mathematics

MDPI

Article

Recognition and Analysis of Image Patterns Based on Latin Squares by Means of Computational Algebraic Geometry

Raúl M. Falcón

Department of Applied Mathematics I, University of Seville, 41012 Sevilla, Spain; rafalgan@us.es

Abstract: With the particular interest of being implemented in cryptography, the recognition and analysis of image patterns based on Latin squares has recently arisen as an efficient new approach for classifying partial Latin squares into isomorphism classes. This paper shows how the use of a Computer Algebra System (CAS) becomes necessary to delve into this aspect. Thus, the recognition and analysis of image patterns based on these combinatorial structures benefits from the use of computational algebraic geometry to determine whether two given partial Latin squares describe the same affine algebraic set. This paper delves into this topic by focusing on the use of a CAS to characterize when two partial Latin squares are either partial transpose or partial isotopic.

Keywords: image pattern recognition; partial Latin square; affine algebraic set; isomorphism; partial transpose; partial isotopic

MSC: 05B15; 20N05; 68T10

Citation: Falcón, R.M. Recognition and Analysis of Image Patterns Based on Latin Squares by Means of Computational Algebraic Geometry. *Mathematics* **2021**, *9*, 666. https://doi.org/10.3390/math9060666

Academic Editor: Eugenio Roanes-Lozano

Received: 24 February 2021
Accepted: 18 March 2021
Published: 21 March 2021

1. Introduction

An $n \times n$ array is said to be a *partial Latin square of order n* if each one of its cells either is empty or contains an element of a finite set of n symbols so that each symbol occurs at most once in each row and at most once in each column. If there are no empty cells, then the array is called a *Latin square*. Latin squares play a relevant role in cryptography [1–3]. Of particular interest for the aim of this paper, the generation of scramblers in symmetric cryptography by means of encryption–decryption processes having Latin squares as cryptographic keys is remarkable [4–8]. The exponential growth of Latin squares [9–11] ensures the robustness of these symmetric-key algorithms against brute force and statistical attacks. In addition, appropriate choices of Latin squares produce effective symmetric-key algorithms with high period growths [12]. In this regard, the distribution of Latin squares into isomorphism classes play a fundamental role. It is so that pseudo-random sequences derived from non-isomorphic Latin squares give rise to certain image patterns [13,14], whose algebraic and geometrical properties enable one to distinguish between fractal and non-fractal Latin squares [15,16].

Distributing (partial) Latin squares into isomorphism classes indeed constitutes a main problem in the theory of (partial) Latin squares. Currently, only the number of isomorphism classes of Latin squares of order $n \leq 11$ is known [9–11], as well as that of partial Latin squares of order $n \leq 6$ [17,18]. To obtain these last values, the computation of reduced Gröbner bases of ideals associated to partial Latin squares has played a relevant role. Such a computation is, however, extremely sensitive to the number of involved variables and the length and degree of the corresponding generators [19–22]. Thus, although distinct techniques concerning computational algebraic geometry have been implemented since the original work of Bayer [23] for solving the classical problems of counting, enumerating and classifying partial Latin squares [17,18,24–29] and solving related problems such as completing sudokus [30–32], their computational cost makes it very difficult to deal with partial Latin squares of high orders.

The study of new invariants concerning partial Latin square isomorphisms has turned out to be an optimal approach to reduce this computational cost [33–35]. This paper delves in particular into those invariants that are related to affine algebraic sets associated to the partial Latin squares under consideration. In this regard, let us recall that the affine algebraic set in a multivariate polynomial ring $\mathbb{K}[\{x_1, \ldots, x_n\}]$ of a partial Latin square $L = (l_{i,j})$ of order n, with set of symbols $[n] := \{1, \ldots, n\}$, was defined by Falcón, R.M. et al [36] as the set of zeros of the binomial ideal

$$I(L) := \left\langle x_i x_j - x_{l_{i,j}} \colon 1 \leq i, j, l_{i,j} \leq n \right\rangle. \tag{1}$$

Isomorphic partial Latin squares give rise to isomorphic affine algebraic sets. Thus, Gröbner bases have played a relevant role for distinguishing, in a computationally fast way, image patterns arisen from non-isomorphic Latin squares. In any case, the study of affine algebraic sets associated to Latin squares is still in the very initial stage. Thus, for instance, their distribution into isomorphism classes is only known for $n \leq 3$ [36]. To deal with higher orders, it is necessary to delve into two new ways of classifying partial Latin squares. More specifically, it is necessary to characterize when two partial Latin squares are partial transpose and/or partial isotopic. In both cases, the partial Latin squares under consideration may give rise to the same affine algebraic set.

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. In Section 3, the notion of standard set of image patterns associated to a Latin square is introduced, which may constitute a fast computational way for distinguishing non-isomorphic Latin squares. To this end, the use of a new affine algebraic set associated to each of these image patterns is proposed. Finally, two new ideals are described in Section 4, whose respective affine algebraic sets are uniquely identified with the set of partial Latin squares that are partial transpose of another given partial Latin square, and the set of partial isotopisms between two given partial Latin squares of the same order and weight.

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 of [37,38] for more details on both topics.

2.1. Partial Latin Squares

Let $\mathcal{L}_n$ be the set of partial Latin squares of order n having the already mentioned set $[n]$ as set of symbols. Every partial Latin square $L = (l_{i,j}) \in \mathcal{L}_n$ is determined by its *set of entries*

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

Therefore, the cardinality of this set coincides with the number of non-empty cells within the partial Latin square L. It is termed the *weight* of L. From here on, let $\mathcal{L}_{n;m}$ denote the subset of partial Latin squares in the set $\mathcal{L}_n$ of weight m.

Let S_n denote the symmetric group on the set $[n]$. Every triple $\theta = (f, g, h) \in S_n^3$ preserves the set $\mathcal{L}_{n;m}$. It constitutes an *isotopism* of partial Latin squares, where the bijections f, g and h correspond, respectively, to a permutation of rows, a permutation of columns and a permutation of symbols of the partial Latin square under consideration. More specifically, the isotopism θ acts on any given partial Latin square $L \in \mathcal{L}_{n;m}$ by giving rise to its *isotopic* partial Latin square $L^\theta \in \mathcal{L}_{n;m}$, where

$$\mathrm{Ent}(L^\theta) = \{(f(i), g(j), h(k)) \colon (i, j, k) \in \mathrm{Ent}(L)\}.$$

If $f = g = h$, then the isotopism θ constitutes an *isomorphism*. In such a case, the partial Latin squares L and L^θ are said to be *isomorphic*. Throughout this paper, the computation

of isotopisms and isomorphisms among partial Latin squares is done by making respective use of the procedures *isot* and *isom* of the library *pls.lib*, available online

at http://personales.us.es/raufalgan/LS/pls.lib (accessed on 28 February 2021), for the open Computer Algebra System (CAS) for polynomial computations SINGULAR [39].

Isotopic and isomorphic are equivalence relations among partial Latin squares. The distribution into such classes is known for order $n \leq 11$ in the case of dealing with Latin squares [9–11] and for order $n \leq 6$ in the case of dealing with partial Latin squares [17,18]. Partial transpose are partial isotopic are two other binary relations among partial Latin squares of the same order and weight, whose study is still in teh very initial stage. Although the original definitions were established by Falcón, R.M. et al [36] as equivalence relations, it is not so. In what follows, we particularize both definitions in order to obtain two new equivalence relations among partial Latin squares of the same order and weight. To this end, let us consider two partial Latin squares L_1 and L_2 in $\mathcal{L}_{n;m}$.

We say that L_2 is *partial transpose* of L_1 if and only if the following two conditions hold.

1. For each entry $(i,j,k) \in \mathrm{Ent}(L_2) \setminus \mathrm{Ent}(L_1)$, we have that $(j,i,k) \in \mathrm{Ent}(L_1)$.
2. For each entry $(i,j,k) \in \mathrm{Ent}(L_1) \setminus \mathrm{Ent}(L_2)$, we have that $(j,i,k) \in \mathrm{Ent}(L_2)$.

Being partial transpose generalizes, therefore, the classical concept of being transpose. Notice that the second condition that we have just described was not explicitly indicated by Falcón, R.M. et al [36]. Nevertheless, as is illustrated in the following example, this condition is mandatory in order to obtain a symmetric relation.

Example 1. *The partial Latin squares*

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

both of them in $\mathcal{L}_{4;8}$, satisfy the first described condition in order to ensure that L_2 is partial transpose of L_1. Nevertheless, such a condition is not satisfied for ensuring that L_1 is partial transpose of L_2, because the entry $(2,4,3) \in \mathrm{Ent}(L_1) \setminus \mathrm{Ent}(L_2)$ and $(4,2,3) \notin \mathrm{Ent}(L_2)$.

Now, let $P \subseteq \mathrm{Ent}(L_1) \cap \mathrm{Ent}(L_2)$. We say that L_2 is *P-partial isotopic* to L_1 if there exists an isotopism $(f,g,h) \in S_n^3$ such that

$$\mathrm{Ent}(L_2) \setminus P = \{(f(i),g(j),h(k)) \colon (i,j,k) \in \mathrm{Ent}(L_1) \setminus P\}.$$

In such a case, we say that the triple (f,g,h) is a *P-partial isotopism* (a *partial isotopism*, when there is no place for confusion) from L_1 to L_2. The just described binary relation of being P-partial isotopic constitutes an equivalence relation among partial Latin squares of the same order and weight, as well as containing the subset P in their respective sets of entries. Further, if two partial Latin squares are isotopic, then they are $\emptyset$-partial isotopic. More specifically, every isotopism from L_1 to L_2 is also a partial isotopism between such partial Latin squares.

The subset $P \subseteq \mathrm{Ent}(L_1) \cap \mathrm{Ent}(L_2)$ was not established as an essential part of the original definition of being partial isotopic introduced by Falcón, R.M. et al. [36]. Nevertheless, if it is not considered as such, then the resulting binary relation is intransitive. The following example illustrates this fact. In this example, and from now on, to make much clearer the understanding of the subset P associated to any given partial isotopism in S_n^3, we denote $L(P)$ the partial Latin square of order n satisfying that $\mathrm{Ent}(L(P)) = P$.

Example 2. *The Latin squares*

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

are isotopic (and, hence, $\emptyset$-partial isotopic) by means of the isotopism $((34), \mathrm{Id}, \mathrm{Id}) \in S_4^3$, that is, by switching their third and fourth rows. It is readily verified that the Latin square L_2 is P-partial isotopic to

$$L_3 \equiv \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&4&1&3\\\hline 3&1&4&2\\\hline 4&3&2&1\\\hline\end{array}$$

where $P = \mathrm{Ent}(L_2) \cap \mathrm{Ent}(L_3)$. That is,

$$L(P) \equiv \begin{array}{|c|c|c|c|}\hline 1&2&3&4\\\hline 2&&&3\\\hline 3&&&2\\\hline 4&3&2&1\\\hline\end{array}$$

To this end, it is enough to consider, for instance, the partial isotopism $((23), \mathrm{Id}, \mathrm{Id}) \in S_4^3$. Nevertheless, as shown in Example 8, no partial isotopism exists from L_1 to L_3.

The following example illustrates all the previous definitions in case of dealing with partial Latin squares with empty cells.

Example 3. *The partial Latin squares*

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

both of them in the set $\mathcal{L}_{4;8}$, are partial transpose of each other. Notice, for instance, that the first condition of the definition holds because

$$\mathrm{Ent}(L_2) \setminus \mathrm{Ent}(L_1) = \{(1,3,4),\ (3,1,3),\ (3,2,4),\ (4,2,3)\}$$

and

$$\{(3,1,4),\ (1,3,3),\ (2,3,4),\ (2,4,3)\} \subset \mathrm{Ent}(L_1).$$

The second condition holds similarly. In addition, one can find a partial isotopism between both partial Latin squares L_1 and L_2. To this end, it is enough to consider the isotopism $\theta = ((1423), (1324), \mathrm{Id}) \in S^3$ and the subset $P = \mathrm{Ent}(L_1) \cap \mathrm{Ent}(L_2)$. That is,

$$L(P) \equiv \begin{array}{|c|c|c|c|}\hline 1&2&&\\\hline &&&\\\hline &&1&\\\hline &&2&\\\hline\end{array} \in \mathcal{L}_{4;4}$$

In particular,

$$L(\mathrm{Ent}(L_1) \setminus P)^{\theta} = L(\mathrm{Ent}(L_2) \setminus P) \equiv \begin{array}{|c|c|c|c|}\hline & & 4 & \\ \hline & & & \\ \hline 3 & 4 & & \\ \hline & 3 & & \\ \hline \end{array} \in \mathcal{L}_{4;4}.$$

Notice that both partial Latin squares L_1 and L_2 are neither transpose nor isotopic of each other.

