigroup string processing: Part 2. In: Proceedings of Macedonian Academy of Sciences and Arts for Mathematical and Technical Sciences XXI, 1-2, pp. 15–32 (2000)
37. McKay, B.D., Meynert, A., Myrvold, W.: Small Latin squares, quasigroups, and loops. J. Combin. Des. **15**, 98–119 (2007)
38. Moldovyan, N.A., Shcherbacov, A.V., Shcherbacov, V.: On Some Applications of Quasigroups in Cryptography. In: Workshop on Foundations of Informatics, pp. 331–340. Acad. Sci. Moldova, Inst. Math. Comput. Sci., Chişinău (2015)
39. Moldovyan, N.A., Shcherbacov, A.V., Shcherbacov, V.A.: Some applications of quasigroups in cryptology. Comput. Sci. J. Moldova **24**, 55–67 (2016)
40. Möller, H.M.: On decomposing systems of polynomial equations with finitely many solutions. Appl. Algebra Engrg. Comm. Comput. **4**, 217–230 (1993)
41. Shcherbacov, V.: Elements of quasigroup theory and applications. Monographs and Research Notes in Mathematics. CRC Press, Boca Raton (2017)
42. Stones, D.S.: Symmetries of partial Latin squares. Eur. J. Combin. **34**, 1092–1107 (2013)
43. Stones, R.J., Falcón, R.M., Kotlar, D., Marbach, T.G.: Computing autotopism groups of partial Latin rectangles: a pilot study. Submitted (2018)
44. Stones, R.J., Su, M., Liu, X., Wang, G., Lin, S.: A Latin square autotopism secret sharing scheme. Des. Codes Cryptogr. **80**, 635–650 (2015)