Let us finish this subsection by focusing on the description of the image patterns based on a given Latin square. To this end, let us recall that every Latin square in the set $\mathcal{L}_{n;n^2}$ constitutes the multiplication table of a *quasigroup* $([n], \cdot)$, where the set $[n]$ is 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 $[n]$, for all $a, b \in [n]$. Equivalently, the set $[n]$ is endowed with a left-division $\backslash$ and a right-division $/$, so that $x = a \backslash b$ in the first equation, and $y = b/a$ in the second one.

Let $T = t_1 t_2 \dots t_m$ be a plaintext, with $t_i \in [n]$, for all $i \leq m$. For each positive integer $s \leq n$, it is defined [6–8] the encrypted string

$$E_s(T) := e_1 e_2 \dots e_m,$$

where

$$e_i := \begin{cases} s \cdot t_1, & \text{if } i = 1, \\ e_{i-1} \cdot t_i, & \text{otherwise.} \end{cases}$$

The resulting string can be desencrypted by means of a decryption map D_s based on the already mentioned left-division. More specifically,

$$t_i = \begin{cases} s \backslash e_1, & \text{if } i = 1, \\ e_{i-1} \backslash e_i, & \text{otherwise.} \end{cases}$$

The sequential implementation of the just described encryption may give rise to image patterns with certain fractal properties [13–16]. More specifically, if $S = (s_1, \dots, s_{r-1})$ is an $(r-1)$-tuple of positive integers such that $s_i \leq n$, for all $i < r$, then the $r \times m$ *image pattern* $\mathcal{P}_{S,T}(L) = (p_{i,j})$ is defined as the $r \times m$ array satisfying that, for each positive integer $j \leq m$, we have that

$$p_{i,j} := \begin{cases} t_j, & \text{if } i = 1, \\ s_{i-1} \cdot p_{i-1,1}, & \text{if } i > 1 \text{ and } j = 1, \\ p_{i,j-1} \cdot p_{i-1,j}, & \text{otherwise.} \end{cases} \tag{2}$$

The image patterns arisen from the set of Latin squares of a given order only depend on the distribution of the latter into isomorphism classes. More specifically, the following result is known.

Lemma 1 ([36])**.** *Let L_1 and L_2 be two Latin squares in $\mathcal{L}_{n;n^2}$ that are isomorphic by means of an isomorphism $(f, f, f) \in S_n^3$. Let $S = (s_1, \dots, s_{r-1})$ and $f(S) = (f(s_1), \dots, f(s_{r-1}))$ be two $(r-1)$-tuples of positive integers, such that $s_i \leq n$, for all $i < r$, and let $T = t_1 \dots t_m$ and $f(T) = f(t_1) \dots f(t_m)$ be two plaintexts, with $t_i \in [n]$, for all $i \leq m$. Then, the $r \times m$ image patterns $\mathcal{P}_{S,T}(L_1) = (p_{i,j})$ and $\mathcal{P}_{f(S),f(T)}(L_2) = (p'_{i,j})$ coincide up to permutation of symbols. More specifically, $p'_{i,j} = f(p_{i,j})$, for all positive integers $i \leq r$ and $j \leq m$.*

2.2. Computational Algebraic Geometry

From here on, let $\mathbb{K}[X]$ denote the multivariate polynomial ring over a field $\mathbb{K}$ that is defined on a finite set X of n variables. A point $P \in \mathbb{K}^n$ is a *zero* of a set $S \subseteq \mathbb{K}[X]$ if $f(P) = 0$, for all $f \in S$. The set of all these zeros constitutes an *affine algebraic set* in $\mathbb{K}^n$. It is *irreducible* if it cannot be decomposed into two nonempty proper affine algebraic sets. The *dimension* $\dim(V)$ of an affine algebraic set V is the maximal number of its irreducible components minus one. Further, two affine algebraic sets V_1 and V_2 in $\mathbb{K}^n$ are *isomorphic* if there exists a bijective map $\phi : V_1 \to V_2$ such that $\phi(P) = (f_1(P), \ldots, f_n(P))$ and $\phi^{-1}(Q) = (g_1(Q), \ldots, g_n(Q))$, for all $(P, Q) \in V_1 \times V_2$, where $f_i, g_i \in \mathbb{K}[X]$, for all $i \leq n$. The map ϕ constitutes an *isomorphism* from V_1 to V_2. An *isomorphism invariant* of affine algebraic sets is any property of the latter that is preserved by isomorphisms.

An *ideal* of the multivariate polynomial ring $\mathbb{K}[X]$ is a subset $I \subseteq \mathbb{K}[X]$ such 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 $q \in \mathbb{K}[X]$. It is said to be *generated by* a set of polynomials $\{p_1, \ldots, p_k\} \subseteq \mathbb{K}[X]$ if it is defined as

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

It is *binomial* if all its generators are. Further, it is *radical* if $p \in I$, for all $p \in \mathbb{K}[X]$ such that $p^m \in I$, for some positive integer m. Finally, it is *zero-dimensional* if $\dim(\mathcal{V}_{\mathbb{K}}(I)) = 0$, where $\mathcal{V}_{\mathbb{K}}(I)$ is the affine algebraic set in $\mathbb{K}^n$ formed by all the zeros of the polynomials within I. This dimension can be obtained from the reduced Gröbner basis of the ideal I [40–42]. Let us recall in this regard that the *leading monomial* of a polynomial is its largest monomial with respect to a given multiplicative well-ordering whose smallest element is the constant monomial 1. Then, a *Gröbner basis* of an ideal I is any subset within I whose leading monomials generate the so-called *initial ideal*, which is generated in turn by all the leading monomials of the non-zero polynomials of I. If the ideal I is zero-dimensional and radical, then the number of monomials that are not contained in its initial ideal coincides with the cardinality of $\mathcal{V}_{\mathbb{K}}(I)$. Further, a Gröbner basis is *reduced* if all its polynomials are monic and no monomial of its polynomials is generated by the leading monomials of the rest of polynomials. The reduced Gröbner basis of an ideal is unique. It can always be computed from Buchberger's algorithm [43]. Arisen from this algorithm, one can find the more efficient direct methods described by the algorithms F_4 and F_5 [44,45] and the algorithm *slimgb* [46].

Throughout this paper, all the computations concerning Gröbner bases are carried out on an *Intel Core i7-8750H CPU (6 cores), with a 2.2 GHz processor and 8 GB of RAM*, with a maximum running time of less than 1 s. All of them are done by making use of the algorithm *slimgb* that is implemented in the CAS SINGULAR. As multiplicative well-ordering, it has been chosen the degree reverse lexicographical ordering. Finally, all the computations are done on either the field $\mathbb{Q}$ of rational numbers or the field $\mathbb{C}$ of complex numbers. In the first case, the following result holds.

Theorem 1 ([22]). *The arithmetic complexity of computing the reduced Gröbner basis of a zero-dimensional ideal* $I = \langle p_1, \ldots, p_m \rangle \subset \mathbb{Q}[\{x_1, \ldots, x_n\}]$ *is bounded above by the value* $\max\left\{\sum_{i=1}^{m} n h_i \binom{n+d_i}{n}, \left(\frac{1}{m}\sum_{i=1}^{m} d_i\right)^n\right\}$, *where* h_i *denotes the maximum size of the coefficients of the generator* p_i, *and* d_i *denotes its maximum degree, for all* $i \leq m$.

The following example focuses on the computation of the affine algebraic set of a partial Latin square, which is described in the Introduction.

Example 4. *Let us consider the partial Latin square* $L_1 \in \mathcal{L}_{4;8}$ *described in Example 3. To compute the affine algebraic set in the multivariate polynomial ring* $\mathbb{Q}[\{x_1, x_2, x_3, x_4\}]$ *of* L_1, *we obtain from Definition 1 the binomial ideal* $I(L_1)$ *defined as*

$$\left\langle x_1^2 - x_1,\ x_1x_2 - x_2,\ x_1x_3 - x_3, x_2x_3 - x_4,\ x_2x_4 - x_3,\ x_1x_3 - x_4,\ x_3^2 - x_1,\ x_3x_4 - x_2 \right\rangle.$$

A reduced Gröbner basis of this binomial ideal is the subset

$$\left\{x_1 - x_2,\ x_3 - x_4,\ x_2^2 - x_2,\ x_2x_4 - x_3,\ x_4^2 - x_1\right\} \subset I(L_1).$$

Hence, the ideal $I(L_1)$ is zero-dimensional. Its associated affine algebraic set is

$$\mathcal{V}_{\mathbb{Q}}(I(L_1)) = \{(0,0,0,0),\ (1,1,1,1),\ (1,1,-1,-1)\}.$$

Being partial transpose and being P-partial isotopic, for some $P \subset [n] \times [n] \times [n]$, are two equivalence relations in the set $\mathcal{L}_{n;m}$ that give rise to identical affine algebraic sets. Concerning the first of them, the following direct result is known.

Lemma 2 ([36]). *If two partial Latin squares of the same order and weight are partial transpose of each other, then their related affine algebraic sets coincide.*

Nevertheless, some assumptions are required for the second equivalence relation. In this regard, let us recall that the binomial ideal $I(L)$ associated to a partial Latin square $L \in \mathcal{L}_n$ determines the following partition of the set $[n]$.

$$\mathrm{Part}(L) := \{\{k \in [n]\colon\ x_m - x_k \in I(L)\}\colon\ m \in [n]\}$$

Then, the following result holds.

Proposition 1 ([36]). *Let $L_1, L_2 \in \mathcal{L}_{n;m}$ be P-partial isotopic, for some subset $P \subseteq \mathrm{Ent}(L_1) \cap \mathrm{Ent}(L_2)$. If $\mathrm{Part}(L_1) = \mathrm{Part}(L_2)$, then $\mathcal{V}_{\mathbb{K}}(L_1) = \mathcal{V}_{\mathbb{K}}(L_2)$, whatever the field $\mathbb{K}$ is.*

Example 5. *Let us consider again the multivariate polynomial ring $\mathbb{Q}[\{x_1, x_2, x_3, x_4\}]$. Since the partial Latin squares L_1 and L_2 described in Example 3 are partial transpose of each other, Lemma 2 implies that $\mathcal{V}_{\mathbb{Q}}(I(L_2)) = \mathcal{V}_{\mathbb{Q}}(I(L_1))$, which is described in Example 4. Now, let us consider the following three partial Latin squares in $\mathcal{L}_{4;8}$.*

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

Notice that L_2' is P-partial isotopic to L_1 by means of the isotopism $((14), \mathrm{Id}, \mathrm{Id}) \in S_4^3$ and the subset $P \subset \mathrm{Ent}(L_1) \cap \mathrm{Ent}(L_2')$ such that $\mathrm{Ent}(L_1) \setminus P = \{(1,1,1)\}$. Further, L_2'' and L_2''' are both isotopic (and, hence, $\emptyset$-partial isotopic) to L_1 by means, respectively, of the isotopisms $(\mathrm{Id}, \mathrm{Id}, (13)(24))$ and $((132), \mathrm{Id}, \mathrm{Id})$ in S_4^3.

A simple computation enables us to ensure that the reduced Gröbner basis of the binomial ideals $I(L_1)$ and $I(L_2')$ coincide and, hence, $\mathcal{V}_{\mathbb{Q}}(I(L_2')) = \mathcal{V}_{\mathbb{Q}}(I(L_1))$. This equality also holds from Proposition 1 and the fact that $\mathcal{P}(L_1) = \mathcal{P}(L_2') = \{\{1,2\}, \{3,4\}\}$, which derives straightforwardly in any case from the mentioned coincidence of reduced Gröbner bases.

Proposition 1 also enables us to ensure that $\mathcal{V}_{\mathbb{Q}}(I(L_2'')) = \mathcal{V}_{\mathbb{Q}}(I(L_1))$, but, here, the reduced Gröbner basis of the binomial ideal $I(L_2'')$ differs from that one of $I(L_1)$. More specifically, the reduced Gröbner basis of $I(L_2'')$ is the subset

$$\left\{x_1 - x_2,\ x_3 - x_4,\ x_2x_4 - x_1,\ x_2^2 - x_3,\ x_4^2 - x_4\right\} \subset I(L_2'').$$

Finally, the reduced Gröbner basis of the binomial ideal $I(L_2''')$ *is the subset*

$$\left\{x_1 - x_2,\, x_2 - x_4,\, x_3 - x_4,\, x_4^2 - x_4\right\} \subset I(L_2'').$$

Hence, $\mathcal{P}(L_2''') = \{\{1,2,3,4\}\} \neq \mathcal{P}(L_1)$ *and* $\mathcal{V}(L_2''') = \{(0,0,0,0),\, (1,1,1,1)\}$.

3. Standard Image Patterns Associated to Latin Squares

Lemma 1 establishes the existing relationship among image patterns arisen from Latin squares and the distribution into isomorphism classes of the latter. This section focuses on a particular subset of image patterns, which may enable one to determine, even from a visual way, whether two Latin squares are not isomorphic. In this regard, let m, n, r and s be four positive integers such that $s \leq n$. We define the *s-standard* $r \times m$ *image pattern* associated to a Latin square $L \in \mathcal{L}_{n;n^2}$ as $\mathcal{P}_{r,m;s}(L) := \mathcal{P}_{S,T}(L)$, where S is the constant $(r-1)$-tuple $(s,\ldots,s)$ and T is the constant plaintext $s \ldots s$ of length m. We call it *constant* if all its entries coincide. In addition, we term the set $\{\mathcal{P}_{r,m;s} \colon\ s \in [n]\}$ the *standard set* of $r \times m$ image patterns associated to L. From Lemma 1, if the standard sets of $r \times m$ image patterns associated to two Latin squares do not coincide up to permutation of symbols, then these Latin squares are not isomorphic. As such, the analysis of standard sets turns out to be of particular interest for distinguishing non-isomorphic Latin squares even from a simple visual way.

To illustrate this fact, let us focus on the standard 90×90 image patterns associated to each one of the 35 isomorphism classes in which the set of Latin squares of order $n = 4$ is distributed. (The case $n = 3$ was already analyzed by Falcón, R.M. et al. [36].) A representative of each one of these classes is described in Figure 1. Their respective standard image patterns are shown in Figure 2. It is formed by four collages in form of 7×5 arrays. They were created by means of the commands *Colorize* and *ImageAssemble* in WOLFRAM MATHEMATICA [47]. Each standard image pattern is represented as a pixel array so that each symbol is uniquely replaced by a color within a given palette of four colors. Each cell within any of these arrays constitutes the corresponding standard image pattern that is associated to the Latin square described at the same position within Figure 1. The union of the four standard images patterns associated to such a Latin square constitutes its standard set of 90×90 image patterns.

These standard sets can be distributed according to the following classification.

1. **Constant standard image patterns**.
   A simple observation of the monochromatic cells in Figure 2 enables us to determine this type of standard image patterns. Notice that the s-standard image pattern of a Latin square $L = (l_{i,j})$ is constant if and only if $l_{s,s} = s$.
2. **Fractal standard image patterns**.
   From a simple visual inspection, one can observe that some of the cells in Figure 2 have a fractal character. It is the case, for instance, of the 2-standard image pattern associated to the Latin square $L_{4.1}$.
3. **Non-fractal standard image patterns**.
   The remaining cells do not have a clear fractal character. Their spectrum goes from what one may label as a chaotic behavior (see, for instance, the 2-standard image pattern associated to $L_{4.30}$) to a shadow of fractal behavior (see, for instance, the 2-standard image pattern related to $L_{4.11}$). In any case, we do not distinguish in this paper the fractal gradation of the image patterns under consideration.

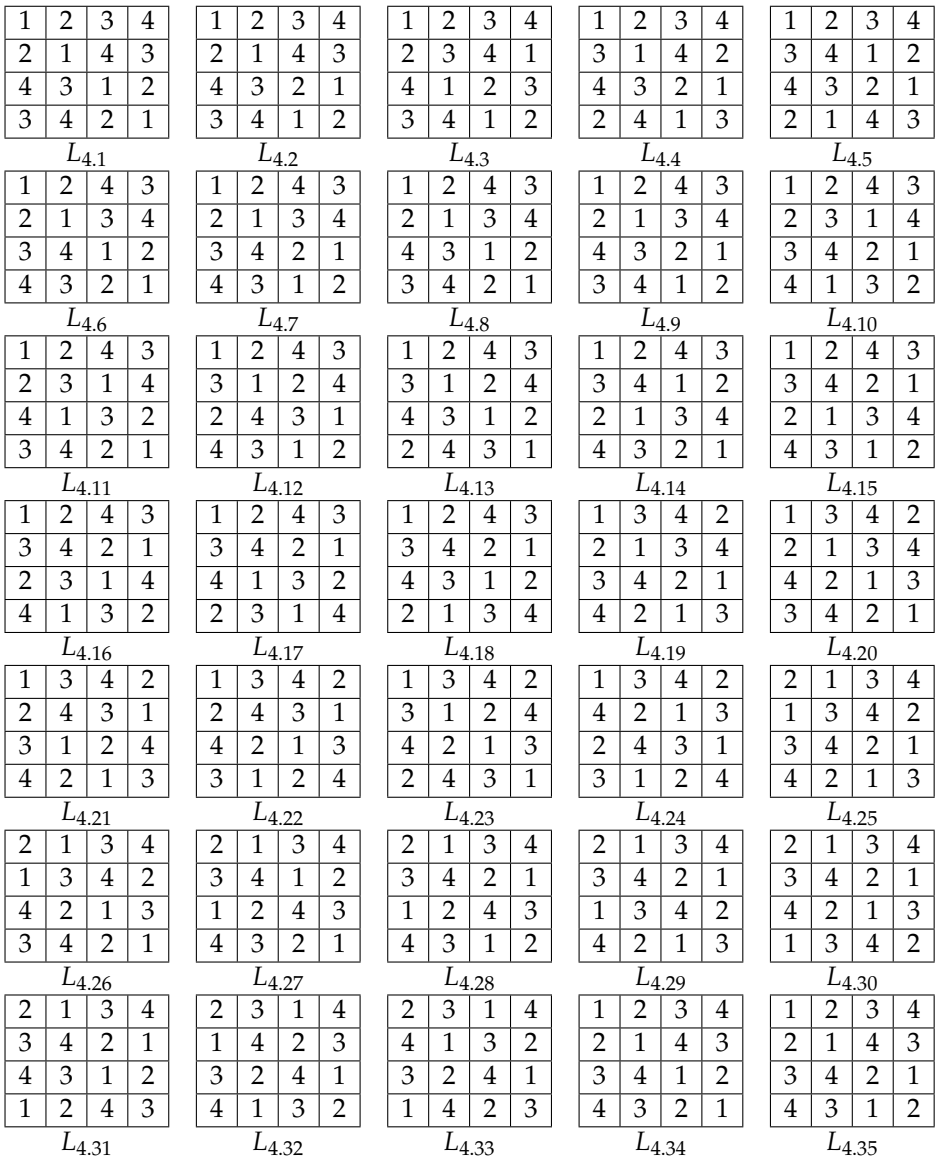

Figure 1. Isomorphism classes of Latin squares of order four.

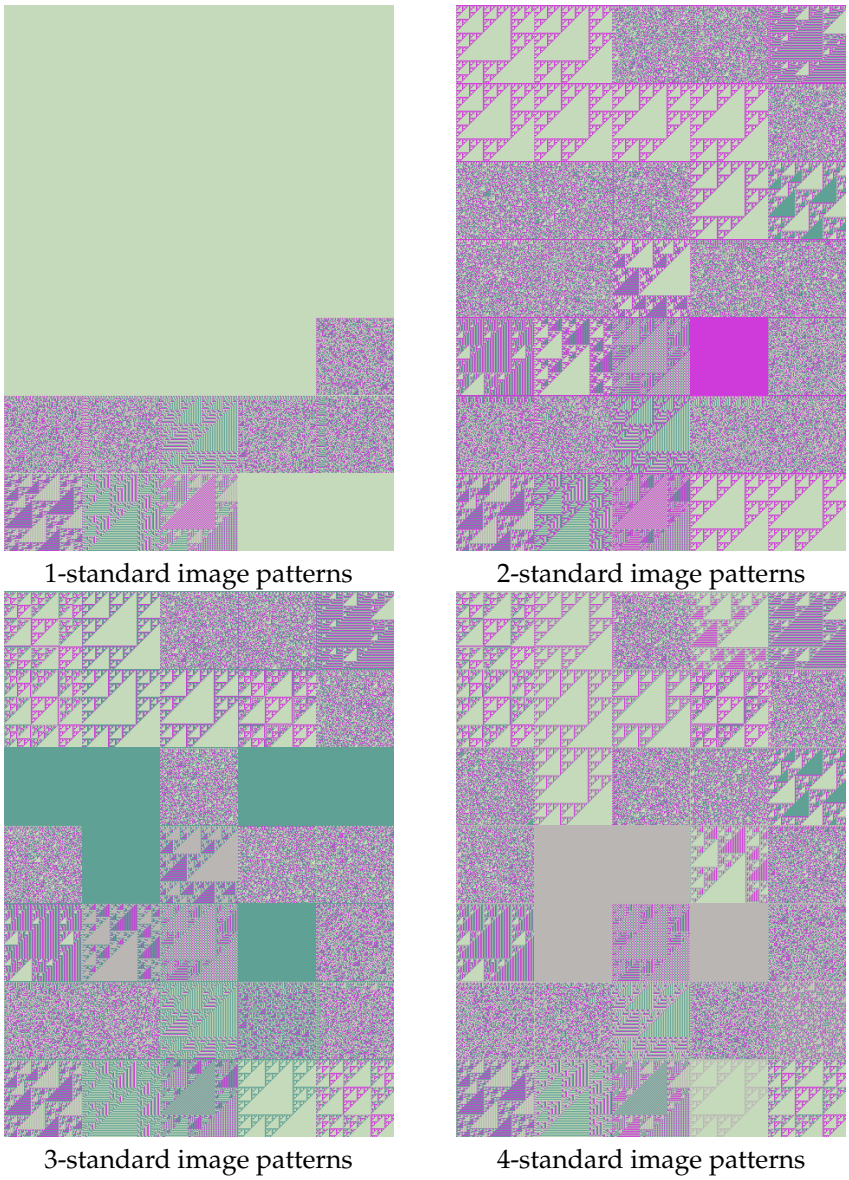

Figure 2. Standard 90×90 image patterns associated to the 35 representatives of isomorphism classes of Latin squares of order four described in Figure 1.

Table 1 shows the values $\sharp \mathrm{cs}_i$ and $\sharp \mathrm{fs}_i$ corresponding, respectively, to the number of constant and fractal standard image patterns within the standard set of 90×90 image patterns of the Latin square $L_{4.i}$ in Figure 1, for every positive integer $i \leq 35$. As introduced above, the number of its non-fractal standard image patterns would be, therefore, $4 - \sharp \mathrm{cs}_i - \sharp \mathrm{fs}_i$. Notice that the first parameter characterizes the isomorphism classes having $L_{4.17}$ and $L_{4.24}$ as representatives, which are the only ones containing respectively three and four constant standard image patterns.

In addition, the representative $L_{4.11}$ is the only one that is associated to two constant and two non-fractal standard image patterns. The remaining standard sets are not easy to distinguish visually, particularly those ones containing non-fractal standard image patterns. An alternative approach to deal with these cases consists of making use of different techniques concerning computational algebraic geometry [36].

Table 1. Number of constant ($\sharp cs_i$), fractal ($\sharp fs_i$) and non-fractal ($\sharp nfs_i$) 90×90 standard image patterns associated to the 35 representatives ($L_{4.i}$) described in Figure 1.

i	$\sharp cs_i$	$\sharp fs_i$	i	$\sharp cs_i$	$\sharp fs_i$	i	$\sharp cs_i$	$\sharp fs_i$
1	1	3	13	1	0	25	0	0
2	1	3	14	2	1	26	0	0
3	1	0	15	2	2	27	0	0
4	1	1	16	1	0	28	0	4
5	1	3	17	3	0	29	0	0
6	1	3	18	2	2	30	0	0
7	1	3	19	1	1	31	0	4
8	1	3	20	1	0	32	0	4
9	1	3	21	1	3	33	0	4
10	1	0	22	2	2	34	1	3
11	2	0	23	1	3	35	1	3
12	2	1	24	4	0			

Let us define the affine algebraic set associated to the s-standard $r \times m$ image pattern $\mathcal{P}_{r,m;s}(L) = (p_{i,j})$ of a Latin square $L \in \mathcal{L}_{n;n^2}$ in the multivariate polynomial ring $\mathbb{Q}[\{x_1, \ldots, x_n\}]$ as the set of zeros of the binomial ideal

$$I(\mathcal{P}_{r,m;s}(L)) := \langle\, x_{p_{i,j-1}} x_{p_{i-1,j}} - x_{p_{i,j}} \colon 1 < i \leq r,\, 1 < j \leq m \,\rangle.$$

From (1) and (2), it is $I(\mathcal{P}_{r,m;s}(L)) \subseteq I(L)$ and hence, $\mathcal{V}_{\mathbb{Q}}(I(L)) \subseteq \mathcal{V}_{\mathbb{Q}}(I(\mathcal{P}_{r,m;s}(L)))$.

Example 6. *Let us consider the Latin square $L_{4.12}$ described in Figure 1 and the multivariate polynomial ring $\mathbb{C}[\{x_1, x_2, x_3, x_4\}]$. The reduced Gröbner basis associated to the binomial ideal $I(L_{4.12})$ is the subset*

$$\left\{x_1 - x_4,\, x_2 - x_4,\, x_3 - x_4,\, x_4^2 - x_2\right\} \subset I(L_{4.12}),$$

whereas that one associated to the ideal $I(\mathcal{P}_{90,90;4}(L_{4.12}))$ is the subset

$$\left\{x_1 - x_2,\, x_3 - x_4,\, x_2^2 - x_2,\, x_2 x_4 - x_4,\, x_4^2 - x_2\right\} \subset I(\mathcal{P}_{90,90;4}(L)).$$

Hence, both ideals are zero-dimensional. Their associated affine algebraic sets are

$$\mathcal{V}_{\mathbb{C}}(I(L_{4.12})) = \{(0,0,0,0),\, (1,1,1,1)\}$$

and

$$\mathcal{V}_{\mathbb{C}}(I(\mathcal{P}_{90,90;4}(L_{4.12}))) = \{(0,0,0,0),\, (1,1,1,1),\, (1,1,-1,-1)\}.$$

Of course, if the standard sets of $r \times m$ image patterns associated to two Latin squares of the same order n coincide, up to permutation of symbols, then the multisets formed by the respective cardinalities of each one of the n affine algebraic sets related to their standard image patterns must also coincide. In particular, from Lemma 1, these multisets coincide for any two isomorphic Latin squares. To illustrate these aspects, Table 2 shows all these cardinalities for the standard image patterns described in Figure 2. It is so that there exist ten isomorphism classes of Latin squares of order four that are related to the multiset $\{2, 2, 2, \infty\}$, nine classes to $\{2, 2, 2, 2\}$, six classes to $\{3, 3, \infty, \infty\}$, four classes to $\{2, 2, \infty, \infty\}$, two classes to $\{2, 3, \infty, \infty\}$ and another two classes to $\{\infty, \infty, \infty, \infty\}$. Moreover, there are two isomorphism classes that are characterized by their respective multisets. Their representatives are the Latin squares $L_{4.17}$ and $L_{4.35}$, which are, respectively, associated to the multisets $\{2, \infty, \infty, \infty\}$ and $\{5, 5, \infty, \infty\}$. In addition, notice that the combination of Tables 1 and 2 characterizes the isomorphism class having the Latin square $L_{4.34}$ as its representative.

Table 2. Cardinalities ($\sharp V_{i,s}$) of the affine algebraic set $\mathcal{V}_{\mathbb{Q}}(I(\mathcal{P}_{90,90;s}(L_{4.i})))$, for all positive integers $i \leq 35$ and $s \leq 4$.

i	$\sharp V_{i,1}$	$\sharp V_{i,2}$	$\sharp V_{i,3}$	$\sharp V_{i,4}$	i	$\sharp V_{i,1}$	$\sharp V_{i,2}$	$\sharp V_{i,3}$	$\sharp V_{i,4}$
1	∞	∞	3	3	19	∞	2	2	2
2	∞	∞	3	3	20	∞	2	2	2
3	∞	2	2	2	21	∞	2	2	2
4	∞	2	2	2	22	∞	2	2	∞
5	∞	2	2	2	23	∞	2	2	2
6	∞	∞	3	3	24	∞	∞	∞	∞
7	∞	∞	3	3	25	2	2	2	2
8	∞	∞	3	3	26	2	2	2	2
9	∞	∞	3	3	27	2	2	2	2
10	∞	2	2	2	28	2	2	2	2
11	∞	2	∞	2	29	2	2	2	2
12	∞	2	∞	3	30	2	2	2	2
13	∞	2	2	2	31	2	2	2	2
14	∞	3	∞	2	32	2	2	2	2
15	∞	2	∞	2	33	2	2	2	2
16	∞	2	2	2	34	∞	∞	∞	∞
17	∞	2	∞	∞	35	∞	∞	5	5
18	∞	2	2	∞					

To facilitate the recognition and analysis of similar standard sets for distinguishing non-isomorphic Latin squares of the same order n, even from a simple visual observation, one may focus on those ones having exactly the same positive number of fractal standard image patterns, as well as the same number of constant standard image patterns and the same multisets of cardinalities of their related affine algebraic sets. Let us illustrate this fact with the case $n = 4$, by means of the values in Tables 1 and 2 concerning the standard sets described in Figure 2.

- The standard sets of both Latin squares $L_{4.4}$ and $L_{4.19}$ are the only ones having exactly one constant and one fractal standard image patterns. To prove that they are indeed non-isomorphic, it is enough to focus on their fractal standard image patterns. In both cases, they correspond to their respective 4-standard image patterns, for which a simple visual observation of Figure 2 enables us to ensure that they are not coincident, even after a permutation of colors.
- A similar reasoning may be done for the standard sets of the Latin squares $L_{4.15}$, $L_{4.18}$ and $L_{4.22}$, which are the only ones having two constant and two fractal standard image patterns. A simple observation of Figure 2 enables us to ensure that their respective sets of fractal standard image patterns are pairwise distinct, even after a permutation of colors.
- The same happens with the four Latin squares $L_{4.28}$, $L_{4.31}$, $L_{4.32}$ and $L_{4.33}$.
- A more interesting case is that one concerning the eleven isomorphism classes whose respective standard sets contain exactly one constant and three fractal standard image patterns. Table 2 partitions them into four disjoint subsets. Two of them have already been characterized by these parameters. They correspond to the Latin squares $L_{4.34}$ and $L_{4.35}$. The other two subsets are the following ones.
  - The subset formed by the three Latin squares $L_{4.5}$, $L_{4.21}$ and $L_{4.23}$. Similarly to the previous cases, their standard sets are visually characterized in a simple way.
  - The subset formed by the six Latin squares $L_{4.1}$, $L_{4.2}$, $L_{4.6}$, $L_{4.7}$, $L_{4.8}$ and $L_{4.9}$. Here, the visual distinction of their fractal standard image patterns in Figure 2 is not so evident. It is so that all their 2-standard image patterns coincide and a much more detailed observation of their 3- and 4-standard sets is required for ensuring that their standard sets are pairwise distinct.

- A detailed observation is also required for distinguishing visually the standard sets of the Latin squares $L_{4.12}$ and $L_{4.14}$, both of them containing exactly two constant and one fractal standard image pattern. More specifically, it may be checked (either visually or by making use of Definition 2) that the second row of the fractal standard image pattern of $L_{4.12}$ contains all the four colors or symbols under consideration, whereas that one of $L_{4.14}$ only contains two of them.

None of the standard sets of the remaining ten isomorphism classes contains fractal standard image patterns, which makes much more difficult their visual distinction. According to their respective parameters, they can be partitioned into the following two sets.

- The subset formed by the five Latin squares $L_{4.3}$, $L_{4.10}$, $L_{4.13}$, $L_{4.16}$ and $L_{4.20}$. Their standard sets contains exactly one constant standard image patterns. Notice that $L_{4.3}$ and $L_{4.13}$ are respective transpose of $L_{4.10}$ and $L_{4.20}$.
- The subset formed by the five Latin squares $L_{4.25}$, $L_{4.26}$, $L_{4.27}$, $L_{4.29}$ and $L_{4.30}$. None of their standard sets contain constant standard image patterns.

A possible approach to analyze the non-fractal standard image patterns of both subsets is reducing their dimension, which is equivalent to zoom in to the left upper corner of the original standard image patterns. Based on this approach, it is simply verified from the results in Figures 3 and 4 that the standard sets of 3×3 image patterns associated to these two subsets are pairwise distinct, even allowing a possible permutation of symbols.

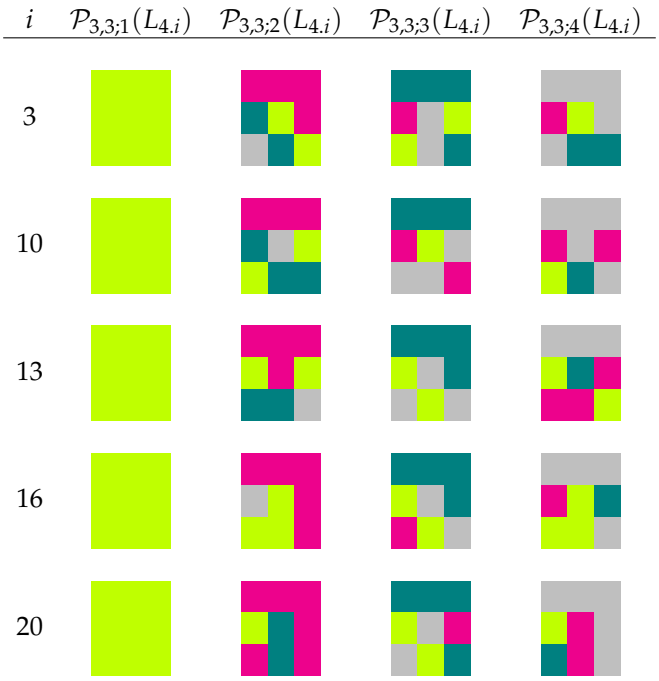

Figure 3. Standard 3×3 image patterns associated to $L_{4.3}$, $L_{4.10}$, $L_{4.13}$, $L_{4.16}$ and $L_{4.20}$.

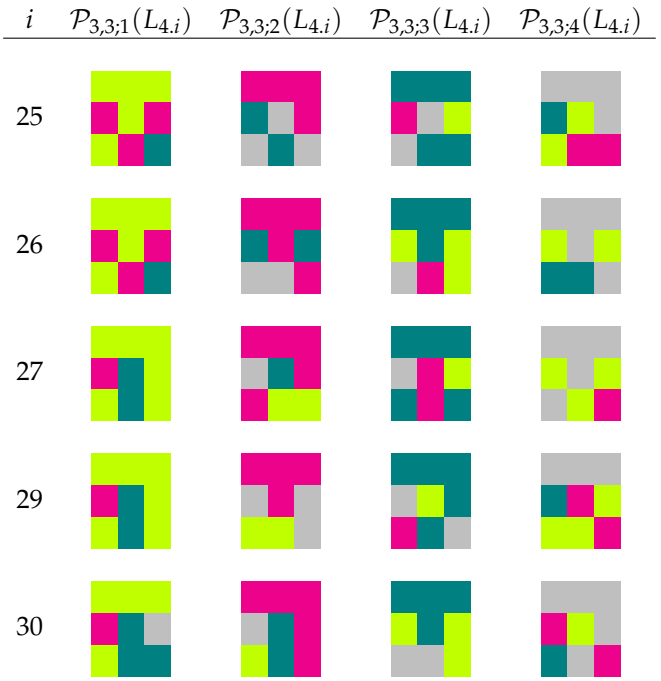

Figure 4. Standard 3×3 image patterns associated to $L_{4.25}$, $L_{4.26}$, $L_{4.27}$, $L_{4.29}$ and $L_{4.30}$.

4. A Computational Algebraic Geometry Approach to Deal with Being Either Partial Transpose or Partial Isotopic

We show in Section 3 how the computation of isomorphism invariants concerning affine algebraic sets based on a set of Latin squares plays a fundamental role in the recognition and analysis of their related image patterns. Apart from these invariants, the existence of certain equivalence relations among partial Latin squares of the same order and weight is also known [36], which give rise to the same or isomorphic affine algebraic sets. It is the case of being partial transpose and being P-partial isotopic, for some subset $P \subset [n] \times [n] \times [n]$ (see Lemma 2 and Proposition 1). Let us finish this paper by showing how computational algebraic geometry is also an interesting approach to deal with both equivalence relations. To this end, let us introduce a pair of ideals within a multivariate polynomial ring, whose respective affine algebraic sets are respectively identified with the set of partial Latin squares that are partial transpose of another given partial Latin square, and the set of partial isotopisms between two partial Latin squares.

Firstly, for each positive integer n, we consider the set of n^3 variables

$$X_n^{\mathrm{PT}} := \{x_{ijk} \colon 1 \leq i, j, k \leq n\}.$$

Then, for each positive integer $m \leq n^2$, it is known [18] (see also [27,29] for a pair of first approaches in this regard) that the set $\mathcal{L}_{n;m}$ is uniquely identified with the set of zeros of the affine algebraic set of the following ideal in $\mathbb{Q}[X_n^{\mathrm{PT}}]$.

$$\begin{aligned} I_{n;m} := & \left\langle x_{ijk}^2 - x_{ijk} \colon 1 \leq i, j, k \leq n \right\rangle \\ & + \left\langle x_{ijk} x_{i'jk} \colon 1 \leq i, i', j, k \leq n,\ i < i' \right\rangle \\ & + \left\langle x_{ijk} x_{ij'k} \colon 1 \leq i, j, j', k \leq n,\ j < j' \right\rangle \\ & + \left\langle x_{ijk} x_{ijk'} \colon 1 \leq i, j, k, k' \leq n,\ k < k' \right\rangle \\ & + \left\langle m - \sum_{i,j,k=1}^{n} x_{ijk} \right\rangle. \end{aligned}$$

Let us recall here that the sum of two ideals I and J is the ideal $I+J=\{i+j\colon\ i\in I,\ j\in J\}$. Each addend constitutes a subideal of the resulting ideal. Hence, our ideal I_n is the sum of four subideals. The first one implies that any zero of I_n is of the form $(a_{111},\ldots,a_{nnn})\in\{0,1\}^{n^3}$. The remaining subideals imply that this zero is uniquely identified with a partial Latin square $L=(l_{i,j})\in\mathcal{L}_{n;m}$ such that $l_{i,j}=k\in[n]$ if and only if $a_{ijk}=1$.

Now, for each partial Latin square $L\in\mathcal{L}_{n;m}$, let us define the following ideal in the multivariate polynomial ring $\mathbb{Q}[X_n^{\mathrm{PT}}]$.

$$I_{\mathrm{PT}}(L):=I_{n;m}+\Big\langle\,(x_{ijk}-1)\cdot(x_{jik}-1)\colon\ (i,j,k)\in\mathrm{Ent}(L)\,\Big\rangle \\ \Big\langle\,x_{ijk},\,x_{jik}\colon\ \{(i,j,k),\,(j,i,k)\}\cap\mathrm{Ent}(L)=\emptyset,\,1\leq i,j,k\leq n\,\Big\rangle.$$

Lemma 3. *The set of partial Latin squares that are partial transpose to a partial Latin square $L\in\mathcal{L}_{n;m}$ is uniquely identified with the affine algebraic set of the ideal $I_{\mathrm{PT}}(L)$.*

Proof. Let $(a_{111},\ldots,a_{nnn})\in\{0,1\}^{n^3}$ be a zero of the ideal $I_{\mathrm{PT}}(L)$. In particular, it must be a zero of the ideal $I_{n;m}$ and, hence, it is uniquely identified with a partial Latin square $L'\in\mathcal{L}_{n;m}$ such that $(i,j,k)\in\mathrm{Ent}(L')$ if and only if $a_{ijk}=1$. From the subideal

$$\Big\langle\,(x_{ijk}-1)\cdot(x_{jik}-1)\colon\ (i,j,k)\in\mathrm{Ent}(L)\,\Big\rangle,$$

we have that, if $(i,j,k)\in\mathrm{Ent}(L)$, then either $a_{ijk}=1$ or $a_{jik}=1$. As a consequence, if $(i,j,k)\in\mathrm{Ent}(L)\setminus\mathrm{Ent}(L')$, then $(j,i,k)\in\mathrm{Ent}(L')$.

Now, let $(i,j,k)\in\mathrm{Ent}(L')\setminus\mathrm{Ent}(L)$. In particular, it must be $a_{ijk}=1$. If $(j,i,k)\notin\mathrm{Ent}(L)$, then the last subideal describing $I_{\mathrm{PT}}(L)$ implies that $a_{ijk}=0$, which is a contradiction. Hence, $(j,i,k)\in\mathrm{Ent}(L)$. Therefore, the partial Latin squares L and L' are partial transpose of each other. □

Example 7. *Let us consider the partial Latin square*

$$L\equiv\begin{array}{|c|c|c|}\hline 1&2&\\\hline 3&&1\\\hline 2&&3\\\hline\end{array}\in\mathcal{L}_{3;5}.$$

The reduced Gröbner basis of the ideal $I_{\mathrm{PT}}(L)\subset\mathbb{Q}[X_3^{\mathrm{PT}}]$ is the subset

$$\begin{array}{ll}&\{x_{321}^2-x_{321},\,x_{312}^2-x_{312},\,x_{231}+x_{321}-1,\,x_{213}-x_{312},\,x_{212}+x_{312}-1\}\\ \cup&\{x_{132}+x_{312}-1,\,x_{123}+x_{312}-1,\,x_{122}-x_{312},\,x_{333}-1,\,x_{111}-1,\,x_{332},\,x_{331},\,x_{323}\}\\ \cup&\{x_{322},x_{313},x_{311},x_{233},x_{232},x_{223},x_{222},x_{221},x_{211},x_{133},x_{131},x_{121},x_{113},x_{112}\}\subset I_{\mathrm{PT}}(L).\end{array}$$

Hence, the affine algebraic set of the ideal $I_{\mathrm{PT}}(L)$ is formed by four points that are uniquely associated to L and the following three partial Latin squares.

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

From Lemma 3, computational algebraic geometry can be used for distributing partial Latin squares of the same order n according to the equivalence relation of being partial transpose. The following result establishes the computational cost that is required to this end in case of being $n\geq 2$. (The case $n=1$ is trivial.)

Theorem 2. *Let $L\in\mathcal{L}_n$, with $n\geq 2$. The arithmetic complexity of computing the reduced Gröbner basis of the ideal $I_{\mathrm{PT}}(L)$ over the field $\mathbb{Q}$ is bounded above by*

$$\left(\frac{2\left(3n^3-3n^2+9n+|\mathrm{Ent}(L)|\right)+\alpha_1+2\alpha_2+1}{3n^3-3n^2+9n+|\mathrm{Ent}(L)|+\alpha_1+2\alpha_2+1}\right)^{n^3}<2^{n^3},$$

where

$$\alpha_1:=|\{(i,i,k)\notin \mathrm{Ent}(L)\colon\ 1\leq i,k\leq n\}|$$

and

$$\alpha_2:=|\{(i,j,k)\colon \{(i,j,k),\,(j,i,k)\}\cap \mathrm{Ent}(L)=\emptyset,\ 1\leq i<j\leq n,\ 1\leq k\leq n\}|.$$

Proof. The ideal $I_{\mathrm{PT}}(L)$ is zero-dimensional, because $\mathcal{V}_{\mathbb{Q}}(I_{\mathrm{PT}}(L))\subset\{0,1\}^{n^3}$. Thus, the result holds from Theorem 1 and the generators of this ideal, whose coefficients have all of them size one. To see it, Table 3 shows the maximum degree of each one of these generators, together with the number of generators of each type. Then, the result follows because, from Theorem 1, the required arithmetic complexity is bounded above by the maximum value between

$$n^3\left(\left(3n^3-3n^2+9n+|\mathrm{Ent}(L)|\right)\binom{n^3+2}{n^3}+(\alpha_1+2\alpha_2+1)(n^3+1)\right)$$

and

$$\left(\frac{2\left(3n^3-3n^2+9n+|\mathrm{Ent}(L)|\right)+\alpha_1+2\alpha_2+1}{3n^3-3n^2+9n+|\mathrm{Ent}(L)|+\alpha_1+2\alpha_2+1}\right)^{n^3}.$$

□

Table 3. Study of the generators of the ideal $I_{\mathrm{PT}}(L)$.

Generator Type	Maximum Degree	Number of Generators
$x_{ijk}^2-x_{ijk}$	2	$3n$
$x_{ijk}x_{i'jk}$	2	n^3-n^2+2n
$x_{ijk}x_{ij'k}$	2	n^3-n^2+2n
$x_{ijk}x_{ijk'}$	2	n^3-n^2+2n
$m-\sum_{i,j,k=1}^{n}x_{ijk}$	1	1
$(x_{ijk}-1)\cdot(x_{jik}-1)$	2	$\lvert\mathrm{Ent}(L)\rvert$
x_{iik}	1	α_1
x_{ijk} (with $i\neq j$)	1	$2\alpha_2$

A computational algebraic geometry approach can also be described in the case of dealing with the equivalence relation of being P-partial isotopic, for some subset $P\subset[n]\times[n]\times[n]$. It follows similarly to the approach concerning the equivalence relation of being isotopic, which was described in (Theorem 13, [18]). To this end, for each positive integer n, let us consider the set of $3n^2$ variables

$$X_n^{\mathrm{PI}}:=\{x_{ij},\,y_{ij},\,z_{ij}\colon\ 1\leq i,j\leq n\}.$$

Then, for each pair of partial Latin squares $L_1 = (l_{i,j})$ and $L_2 = (l'_{i,j})$ in the set $\mathcal{L}_{n;m}$, let us define the following ideal in the multivariate polynomial ring $\mathbb{Q}[X_n^{\mathrm{PI}}]$.

$$\begin{aligned} I_{\mathrm{PI}}(L_1, L_2) := & \left\langle x_{ij}^2 - x_{ij},\, y_{ij}^2 - y_{ij},\, z_{ij}^2 - z_{ij} \colon 1 \le i, j \le n \right\rangle \\ & + \left\langle 1 - \sum_{j=1}^{n} x_{ij},\, 1 - \sum_{j=1}^{n} x_{ji} \colon 1 \le i \le n \right\rangle \\ & + \left\langle 1 - \sum_{j=1}^{n} y_{ij},\, 1 - \sum_{j=1}^{n} y_{ji} \colon 1 \le i \le n \right\rangle \\ & + \left\langle 1 - \sum_{j=1}^{n} z_{ij},\, 1 - \sum_{j=1}^{n} z_{ji} \colon 1 \le i \le n \right\rangle \\ & + \left\langle x_{ii'} y_{jj'} (z_{l_{i,j} l'_{i',j'}} - 1) \colon 1 \le i, i', j, j', l_{i,j}, l'_{i',j'} \le n, \text{ with } l_{i,j} \ne l'_{i,j} \right\rangle \\ & + \left\langle x_{ii'} y_{jj'} \colon 1 \le i, i', j, j' \le n,\, l_{i,j} = \emptyset \notin \left\{ l'_{i,j},\, l'_{i',j'} \right\} \right\rangle \\ & + \left\langle x_{ii'} y_{jj'} \colon 1 \le i, i', j, j' \le n,\, l_{i,j} = l'_{i,j} = \emptyset \ne l'_{i',j'} \right\rangle \\ & + \left\langle x_{ii'} y_{jj'} \colon 1 \le i, i', j, j' \le n,\, l_{i,j} \ne \emptyset = l'_{i',j'} \text{ and } l_{i,j} \ne l'_{i,j} \right\rangle. \end{aligned}$$

Lemma 4. *Two partial Latin squares L_1 and L_2 in the set $\mathcal{L}_{n;m}$ are P-partial isotopic, for some subset $P \subset [n] \times [n] \times [n]$, if and only if the affine algebraic set of the ideal $I_{\mathrm{PI}}(L_1, L_2)$ is non-empty.*

Proof. Let us suppose the existence of a zero $(a_{11}, \ldots, a_{nn}, b_{11}, \ldots, b_{nn}, c_{11}, \ldots, c_{nn}) \in \{0,1\}^{3n^2}$ of the ideal $I_{\mathrm{PI}}(L_1, L_2)$. The first three subideals describing this ideal imply that this zero is uniquely related to an isotopism $(f, g, h) \in S_n^3$ such that, for each pair of positive integers $i, j \le n$, the following assertions hold.

- $f(i) = j$ if and only if $a_{ij} = 1$.
- $g(i) = j$ if and only if $b_{ij} = 1$.
- $h(i) = j$ if and only if $c_{ij} = 1$.

The fourth subideal implies that this isotopism constitutes a one-to-one map from $\mathrm{Ent}(L_1) \setminus \mathrm{Ent}(L_2)$ to $\mathrm{Ent}(L_2)$. The fifth one implies that, if the cell (i, j) is empty in L_1 but not in L_2, then the former cannot be mapped to a non-empty cell in L_2. Further, the sixth subideal implies that, if the cell (i, j) is empty in both L_1 and L_2, then it cannot be mapped to a non-empty cell in L_2. Finally, the last subideal implies that, if the cell (i, j) contains distinct symbols in L_1 and L_2, then it cannot be mapped to an empty cell in L_2. Under such assumptions, it is readily verified that the zero under consideration is uniquely identified with a P-partial isotopism from L_1 to L_2, where $P \subseteq \mathrm{Ent}(L_1) \cap \mathrm{Ent}(L_2)$. □

Example 8. *Let us consider the Latin squares L_1 and L_3 in Example 2. The reduced Gröbner basis of the ideal $I_{\mathrm{PI}}(L_1, L_3) \subset \mathbb{Q}[X_4^{\mathrm{PI}}]$ is the subset $\{1\} \subset I_{\mathrm{PI}}(L_1, L_3)$. Thus, the related affine algebraic set is empty and hence, no partial isotopism exists between L_1 and L_3.*

Example 9. *Let us consider the partial Latin square L_1 and L_2 described in Example 3. The reduced Gröbner basis of the ideal $I_{\mathrm{PI}}(L_1, L_2) \subset \mathbb{Q}[X_4^{\mathrm{PI}}]$ is the subset*

$$\begin{aligned} & \{z_{22}^2 - z_{22},\, z_{21} + z_{22} - 1,\, z_{12} + z_{22} - 1,\, z_{11} - z_{22},\, z_{44} - 1,\, z_{43},\, z_{42},\, z_{41},\, z_{34},\, z_{33} - 1\} \\ \cup\ & \{z_{32},\, z_{31},\, z_{24},\, z_{23},\, z_{14},\, z_{13},\, y_{44},\, y_{43},\, y_{42},\, y_{41} - 1,\, y_{34},\, y_{33},\, y_{32} - 1,\, y_{31},\, y_{24} - 1,\, y_{23}\} \\ \cup\ & \{y_{22},\, y_{21},\, y_{14},\, y_{13} - 1,\, y_{12},\, y_{11},\, x_{44},\, x_{43},\, x_{42} - 1,\, x_{41},\, x_{34},\, x_{33},\, x_{32},\, x_{31} - 1,\, x_{24}\} \\ \cup\ & \{x_{23} - 1,\, x_{22},\, x_{21},\, x_{14} - 1,\, x_{13},\, x_{12},\, x_{11}\} \subset I_{\mathrm{PI}}(L_1, L_2). \end{aligned}$$

Hence, the affine algebraic set of the ideal $I_{\mathrm{PI}}(L_1, L_2)$ is formed by two points that are uniquely associated to the isotopisms $((1423), (1324), (12))$ and $((1423), (1324), \mathrm{Id})$ in S_4^3. Both of them constitute P-partial isotopisms from L_1 to L_2, where $P = \mathrm{Ent}(L_1) \cap \mathrm{Ent}(L_2)$.

From Lemma 4, computational algebraic geometry can be used for distributing partial Latin squares according to the equivalence relation of being P-partial isotopic, for some subset $P \subset [n] \times [n] \times [n]$. The following result establishes the computational cost that is required to this end in case of being $n > 2$. (The case $n = 1$ is trivial.)

Theorem 3. *Let L_1 and L_2 be two partial Latin squares in $\mathcal{L}_n$, with $n \geq 2$. The arithmetic complexity of computing the reduced Gröbner basis of the ideal $I_{\mathrm{PI}}(L_1, L_2)$ over the field $\mathbb{Q}$ is bounded above by*

$$\left(\frac{3\beta_1 + 2(3n^2 + \beta_2 + \beta_3 + \beta_4) + 6n}{3n^2 + 6n + \beta_1 + \beta_2 + \beta_3 + \beta_4}\right)^{3n^2} < 3^{3n^2},$$

where

$$\beta_1 := \left|\left\{(i, i', j, j') \in [n] \times [n] \times [n] \times [n] \colon\ l_{i,j}, l'_{i',j'} \in [n],\ l_{i,j} \neq l'_{i',j'}\right\}\right|,$$

$$\beta_2 := \left|\left\{(i, i', j, j') \in [n] \times [n] \times [n] \times [n] \colon\ l_{i,j} = \emptyset \notin \left\{l'_{i,j}, l'_{i',j'}\right\}\right\}\right|,$$

$$\beta_3 := \left|\left\{(i, i', j, j') \in [n] \times [n] \times [n] \times [n] \colon\ l_{i,j} = l'_{i,j} = \emptyset \neq l'_{i',j'}\right\}\right|$$

and

$$\beta_4 := \left|\left\{(i, i', j, j') \in [n] \times [n] \times [n] \times [n] \colon\ l_{i,j} \neq \emptyset = l'_{i',j'} \text{ and } l_{i,j} \neq l'_{i,j}\right\}\right|$$

Proof. The ideal $I_{\mathrm{PI}}(L_1, L_2)$ is zero-dimensional, because $\mathcal{V}_{\mathbb{Q}}(I_{\mathrm{PI}}(L)) \subset \{0, 1\}^{3n^2}$. Then, similarly to the proof of Theorem 2, the result holds from Theorem 1 and the generators of this ideal, whose coefficients have all of them size one. To see it, Table 4 shows the maximum degree of each one of these generators, together with the number of generators of each type. Then, the result holds because, from Theorem 2, the required arithmetic complexity is bounded above by the maximum value between

$$3n^2\left(\beta_1\binom{3n^2+3}{3n^2} + (3n^2 + \beta_2 + \beta_3 + \beta_4)\binom{3n^2+2}{3n^2} + 6n(3n^2+1)\right).$$

and

$$\left(\frac{3\beta_1 + 2(3n^2 + \beta_2 + \beta_3 + \beta_4) + 6n}{3n^2 + 6n + \beta_1 + \beta_2 + \beta_3 + \beta_4}\right)^{3n^2}.$$

□

Table 4. Study of the generators of the ideal $I_{\mathrm{PI}}(L_1, L_2)$.

Generator Type	Maximum Degree	Number of Generators
$x_{ij}^2 - x_{ij}$	2	n^2
$y_{ij}^2 - y_{ij}$	2	n^2
$z_{ij}^2 - z_{ij}$	2	n^2
$1 - \sum_{j=1}^{n} x_{ij}$	1	n
$1 - \sum_{j=1}^{n} x_{ji}$	1	n
$1 - \sum_{j=1}^{n} y_{ij}$	1	n
$1 - \sum_{j=1}^{n} y_{ji}$	1	n
$1 - \sum_{j=1}^{n} z_{ij}$	1	n
$1 - \sum_{j=1}^{n} z_{ji}$	1	n
$x_{ii'}y_{jj'}(z_{l_{i,j}l'_{i',j'}} - 1)$	3	β_1
$x_{ii'}y_{jj'}$	2	$\beta_2 + \beta_3 + \beta_4$

5. Conclusions and Further Work

In this paper, we show the relevant role that computational algebraic geometry plays in the recognition and analysis of image patterns associated to Latin squares. To this end, we introduce the concepts of standard image pattern and standard set of a given Latin square. Moreover, a new affine algebraic set associated to any such image pattern is described, whose isomorphism invariants can be used for distinguishing different standard sets and hence, for determining in a computationally fast way (even visually) whether two Latin squares are not isomorphic.

The main limitation of the methodology here proposed is the exponential complexity for computing Gröbner bases, which is highly dependent on the number of underlying variables. This number coincides in our case with the order of the Latin square under consideration. Due to it, this limitation is not an inconvenience at all for dealing with the smallest orders for which no results on the distribution of Latin squares into isomorphism classes is known ($n \geq 12$). In fact, this computational approach turns out to be an efficient way for dealing with Latin squares of much higher orders. To illustrate this fact, let us consider the Latin square of order 256 that is represented by colors in Figure 5. It was randomly constructed by following Algorithm 1 in [48], which gives rise to random Latin squares with possible implementation in cryptography. Notice in any case that every Latin square generated in this way is isotopic to a diagonally cyclic Latin square [49]. Figure 6 shows the running time required by an *Intel Core i7-8750H CPU (6 cores), with a 2.2 GHz processor and 8 GB of RAM* for computing both the reduced Gröbner basis of the binomial ideal associated to the s-standard 90×90 image pattern of this Latin square described in Figure 5, for every positive integer $s \leq 256$, together with the cardinality of its related affine algebraic set. The maximum running time was 3.45 s, which is reached for $s = 101$.

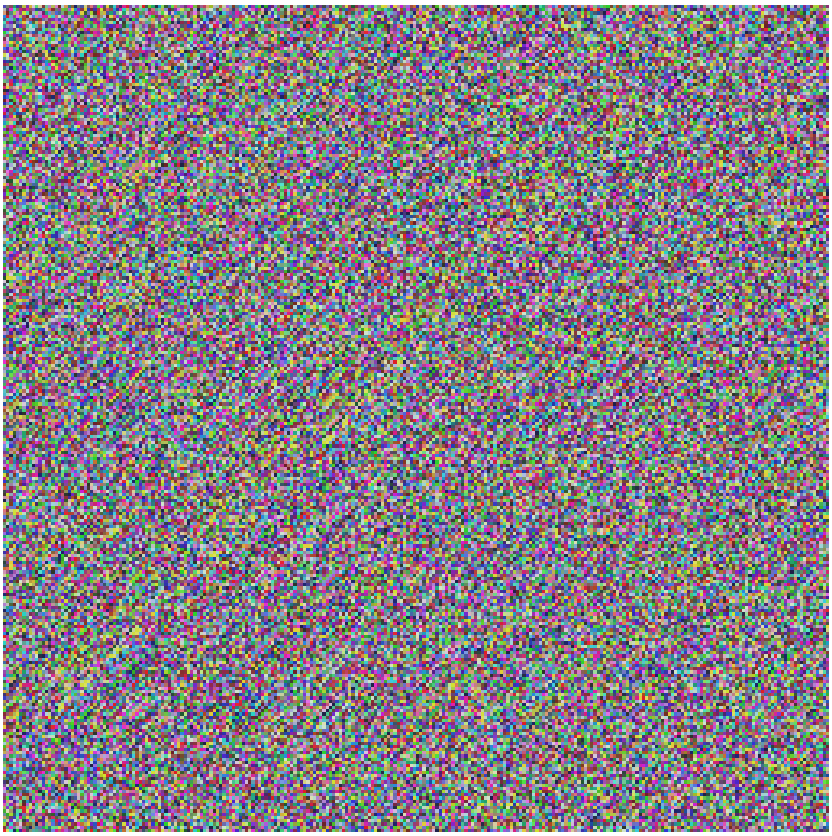

Figure 5. Latin square of order 256 represented by colors.

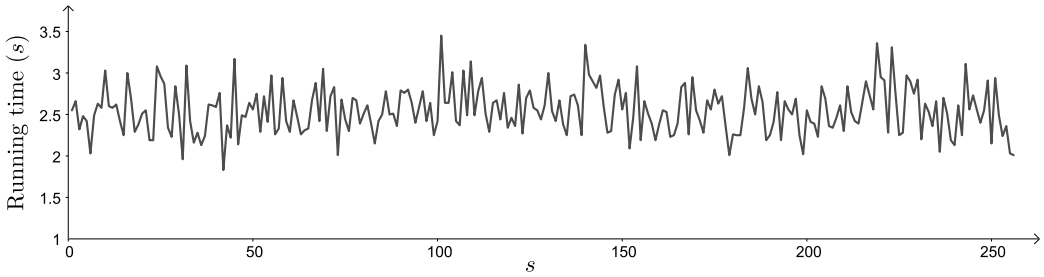

Figure 6. Running time (in seconds) required for computing the cardinality of the set $\mathcal{V}_{\mathbb{C}}(I(\mathcal{P}_{90,90;s}(L)))$, with $1 \leq s \leq 256$, and L being the Latin square described in Figure 5.

It is remarkable that the methodology here described may be particularized in order to make more efficient the computation of group isomorphisms. Let us recall in this regard that every associative quasigroup constitutes a group. To illustrate this fact, let us consider both the dihedral and the abelian groups of order six, whose respective multiplication tables are the Latin squares

$$\mathcal{D}_6 \equiv \begin{array}{|c|c|c|c|c|c|}\hline 1&2&3&4&5&6\\\hline 2&3&1&5&6&4\\\hline 3&1&2&6&4&5\\\hline 4&6&5&1&3&2\\\hline 5&4&6&2&1&3\\\hline 6&5&4&3&2&1\\\hline\end{array} \quad \text{and} \quad \mathcal{Z}_6 \equiv \begin{array}{|c|c|c|c|c|c|}\hline 1&2&3&4&5&6\\\hline 2&3&4&5&6&1\\\hline 3&4&5&6&1&2\\\hline 4&5&6&1&2&3\\\hline 5&6&1&2&3&4\\\hline 6&1&2&3&4&5\\\hline\end{array}.$$

Their respective standard sets of 90×90 image patterns are shown in the 2×6 collage of Figure 7. Both standard sets are formed by a constant and five fractal standard image

patterns. It is readily verified from a visual way that the standard set of the dihedral group (top row of the collage) does not coincide with the standard set of the abelian group (bottom row of the collage), even allowing a possible permutation of symbols. In this simple way, we may ensure that these two groups are not isomorphic.

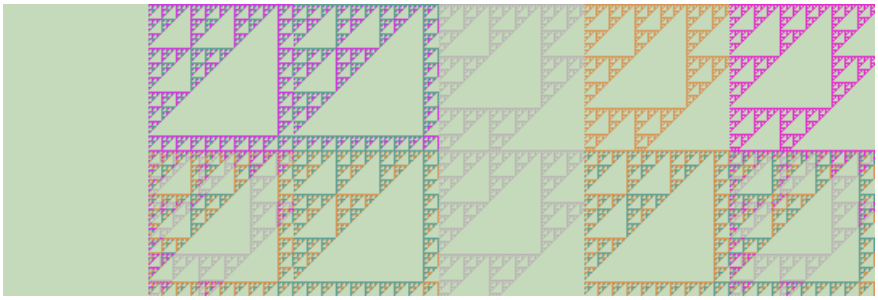

Figure 7. Standard sets of 90×90 image patterns associated to the dihedral group (**top**) and the abelian group (**bottom**) of order six.

A similar conclusion arises from the computation of the reduced Gröbner bases concerning both types of affine algebraic sets associated to the dihedral and the abelian group of order six. From this computation, we have that

$$|\mathcal{V}_{\mathbb{C}}(I(\mathcal{D}_6))| = 3 \qquad \text{and} \qquad |\mathcal{V}_{\mathbb{C}}(I(\mathcal{Z}_6))| = 7.$$

In addition, we have that $|\mathcal{V}_{\mathbb{C}}(I(\mathcal{P}_{90,90;s}(\mathcal{D}_6)))| = \infty$, for every positive integer $s \leq 6$, but

$$|\mathcal{V}_{\mathbb{C}}(I(\mathcal{P}_{90,90;2}(\mathcal{Z}_6)))| = |\mathcal{V}_{\mathbb{C}}(I(\mathcal{P}_{90,90;6}(\mathcal{Z}_6)))| = 7.$$

Further, the methodology here described can be generalized for other types of arrays non-subjected to the Latin square condition. In this regard, it would be interesting to delve, for instance, into the study of standard sets of image patterns associated to (partial) semigroups or, more generally, to (partial) magmas. Even if they may not be endowed with a left or right division (as quasigroups are), their multiplication tables enable us to define $r \times m$ image patterns based on these algebraic structures by making use to this end of the corresponding conditions described in (2) (see [50], for a first approach in this regard in case of dealing with magmas).

These conditions may be taken into account to deal also with arrays related to other types of mathematical structures, not only algebraic ones. To illustrate this aspect, let us focus on the classical problem in graph theory of determining whether two given graphs are isomorphic or not. Every adjacency matrix of a given simple graph of order n is a binary symmetric $n \times n$ array with main diagonal of zeros. It may be considered the multiplication table of a finite magma of set of symbols $\{0, 1, \ldots, n-1\}$ from which one could define $r \times m$ image patterns satisfying the corresponding conditions in (2). Then, standard sets of s-standard image patterns, with $s \in \{0, 1 \ldots, n-1\}$, could be defined similarly to those ones described in Section 3. In this way, the standard set of two isomorphic regular graphs would always coincide, up to permutations of symbols. This fact may therefore be used for distinguishing non-isomorphic regular graphs, even from a visual way. Thus, for instance, the following two arrays constitute respective incidence matrices of the complete graph K_4 and the cycle C_4.

0	1	1	1
1	0	1	1
1	1	0	1
1	1	1	0

0	1	0	1
1	0	1	0
0	1	0	1
1	0	1	0

The standard sets of the 90×90 image patterns associated to both graphs are shown in the 2×4 collage of Figure 8. Notice that the standard set of the complete graph K_4 (top

row of the collage) is formed by one constant and three fractal image patterns, whereas that one of the cycle C_4 is formed by one constant, two fractal and one almost constant (except for its first row, the 3-standard image pattern is monochromatic) image patterns. Hence, these two regular graphs are not isomorphic.

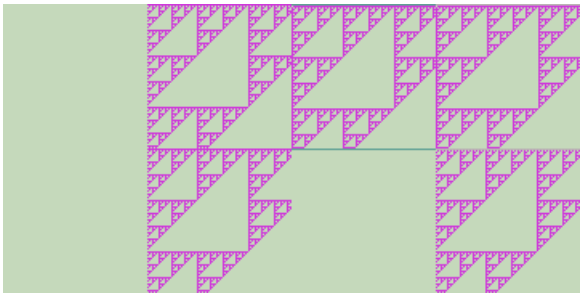

Figure 8. Standard sets of 90×90 image patterns associated to the complete graph K_4 (**top**) and the cycle C_4 (**bottom**).

These examples illustrate the relevance that standard sets of image patterns may have for distributing distinct types of algebraic and combinatorial structures into isomorphism classes. A much more comprehensive study dealing with their recognition and analysis is required in any case. It is established as further work. Similar to the methodology here implemented, computational algebraic geometry may be an interesting approach to this end. Furthermore, notice that this paper has not dealt with the fractal gradation of the image patterns under consideration. A comprehensive analysis of their fractal dimensions is of particular interest in order to improve the efficiency of this computational approach.

This paper also focuses on the possible use of computational algebraic geometry for dealing with the distribution of partial Latin squares according to the equivalence relations of being either partial transpose or P-partial isotopic, for some subset $P \subset [n] \times [n] \times [n]$. An exhaustive enumeration of these classes is also established as further work. Concerning the distribution into P-partial isotopism classes, it is required to delve into the study of P-partial autotopisms (that is, P-partial isotopisms from a partial Latin square to itself) and make use of the Orbit-Stabilizer Theorem in a similar way to the already studied distribution of partial Latin squares into isotopism classes [18].

Again, the main limitation of the methodology here introduced is the high dependence on the number of variables required by each one of the affine algebraic sets under consideration. To see it, it has been made use of the already mentioned Algorithm 1 described in [48] in order to obtain random Latin squares on which the computational efficiency of using Gröbner bases has been checked for determining both the set of Latin squares that are partial transpose of another given Latin square, and the set of partial autotopisms of a Latin square. Figure 9 shows the running time required by our computer system for computing both the reduced Gröbner basis of the corresponding ideal, together with the cardinality of its related affine algebraic set. Notice that only the relationship of being partial transpose seems to be useful for dealing by itself with the smallest orders for which no results on the distribution of Latin squares into isomorphism classes is known ($n \geq 12$). It is not the case of the equivalence relation of being P-partial isotopic, for some subset $P \subset [n] \times [n] \times [n]$, whose exponential growth starts visibly much before, even from order $n = 5$. It agrees with the fact that this equivalence relation comprehends that one of being isotopic, for which previous studies [18] have already revealed the advantages of using some extra Latin square isomorphism invariant for reducing the computational cost of an analogous algebraic geometry approach. Similar studies concerning this new equivalence relation are, therefore, required and established as further work. In this regard, the joint use of the Latin square isomorphism invariants recently introduced in [34,35] may be of particular interest.

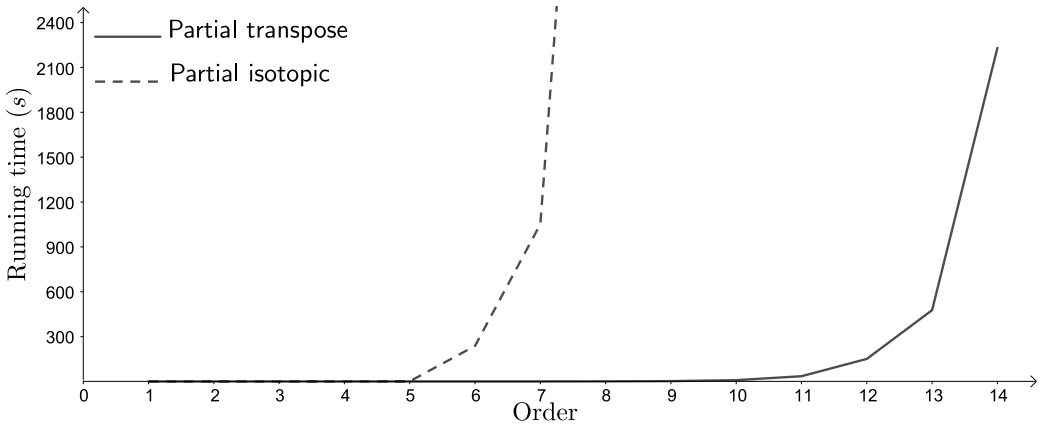

Figure 9. Running time (in seconds) required for computing the cardinality of the set $\mathcal{V}_{\mathbb{Q}}(I_{\mathrm{PT}}(L))$, for random Latin squares $L \in \mathcal{L}_n$, with $1 \leq n \leq 14$.

It is also interesting to illustrate the computational efficiency of these two approaches in case of dealing with partial Latin squares with empty cells, whose distribution into isomorphism classes is only known [17,18] for order $n \leq 6$. Firstly, let us focus on the use of Gröbner bases for determining the set of partial Latin squares that are partial transpose of another given partial Latin square. To this end, a partial Latin square in the set $\mathcal{L}_{10;m}$ was randomly constructed, for each positive integer $m \leq 100$, by means of Method (A) described in [34]. The latter consists of adding sequentially a set of feasible random entries to an empty partial Latin square until the desired weight is reached. Figure 10 shows the running time required by our computer system for determining both the reduced Gröbner basis of the corresponding ideals and the cardinalities of their related affine algebraic sets. The maximum running time was 13.99 s, which is reached for $m = 50$. It is remarkable the slightly decreasing tendency of this running time with respect to the weight of the partial Latin square under consideration.

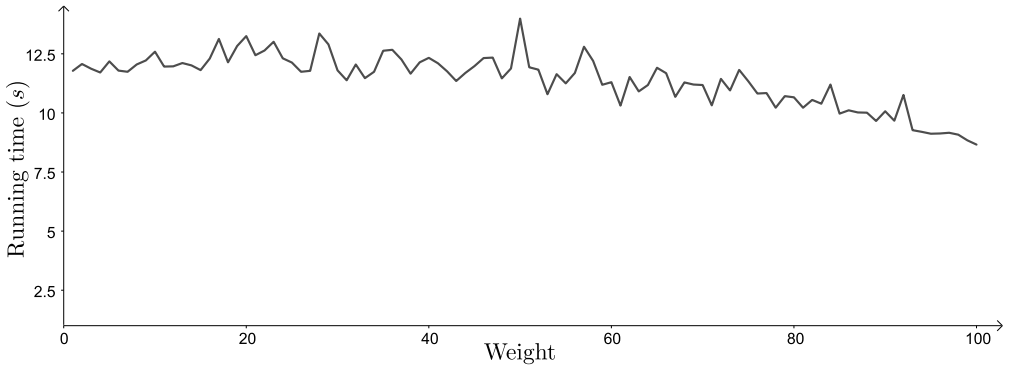

Figure 10. Running time (in seconds) required for computing the cardinality of the set $\mathcal{V}_{\mathbb{Q}}(I_{\mathrm{PT}}(L))$, for random partial Latin squares $L \in \mathcal{L}_{10;m}$, with $1 \leq m \leq 100$.

Now, to illustrate the computational efficiency of using Gröbner bases for determining the set of P-partial isotopisms between two given partial Latin squares, for some subset $P \subset [n] \times [n] \times [n]$, the mentioned method of adding random entries has been used to construct a pair of random partial Latin squares in the set $\mathcal{L}_{7;m}$, for each positive integer $m \leq 49$. (Recall that $n = 7$ is the first order for which no result on the distribution into isotopism classes is known.) Figure 11 shows the running time required by our computer system for determining both the reduced Gröbner basis of the corresponding ideals and the cardinalities of their related affine algebraic sets. The maximum running time has been 102.43 s, which is reached for $m = 49$ (the Latin square case). The fast exponential growth

of running time is remarkable for dense partial Latin squares. Partial Latin squares with either only one filled cell of with more or less the same number of empty and filled cells seem also to require more running time. All these cases turned out to be related to a high number of partial isotopisms. In any case, a much more comprehensive computational analysis concerning orders, weights and particular isomorphism classes of partial Latin squares is required for distinguishing potential bottlenecks in the computation of related Gröbner bases.

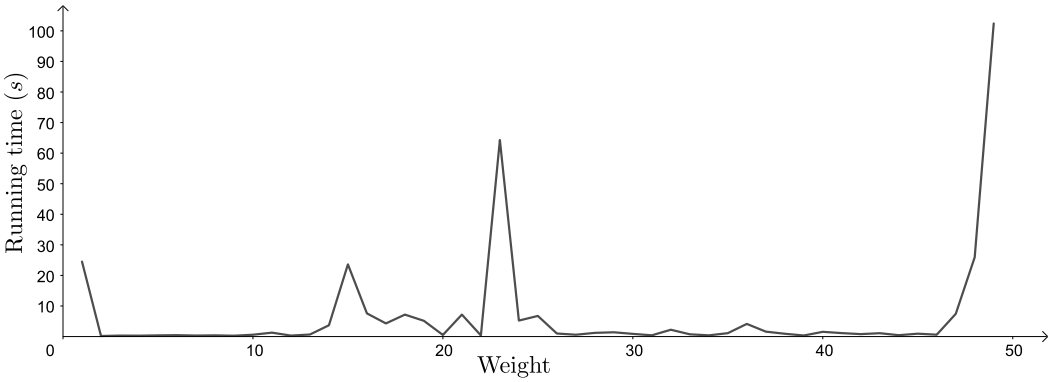

Figure 11. Running time (in seconds) required for computing the cardinality of the set $\mathcal{V}_{\mathbb{Q}}(I_{\mathrm{PI}}(L,L))$, for random partial Latin squares $L \in \mathcal{L}_{7;m}$, with $1 \leq m \leq 49$.

Let us finish this section by establishing the following open problems to deal also with as further work on this topic.

Problem 1. *What are the minimum and maximum numbers of partial Latin squares that are partial transpose of a partial Latin square in* $\mathcal{L}_{n;m}$*?*

Problem 2. *What are the minimum and the maximum numbers of distinct partial Latin squares for which there is at least one P-partial isotopism to a partial Latin square in* $\mathcal{L}_{n;m}$*, for some subset* $P \subset [n] \times [n] \times [n]$*?*

Problem 3. *What is the maximum cardinality of a subset* $P \subset [n] \times [n] \times [n]$ *for which a P-partial isotopism exists between two distinct partial Latin squares in* $\mathcal{L}_{n;m}$*?*

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: This work was partially supported by the Research Project FQM-016 from Junta de Andalucía. In addition, the author wants to express his gratitude to the anonymous referees for the comprehensive reading of the paper and their pertinent comments and suggestions, which helped improve the manuscript. Particularly, the author is very grateful for the interesting suggestions concerning the computational complexity of the proposed approach.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Moldovyan, N.A.; Shcherbacov, A.V.; Shcherbacov, V.A. On some applications of quasigroups in cryptography. In *Workshop on Foundations of Informatics*; Acad. Sci. Moldova, Inst. Math. Comput. Sci.: Chişinău, Moldova, 2015; pp. 331–340.
2. Moldovyan, N.A.; Shcherbacov, A.V.; Shcherbacov, V.A. Some applications of quasigroups in cryptology. *Comput. Sci. J. Mold.* **2016**, *24*, 55–67.
3. Shcherbacov, V. *Elements of Quasigroup Theory and Applications*; Monographs and Research Notes in Mathematics; CRC Press: Boca Raton, FL, USA, 2017.
4. Koscielny, C. A method of constructing quasigroup-based stream-ciphers. *Int. J. Appl. Math Comp. Sci.* **1996**, *6*, 109–121.
5. Koscielny, C.; Mullen, G.L. A quasigroup-based public-key cryptosystem. *Int. J. Appl. Math. Comp. Sci.* **1999**, *9*, 955–963.

6. Markovski, S.; Gligoroski, D.; Andova, S. Using quasigroups for one-one secure encoding. In Proceedings of the Eight Conference Logic and Computer Science (LIRA), Novi Sad, Serbia, 1–4 September 1997; pp. 157–162.
7. Markovski, S.; Gligoroski, D.; Bakeva, V. Quasigroup string processing: Part 1. *Contrib. Sec. Math. Tech. Sci. MANU* **1999**, *XX*, 13–28. [CrossRef]
8. Markovski, S.; Kusakatov, V. Quasigroup string processing: Part 2. *Contrib. Sec. Math. Tech. Sci. MANU* **2000**, *XXI*, 15–32. [CrossRef]
9. Kolesova, G.; Lam, C.W.H.; Thiel, L. On the number of 8×8 Latin squares. *J. Comb. Theory Ser. A* **1990**, *54*, 143–148. [CrossRef]
10. Hulpke, A.; Kaski, P.; Östergård, P.R.J. The number of Latin squares of order 11. *Math. Comp.* **2011**, *80*, 1197–1219. [CrossRef]
11. McKay, B.D.; Meynert, A.; Myrvold, W. Small Latin squares, quasigroups, and loops. *J. Comb. Des.* **2007**, *15*, 98–119. [CrossRef]
12. Dimitrova, V.; Markovski, J. On quasigroup pseudo random sequence generator. In Proceedings of the First Balkan Conference in Informatics, Thessaloniki, Greece, 19–21 November 2003; Manolopoulos, Y., Spirakis, P., Eds.; pp. 393–401.
13. Markovski, S.; Gligoroski, D.; Markovski, J. Classification of quasigroups by random walk on torus. *J. Appl. Math. Comput.* **2005**, *19*, 57–75. [CrossRef]
14. Markovski, S.; Dimitrova, V.; Samardjiska, S. Identity sieves for quasigroups. *Quasigroups Relat. Syst.* **2010**, *18*, 149–163.
15. Dimitrova, V.; Markovski, S. Classification of quasigroups by image patterns. In *Proceedings of the Fifth International Conference for Informatics and Information Technology*; Faculty of Computer Science and Engineering, Ss. Cyril and Methodius University in Skopje, N. Macedonia: Bitola, Macedonia, 2007; pp. 152–160.
16. Dimitrova, V.; Markovski, S.; Mileva, A. Periodic quasigroup string transformations. *Quasigroups Relat. Syst.* **2009**, *17*, 191–204.
17. Falcón, R.M.; Stones, R.J. Classifying partial Latin rectangles. *Electron. Notes Discret. Math.* **2015**, *49*, 765–771. [CrossRef]
18. Falcón, R.M.; Stones, R.J. Enumerating partial Latin rectangles. *Electron. J. Comb.* **2020**, *27*, P2.47.
19. Lakshman, Y.N. A single exponential bound on the complexity of computing Gröbner bases of zero-dimensional ideals. In *Effective Methods in Algebraic Geometry (Castiglioncello, 1990)*; Progr. Math. 94; Birkhäuser: Boston, MA, USA, 1991; pp. 227–234.
20. Gao, S. Counting Zeros over Finite Fields Using Gröbner Bases. Master's Thesis, Carnegie Mellon University, Pittsburgh, PA, USA, 2009.
21. Hashemi, A. Nullstellensätze for zero-dimensional Gröbner bases. *Comput. Complex.* **2009**, *18*, 155–168. [CrossRef]
22. Hashemi, A.; Lazard, D. Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving. *Internat. J. Algebra Comput.* **2011**, *21*, 703–713. [CrossRef]
23. Bayer, D. The Division Algorithm and the Hilbert Scheme. PhD. Thesis, Harvard University, Cambridge, MA, USA, 1982.
24. Adams, W.; Loustaunau, P. An introduction to Gröbner bases. In *Graduate Studies in Mathematics 3*; American Mathematical Society: Providence, RI, USA, 1994.
25. Falcón, R.M.; Martín-Morales, J. Gröbner bases and the number of Latin squares related to autotopisms of order ≤ 7. *J. Symb. Comput.* **2007**, *42*, 1142–1154. [CrossRef]
26. Falcón, R.M. The set of autotopisms of partial Latin squares. *Discret. Math.* **2013**, *313*, 1150–1161. [CrossRef]
27. Falcón, R.M. Enumeration and classification of self-orthogonal partial Latin rectangles by using the polynomial method. *Eur. J. Comb.* **2015**, *48*, 215–223. [CrossRef]
28. Falcón, O.J.; Falcón, R.M.; Nú nez, J.; Pacheco, A.M.; Villar, M.T. Computation of isotopisms of algebras over finite fields by means of graph invariants. *J. Comp. Appl. Math.* **2017**, *318*, 307–315. [CrossRef]
29. Falcón, R.M.; Falcón, O.J.; Núnez, J. Counting and enumerating partial Latin rectangles by means of computer algebra systems and CSP solvers. *Math. Methods Appl. Sci.* **2018**, *41*, 7236–7262. [CrossRef]
30. Gago-Vargas, J.; Hartillo-Hermoso, I.; Martín-Morales, J.; Ucha-Enríquez, J.M. Sudokus and Gröbner bases not only a divertimento. In *International Workshop on Computer Algebra in Scientific Computing*; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4194, pp. 155–165.
31. Arnold, E.; Lucas, S.; Taalman, L. Gröbner basis representations of sudoku. *Coll. Math. J.* **2010**, *41*, 101–112. [CrossRef]
32. Sato, Y.; Inoue, S.; Suzuki, A.; Nabeshi, K.; Sakai, K. Boolean Gröbner bases. *J. Symb. Comp.* **2011**, *46*, 622–632. [CrossRef]
33. Falcón, R.M.; Stones, R.J. Partial Latin rectangle graphs and autoparatopism groups of partial Latin rectangles with trivial autotopism groups. *Discret. Math.* **2017**, *340*, 1242–1260. [CrossRef]
34. Danan, E.; Falcon, R.M.; Kotlar, D.; Marbach, T.G.; Stones, R.J. Refining invariants for computing autotopism groups of partial Latin rectangles. *Discret. Math.* **2020**, *343*, 111812. [CrossRef]
35. Stones, R.J.; Falcón, R.M.; Kotlar, D.; Marbach, T.G. Computing autotopism groups of partial Latin rectangles. *J. Exp. Algorithmics* **2020**, *25*, 1–39. [CrossRef]
36. Falcón, R.M.; Álvarez, V.; Gudiel, F. A Computational Algebraic Geometry approach to analyze pseudo-random sequences based on Latin squares. *Adv. Comput. Math.* **2019**, *45*, 1769–1792. [CrossRef]
37. Dénes, J.; Keedwell, A.D. *Latin Squares and Their Applications*; Academic Press: New York, NY, USA; London, UK, 1974.
38. Kreuzer, M.; Robbiano, L. *Computational Commutative Algebra 1*; Springer: Berlin/Heidelberg, Germany, 2000.
39. Decker, W.; Greuel, G.M.; Pfister, G.; Schönemann, H. SINGULAR *4-2-0. A computer Algebra System for Polynomial Computations*. Available online: http://www.singular.uni-kl.de (accessed on 28 February 2021).
40. Lazard, D. Solving zero-dimensional algebraic systems. *J. Symb. Comput.* **1992**, *13*, 117–131. [CrossRef]
41. Möller, H.M. On decomposing systems of polynomial equations with finitely many solutions. *Appl. Algebra Eng. Commun. Comput.* **1993**, *4*, 217–230. [CrossRef]

42. Hillebrand, D. Triangulierung nulldimensionaler Ideale—Implementierung und Vergleich zweier Algorithmen. Master's Thesis, Universitaet Dortmund, Dortmund, Germany, 1999.
43. Buchberger, B. An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *J. Symb. Comput.* **2006**, *41*, 475–511. [CrossRef]
44. Faugére, J.C. A new efficient algorithm for computing Gröbner bases (F_4). *J. Pure Appl. Algebra* **1999**, *139*, 61–88. [CrossRef]
45. Faugére, J.C. A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5). In Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, Lille, France, 7–10 July 2002; pp. 75–83.
46. Brickenstein, M. Slimgb: Gröbner bases with slim polynomials. *Rev. Mat. Complut.* **2010**, *23*, 453–466. [CrossRef]
47. Wolfram Research, Inc. *Mathematica*; Version 12.2; Wolfram: Champaign, IL, USA, 2020.
48. Lin, M.; Long, F.; Guo, L. Grayscale image encryption based on Latin square and cellular neural network. In Proceedings of the 2016 Chinese Control and Decision Conference (CCDC), Yinchuan, China, 28–30 May 2016; pp. 2787–2793.
49. Wanless, I.M. Diagonally cyclic Latin squares. *Eur. J. Comb.* **2004**, *25*, 393–413. [CrossRef]
50. Markovski, S.; Bakeva, V.; Dimitrova, V. Representation of algebraic structures by Boolean functions and its applications. In Proceedings of the 9th International Conference ICT Innovations 2017, Skopje, Macedonia, 18–23 September 2017; pp. 229–239.